

Mise en réseau vSphere

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 8.0

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 la mise en réseau vSphere 12

1 Introduction à la mise en réseau vSphere 13

2 Configuration de la mise en réseau avec des commutateurs vSphere Standard 18

Créer un commutateur vSphere standard 20

Configuration de groupes de ports pour des machines virtuelles 22

Ajout d'un groupe de ports de machine virtuelle 22

Modifier un groupe de ports de commutateur standard 24

Supprimer un groupe de ports d'un commutateur standard vSphere 24

Propriétés des commutateurs standard vSphere 25

Modifier la taille du MTU sur un vSphere Standard Switch 25

Modifier la vitesse d'un adaptateur physique 26

Ajouter et associer des adaptateurs physiques dans un commutateur standard vSphere 26

Afficher le diagramme de la topologie d'un commutateur standard vSphere 27

3 Configuration de la mise en réseau avec vSphere Distributed Switches 29

Qu'est-ce que la compatibilité des déchargements réseau ? 34

Créer un vSphere Distributed Switch 35

Mettre à niveau un vSphere Distributed Switch vers une nouvelle version 37

Modifier les paramètres généraux et avancés de vSphere Distributed Switch 39

Gérer la mise en réseau sur plusieurs hôtes sur un vSphere Distributed Switch 40

Ajouter des hôtes à un vSphere Distributed Switch 43

Configurer des adaptateurs réseau physiques sur un vSphere Distributed Switch 46

Migrer des adaptateurs VMkernel vers un vSphere Distributed Switch 48

Créer un adaptateur VMkernel dans un vSphere Distributed Switch 49

Migrer la mise en réseau de machines virtuelles vers vSphere Distributed Switch 51

Supprimer des hôtes d'un vSphere Distributed Switch 52

Gestion de la mise en réseau sur des commutateurs proxy hôtes 53

Migrer des adaptateurs réseau sur un hôte vers un vSphere Distributed Switch 53

Migrer un adaptateur VMkernel sur un hôte vers un vSphere Standard Switch 54

Attribuer une carte réseau physique d'un hôte à un vSphere Distributed Switch 55

Supprimer une carte réseau physique d'un vSphere Distributed Switch 55

Suppression des cartes réseau des machines virtuelles actives 56

Groupes de ports distribués 56

Ajouter un groupe de ports distribués 57

Modifier les paramètres généraux d'un groupe de ports distribués 63

Supprimer un groupe de ports distribués	64
Utilisation des ports distribués	64
Surveiller l'état des ports distribués	64
Définir les paramètres de ports distribués	65
Configurer la mise en réseau de machines virtuelles sur un vSphere Distributed Switch	65
Migrer des machines virtuelles vers ou depuis vSphere Distributed Switch	66
Connecter une machine virtuelle individuelle à un groupe de ports distribués	66
Diagrammes de la topologie d'un vSphere Distributed Switch	67
Afficher la topologie d'un vSphere Distributed Switch	68
Afficher la topologie d'un commutateur de proxy hôte	69
Afficher la topologie du commutateur de déchargements réseau	69
4 Comment configurer la mise en réseau d'adaptateurs VMkernel ?	71
Couche de mise en réseau VMkernel	72
Afficher les informations sur les adaptateurs VMkernel d'un hôte	75
Créer un adaptateur VMkernel dans un commutateur vSphere standard	76
Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch	79
Modifier la configuration d'un adaptateur VMkernel	82
Remplacer la passerelle par défaut d'un adaptateur VMkernel	84
Configurer la passerelle de l'adaptateur VMkernel avec les commandes esxcli	85
Configurer le fichier resolv.conf à l'aide de commandes esxcli	86
Configurer le fichier d'hôtes DNS à l'aide des commandes ESXCLI	88
Afficher la configuration de la pile TCP/IP sur un hôte	89
Modifier la configuration de la pile TCP/IP d'un hôte	90
Notification explicite de congestion	91
Créer une pile TCP/IP personnalisée	91
Supprimer un adaptateur VMkernel	92
5 Prise en charge de LACP sur vSphere Distributed Switch	93
Configurer l'association et le basculement LACP pour les groupes de ports distribués	96
Configurer un groupe d'agrégation de liens afin de gérer le trafic pour des groupes de ports distribués	96
Modifier un groupe d'agrégation de liens	102
Limitations de la prise en charge de LACP sur un vSphere Distributed Switch	103
6 Configurations réseau de sauvegarde et de restauration	105
Sauvegarder et restaurer une configuration vSphere Distributed Switch	105
Exporter les configurations de vSphere Distributed Switch	105
Importer la configuration d'un vSphere Distributed Switch	106
Restaurer une configuration de vSphere Distributed Switch	107
Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere	108
Exporter les configurations de groupe de ports distribués vSphere	108

- Importer une configuration de groupe de ports distribués vSphere 109
- Restaurer une configuration de groupe de ports distribués vSphere 109
- Intégration du gestionnaire de configuration ESXi 110
 - Exporter la configuration de l'hôte 110
 - Importer la configuration de l'hôte 111

7 Récupération et restauration du réseau de gestion 113

- Restauration de mise en réseau vSphere 113
 - Désactiver la restauration de la mise en réseau 115
 - Désactiver la restauration réseau à l'aide du fichier de configuration de vCenter Server 115
- Résoudre les erreurs dans la configuration du réseau de gestion sur un vSphere Distributed Switch 116

8 Stratégies de mise en réseau vSphere 117

- Appliquer les stratégies de mise en réseau sur vSphere Standard ou Distributed Switch 118
- Configurer le remplacement des stratégies de mise en réseau au niveau des ports 120
- Présentation de la stratégie d'association et de basculement 121
 - Algorithmes d'équilibrage de charge disponibles pour les commutateurs virtuels 123
 - Route basée sur le port virtuel d'origine 124
 - Route basée sur le hachage MAC source 124
 - Route basée sur le hachage IP 125
 - Route basée sur la charge NIC physique 127
 - Utiliser la commande de basculement explicite 128
 - Configurer l'association de cartes réseau, le basculement et l'équilibrage de charge sur un commutateur ou un groupe de ports vSphere standard 128
 - Configurer l'association de cartes réseau, le basculement et l'équilibrage de charge sur un groupe de ports distribués ou un port distribué 130
- Présentation de la stratégie VLAN 133
 - Configurer le balisage VLAN sur un port distribué ou un groupe de ports distribués 133
 - Configurer le balisage VLAN sur un port ou un groupe de ports de liaisons montantes 134
- Présentation de la stratégie de sécurité 136
 - Configurer la stratégie de sécurité d'un groupe de ports standard ou d'un commutateur vSphere standard 136
 - Configurer la règle de sécurité d'un port distribué ou d'un groupe de ports distribués 138
- Qu'est-ce que la stratégie de formation de trafic ? 140
 - Configurer la formation du trafic d'un groupe de ports ou d'un commutateur vSphere standard 141
 - Modifier la stratégie de formation du trafic sur un port distribué ou un groupe de ports distribués 142
- Présentation de la stratégie d'allocation des ressources 143
 - Modifier la règle d'allocation des ressources d'un groupe de ports distribués 144
- Présentation de la stratégie de surveillance 144
 - Gérer la surveillance NetFlow sur un port distribué ou un groupe de ports distribués 144

- Qu'est-ce que la stratégie de filtrage et de balisage du trafic ? 145
 - Filtrage et marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante 146
 - Activer le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante 147
 - Marquer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante 147
 - Filtrer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante 150
 - Utilisation de règles de trafic réseau sur un groupe de ports distribués ou un groupe de ports de liaison montante 151
 - Désactiver le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante 155
 - Filtrage et marquage du trafic sur un port distribué ou un port de liaison montante 155
 - Activer le filtrage et le balisage du trafic d'un port distribué ou d'un port de liaison montante 156
 - Marquer le trafic sur un port distribué ou un port de liaison montante 157
 - Filtrer le trafic sur un port distribué ou un port de liaison montante 159
 - Utilisation des règles de trafic réseau sur un port distribué ou un port de liaison montante 161
 - Désactiver le filtrage et le marquage du trafic sur un port distribué ou un port de liaison montante 165
 - Qualification du trafic pour le filtrage et le balisage 166
 - Qualificateur de trafic système 166
 - Qualificateur de trafic MAC 166
 - Qualificateur de trafic IP 168
 - Gérer les règles pour plusieurs groupes de ports sur vSphere Distributed Switch 169
 - Règles de blocage des ports 173
 - Modifier la règle de blocage des ports d'un groupe de ports distribués 174
 - Modifier la stratégie de blocage d'un port distribué ou d'un port de liaison montante 174
 - Présentation de la stratégie d'apprentissage MAC 175

9 Utilisation de VLAN pour isoler le trafic réseau 176

- Configuration VLAN 176
- VLAN privés 177
 - Créer un VLAN privé 177
 - Supprimer un VLAN privé principal 178
 - Supprimer un VLAN privé secondaire 179

10 Gérer les ressources réseau 180

- DirectPath I/O 180
 - Activer le relais d'un périphérique réseau sur un hôte 181
 - Configurer un périphérique PCI sur une machine virtuelle 181
- Présentation de la virtualisation des E/S à racine unique (SR-IOV) 182

Prise en charge SR-IOV	183
Architecture et interaction des composants SR-IOV	185
Interaction entre vSphere et fonction virtuelle	187
DirectPath I/O vs SR-IOV	189
Configurer une machine virtuelle pour utiliser SR-IOV	189
Activer SR-IOV sur un adaptateur physique d'hôte	190
Attribuer une fonction virtuelle en tant qu'adaptateur relais SR-IOV à une machine virtuelle	190
Options de mise en réseau pour le trafic associé à une machine virtuelle sur laquelle SR-IOV est activé	192
Utilisation d'un adaptateur physique SR-IOV pour gérer le trafic des machines virtuelles	192
Activer SR-IOV à l'aide de profils d'hôte ou d'une commande ESXCLI	193
Activer SR-IOV dans un profil d'hôte	193
Activer SR-IOV sur l'adaptateur physique d'un hôte à l'aide d'une commande ESXCLI	194
La mise sous tension d'une machine virtuelle qui utilise une fonction virtuelle SR-IOV échoue, car l'hôte n'a plus de vecteurs d'interruption	195
Technologie RDMA (Remote Direct Memory Access) pour machines virtuelles	197
Prise en charge de PVRDMA	197
Configurer un hôte ESXi pour PVRDMA	199
Baliser un adaptateur VMkernel pour PVRDMA	199
Activer la règle de pare-feu pour PVRDMA	200
Attribuer un adaptateur PVRDMA à une machine virtuelle	200
Configurer une machine virtuelle pour utiliser les points de terminaison natifs PVRDMA	201
Configurer une machine virtuelle pour utiliser le mode VRDMA asynchrone	202
Configuration de réseau requise RoCE (RDMA over Converged Ethernet)	203
Configurer des adaptateurs réseau RDMA	204
Afficher l'adaptateur réseau compatible RDMA	204
Configurer des adaptateurs réseau RDMA	205
Trames jumbo	207
Activer les trames Jumbo sur un vSphere Distributed Switch	208
Activer les trames jumbo sur un commutateur standard vSphere	208
Activer les trames jumbo pour un adaptateur VMkernel	209
Activer la prise en charge de Trames jumbo sur une machine virtuelle	209
délestage de segmentation TCP	210
Gérer le TSO logiciel dans VMkernel	210
Comment déterminer si TSO est pris en charge sur les adaptateurs réseau physiques sur un hôte ESXi	211
Gérer TSO sur un hôte ESXi	211
Comment savoir si le TSO est activé sur un hôte ESXi ?	212
Gérer TSO sur une machine virtuelle Linux	212
Gérer TSO sur une machine virtuelle Windows	213
LRO (Large Receive Offload)	214

Gérer LRO matériel pour tous les adaptateurs VMXNET3 sur un hôte ESXi	214
Gérer LRO logiciel pour tous les adaptateurs VMXNET3 sur un hôte ESXi	214
Déterminer si LRO est activé pour les adaptateurs VMXNET3 sur un hôte ESXi	215
Modifier la taille du tampon LRO pour les adaptateurs VMXNET 3	215
Activer ou désactiver LRO pour tous les adaptateurs VMkernel sur un hôte ESXi	216
Modifier la taille de la mémoire tampon LRO pour tous les adaptateurs VMkernel	216
Gérer LRO sur un adaptateur VMXNET3 sur une machine virtuelle Linux	217
Gérer LRO sur un adaptateur VMXNET3 sur une machine virtuelle Windows	217
Gérer LRO globalement sur une machine virtuelle Windows	218
NetQueue et performances réseau	219
Activer NetQueue sur un hôte	219
Désactiver NetQueue sur un hôte	219

11 vSphere Network I/O Control 221

Qu'est-ce que vSphere Network I/O Control ?	221
Activer Network I/O Control sur un vSphere Distributed Switch	222
Allouer de la bande passante au trafic système	223
Paramètres d'allocation de bande passante pour le trafic système	224
Exemple de réservation de bande passante pour le trafic système	224
Allocation de bande passante pour le trafic système	225
Allouer de la bande passante au trafic de la machine virtuelle	226
Allouer de la bande passante à des machines virtuelles	226
Paramètres d'allocation de bande passante pour le trafic de machine virtuelle	228
Contrôle d'admission pour la bande passante des machines virtuelles	229
Créer un pool de ressources réseau	230
Ajouter un groupe de ports distribués à un pool de ressources réseau	232
Configurer l'allocation de bande passante d'une machine virtuelle	232
Configurer l'allocation de bande passante sur plusieurs machines virtuelles	234
Modifier le quota d'un pool de ressources réseau	235
Supprimer un groupe de ports distribués d'un pool de ressources réseau	236
Supprimer un pool de ressources réseau	236
Retirer un adaptateur physique de l'étendue de Network I/O Control	237

12 Gestion des adresses MAC 238

Attribution d'adresses MAC depuis vCenter Server	238
Allocation de VMware OUI	239
Allocation d'adresse MAC par préfixe	240
Allocation d'adresse MAC basée sur plage	240
Attribution d'une adresse MAC	241
Basculer vers ou ajuster les allocations basées sur préfixe ou sur plage	241
Définir ou modifier le type d'allocation	242

- Génération d'adresse MAC sur des hôtes ESXi 243
- Définition d'une adresse MAC statique sur une machine virtuelle 244
 - VMware OUI dans les adresses MAC statiques 244
 - Attribuer une adresse MAC statique 245
 - Attribuer une adresse MAC statique dans le fichier de configuration de la machine virtuelle 245

13 Configurer vSphere pour IPv6 247

- Connectivité IPv6 vSphere 247
- Déployer vSphere sur IPv6 249
 - Activer IPv6 sur une installation vSphere 249
 - Activer IPv6 sur un environnement vSphere mis à niveau 250
- Activer ou désactiver la prise en charge d'IPv6 sur un hôte 253
- Configurer IPv6 sur un hôte ESXi 253
- Configurer IPv6 sur vCenter Server 254

14 Surveiller la connexion réseau et le trafic 256

- Capturer des paquets réseau 256
- Capture et suivi des paquets réseau à l'aide de l'utilitaire pktcap-uw 258
 - Syntaxe de la commande pktcap-uw pour la capture de paquets 258
 - Syntaxe de la commande pktcap-uw pour le suivi de paquets 261
 - Options de pktcap-uw pour le contrôle de sortie 262
 - Options de pktcap-uw pour le filtrage de paquets 263
 - Capture de paquets à l'aide de l'utilitaire pktcap-uw 265
 - Capturer les paquets reçus sur un adaptateur physique 265
 - Capturer des paquets pour un adaptateur de machine virtuelle VMXNET3 268
 - Capturer des paquets pour un adaptateur VMkernel 270
 - Capturer de paquets abandonnés 272
 - Capturer des paquets au niveau de DVFilter 273
 - Utilisation des points de capture de l'utilitaire pktcap-uw 274
 - Suivi de paquets à l'aide de l'utilitaire pktcap-uw 277
- Configurer les paramètres NetFlow d'un vSphere Distributed Switch 278
- Présentation de la mise en miroir de ports 279
 - Interopérabilité de la mise en miroir de ports 280
 - Créer une session de mise en miroir de ports 282
 - Sélectionner un type de session de mise en miroir de ports 282
 - Spécifier le nom et les informations de session de mise en miroir de ports 283
 - Sélectionner les sources de mise en miroir de ports 284
 - Sélectionner les destinations de mise en miroir de ports et vérifier les paramètres 285
 - Afficher les détails de la session de mise en miroir de ports 287
 - Modifier les détails, les sources et les destinations de session de mise en miroir de port 287
- Contrôle de santé de vSphere Distributed Switch 289

- Gérer le contrôle de santé vSphere Distributed Switch 289
- Afficher l'état de santé de vSphere Distributed Switch 290
- Switch Discovery Protocol 290
 - Activer le protocole découverte Cisco (CDP) sur un vSphere Distributed Switch 291
 - Activer le protocole LLDP (Link Layer Discovery Protocol) sur un vSphere Distributed Switch 291
 - Afficher les informations de commutateur 292
 - Afficher le diagramme de la topologie d'un commutateur virtuel distribué NSX 293
- 15 Configurer des profils de protocole pour la mise en réseau de machines virtuelles 294**
 - Ajouter un profil de protocole réseau 295
 - Sélectionner le nom et le réseau du profil de protocole réseau 297
 - Spécifier la configuration IPv4 du profil de protocole réseau 297
 - Spécifier la configuration IPv6 du profil de protocole réseau 298
 - Spécifier une configuration DNS et d'autres configurations de profil de protocole réseau 299
 - Terminer le profil de protocole réseau 299
 - Associer un groupe de ports à un profil de protocole réseau 299
 - Utiliser un profil de protocole réseau pour allouer des adresses IP à une machine virtuelle ou à un vApp 300
- 16 Qu'est-ce que le filtrage multidiffusion ? 302**
 - Modes de filtrage multidiffusion 302
 - Activer l'écoute multidiffusion sur un vSphere Distributed Switch 304
 - Modifier l'intervalle d'interrogation pour l'écoute multidiffusion 304
 - Modifier le nombre d'adresses IP sources pour IGMP et MLD 305
- 17 Présentation d'un déploiement de réseau sans état 306**
- 18 Meilleures pratiques de mise en réseau vSphere 309**
- 19 Dépanner la mise en réseau vSphere 311**
 - Directives pour le dépannage 312
 - Identification des symptômes 312
 - Définition de l'espace de problème 312
 - Test de solutions possibles 313
 - Dépannage avec les journaux vCenter Server 314
 - Dépanner l'allocation d'adresses MAC 315
 - Adresses MAC dupliquées de machines virtuelles appartenant à un même réseau 315
 - Échec de la tentative de mise sous tension d'une machine virtuelle en raison d'un conflit d'adresses MAC 318
 - Impossible de supprimer un hôte d'un vSphere Distributed Switch 319

- Hôtes d'un commutateur vSphere Distributed Switch qui perdent la connectivité à vCenter Server 320
- Alarme indiquant une perte de redondance du réseau sur un hôte 322
- Les machines virtuelles perdent leur connectivité après la modification de l'ordre de basculement des liaisons montantes d'un groupe de ports distribués 323
- Impossible d'ajouter un adaptateur physique à un vSphere Distributed Switch 324
- Dépanner les charges de travail activées pour SR-IOV 325
 - Une charge de travail compatible SR-IOV ne peut pas communiquer après la modification de son adresse MAC 325
- Une machine virtuelle exécutant un client VPN provoque un déni de service pour les machines virtuelles sur l'hôte ou sur un cluster vSphere HA 326
- Faible débit pour les charges de travail UDP sur des machines virtuelles Windows 329
- Des machines virtuelles situées dans un même groupe de ports distribués mais sur des hôtes différents ne peuvent pas communiquer entre elles 331
- Les tentatives de mise sous tension d'un vApp migré échouent, car le profil de protocole associé est manquant 332
- Restauration d'une opération de configuration de mise en réseau et déconnexion d'un hôte de vCenter Server 333

À propos de la mise en réseau vSphere

Le document *Mise en réseau vSphere* donne des informations sur la configuration de la mise en réseau de VMware vSphere[®], notamment comment créer des commutateurs distribués vSphere et des commutateurs standard vSphere.

La documentation *Mise en réseau vSphere* donne également des informations sur la surveillance des réseaux, la gestion des ressources réseau et les meilleures pratiques de mise en réseau.

VMware prend l'intégration au sérieux. Pour promouvoir ce principe au sein de notre communauté de clients, de partenaires et interne, nous créons du contenu à l'aide d'une langue inclusive.

Public cible

Les informations présentées sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de la configuration réseau et des machines virtuelles.

Introduction à la mise en réseau vSphere

1

Découvrez les concepts de base de la mise en réseau vSphere ainsi que les processus d'installation et de configuration d'un réseau dans un environnement vSphere.

Concepts de mise en réseau

Quelques concepts sont essentiels pour bien comprendre la mise en réseau virtuelle. Si vous êtes un nouvel utilisateur de vSphere, il peut s'avérer utile de consulter ces concepts.

Concept de mise en réseau	Description
Réseau physique	Réseau de machines physiques connectées de sorte à pouvoir échanger des données. VMware ESXi s'exécute sur une machine physique.
Réseau virtuel	Réseau de machines virtuelles fonctionnant sur une machine physique unique, qui sont connectées logiquement entre elles de sorte à pouvoir échanger des données. Des machines virtuelles peuvent être connectées à des réseaux virtuels que vous créez lorsque vous ajoutez un réseau.
Réseau opaque	<p>Un réseau opaque est un réseau créé et géré par une entité distincte extérieure à vSphere. Par exemple, les réseaux logiques créés et gérés par VMware NSX[®] apparaissent en tant que réseaux opaques de type nsx.LogicalSwitch dans vCenter Server. Sélectionnez un réseau opaque comme sauvegarde d'un adaptateur réseau de machine virtuelle. Pour gérer un réseau opaque, utilisez les outils de gestion qui y sont associés tels que VMware NSXVMware NSX[®] Manager™ ou les outils de gestion de VMware NSX APIVMware NSX[®].</p> <p>Note Avec VMware NSX[®] 3.0, il est désormais possible d'exécuter NSX directement sur vSphere Distributed Switch (vDS) version 7.0 ou ultérieure. Ces réseaux ne sont pas opaques et sont identifiés comme des segments logiques NSX s'exécutant sur vDS 7.0. Pour plus d'informations, consultez l'article KB #79872 de la base de connaissances.</p>

Concept de mise en réseau	Description
Commutateur Ethernet physique	<p>Un commutateur Ethernet physique gère le trafic du réseau entre les machines sur le réseau physique. un commutateur possède plusieurs ports, et chacun peut être connecté à une machine unique ou à un autre commutateur sur le réseau. Chaque port peut être configuré pour se comporter de certaines manières, selon les besoins de la machine à laquelle il est connecté. Le commutateur connaît les hôtes qui sont connectés à ces ports et utilise ces informations pour acheminer le trafic aux machines physiques appropriées. Les commutateurs constituent le cœur d'un réseau physique. Plusieurs commutateurs peuvent être reliés entre eux pour former des réseaux plus grands.</p>
Commutateur standard vSphere	<p>Il fonctionne de la même manière qu'un commutateur Ethernet physique. Il détecte les machines virtuelles qui sont logiquement connectées à chacun de ces ports virtuels et utilise ces informations pour acheminer le trafic aux machines virtuelles appropriées. Un commutateur standard vSphere peut être connecté à des commutateurs physiques à l'aide d'adaptateurs Ethernet physiques, aussi appelés Cartes de liaison montante, afin de joindre des réseaux virtuels à des réseaux physiques. Ce type de connexion est semblable à une connexion de commutateurs physiques entre eux visant à créer un réseau plus grand. Même si un commutateur standard vSphere fonctionne de façon similaire à un commutateur physique, il ne dispose pas de certaines fonctionnalités avancées d'un commutateur physique.</p>
vSphere Distributed Switch	<p>Un vSphere Distributed Switch fait office de commutateur unique sur tous les hôtes associés dans un centre de données pour assurer de manière centralisée le provisionnement, l'administration et la surveillance des réseaux virtuels. Lorsque vous configurez un vSphere Distributed Switch sur le système vCenter Server, la configuration est propagée à tous les hôtes associés au commutateur. Cela permet aux machines virtuelles de conserver une configuration de mise en réseau cohérente pendant qu'elles migrent sur plusieurs hôtes.</p>
Commutateur de proxy hôte	<p>Commutateur standard masqué qui réside sur tous les hôtes associés à un vSphere Distributed Switch. Le commutateur de proxy hôte reproduit la configuration de mise en réseau définie sur le vSphere Distributed Switch de l'hôte particulier.</p>

Concept de mise en réseau	Description
Groupe de ports standard	Les services réseau se connectent aux commutateurs standard via des groupes de ports. Les groupes de ports définissent la manière dont une connexion à un réseau est établie via le commutateur. Généralement, un seul commutateur standard est associé à un ou plusieurs groupes de ports. Un groupe de ports spécifie les options de configuration de ports, telles que les restrictions de bande passante et les stratégies de balisage VLAN pour chaque port membre.
Port distribué	Port distribué sur un vSphere Distributed Switch qui se connecte au VMkernel d'un hôte ou à l'adaptateur réseau d'une machine virtuelle.
Groupe de ports distribués	Groupe de ports distribués, associés à un vSphere Distributed Switch, qui définit les options de configuration de chaque port membre. Les groupes de ports définissent la manière dont une connexion au réseau est établie via le vSphere Distributed Switch.
Groupe de ports distribués NSX	Groupe de ports distribués, associés à un vSphere Distributed Switch, qui définit les options de configuration de chaque port membre. Pour distinguer les groupes de ports distribués vSphere et les groupes de ports NSX, dans vSphere Client, le commutateur virtuel distribué NSX, et son groupe de ports associé, est identifié par l'icône  . NSX s'affiche comme un réseau opaque dans vCenter Server et vous ne pouvez pas configurer les paramètres de NSX dans vCenter Server. Les paramètres NSX affichés sont en lecture seule. Vous configurez les groupes de ports distribués NSX à l'aide de VMware NSX® Manager ou des outils de gestion de VMware NSX API. Pour en savoir plus sur la configuration de NSX, reportez-vous à la documentation <i>NSX Data Center for vSphere</i> .
Plug-in NSX Manager Appliance	NSX Manager Appliance peut être installé à partir de vSphere Web Client. Vous n'avez pas besoin d'effectuer d'opérations d'installation à partir de l'interface utilisateur de NSX Manager. Une fois NSX Manager installé, NSX s'affiche sous la forme d'un plug-in dans l'instance de vCenter Server prête à installer VMware NSX pour les cas d'utilisation de mise en réseau virtuelle ou de sécurité. Pour plus d'informations, reportez-vous à la documentation de <i>VMware NSX</i> . Cette fonctionnalité est disponible sur VMware vSphere 7.0 Update 3 et versions ultérieures, et VMware NSX® 3.2 et versions ultérieures.
Association de cartes réseau	L'association de carte réseau se produit lorsque plusieurs cartes de liaison montante sont associées à un seul commutateur pour former une association. Une association peut partager la charge de trafic entre des réseaux physiques et virtuels parmi certains ou tous ses membres, ou fournir un basculement passif en cas de défaillance matérielle ou de panne réseau.

Concept de mise en réseau	Description
VLAN	Le VLAN permet à un segment LAN physique unique d'être davantage segmenté de sorte que des groupes de ports soient isolés les uns des autres comme s'ils se trouvaient sur des segments physiquement différents. La norme est 802.1Q.
Couche de mise en réseau VMkernel TCP/IP	La couche réseau VMkernel assure la connectivité des hôtes et gère le trafic d'infrastructure standard de vSphere vMotion, du stockage IP, de Fault Tolerance et de vSAN.
Stockage IP	Toute forme de stockage utilisant la communication réseau TCP/IP comme fondation. iSCSI et NFS peuvent être utilisés comme des banques de données de machine virtuelle et pour le montage direct des fichiers .ISO, qui sont présentés comme des CD-ROM aux machines virtuelles.
Délestage de segmentation TCP	TSO (TCP Segmentation Offload) permet à une pile TCP/IP d'émettre de très grandes trames (jusqu'à 64 Ko), même si l'unité de transmission maximale (MTU) de l'interface est plus petite. La carte réseau sépare alors la grande trame en trames adaptées à la taille MTU, et ajoute une copie ajustée des en-têtes initiaux TCP/IP.

Services de réseau

Un réseau virtuel fournit plusieurs services à l'hôte et aux machines virtuelles. Vous pouvez activer deux types de service réseau dans ESXi :

- Connecter des machines virtuelles au réseau physique et entre elles.
- Connecter des services VMkernel (tels que NFS, iSCSI ou vMotion) au réseau physique.

Prise en charge de VMware ESXi Dump Collector

ESXi Dump Collector envoie l'état de la mémoire de VMkernel, c'est-à-dire un vidage de la mémoire à un serveur réseau lorsque le système détecte une panne majeure. ESXi Dump Collector dans ESXi prend en charge les commutateurs vSphere standard et les commutateurs vSphere Distributed Switch. ESXi Dump Collector peut également utiliser un adaptateur de liaison montante active à partir de l'association du groupe de ports qui gère l'adaptateur VMkernel pour Dump Collector.

Les modifications de l'adresse IP pour l'interface d'ESXi Dump Collector sont automatiquement mises à jour si les adresses IP de l'adaptateur VMkernel configuré changent. ESXi Dump Collector ajuste également sa passerelle par défaut si la configuration de passerelle de l'adaptateur VMkernel change.

Si vous tentez de supprimer l'adaptateur réseau VMkernel utilisé par ESXi Dump Collector, l'opération échoue et un message d'avertissement s'affiche. Pour supprimer l'adaptateur réseau VMkernel, désactivez la collecte de vidage mémoire et supprimez l'adaptateur.

Il n'y a pas d'authentification ou de chiffrement dans la session de transfert de fichiers à partir d'un hôte bloqué vers ESXi Dump Collector. Lorsque cela est possible, vous pouvez configurer ESXi Dump Collector sur un VLAN distinct pour isoler le vidage de mémoire d'ESXi du trafic réseau normal.

Pour obtenir des informations sur l'installation et la configuration d'ESXi Dump Collector, reportez-vous à la documentation *Installation et configuration de vCenter Server*.

Configuration de la mise en réseau avec des commutateurs vSphere Standard

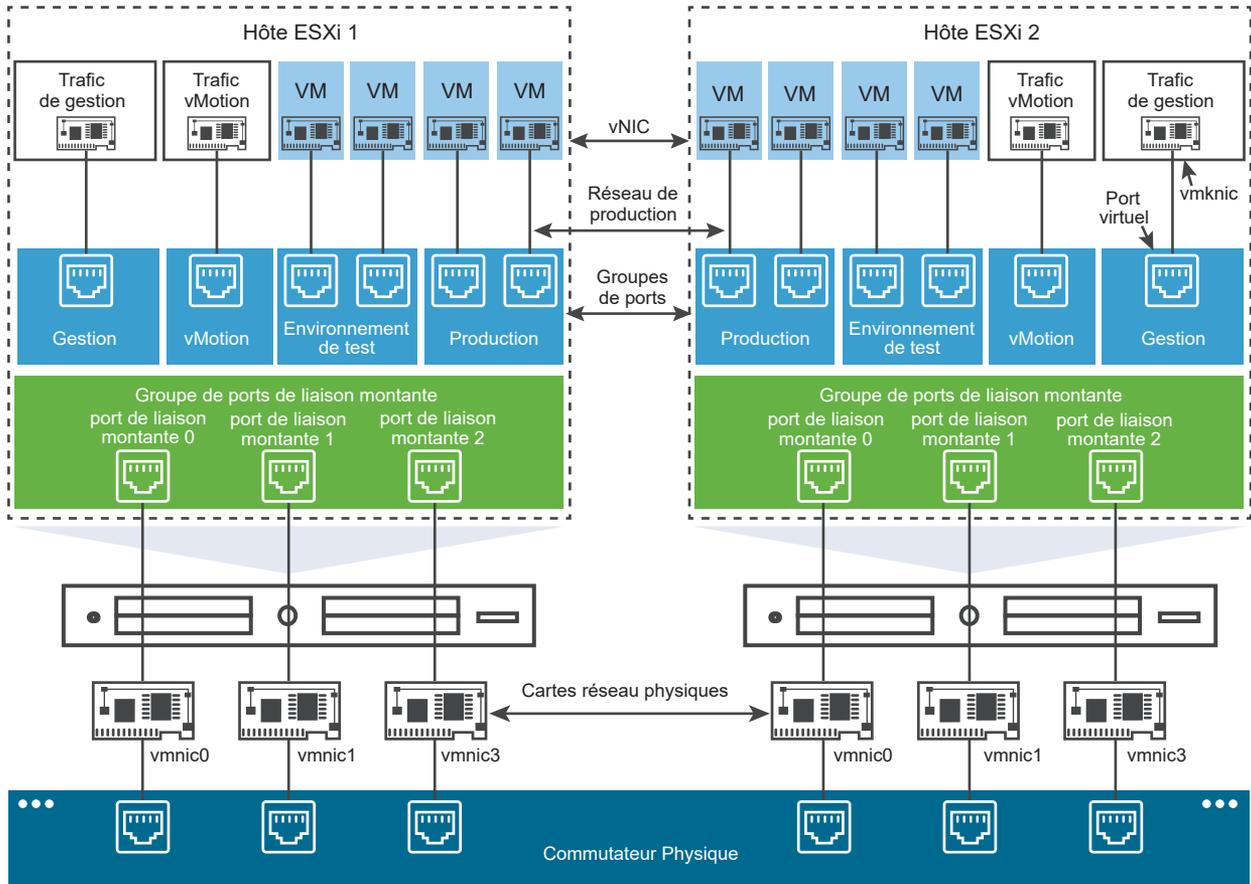
2

Les commutateurs vSphere Standard gèrent le trafic réseau au niveau de l'hôte dans un déploiement vSphere. Vous pouvez créer des périphériques réseau abstraits appelés commutateurs vSphere Standard. Découvrez comment utiliser les commutateurs standard pour assurer la connectivité réseau des hôtes et des machines virtuelles. Un commutateur standard peut faire transiter le trafic en interne entre les machines virtuelles d'un même réseau VLAN et se connecter à des réseaux externes.

Présentation du commutateur standard

Pour assurer la connectivité réseau des hôtes et des machines virtuelles, connectez les cartes réseau physiques des hôtes aux ports de liaison montante du commutateur standard. Les machines virtuelles disposent d'adaptateurs réseau (vNIC) que vous connectez à des groupes de ports sur le commutateur standard. Chaque groupe de ports peut utiliser une ou plusieurs cartes réseau physiques pour gérer son trafic réseau. Si un groupe de ports n'est connecté à aucune carte réseau physique, les machines virtuelles du même groupe de ports peuvent uniquement communiquer entre elles, mais pas avec le réseau externe.

Figure 2-1. Architecture de commutation standard vSphere



Un commutateur standard vSphere ressemble à un commutateur Ethernet physique. Les adaptateurs réseau et les cartes réseau physiques de la machine virtuelle sur l'hôte utilisent les ports logiques du commutateur, tandis que chaque adaptateur utilise un seul port. Chaque port logique dans le commutateur standard est membre d'un seul groupe de ports. Pour plus d'informations sur le nombre maximum de ports et de groupes de ports autorisés, voir *Maxima de configuration*.

Groupes de ports standard

Sur un commutateur standard, chaque groupe de ports est identifié par une étiquette de réseau qui doit être unique pour l'hôte actuel. Vous pouvez utiliser des étiquettes de réseau pour rendre la configuration de la mise en réseau des machines virtuelles compatible entre les hôtes. Vous devez donner la même étiquette aux groupes de ports d'un centre de données qui utilisent des cartes réseau physiques connectées à un domaine de diffusion sur le réseau physique. À l'inverse, si deux groupes de ports sont connectés à des cartes réseau physiques sur différents domaines de diffusion, les groupes de ports doivent avoir des étiquettes distinctes.

Par exemple, vous pouvez créer les groupes de ports *Production* et *Environnement de test* comme réseaux de machines virtuelles sur les hôtes qui partagent le même domaine de diffusion sur le réseau physique.

L'ID de VLAN est facultative. Elle permet de limiter le trafic du groupe de ports à un segment Ethernet logique dans le réseau physique. Pour que les groupes de ports reçoivent le trafic vu par le même hôte, mais de plusieurs VLAN, l'ID de VLAN doit être défini sur VGT (VLAN 4095).

Nombre de ports standard

Pour optimiser l'utilisation des ressources hôtes sur les hôtes ESXi, le nombre de ports des commutateurs standard fluctue de manière dynamique. Un commutateur standard sur un hôte de ce type peut augmenter en volume pour accueillir le nombre maximal de ports pris en charge par l'hôte.

Ce chapitre contient les rubriques suivantes :

- [Créer un commutateur vSphere standard](#)
- [Configuration de groupes de ports pour des machines virtuelles](#)
- [Propriétés des commutateurs standard vSphere](#)

Créer un commutateur vSphere standard

Créez un commutateur vSphere standard pour assurer la connectivité réseau des hôtes et des machines virtuelles et pour gérer le trafic VMkernel. Selon le type de connexion que vous souhaitez créer, vous pouvez créer un commutateur vSphere standard avec un adaptateur VMkernel, connecter uniquement les adaptateurs réseau physiques au nouveau commutateur ou créer le commutateur avec un groupe de ports de machine virtuelle.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Cliquez sur **Ajouter une mise en réseau**.
- 4 Sélectionnez un type de connexion pour lequel vous souhaitez utiliser le nouveau commutateur standard et cliquez sur **Suivant**.

Option	Description
Adaptateur réseau VMkernel	Créez un nouvel adaptateur VMkernel pour gérer le trafic de gestion des hôtes, vMotion, le stockage réseau, Fault Tolerance ou le trafic vSAN.
Adaptateur réseau physique	Ajoutez des adaptateurs réseau physiques à un commutateur standard nouveau ou existant.
Groupe de ports de machine virtuelle pour un commutateur standard	Créez un groupe de ports pour la mise en réseau de machines virtuelles.

- 5 Sélectionnez **Nouveau commutateur standard** puis cliquez sur **Suivant**.

- 6 Ajoutez des adaptateurs réseau physiques au nouveau commutateur standard.
 - a Sous Adaptateurs assignés, cliquez sur **Ajouter les adaptateurs**.
 - b Sélectionnez un ou plusieurs adaptateurs réseau physiques dans la liste et cliquez sur **OK**.
 Pour maximiser le débit et pour assurer la redondance, configurez au moins deux adaptateurs réseau physiques dans la liste Actif.
 - c (Facultatif) Utilisez les flèches **Monter** et **Descendre** dans la liste **Adaptateurs assignés** pour modifier la position de l'adaptateur.
 - d Cliquez sur **Suivant**.
- 7 Si vous créez le commutateur standard avec un adaptateur VMkernel ou un groupe de ports de machine virtuelle, entrez les paramètres de connexion de l'adaptateur ou du groupe de ports.

Option	Description
adaptateur VMkernel	<ol style="list-style-type: none"> a Entrez un libellé qui indique le type de trafic de l'adaptateur VMkernel (vMotion, par exemple). b Entrez un ID de VLAN pour identifier le VLAN que le trafic réseau de l'adaptateur VMkernel utilisera. c Sélectionnez IPv4 et/ou IPv6. d Sélectionnez une option dans le menu déroulant pour définir la taille MTU. Si vous sélectionnez Personnalisé, entrez une valeur pour la taille MTU. Vous pouvez activer les trames Jumbo en définissant une valeur MTU supérieure à 1500. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9000 octets. e Sélectionnez une pile TCP/IP. Une fois que vous avez défini une pile TCP/IP pour l'adaptateur VMkernel, elle ne peut plus être modifiée. Si vous sélectionnez la pile TCP/IP de provisionnement ou vMotion, seule cette pile pourra être utilisée pour gérer le trafic de provisionnement ou vMotion sur l'hôte. f Si vous utilisez la pile TCP/IP par défaut, effectuez la sélection à partir des services disponibles. g Configurez les paramètres IPv4 et IPv6.
Groupe de ports de machine virtuelle	<ol style="list-style-type: none"> a Entrez une étiquette réseau pour le groupe de ports ou acceptez l'étiquette générée. b Définissez l'ID VLAN pour configurer le traitement VLAN dans le groupe de ports.

- 8 Sur la page Prêt à terminer, cliquez sur **Terminer**.

Étape suivante

- Il peut s'avérer nécessaire de modifier la stratégie d'association et de basculement du nouveau commutateur standard. Par exemple, si l'hôte est connecté à Etherchannel sur le commutateur physique, vous devez configurer le commutateur vSphere standard par le biais de l'algorithme d'équilibrage de charge Route basée sur le hachage IP. Consultez [Présentation de la stratégie d'association et de basculement](#) pour plus d'informations.

- Si vous créez le commutateur standard avec un groupe de ports pour la mise en réseau de machines virtuelles, connectez les machines virtuelles au groupe de ports.

Configuration de groupes de ports pour des machines virtuelles

Vous pouvez ajouter ou modifier un groupe de ports de machines virtuelles pour configurer la gestion du trafic sur un ensemble de machines virtuelles.

L'assistant **Ajouter une mise en réseau** de vSphere Client vous aide à créer un réseau virtuel auquel les machines virtuelles peuvent se connecter, ainsi qu'un commutateur standard vSphere. Il vous aide également à définir les paramètres d'une étiquette réseau.

Lorsque vous définissez les réseaux de machines virtuelles, envisagez de prendre les mesures pour migrer les machines virtuelles dans le réseau entre les hôtes. Si c'est le cas, assurez-vous que le même domaine de diffusion est accessible par les deux hôtes (c'est-à-dire le même sous-réseau de couche 2).

ESXi ne prend pas en charge la migration de machines virtuelles entre des hôtes de différents domaines de diffusion, car la machine virtuelle migrée peut nécessiter des systèmes et des ressources auxquels elle n'aurait plus accès dans le nouveau réseau. Même si la configuration réseau est définie comme un environnement haute disponibilité ou comprend des commutateurs intelligents qui peuvent répondre aux besoins de la machine virtuelle sur différents réseaux, vous pouvez rencontrer des délais d'attente lors des mises à niveau de la table ARP (Protocole de résolution d'adresse) et de la reprise du trafic réseau pour les machines virtuelles.

Les machines virtuelles atteignent les réseaux physiques via des adaptateurs de liaison montante. Un commutateur standard vSphere peut transférer des données vers des réseaux externes uniquement quand un ou plusieurs adaptateurs réseau y sont connectés. Quand au moins deux adaptateurs sont connectés à un seul commutateur standard, ils sont associés de manière transparente.

Ajout d'un groupe de ports de machine virtuelle

Ajoutez des groupes de ports de machine virtuelle dans un commutateur standard vSphere pour fournir la connectivité et une configuration réseau commune à un ensemble de machines virtuelles.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Ajouter une mise en réseau**.
- 3 Dans **Sélectionner le type de connexion**, sélectionnez **Groupe de ports de machine virtuelle pour un commutateur standard** puis cliquez sur **Suivant**.
- 4 Dans **Sélectionner un périphérique cible**, sélectionnez un commutateur standard existant ou créez un nouveau commutateur standard.

- 5 Si le nouveau groupe de ports concerne un commutateur standard existant, naviguez jusqu'à ce commutateur.
 - a Cliquez sur **Parcourir**.
 - b Sélectionnez un commutateur standard de la liste et cliquez sur **OK**.
 - c Cliquez sur **Suivant** et passez à l'[Étape 7](#).

- 6 (Facultatif) Si vous choisissez de créer un commutateur standard, entrez une valeur pour la taille MTU et cliquez sur **Suivant**.

Vous pouvez créer un commutateur standard avec ou sans adaptateurs.

Si vous créez un commutateur standard sans adaptateurs réseau physique, l'ensemble du trafic sur le commutateur est limité au commutateur. Aucun autre hôte sur le réseau physique ou les machines virtuelles sur les autres commutateurs standard ne peut envoyer du trafic sur ce commutateur standard. Vous pouvez créer un commutateur standard sans adaptateurs réseau physiques si vous voulez que les machines virtuelles d'un groupe puisse communiquer entre elles, mais pas avec les hôtes ou les machine virtuelle qui n'appartiennent pas au groupe.

- a Cliquez sur **Ajouter des adaptateurs**.
 - b Sélectionnez un adaptateur dans la liste **Adaptateurs réseau**, puis cliquez sur **OK**.
 - c (Facultatif) Utilisez les flèches haut et bas dans la liste **Adaptateurs affectés** pour chanter la position de l'adaptateur si nécessaire.
 - d Cliquez sur **Suivant**.
- 7 Dans la page Paramètres de connexion, identifiez le trafic des ports du groupe.
 - a Entrez une **Étiquette réseau** pour le groupe de ports ou acceptez l'étiquette générée.

Note Les noms des groupes de ports ne doivent pas contenir de caractère deux-points (:).

- b Définissez l'**ID VLAN** pour configurer le traitement VLAN dans le groupe de ports. L'ID VLAN reflète également le mode de balisage VLAN dans le groupe de ports.

Mode de balisage VLAN	ID VLAN	Description
Balisage de commutateur externe (EST)	0	Le commutateur virtuel ne transmet pas le trafic associé à un VLAN.
Balisage d'invité virtuel (VGT)	4095	Les machines virtuelles gèrent des VLAN. Le commutateur virtuel transmet le trafic provenant de n'importe quel réseau VLAN.

- c Cliquez sur **Suivant**.
- 8 Vérifiez les paramètres du groupe de ports dans la page Prêt à terminer et cliquez sur **Terminer**.
Cliquez sur **Précédent** si vous souhaitez modifier des paramètres.

Modifier un groupe de ports de commutateur standard

À l'aide de vSphere Client, modifiez le nom et l'ID VLAN d'un groupe de ports de commutateur standard et remplacez les règles de mise en réseau au niveau du groupe de ports.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste.
Le diagramme de la topologie du commutateur s'affiche.
- 4 Dans le diagramme de la topologie du commutateur, cliquez sur le nom du groupe de ports.
- 5 En regard du titre du diagramme de topologie, cliquez sur les trois points verticaux et sélectionnez **Modifier les paramètres**.
- 6 Dans la page Propriétés, renommez le groupe de ports dans le champ de texte **Étiquette réseau**.
- 7 Configurez le balisage VLAN dans le menu déroulant **ID VLAN**.

Mode de balisage VLAN	ID VLAN	Description
Balisage de commutateur externe (EST)	0	Le commutateur virtuel ne transmet pas le trafic associé à un VLAN.
Balisage d'invité virtuel (VGT)	4095	Les machines virtuelles gèrent des VLAN. Le commutateur virtuel transmet le trafic provenant de n'importe quel réseau VLAN.

- 8 Sur la page Sécurité, remplacez les paramètres du commutateur pour assurer la protection contre les modifications d'adresse MAC, les fausses transmissions et pour exécuter les machines virtuelles en mode promiscuité.
- 9 Dans la page Formation du trafic, remplacez, au niveau du groupe de ports, les tailles moyenne et maximale de la bande passante et celle des ruptures.
- 10 Dans la page Association et basculement, remplacez les paramètres d'association et de basculement hérités du commutateur standard.

Vous pouvez configurer la distribution et le réacheminement du trafic entre les adaptateurs physiques associés au groupe de ports. Vous pouvez également modifier l'ordre dans lequel les adaptateurs physiques de l'hôte sont utilisés en cas de panne.
- 11 Cliquez sur **OK**.

Supprimer un groupe de ports d'un commutateur standard vSphere

Vous pouvez supprimer des groupes de ports de commutateurs standard vSphere si vous n'avez plus besoin d'utiliser les réseaux étiquetés associés.

Conditions préalables

Assurez-vous qu'aucune machine virtuelle connectée au groupe de ports à supprimer n'est sous tension.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard.
- 4 Dans le diagramme de topologie du commutateur, sélectionnez le groupe de ports à supprimer en cliquant sur son étiquette.
- 5 Dans la barre d'outils de la topologie de commutation, cliquez sur l'icône d'action **Supprimer**.

Propriétés des commutateurs standard vSphere

Les paramètres de commutateur standard vSphere contrôlent les valeurs par défaut des commutateurs des ports, qui peuvent être remplacées par des paramètres de groupe de ports pour chaque commutateur standard. Vous pouvez éditer les propriétés des commutateurs, telles que la configuration de la liaison montante et le nombre de ports disponibles.

Nombre de ports sur les hôtes ESXi

Pour optimiser l'utilisation des ressources hôtes sur les hôtes ESXi, les ports des commutateurs virtuels évoluent de manière dynamique. Sur ce type d'hôte, un commutateur peut se développer jusqu'à inclure le nombre maximal de ports pris en charge sur l'hôte. La limite de port est déterminée en fonction du nombre maximal de machines virtuelles que l'hôte peut gérer.

Modifier la taille du MTU sur un vSphere Standard Switch

Modifier la taille de l'unité de transmission maximale (MTU) sur un vSphere Standard Switch pour améliorer l'efficacité de mise en réseau en augmentant la quantité de données de charge utile transmise par paquet, ce qui revient à activer les trames jumbo.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la table et cliquez sur **Modifier les paramètres**.
- 4 Modifiez la valeur **MTU (octets)** du commutateur standard.

Vous pouvez activer les trames Jumbo en définissant une valeur MTU supérieure à 1500. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9000 octets.

- 5 Cliquez sur **OK**.

Modifier la vitesse d'un adaptateur physique

Vous pouvez modifier la vitesse et le duplex de la connexion d'un adaptateur physique pour transférer des données selon le débit du trafic.

Si l'adaptateur réseau physique prend en charge SR-IOV, vous pouvez l'activer et configurer le nombre de fonctions virtuelles à utiliser pour la mise en réseau des machines virtuelles.

Procédure

- 1 Dans vSphere Client, accédez à un hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Adaptateurs physiques**.

Les adaptateurs réseau physiques de l'hôte s'affichent dans un tableau qui comporte des détails sur chaque adaptateur réseau physique.

- 3 Sélectionnez l'adaptateur réseau physique dans la liste et cliquez sur l'icône **Modifier les paramètres de l'adaptateur**.
- 4 Sélectionnez la vitesse et le mode duplex de l'adaptateur réseau physique dans le menu déroulant.

Les paramètres de vitesse et de duplex que vous sélectionnez doivent correspondre à ceux configurés sur le commutateur physique. La vitesse est le débit de l'interface, généralement indiquée en mégabits par seconde (Mbits/s). Le duplex fait référence à la manière dont les données circulent sur l'interface.

- 5 Cliquez sur **OK**.

Ajouter et associer des adaptateurs physiques dans un commutateur standard vSphere

Affectez un adaptateur physique à un commutateur standard pour fournir une connectivité aux machines virtuelles et aux adaptateurs VMkernel de l'hôte. Vous pouvez former une association de cartes réseau pour répartir le volume du trafic et configurer le basculement.

L'association des cartes réseau combine plusieurs connexions réseau pour augmenter le débit et fournir la redondance en cas de panne d'une liaison. Pour créer une association, vous associez plusieurs adaptateurs physiques à un seul commutateur standard vSphere.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard auquel vous souhaitez ajouter un adaptateur physique.
- 4 Cliquez sur **Gérer adaptateurs physiques**.

- 5 Ajoutez un ou plusieurs adaptateurs réseau physiques disponibles au commutateur.
 - a Cliquez sur **Ajouter des adaptateurs**, sélectionnez un ou plusieurs adaptateurs réseau dans la liste et cliquez sur **OK**.

Les adaptateurs sélectionnés figurent dans la liste du groupe de basculement située sous la liste Adaptateurs assignés.

- b (Facultatif) Utilisez les flèches haut et bas pour changer la position d'un adaptateur dans les groupes de basculement.

Le groupe de basculement détermine le rôle de l'adaptateur pour l'échange de données avec le réseau externe, c'est-à-dire, actif, en veille ou inutilisé. Par défaut, les adaptateurs sont ajoutés aux commutateurs standards dans un rôle actif.

- 6 Cliquez sur **OK** pour appliquer la configuration des adaptateurs physiques.

Afficher le diagramme de la topologie d'un commutateur standard vSphere

Vous pouvez examiner la structure et les composants d'un commutateur standard vSphere en utilisant son diagramme de la topologie.

Le diagramme de la topologie d'un commutateur standard fournit une représentation visuelle des adaptateurs et des groupes de ports connectés au commutateur.

À partir du diagramme, vous pouvez modifier les paramètres d'un groupe de ports sélectionné et d'un adaptateur sélectionné.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard dans la liste.

Résultats

Le diagramme apparaît sous la liste de commutateurs virtuels sur l'hôte.

Exemple : Diagramme d'un commutateur standard qui connecte VMkernel et les machines virtuelles au réseau

Dans votre environnement virtuel, un commutateur vSphere standard gère les adaptateurs VMkernel pour vSphere vMotion et pour le réseau de gestion, et les machines virtuelles regroupées. Le diagramme de la topologie centrale permet notamment de déterminer si une machine virtuelle ou un adaptateur VMkernel est connecté au réseau externe et d'identifier l'adaptateur physique qui transmet les données.

Figure 2-2. Diagramme de la topologie d'un commutateur standard vSphere

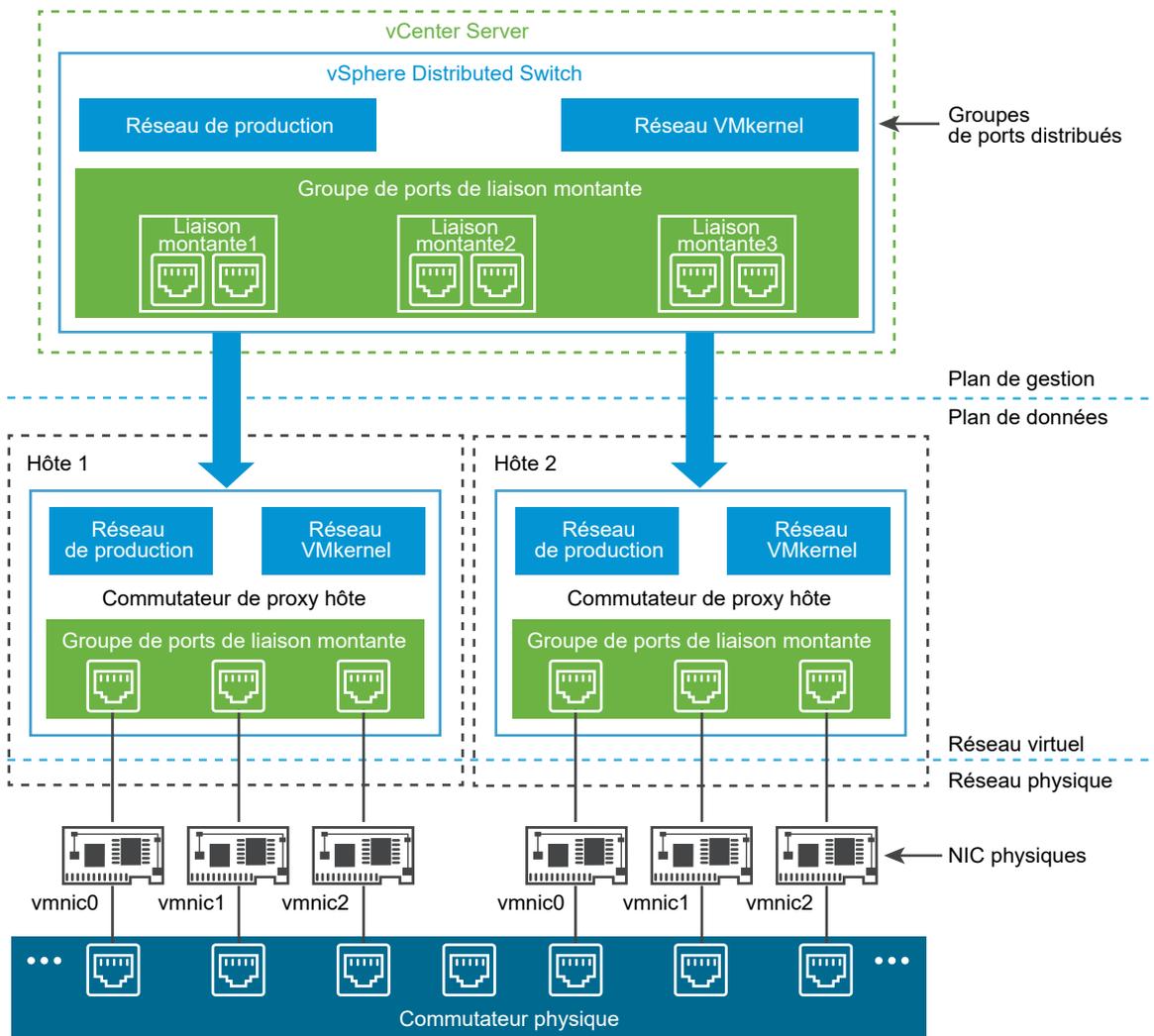


Configuration de la mise en réseau avec vSphere Distributed Switches

3

Avec des vSphere Distributed Switches, vous pouvez installer et configurer les communications réseau dans un environnement vSphere.

Figure 3-1. Architecture de vSphere Distributed Switch



Dans vSphere, un commutateur réseau est constitué de deux sections logiques : le plan de données et le plan de gestion. Le plan de données implémente par exemple la commutation, le filtrage et le balisage des paquets. Le plan de gestion est la structure de contrôle utilisée pour configurer les fonctionnalités du plan de données. Tout commutateur vSphere standard contient un plan de données et un plan de gestion, et chaque commutateur standard est configuré et mis à jour individuellement.

Dans un vSphere Distributed Switch, le plan de données et le plan de gestion sont séparés. La fonctionnalité de gestion du commutateur distribué réside dans le système vCenter Server qui vous permet d'administrer la configuration de mise en réseau de votre environnement au niveau d'un centre de données. Le plan de données reste défini localement sur chaque hôte associé au commutateur distribué. Dans le commutateur distribué, la section de plan de données est appelée « commutateur de proxy hôte ». La configuration de mise en réseau que vous créez dans vCenter Server (le plan de gestion) est automatiquement envoyée à tous les commutateurs de proxy hôtes (le plan de données).

Le vSphere Distributed Switch introduit deux abstractions qui vous permettent de créer une configuration de mise en réseau cohérente pour les cartes réseau physiques, les machines virtuelles et les services VMkernel.

Groupe de ports de liaison montante

Un groupe de ports de liaison montante ou groupe de ports dvUplink est défini au cours de la création du commutateur distribué et peut présenter une ou plusieurs liaisons montantes. Une liaison montante est un modèle que vous utilisez pour configurer les connexions physiques des hôtes ainsi que les stratégies de basculement et d'équilibrage de charge. Vous mappez les cartes réseau physiques des hôtes aux liaisons montantes configurées sur le commutateur distribué. Au niveau de l'hôte, chaque carte réseau physique est connectée à un port de liaison montante avec un ID particulier. Lorsque vous définissez des stratégies de basculement et d'équilibrage de charge sur les liaisons montantes, elles sont automatiquement propagées aux commutateurs de proxy hôtes ou au plan de données. Cela vous permet d'appliquer des configurations de basculement et d'équilibrage de charge cohérentes aux cartes réseau physiques de tous les hôtes associés au commutateur distribué.

Groupe de ports distribués

Les groupes de ports distribués assurent la connectivité réseau des machines virtuelles et la gestion du trafic VMkernel. Chaque groupe de ports distribués est identifié à l'aide d'une étiquette réseau qui doit être unique dans le centre de données actuel. Les stratégies d'association de cartes réseau, de basculement, d'équilibrage de charge, de VLAN, de sécurité, de formation du trafic, etc. sont configurées sur les groupes de ports distribués. Tous les ports virtuels connectés à un groupe de ports distribués partagent les mêmes propriétés : celles qui sont configurées pour le groupe de ports distribués. De même que pour les groupes de ports de liaison montante, la configuration que vous attribuez aux groupes de ports distribués dans vCenter Server (le plan de gestion) se propage automatiquement à tous les hôtes du commutateur distribué via leurs commutateurs de proxy hôtes (le plan de données). Ainsi, pour configurer un groupe de machines virtuelles de manière à ce qu'elles partagent la

même configuration de mise en réseau, il vous suffit de les associer au même groupe de ports distribués.

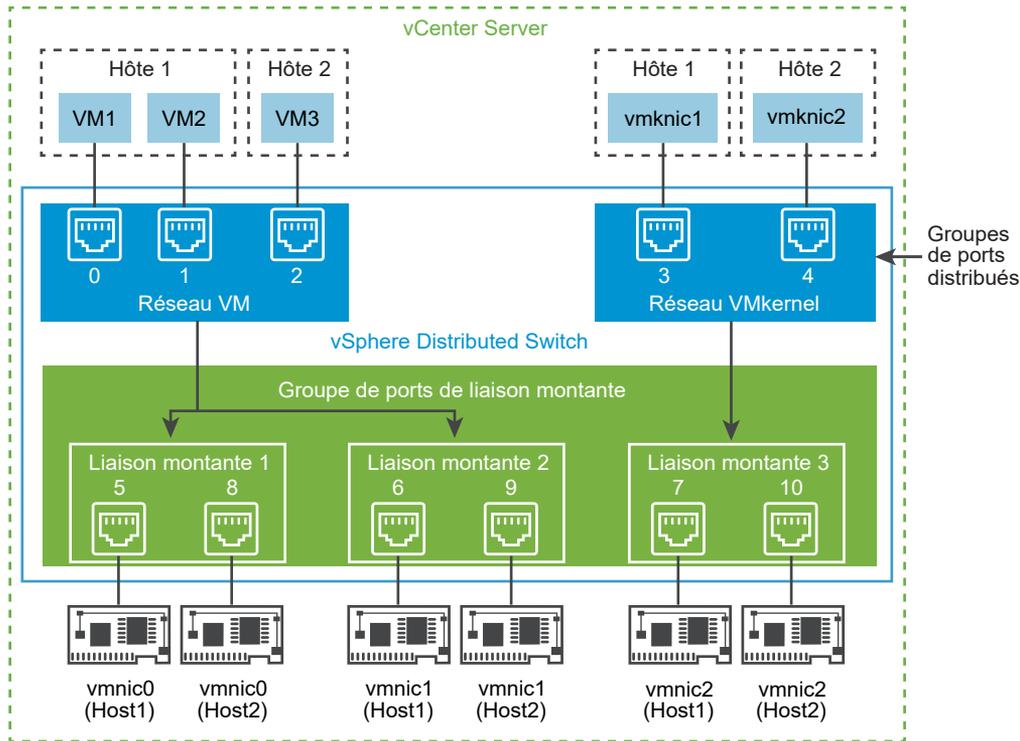
Par exemple, supposons que vous créez un vSphere Distributed Switch sur votre centre de données et que vous lui associez deux hôtes. Vous configurez trois liaisons montantes pour le groupe de ports de liaison montante et connectez une carte réseau physique entre chaque hôte et chaque liaison montante. Chaque liaison montante dispose de deux cartes réseau physiques, une de chaque hôte qui lui est mappé. Par exemple, la liaison montante 1 est configurée avec vmnic0 à partir de l'hôte 1 et de l'hôte 2. Ensuite, vous créez les groupes de ports réseau distribués de production et VMkernel pour la mise en réseau des machines virtuelles et les services VMkernel. Une représentation des groupes de ports des réseaux de production et VMkernel est également créée sur les hôtes 1 et 2, respectivement. Toutes les stratégies définies dans les groupes de ports des réseaux de production et VMkernel sont propagées à leurs représentations sur les hôtes 1 et 2.

Pour optimiser l'utilisation des ressources hôtes, le nombre de ports distribués des commutateurs proxy fluctue de manière dynamique. Un commutateur proxy sur un hôte de ce type peut augmenter en volume pour accueillir le nombre maximal de ports pris en charge par l'hôte. La limite de port est déterminée en fonction du nombre maximal de machines virtuelles que l'hôte peut gérer.

Flux de données de vSphere Distributed Switch

Le flux de données des machines virtuelles et des adaptateurs VMkernel vers le réseau physique dépend des stratégies d'association de cartes réseau et d'équilibrage de charge définies pour les groupes de ports distribués. Il dépend également de l'allocation des ports sur le commutateur distribué.

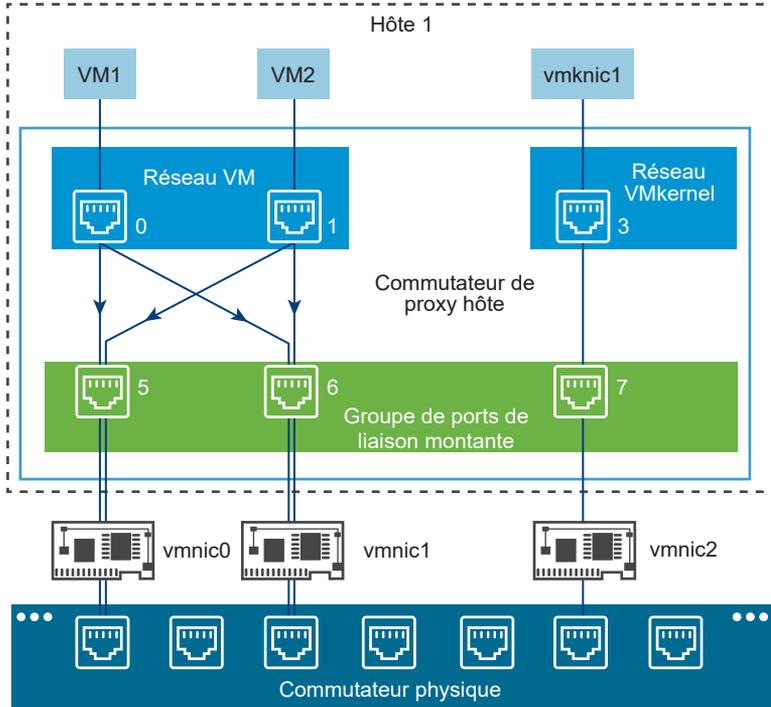
Figure 3-2. Association de cartes réseau et allocation des ports sur un vSphere Distributed Switch



Par exemple, supposons que vous créez des groupes de ports distribués de réseau de machines virtuelles et de réseau VMkernel, respectivement avec 3 et 2 ports distribués. Le commutateur distribué alloue les ports portant les ID 0 à 4 dans l'ordre dans lequel vous avez créé les groupes de ports distribués. Ensuite, vous associez les hôtes 1 et 2 au commutateur distribué. Le commutateur distribué alloue des ports pour chaque carte réseau physique des hôtes, tandis que la numérotation des ports continue à partir de 5 dans l'ordre d'ajout des hôtes. Pour assurer la connectivité réseau de chaque hôte, vous mappez vmnic0 à la liaison montante 1, vmnic1 à la liaison montante 2 et vmnic2 à la liaison montante 3.

Pour assurer la connectivité des machines virtuelles et gérer le trafic VMkernel, vous configurez l'association et le basculement vers les groupes de ports réseau de machines virtuelles et VMkernel. Les liaisons montantes 1 et 2 gèrent le trafic du groupe de ports réseau de machines virtuelles, tandis que la liaison montante 3 gère le trafic du groupe de ports réseau VMkernel.

Figure 3-3. Flux de paquets sur le commutateur de proxy hôte



Côté hôte, le flux de paquets provenant des machines virtuelles et des services VMkernel utilise des ports particuliers pour atteindre le réseau physique. Par exemple, un paquet envoyé depuis la machine virtuelle VM1 sur l'hôte 1 atteint d'abord le port 0 des groupes de ports distribués de réseau de machines virtuelles. Comme les liaisons montantes 1 et 2 gèrent le trafic du groupe de ports réseau de machines virtuelles, le paquet peut poursuivre à partir du port de liaison montante 5 ou 6. Si le paquet utilise le port de liaison montante 5, il continue vers vmnic0 ; s'il utilise le port de liaison montante 6, il continue vers vmnic1.

Ce chapitre contient les rubriques suivantes :

- Qu'est-ce que la compatibilité des déchargements réseau ?
- Créer un vSphere Distributed Switch
- Mettre à niveau un vSphere Distributed Switch vers une nouvelle version
- Modifier les paramètres généraux et avancés de vSphere Distributed Switch
- Gérer la mise en réseau sur plusieurs hôtes sur un vSphere Distributed Switch
- Gestion de la mise en réseau sur des commutateurs proxy hôtes
- Groupes de ports distribués
- Utilisation des ports distribués
- Configurer la mise en réseau de machines virtuelles sur un vSphere Distributed Switch
- Diagrammes de la topologie d'un vSphere Distributed Switch

Qu'est-ce que la compatibilité des déchargements réseau ?

À partir de vSphere 8.0, vSphere Distributed Services Engine vDSE présente l'infrastructure virtuelle en tant qu'architecture distribuée avec l'ajout d'unités de traitement des données (DPU), également appelées SmartNic, qui permettent de décharger des fonctions d'infrastructure des CPU de l'hôte ou du serveur vers les unités de traitement des données (DPU).

Pour plus d'informations sur les DPU, reportez-vous à la section [Présentation de VMware vSphere® Distributed Services Engine™ et de l'accélération de la mise en réseau à l'aide des DPU](#)

La compatibilité des déchargements réseau vous permet de décharger les opérations de mise en réseau sur le périphérique DPU. Vous pouvez décharger la fonctionnalité de mise en réseau de l'hôte ESXi vers DPU pour de meilleures performances. vSphere Distributed Switch soutenu par ESXi sur DPU prend en charge les modes suivants :

- Mode de non-déchargement avant l'activation de NSX : le DPU est utilisé comme une carte réseau traditionnelle.
- Mode de déchargement après NSX : la logique de transfert du trafic est déchargée de l'hôte ESXi vers le vSphere Distributed Switch soutenu par le DPU.

Les hôtes soutenus par DPU sont associés au vSphere Distributed Switch. Il est configuré lors de la création du commutateur distribué. La compatibilité des déchargements réseau ne peut pas être modifiée après l'association d'hôtes au Distributed Switch. Vous pouvez uniquement ajouter des hôtes reposant sur DPU à ces commutateurs distribués. ESXi sur DPU est utilisé en tant que carte réseau traditionnelle jusqu'à ce que le nœud de transport VMware NSX® soit configuré. Le vSphere Distributed Switch sur vCenter Server indique si le déchargement réseau est autorisé lorsque VMware NSX® est activé.

Fonctionnalités prises en charge par vSphere Distributed Switch soutenu par le DPU.

- Création et suppression du vSphere Distributed Switch.
- Gestion de la configuration.
- Contrôle de santé de vSphere Distributed Switch.
- Protocole de contrôle d'agrégation de liens (LACP).
- Mise en miroir de ports.
- LAN privés.
- Link Layer Discovery Protocol.

Note Fonctionnalités non prises en charge par vSphere Distributed Switch soutenu par DPU.

- Network I/O Control.
 - Stratégies de formation du trafic.
 - Filtre DV.
-

Activer les déchargements réseau

Pour activer les déchargements réseau, vous devez effectuer plusieurs étapes dans vCenter Server et dans VMware NSX®.

Étape	Solution
Créer un vSphere Distributed Switch	Créer un vSphere Distributed Switch
Associer des hôtes à vSphere Distributed Switch	Ajouter des hôtes à un vSphere Distributed Switch
Configurer le nœud de transport de l'hôte NSX	Configurer le nœud de transport de l'hôte NSX sur un cluster vSphere Lifecycle Manager sur lequel DPU est activé
Afficher la topologie du vSphere Distributed Switch avec des déchargements réseau	Afficher la topologie du commutateur de déchargements réseau

Créer un vSphere Distributed Switch

Créez un vSphere Distributed Switch sur un centre de données pour gérer la configuration de la mise en réseau de plusieurs hôtes à la fois à partir d'un emplacement centralisé.

Procédure

- 1 Dans vSphere Client, cliquez avec le bouton droit sur un centre de données dans l'arborescence de l'inventaire.
- 2 Sélectionnez **Commutateur distribué > Nouveau commutateur distribué**.
- 3 Sur la page **Nom et emplacement**, entrez un nom pour le nouveau Distributed Switch, ou acceptez le nom généré, puis cliquez sur **Suivant**.
- 4 Sur la page **Sélectionner la version**, sélectionnez une version de Distributed Switch et cliquez sur **Suivant**.

Option	Description
Distributed Switch : 8.0.0	Compatible avec ESXi 8.0 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 7.0.3	Compatible avec ESXi 7.0.3 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 7.0.2	Compatible avec ESXi 7.0.2 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 7.0.0	Compatible avec ESXi 7.0 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.

Option	Description
Distributed Switch : 6.6.0	Compatible avec ESXi 6.7 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 6.5.0	Compatible avec ESXi 6.5 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.

5 Sur la page **Configurer les paramètres**, configurez les paramètres du Distributed Switch.

a Utilisez le menu déroulant pour sélectionner le type de **Compatibilité des déchargements réseau**.

À l'aide de la compatibilité des déchargements réseau, vous pouvez décharger des fonctions de réseau et de sécurité sur le périphérique DPU. Le DPU est une carte réseau disposant d'une capacité de calcul intégrée. Vous pouvez décharger la fonctionnalité de mise en réseau de l'hôte ESXi vers DPU pour de meilleures performances.

- **Aucune** : si vous sélectionnez **Aucune**, la compatibilité Déchargements réseau n'est pas prise en charge.
- **Pensando** : si vous sélectionnez **Pensando**, la compatibilité Déchargements réseau est prise en charge. La fonctionnalité **Network I/O Control** est désactivée.
- **NVIDIA BlueField** : si vous sélectionnez **NVIDIA BlueField**, la compatibilité Déchargements réseau est prise en charge. La fonctionnalité **Network I/O Control** est désactivée.

Note Vous pouvez configurer la compatibilité Déchargements réseau lorsque vous utilisez vSphere Distributed Switch 8.0.0 et versions ultérieures.

b Utilisez les boutons fléchés pour sélectionner le **Nombre de liaisons montantes**.

Les ports de liaison montante connectent le distributed switch aux cartes réseau physiques sur les hôtes associés. Le nombre de ports de liaison montante est le nombre maximal autorisé de connections physiques au commutateur distribué par hôte.

c Utilisez le menu déroulant pour activer ou désactiver **Network I/O Control**.

À l'aide de Network I/O Control, vous pouvez donner la priorité à l'accès aux ressources réseau pour certains types de trafic d'infrastructure et de charge de travail, en fonction des besoins de votre déploiement. Network I/O Control surveille en continu la charge d'E/S sur le réseau et alloue dynamiquement les ressources disponibles.

d (Facultatif) Cochez la case **Créer un groupe de ports par défaut** pour créer un nouveau groupe de ports distribués avec des paramètres par défaut pour le commutateur. Entrez un **Nom de groupe de ports** ou acceptez le nom généré.

Si votre système a des besoins personnalisés en termes de groupe de ports, créez des groupes de ports distribués qui répondent à ces besoins après l'ajout du commutateur distribué.

- 6 Sur la page Prêt à terminer, vérifiez les paramètres que vous avez sélectionnés et cliquez sur **Terminer**.

Utilisez le bouton **Précédent** pour modifier des paramètres.

Résultats

Un Distributed Switch est créé dans le centre de données. Vous pouvez afficher les fonctionnalités prises en charge sur le Distributed Switch ainsi que d'autres détails en naviguant vers le nouveau Distributed Switch et en cliquant sur l'onglet **Résumé**.

Étape suivante

Ajoutez des hôtes au commutateur distribué et configurez leurs adaptateurs réseau sur le commutateur.

Mettre à niveau un vSphere Distributed Switch vers une nouvelle version

Vous pouvez mettre à niveau vSphere Distributed Switch version 6.x vers une version ultérieure. La mise à niveau permet au commutateur distribué de tirer parti des fonctions disponibles uniquement dans la version ultérieure.

La mise à niveau d'un Distributed Switch provoque une brève interruption de service des hôtes et des machines virtuelles reliés au commutateur.

Note Si votre version actuelle de VDS est 6.5, vous pouvez rencontrer une brève interruption de service lors de la mise à niveau de vos commutateurs vers une version ultérieure. Si votre version actuelle de VDS est 6.6 ou une version ultérieure, vous ne risquez pas de rencontrer des interruptions lors de la mise à niveau des commutateurs vers une version ultérieure.

Pour plus d'informations, voir [KB 52621](#).

Note Pour rétablir la connectivité des machines virtuelles et des adaptateurs VMkernel si la mise à niveau échoue, sauvegardez la configuration du commutateur distribué.

Si la mise à niveau échoue, vous pouvez importer le fichier de configuration du commutateur pour recréer le commutateur ainsi que ses groupes de ports et ses hôtes connectés. Reportez-vous aux sections [Exporter les configurations de vSphere Distributed Switch](#) et [Importer la configuration d'un vSphere Distributed Switch](#).

Conditions préalables

- Mettez à niveau vCenter Server vers la version 8.0.
- Mettez à niveau tous les hôtes connectés au Distributed Switch vers ESXi 8.0.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le commutateur distribué et sélectionnez **Mise à niveau > Mettre à niveau le commutateur distribué**.
- 3 Sélectionnez la version de vSphere Distributed Switch vers laquelle vous souhaitez mettre à niveau le commutateur et cliquez sur **Suivant**.

Option	Description
Distributed Switch : 8.0.0	Compatible avec ESXi 8.0.0 et versions ultérieures. Nouvelles fonctionnalités et améliorations. Reportez-vous à la section Qu'est-ce que la compatibilité des téléchargements réseau ? .
Distributed Switch : 7.0.3	Compatible avec ESXi 7.0.3 et versions ultérieures. Nouvelles fonctionnalités et améliorations <ul style="list-style-type: none"> ■ NVMe over TCP. Voir Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch.
Distributed Switch : 7.0.2	Compatible avec ESXi 7.0.2 et versions ultérieures. Nouvelles fonctionnalités et améliorations. <ul style="list-style-type: none"> ■ Mode rapide LACP. Voir Chapitre 5 Prise en charge de LACP sur vSphere Distributed Switch.
Distributed Switch : 7.0.0	Compatible avec ESXi 7.0 et versions ultérieures. Nouvelles fonctionnalités et améliorations. <ul style="list-style-type: none"> ■ Groupe de ports distribués NSX. Voir Présentation des concepts de mise en réseau.
Distributed Switch : 6.6.0	Compatible avec ESXi 6.7 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge. Nouvelles fonctionnalités et améliorations. <ul style="list-style-type: none"> ■ Apprentissage MAC. Reportez-vous à la section Présentation de la stratégie d'apprentissage MAC.
Distributed Switch : 6.5.0	Compatible avec ESXi 6.5 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge. Nouvelles fonctionnalités et améliorations. <ul style="list-style-type: none"> ■ Améliorations de la mise en miroir de ports. Voir Spécifier le nom et les informations de session de mise en miroir de ports.

- 4 Vérifiez la compatibilité de l'hôte et cliquez sur **Suivant**.

Certaines instances d'ESXi connectées aux Distributed Switch peuvent être incompatibles avec la version cible sélectionnée. Mettez à niveau ou supprimez les hôtes incompatibles, ou sélectionnez une autre version de mise à niveau pour le Distributed Switch.

- 5 Complétez la configuration de la mise à niveau et cliquez sur **Terminer**.

Attention Une fois un vSphere Distributed Switch mis à niveau, vous ne pouvez pas le restaurer à une version antérieure. Vous ne pouvez pas non plus ajouter d'hôtes ESXi qui exécutent une version plus récente que celle du commutateur.

Modifier les paramètres généraux et avancés de vSphere Distributed Switch

Les paramètres généraux d'un vSphere Distributed Switch incluent le nom du commutateur et le nombre de liaisons montantes. Les paramètres avancés d'un commutateur distribué incluent notamment le protocole de découverte de Cisco et la taille maximale MTU pour le commutateur.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et sélectionnez le commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **Propriétés**.
- 3 Cliquez sur **Modifier**.
- 4 Cliquez sur **Général** pour modifier les paramètres de vSphere Distributed Switch.

Option	Description
Nom	Entrez le nom du commutateur distribué.
Network I/O Control	Pour activer ou désactiver Network I/O Control , utilisez le menu déroulant. Note Cette option de menu est désactivée si l'option Compatibilité des déchargements réseau est activée.
Compatibilité des déchargements réseau	Pour sélectionner le type de compatibilité des décharges réseau, utilisez le menu déroulant. <ul style="list-style-type: none"> ■ Aucun : si vous sélectionnez Aucun, l'option Compatibilité des déchargements réseau n'est pas activée. ■ Pensando : si vous sélectionnez Pensando l'option Network I/O Control est désactivée. ■ NVIDIA BlueField : si vous sélectionnez NVIDIA BlueField l'option Network I/O Control est désactivée.
Description	Ajoutez ou modifiez une description pour les paramètres du commutateur distribué.

5 Cliquez sur **Avancé** pour modifier les paramètres de vSphere Distributed Switch.

Option	Description
MTU (octets)	Taille de MTU maximale pour le vSphere Distributed Switch. Pour activer les trames Jumbo, définissez une valeur supérieure à 1 500 octets.
Mode de filtrage multidiffusion	<ul style="list-style-type: none"> ■ Basique. Le Distributed Switch transfère le trafic associé à un groupe multidiffusion en fonction d'une adresse MAC générée à partir des 23 derniers bits de l'adresse IPv4 du groupe. ■ Écoute IGMP/MLD. Le Distributed Switch transfère le trafic multidiffusion vers les machines virtuelles conformément aux adresses IPv4 et IPv6 des groupes multidiffusion abonnés en utilisant les messages d'appartenance définis par le protocole de gestion de groupes Internet (IGMP, Internet Group Management Protocol) et par le protocole MLD (Multicast Listener Discovery).
Discovery Protocol	<ul style="list-style-type: none"> a Sélectionnez le protocole CDP (Cisco Discovery Protocol), Link Layer Discovery Protocol ou (désactivé) dans le menu déroulant Type b Affectez à Opération les valeurs Écouter, Annoncer ou Les deux. Pour plus d'informations sur les Protocoles de Découverte, consultez Switch Discovery Protocol .
Contacteur l'administrateur	Entrez le nom et autres détails de l'administrateur pour le commutateur distribué.

6 Cliquez sur **Liaisons montantes** pour modifier les paramètres de vSphere Distributed Switch.

Option	Description
Nombre de liaisons montantes	Sélectionnez Ajouter pour ajouter des ports de liaisons montantes pour le Distributed Switch. Modifiez les noms des liaisons montantes pour modifier les noms des liaisons montantes.

7 Cliquez sur **OK**.

Gérer la mise en réseau sur plusieurs hôtes sur un vSphere Distributed Switch

Pour créer des réseaux virtuels et les gérer sur un vSphere Distributed Switch, vous devez ajouter des hôtes au commutateur et connecter leurs adaptateurs réseau à ce même commutateur. Pour créer une configuration de mise en réseau uniforme sur plusieurs hôtes sur le commutateur distribué, vous pouvez utiliser un hôte comme modèle et appliquer sa configuration à d'autres hôtes.

Tâches de gestion de la mise en réseau d'hôte sur un vSphere Distributed Switch

Vous pouvez ajouter de nouveaux hôtes à un vSphere Distributed Switch, connecter des adaptateurs réseau au commutateur et supprimer des hôtes du commutateur. Dans un environnement de production, vous devrez éventuellement maintenir la connectivité réseau pour des machines virtuelles et les services VMkernel pendant que vous gérez la mise en réseau de l'hôte sur le commutateur distribué.

Ajout d'hôtes à un vSphere Distributed Switch

Envisagez de préparer votre environnement avant d'ajouter de nouveaux hôtes à un commutateur distribué.

- Créez des groupes de ports distribués pour la mise en réseau de la machine virtuelle.
- Créez des groupes de ports distribués pour les services VMkernel. Par exemple, créez des groupes de ports distribués pour le réseau de gestion, vMotion et Fault Tolerance.
- Configurez suffisamment de liaisons montantes sur le commutateur distribué pour toutes les cartes réseau physiques que vous souhaitez connecter au commutateur. Par exemple, si les hôtes que vous souhaitez connecter au commutateur distribué disposent chacun de huit cartes réseau physiques, configurez huit liaisons montantes sur le commutateur distribué.
- Assurez-vous que la configuration du commutateur distribué est préparée pour les services ayant des exigences de mise en réseau spécifiques. Par exemple, iSCSI a des exigences spécifiques pour la configuration d'association et de basculement du groupe de ports distribués où vous connectez l'adaptateur VMkernel iSCSI.

Vous pouvez utiliser l'assistant **Ajouter et gérer des hôtes** pour ajouter plusieurs hôtes à la fois.

Gestion d'adaptateurs réseau sur un vSphere Distributed Switch

Une fois que vous avez ajouté des hôtes à un commutateur distribué, vous pouvez connecter des cartes réseau physiques à des liaisons montantes sur le commutateur, configurer des adaptateurs réseau de machine virtuelle et gérer la mise en réseau des adaptateurs VMkernel.

Si certains hôtes sur un Distributed Switch sont associés à d'autres commutateurs dans votre centre de données, vous pouvez migrer les adaptateurs réseau vers le Distributed Switch ou à partir de celui-ci.

Si vous migrez des adaptateurs réseau de machine virtuelle ou des adaptateurs VMkernel, assurez-vous que les groupes de ports distribués de destination disposent d'au moins une liaison montante active, et que la liaison montante est connectée à une carte réseau physique sur les hôtes. Une autre approche consiste à migrer simultanément les cartes réseau physiques, les adaptateurs réseau virtuels et les adaptateurs VMkernel.

Si vous migrez des cartes réseau physiques, conservez au moins une carte réseau active qui gère le trafic des groupes de ports. Par exemple, si *vmnic0* et *vmnic1* gèrent le trafic du groupe de ports *VM Network*, migrez *vmnic0* et laissez *vmnic1* connectée au groupe.

Regardez la vidéo sur la migration des interfaces de VMkernel et les cartes réseau physiques à un vSphere Distributed Switch.

Suppression d'hôtes d'un vSphere Distributed Switch

Avant de supprimer des hôtes d'un commutateur distribué, vous devez migrer les adaptateurs réseau en cours d'utilisation sur un autre commutateur.

- Pour ajouter des hôtes à un autre commutateur distribué, vous pouvez utiliser l'assistant **Ajouter et gérer des hôtes** pour migrer simultanément tous les adaptateurs réseau des hôtes vers le nouveau commutateur. Vous pouvez ensuite supprimer les hôtes en toute sécurité de leur commutateur distribué actuel.
- Pour migrer la mise en réseau d'hôte vers des commutateurs standard, vous devez migrer les adaptateurs réseau par étapes. Par exemple, supprimez les cartes réseau physiques des hôtes du commutateur distribué en laissant une carte réseau physique sur chaque hôte connectée au commutateur pour maintenir la connectivité réseau. Ensuite, raccordez les cartes réseau physiques aux commutateurs standard et migrez les adaptateurs VMkernel et les adaptateurs réseau de machine virtuelle sur les commutateurs. Enfin, migrez vers les commutateurs standard la carte réseau physique que vous aviez laissée connectée au commutateur distribué.
- [Ajouter des hôtes à un vSphere Distributed Switch](#)
Pour gérer la mise en réseau de votre environnement vSphere à l'aide d'un vSphere Distributed Switch, vous devez associer des hôtes au commutateur. Vous connectez les cartes réseau physiques, les adaptateurs VMkernel et les adaptateurs réseau de machine virtuelle des hôtes au commutateur distribué.
- [Configurer des adaptateurs réseau physiques sur un vSphere Distributed Switch](#)
Pour les hôtes associés à un commutateur distribué, vous pouvez attribuer des cartes réseau physiques aux liaisons montantes du commutateur. Vous pouvez configurer des cartes réseau physiques sur le commutateur distribué pour plusieurs hôtes à la fois.
- [Migrer des adaptateurs VMkernel vers un vSphere Distributed Switch](#)
Migrez les adaptateurs VMkernel vers un commutateur distribué si vous voulez gérer le trafic des services VMkernel en utilisant uniquement ce commutateur et que vous n'avez plus besoin des adaptateurs sur d'autres commutateurs standard ou distribués.
- [Créer un adaptateur VMkernel dans un vSphere Distributed Switch](#)
Créez un adaptateur VMkernel sur les hôtes associés à un commutateur distribué pour fournir une connectivité réseau aux hôtes et gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance et de vSAN.
- [Migrer la mise en réseau de machines virtuelles vers vSphere Distributed Switch](#)
Pour gérer la mise en réseau des machines virtuelles à l'aide d'un commutateur distribué, migrez les adaptateurs réseau des machines virtuelles vers des réseaux étiquetés sur le commutateur.

- [Supprimer des hôtes d'un vSphere Distributed Switch](#)

Supprimez des hôtes d'un vSphere Distributed Switch si vous avez configuré un commutateur différent pour les hôtes.

Ajouter des hôtes à un vSphere Distributed Switch

Pour gérer la mise en réseau de votre environnement vSphere à l'aide d'un vSphere Distributed Switch, vous devez associer des hôtes au commutateur. Vous connectez les cartes réseau physiques, les adaptateurs VMkernel et les adaptateurs réseau de machine virtuelle des hôtes au commutateur distribué.

Conditions préalables

- Vérifiez que vous disposez sur le commutateur distribué de suffisamment de liaisons montantes à attribuer aux cartes réseau physiques que vous souhaitez connecter au commutateur.
- Vérifiez qu'il y a au moins un groupe de ports distribués sur le commutateur distribué.
- Vérifiez que le groupe de ports distribués dispose des liaisons montantes actives configurées dans sa règle d'association et de basculement.

Si vous migrez ou créez des adaptateurs VMkernel pour iSCSI, vérifiez que la règle d'association et de basculement du groupe de ports distribués cible répond aux exigences définies pour iSCSI :

- Vérifiez qu'au moins une liaison montante est active, la liste des éléments en veille est vide et le reste des liaisons montantes est inutilisé.
- Vérifiez qu'une seule carte réseau physique par hôte est attribuée à la liaison montante active.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au Distributed Switch.
- 2 Cliquez avec le bouton droit de la souris et sélectionnez **Ajouter et gérer hôtes**.
- 3 Sur la page Sélectionner une tâche, sélectionnez **Ajout d'hôtes** et cliquez sur **Suivant**.
- 4 Sur la page Sélectionner des hôtes,
 - a sélectionnez le ou les hôtes dans la liste des hôtes disponibles sous **Tous les hôtes**.
 - b Pour afficher les hôtes sélectionnés, cliquez sur **Sélectionné**.
Les hôtes sélectionnés sont affichés.
 - c Pour filtrer les hôtes en fonction de leur compatibilité, cliquez sur **Compatibilité**.

Note Lors de l'ajout d'hôtes au vSphere Distributed Switch avec compatibilité des déchargements réseau, vous pouvez uniquement ajouter des adaptateurs compatibles sauvegardés par un DPU compatible.

- d Pour sélectionner tous les hôtes disponibles, cliquez sur **Sélectionner tout**.

- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Gérer les adaptateurs physiques**, vous pouvez ajouter des adaptateurs réseau au commutateur distribué ou en supprimer, en attribuant une liaison montante ou en annulant cette attribution.
- 7 Pour gérer les adaptateurs sur tous les hôtes ayant le même adaptateur réseau physique, sélectionnez **Adaptateurs sur tous les hôtes**.
 - a Cliquez sur **Sélectionner tout** pour sélectionner tous les hôtes.
 - b Pour attribuer une liaison montante à l'hôte, sélectionnez une liaison montante dans le menu déroulant.
 - c Pour annuler l'attribution d'une liaison montante aux hôtes, sélectionnez **Aucun** dans le menu déroulant.
 - d Pour afficher plus de détails sur les hôtes, développez l'adaptateur réseau répertorié sous **Adaptateurs réseau physiques**.
 - e Vous pouvez afficher les commutateurs qui utilisent cet adaptateur VMkernel dans **Utilisé par commutateur**.

Par exemple, si vous attribuez la liaison montante *uplink1* à *vmnic1*, elle est attribuée à tous les hôtes qui ont *vmnic1* comme adaptateur réseau physique.

- 8 Pour gérer les adaptateurs par hôte, sélectionnez **Adaptateurs par hôte**.
 - a Sélectionnez l'hôte individuel dans la liste.
 - b Pour attribuer une liaison montante à l'hôte, sélectionnez une liaison montante dans le menu déroulant.
 - c Pour annuler l'attribution d'une liaison montante à l'hôte, sélectionnez **Aucun** dans le menu déroulant.

Si vous sélectionnez des adaptateurs réseau physiques attribués à d'autres commutateurs standard ou distribués, ceux-ci sont migrés vers le commutateur distribué actuel.

Pour garantir une configuration de réseau cohérente, vous pouvez connecter la même carte réseau physique sur chaque liaison montante du commutateur distribué.

Par exemple, si vous ajoutez deux hôtes, connectez l'adaptateur *vmnic1* de chaque hôte à *uplink1* sur le commutateur distribué.

- 9 Cliquez sur **Suivant**.

Note Si aucun adaptateur réseau physique n'est attribué à un hôte, un avertissement s'affiche.

- 10 Sur la page **Gérer les adaptateurs VMkernel**, vous pouvez gérer les adaptateurs VMkernel sur le commutateur distribué.

- 11 Pour gérer les adaptateurs VMkernel sur tous les hôtes qui ont le même adaptateur VMkernel, sélectionnez **Adaptateurs sur tous les hôtes**.
 - a Pour sélectionner tous les hôtes, cliquez sur **Sélectionner tout**.
 - b Cliquez sur **Attribuer un groupe de ports**.

Vous pouvez voir tous les groupes de ports disponibles.
 - c Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - d Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
 - e Vous pouvez afficher les commutateurs qui utilisent cet adaptateur VMkernel dans **Utilisé par commutateur**.
 - f Pour afficher plus de détails sur les hôtes, développez l'adaptateur VMkernel répertorié sous **Nom**.

Par exemple, si vous attribuez *DPortGroup1* à *vmk0*, le groupe de ports est attribué à tous les hôtes qui ont *vmk0* comme adaptateur réseau VMkernel.
- 12 Pour gérer l'adaptateur VMkernel par hôte, sélectionnez **Adaptateurs par hôte**.
 - a Sélectionnez l'hôte individuel dans la liste.
 - b Cliquez sur **Attribuer un groupe de ports**.

Vous pouvez voir tous les groupes de ports disponibles.
 - c Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - d Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
- 13 Cliquez sur **Suivant**.
- 14 Sur la page **Migrer la mise en réseau VM**, cochez la case **Migrer la mise en réseau de VM** pour migrer les machines virtuelles vers un commutateur distribué.
- 15 Pour configurer par adaptateur réseau, cliquez sur **Attribuer un groupe de ports**.
 - a Pour attribuer un groupe de ports, cliquez sur **Attribuer**.

Par exemple, le groupe de ports est attribué à toutes les machines virtuelles qui ont le même adaptateur réseau.
 - b Pour annuler l'attribution de groupes de ports, cliquez sur **Annuler l'attribution**.
- 16 Pour configurer par machine virtuelle, cliquez sur **Attribuer un groupe de ports**.
 - a Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - b Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
- 17 Cliquez sur **Suivant**.
- 18 Sur la page **Prêt à terminer** de l'assistant **Ajouter et gérer les hôtes**, vérifiez les paramètres de la machine virtuelle.

19 Cliquez sur **Terminer**.

Vous avez maintenant ajouté un hôte au commutateur vSphere Distributed Switch.

Étape suivante

Les hôtes étant associés au commutateur distribué, vous pouvez gérer les adaptateurs réseau physiques, les adaptateurs VMkernel et les adaptateurs réseau de machine virtuelle.

Configurer des adaptateurs réseau physiques sur un vSphere Distributed Switch

Pour les hôtes associés à un commutateur distribué, vous pouvez attribuer des cartes réseau physiques aux liaisons montantes du commutateur. Vous pouvez configurer des cartes réseau physiques sur le commutateur distribué pour plusieurs hôtes à la fois.

Pour obtenir une configuration de mise en réseau homogène sur l'ensemble des hôtes, vous pouvez attribuer la même carte réseau physique de chaque hôte à la même liaison montante sur le commutateur distribué. Par exemple, vous pouvez attribuer *vmnic1* depuis les hôtes *ESXi A* et *ESXi B* à *Uplink 1*.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit de la souris et sélectionnez **Ajouter et gérer hôtes**.
- 3 Sur la page Sélectionner une tâche, sélectionnez **Gérer la mise en réseau des hôtes** et cliquez sur **Suivant**.
- 4 Sur la page Sélectionner des hôtes, sous **Hôtes membres**, sélectionnez les hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Gérer les adaptateurs physiques**, vous pouvez ajouter des adaptateurs réseau au commutateur distribué ou en supprimer, en attribuant une liaison montante ou en annulant cette attribution.
- 7 Pour gérer les adaptateurs sur tous les hôtes ayant le même adaptateur réseau physique, sélectionnez **Adaptateurs sur tous les hôtes**.

L'utilisateur peut voir -- lors de la sélection d'une option dans le menu déroulant Liaisons montantes. Cette option indique que tous les hôtes ayant le même adaptateur réseau ne peuvent pas être attribués à la même liaison montante.

Par exemple, si *vmnic 0* est attribué à *Uplink 1* dans *ESXI A* et à *Uplink 2* dans *ESXI B*, l'option -- sera sélectionnée dans le menu déroulant. La sélection de cette option et le passage à l'opération suivante ne modifient aucune configuration.

- a Pour attribuer une liaison montante à l'hôte, sélectionnez une liaison montante dans le menu déroulant.
 - b Pour annuler l'attribution d'une liaison montante aux hôtes, sélectionnez **Aucun** dans le menu déroulant.
 - c Vous pouvez afficher les commutateurs qui utilisent cet adaptateur VMkernel dans **Utilisé par commutateur**.
 - d Pour afficher plus de détails sur les hôtes, développez l'adaptateur réseau répertorié sous **Adaptateurs réseau physiques**.
- 8** Pour gérer les adaptateurs par hôte, sélectionnez **Adaptateurs par hôte**.
- a Sélectionnez l'hôte individuel dans la liste.
 - b Pour attribuer une liaison montante à l'hôte, sélectionnez une liaison montante dans le menu déroulant.
 - c Pour annuler l'attribution d'une liaison montante à l'hôte, sélectionnez **Aucun** dans le menu déroulant.

Note Lors de l'ajout d'hôtes au commutateur vSphere Distributed Switch avec compatibilité des déchargements réseau, vous pouvez uniquement ajouter un adaptateur compatible pris en charge par un DPU compatible.

Si vous sélectionnez des cartes réseau déjà attribuées à d'autres commutateurs standard ou distribués, celles-ci sont migrées vers le commutateur distribué actuel.

Pour garantir une configuration de réseau cohérente, vous pouvez connecter la même carte réseau physique sur chaque liaison montante du commutateur distribué.

Par exemple, si vous ajoutez deux hôtes, connectez *vmnic1* de chaque hôte à *Uplink1* sur le commutateur distribué.

- 9** Cliquez sur **Suivant**.

Note Si aucun adaptateur réseau physique n'est attribué à un hôte, un avertissement s'affiche.

- 10** Sur la page **Gérer les adaptateurs VMkernel**, vous pouvez ajouter des adaptateurs VMkernel au commutateur distribué.

- 11** Sur la page **Migrer la mise en réseau VM**, cochez la case **Migrer la mise en réseau de VM** pour migrer les machines virtuelles vers un commutateur distribué.

- 12** Cliquez sur **Suivant**.

- 13** Sur la page **Prêt à terminer** de l'assistant **Ajouter et gérer les hôtes**, vérifiez les paramètres de la machine virtuelle.

14 Cliquez sur **Terminer**.

Migrer des adaptateurs VMkernel vers un vSphere Distributed Switch

Migrez les adaptateurs VMkernel vers un commutateur distribué si vous voulez gérer le trafic des services VMkernel en utilisant uniquement ce commutateur et que vous n'avez plus besoin des adaptateurs sur d'autres commutateurs standard ou distribués.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Sur la page Sélectionner une tâche, sélectionnez **Gérer la mise en réseau des hôtes** et cliquez sur **Suivant**.
- 3 Sur la page Sélectionner des hôtes, sous **Hôtes membres**, sélectionnez les hôtes associés au commutateur distribué.
- 4 Cliquez sur **Suivant**.
- 5 Sur la page **Gérer les adaptateurs physiques**, vous pouvez ajouter des adaptateurs réseau au commutateur distribué ou en supprimer, en attribuant une liaison montante ou en annulant cette attribution.
- 6 Cliquez sur **Suivant**.

Note Si aucun adaptateur réseau physique n'est attribué à un hôte, un avertissement s'affiche.

- 7 Sur la page **Gérer les adaptateurs VMkernel**, vous pouvez gérer les adaptateurs VMkernel sur le commutateur distribué.
- 8 Pour gérer les adaptateurs VMkernel sur tous les hôtes qui ont le même adaptateur VMkernel, sélectionnez **Adaptateurs sur tous les hôtes**.
 - a Cliquez sur **Attribuer un groupe de ports**
Vous pouvez voir tous les groupes de ports disponibles.
 - b Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - c Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
Par exemple, si vous attribuez *DPortGroup1* à *vmk0*, le groupe de ports est attribué à tous les hôtes qui ont *vmk0* comme adaptateur réseau VMkernel.
- 9 Pour afficher plus de détails sur les hôtes, développez l'adaptateur VMkernel répertorié sous **Nom**.
- 10 Vous pouvez afficher les commutateurs qui utilisent cet adaptateur VMkernel dans **Utilisé par commutateur**.

- 11 Pour gérer l'adaptateur VMkernel par hôte, sélectionnez **Adaptateurs par hôte**.
 - a Sélectionnez l'hôte individuel dans la liste.
 - b Cliquez sur **Attribuer un groupe de ports**.
Vous pouvez voir tous les groupes de ports disponibles.
 - c Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - d Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
- 12 Cliquez sur **Suivant**.
- 13 Sur la page **Migrer la mise en réseau VM**, cochez la case **Migrer la mise en réseau de VM** pour migrer les machines virtuelles vers un commutateur distribué.
- 14 Cliquez sur **Suivant**.
- 15 Sur la page **Prêt à terminer** de l'assistant **Ajouter et gérer les hôtes**, vérifiez les paramètres de la machine virtuelle.
- 16 Cliquez sur **Terminer**.

Créer un adaptateur VMkernel dans un vSphere Distributed Switch

Créez un adaptateur VMkernel sur les hôtes associés à un commutateur distribué pour fournir une connectivité réseau aux hôtes et gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance et de vSAN.

Vous devez dédier un groupe de ports distribués pour chaque adaptateur VMkernel. Un adaptateur VMkernel ne doit gérer qu'un seul type de trafic.

Procédure

- 1 Sur la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez à un groupe de ports distribués.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter des adaptateurs VMkernel**.
- 3 Sur la page Sélectionner les hôtes, cliquez sur **Hôtes attachés**, sélectionnez l'un des hôtes associés au commutateur distribué et cliquez sur **OK**.
- 4 Cliquez sur **Suivant**.
- 5 Sur la page Configurer l'adaptateur VMkernel, configurez les paramètres de l'adaptateur VMkernel.

Option	Description
Étiquette réseau	L'étiquette réseau est héritée de l'étiquette du groupe de ports distribués.
Paramètres IP	Sélectionnez IPv4, IPv6 ou les deux.
	Note L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.

Option	Description
MTU	Indiquez si vous souhaitez obtenir le MTU pour l'adaptateur réseau à partir du commutateur ou définir une taille personnalisée. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9 000 octets.
Pile TCP/IP	Sélectionnez une pile TCP/IP dans la liste. Dès que vous configurez une pile TCP/IP pour l'adaptateur VMkernel, vous ne pouvez pas la modifier ultérieurement. Si vous sélectionnez vMotion ou la pile TCP/IP de provisionnement, vous ne pourrez utiliser que ces piles pour gérer le trafic vMotion ou de provisionnement sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés pour les prochaines sessions vMotion. Si vous configurez la pile TCP/IP de provisionnement, les adaptateurs VMkernel de la pile TCP/IP par défaut seront désactivés pour les opérations qui incluent du trafic de provisionnement, par exemple, la migration à froid, le clonage et la migration de snapshot de machine virtuelle.
Services disponibles	<p>Vous pouvez activer des services pour la pile TCP/IP par défaut de l'hôte. Sélectionnez les services souhaités dans la liste des services disponibles :</p> <ul style="list-style-type: none"> ■ vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. La migration avec vMotion vers l'hôte sélectionné est impossible si le service vMotion n'est pas activé pour un adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion. ■ Provisionnement. Gère les données transférées pour la migration à froid, le clonage et la migration de snapshot de machine virtuelle. ■ Journalisation de la tolérance aux pannes. Active la journalisation de Fault Tolerance sur l'hôte. Vous ne pouvez utiliser qu'un seul adaptateur VMkernel pour le trafic FT par hôte. ■ Gestion. Active le trafic de gestion pour l'hôte et vCenter Server. En règle générale, ce type d'adaptateur VMkernel est créé pour les hôtes lors de l'installation du logiciel ESXi. Vous pouvez créer un autre adaptateur VMkernel pour le trafic de gestion sur l'hôte afin d'assurer la redondance. ■ vSphere Replication. Gère les données de réplication sortantes envoyées depuis l'hôte ESXi source vers le serveur vSphere Replication. ■ NFC de vSphere Replication. Gère les données de réplication entrantes sur le site de réplication cible. ■ vSAN. Active le trafic vSAN sur l'hôte. Chaque hôte faisant partie d'un cluster de vSAN doit disposer de ce type d'adaptateur VMkernel. ■ vSphere Backup NFC. Paramètre de port VMkernel pour le trafic NFC de sauvegarde dédié. Le trafic NFC passe par l'adaptateur VMkernel lorsque le service NFC vSphereBackup est activé. ■ NVMe over TCP. Paramètre de port VMkernel pour le trafic de stockage NVMe over TCP dédié. Le trafic de stockage NVMe over TCP passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over TCP est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>. ■ NVMe over RDMA. Paramètre de port VMkernel pour le trafic de stockage NVMe over RDMA dédié. Le trafic de stockage NVMe over RDMA passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over RDMA est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>.

- 6 Sur la page des paramètres IPv4, sélectionnez une option pour l'obtention des adresses IP.

Option	Description
Obtenir automatiquement les paramètres IPv4	Utilisez DHCP pour obtenir les paramètres IP. Un serveur DHCP doit être présent sur le réseau.
Utiliser des paramètres IPv4 statiques	Entrez l'adresse IP IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel. Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la tâche TCP/IP sélectionnée. Pour modifier la passerelle par défaut de VMkernel, sélectionnez Configurer sur les adaptateurs VMkernel ou Configurer sur la pile TCP/IP et entrer une adresse de passerelle .

- 7 Sur la page Paramètres IPv6, sélectionnez une option pour l'obtention des adresses IPv6.

Option	Description
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6. Dans ESXi 6.5 et versions ultérieures, l'annonce du routeur est activée par défaut et prend en charge les indicateurs M et O, conformément à la norme RFC 4861.
Adresses IPv6 statiques	<ul style="list-style-type: none"> a Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau. b Pour modifier la passerelle par défaut de VMkernel, sélectionnez Configurer sur les adaptateurs VMkernel ou Configurer sur la pile TCP/IP et entrer une adresse de passerelle. <p>L'adresse de passerelle par défaut de VMkernel pour IPv6 est obtenue à partir de la pile TCP/IP sélectionnée.</p>

- 8 Vérifiez vos sélections dans la page Prêt à terminer et cliquez sur **Terminer**.

Migrer la mise en réseau de machines virtuelles vers vSphere Distributed Switch

Pour gérer la mise en réseau des machines virtuelles à l'aide d'un commutateur distribué, migrez les adaptateurs réseau des machines virtuelles vers des réseaux étiquetés sur le commutateur.

Conditions préalables

Vérifiez qu'au moins un groupe de ports distribués destiné à la mise en réseau d'une machine virtuelle se trouve sur le commutateur distribué.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Sur la page Sélectionner une tâche, sélectionnez **Gérer la mise en réseau des hôtes** et cliquez sur **Suivant**.

- 3 Sur la page Sélectionner des hôtes, sous **Hôtes membres**, sélectionnez les hôtes associés au commutateur distribué.
- 4 Cliquez sur **Suivant**.
- 5 Sur la page **Gérer les adaptateurs physiques**, vous pouvez ajouter des adaptateurs réseau au commutateur distribué ou en supprimer, en attribuant une liaison montante ou en annulant cette attribution.
- 6 Cliquez sur **Suivant**.

Note Si aucun adaptateur réseau physique n'est attribué à un hôte, un avertissement s'affiche.

- 7 Sur la page **Gérer les adaptateurs VMkernel**, vous pouvez ajouter des adaptateurs VMkernel au commutateur distribué.
- 8 Sur la page **Migrer la mise en réseau VM**, cochez la case **Migrer la mise en réseau de VM** pour migrer les machines virtuelles vers un commutateur distribué.
- 9 Pour configurer par adaptateur réseau, cliquez sur **Attribuer un groupe de ports**.
 - a Pour attribuer un groupe de ports, cliquez sur **Attribuer**.

Par exemple, le groupe de ports est attribué à toutes les machines virtuelles qui ont le même adaptateur réseau.
 - b Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
- 10 Pour configurer par machine virtuelle, cliquez sur **Attribuer un groupe de ports**.
 - a Pour attribuer un groupe de ports, cliquez sur **Attribuer**.
 - b Pour annuler l'attribution d'un groupe de ports, cliquez sur **Annuler l'attribution**.
- 11 Cliquez sur **Suivant**.
- 12 Sur la page **Prêt à terminer** de l'assistant **Ajouter et gérer les hôtes**, vérifiez les paramètres de la machine virtuelle.
- 13 Cliquez sur **Terminer**.

Supprimer des hôtes d'un vSphere Distributed Switch

Supprimez des hôtes d'un vSphere Distributed Switch si vous avez configuré un commutateur différent pour les hôtes.

Conditions préalables

- Vérifiez que les cartes réseau physiques sur les hôtes cibles sont migrées vers un autre commutateur.
- Vérifiez que les adaptateurs VMkernel sur les hôtes sont migrés vers un autre commutateur.
- Vérifiez que les adaptateurs réseau de machine virtuelle sont migrés vers un autre commutateur.

Pour obtenir des informations détaillées sur la migration d'adaptateurs réseau vers des commutateurs différents, reportez-vous à [#unique_45](#)

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sur la page Sélectionner la tâche, sélectionnez **Supprimer des hôtes**, puis cliquez sur **Suivant**.
- 4 Pour supprimer un hôte individuel du commutateur distribué, sélectionnez l'hôte.
- 5 Pour supprimer tous les hôtes du commutateur distribué, cliquez sur **Sélectionner tout**.
- 6 Cliquez sur **Suivant**.
- 7 Cliquez sur **Terminer**.

Gestion de la mise en réseau sur des commutateurs proxy hôtes

Vous pouvez modifier la configuration du commutateur proxy sur chaque hôte associé à un vSphere Distributed Switch. Vous pouvez gérer les cartes réseau physiques, les adaptateurs VMkernel et les adaptateurs réseau des machines virtuelles.

Pour plus d'informations sur la configuration de la mise en réseau VMkernel sur des commutateurs de proxy hôtes, reportez-vous à [Créer un adaptateur VMkernel dans un vSphere Distributed Switch](#).

Migrer des adaptateurs réseau sur un hôte vers un vSphere Distributed Switch

Si des hôtes sont associés à un commutateur distribué, vous pouvez migrer les adaptateurs réseau du commutateur standard vers un commutateur distribué. Vous pouvez migrer simultanément des cartes réseau physiques, des adaptateurs VMkernel et des adaptateurs réseau de machines virtuelles.

Pour migrer des adaptateurs réseau de machine virtuelle ou des adaptateurs VMkernel, assurez-vous que les groupes de ports distribués de destination disposent d'au moins une liaison montante active et que la liaison montante est connectée à une carte réseau physique sur cet hôte. Sinon, migrez à la fois les cartes réseau physiques, les adaptateurs réseau virtuels et les adaptateurs VMkernel.

Pour migrer des cartes réseau physiques, veillez à ce qu'au moins une carte réseau physique gère le trafic des groupes de ports source sur le commutateur standard. Par exemple, si vous migrez une carte réseau physique attribuée à un groupe de ports pour la mise en réseau des machines virtuelles, assurez-vous que le groupe de ports est connecté à au moins une carte réseau physique. Sinon, les machines virtuelles du même réseau VLAN sur le commutateur standard seront connectées entre elles mais pas au réseau externe.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur distribué de destination et cliquez sur l'icône point de suspension en regard de **Gérer adaptateurs physiques**.
- 4 Sélectionnez **Migrer la mise en réseau**.
- 5 Configurez les cartes réseau physiques.
 - a Dans la liste **Sur d'autres commutateurs/non réclamés**, sélectionnez une carte réseau physique, puis cliquez sur **Attribuer une liaison montante**.
 - b Sélectionnez une liaison montante et cliquez sur **OK**.
 - c Cliquez sur **Suivant**.
- 6 Configurez les adaptateurs VMkernel.
 - a Sélectionnez un adaptateur et cliquez sur **Assignez un groupe de ports**.
 - b Sélectionnez un groupe de ports distribués et cliquez sur **OK**.

Vous devez connecter un adaptateur VMkernel à un seul groupe de ports distribués à la fois.
 - c Cliquez sur **Suivant**.
- 7 Configurez les adaptateurs réseau des machines virtuelles.
 - a Cochez la case **Migrer la mise en réseau VM**.
 - b Sélectionnez une machine virtuelle ou un adaptateur réseau de machine virtuelle, puis cliquez sur **Affecter groupe ports**.

Si vous sélectionnez une machine virtuelle, tous les adaptateurs réseau de la machine seront migrés. Si vous sélectionnez un adaptateur réseau, seul cet adaptateur sera migré.
 - c Sélectionnez un groupe de ports distribués dans la liste et cliquez sur **OK**.
 - d Cliquez sur **Suivant**.
- 8 Dans la page Prêt à terminer, vérifiez la nouvelle configuration de mise en réseau et cliquez sur **Terminer**.

Migrer un adaptateur VMkernel sur un hôte vers un vSphere Standard Switch

Si un hôte est associé à un commutateur distribué, vous pouvez migrer les adaptateurs VMkernel du commutateur distribué vers un commutateur standard.

Pour plus d'informations sur la création d'adaptateurs VMkernel sur un vSphere Distributed Switch, consultez [Créer un adaptateur VMkernel dans un vSphere Distributed Switch](#)

Conditions préalables

Assurez-vous que le commutateur standard de destination dispose au moins d'une carte réseau physique.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard de destination dans la liste.
- 4 Cliquez sur **Migrer un adaptateur VMkernel**.
- 5 Sur la page Sélectionner l'adaptateur VMkernel, sélectionnez l'adaptateur réseau virtuel à migrer vers le commutateur standard dans la liste.
- 6 Dans la page Configurer les paramètres, modifiez les valeurs **Étiquette réseau** et **ID VLAN** pour l'adaptateur réseau.
- 7 Dans la page Prêt à terminer, vérifiez les informations de migration, puis cliquez sur **Terminer**. Cliquez sur **Précédent** pour changer des paramètres.

Attribuer une carte réseau physique d'un hôte à un vSphere Distributed Switch

Vous pouvez attribuer des cartes réseau physiques à un hôte associé à un commutateur distribué vers un port de liaison montante sur le commutateur de proxy hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur distribué dans la liste.
- 4 Cliquez sur **Gérer adaptateurs physiques**.
- 5 Sélectionnez une liaison montante disponible dans la liste et cliquez sur **Ajouter des adaptateurs**.
- 6 Sélectionnez une carte réseau physique et cliquez sur **OK**.

Supprimer une carte réseau physique d'un vSphere Distributed Switch

Vous pouvez supprimer la carte réseau d'un hôte d'une liaison montante d'un vSphere Distributed Switch.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur distribué.
- 4 Cliquez sur **Gérer adaptateurs physiques**.
- 5 Sélectionnez une liaison montante, puis cliquez sur **Supprimez la sélection**.
- 6 Cliquez sur **OK**.

Étape suivante

Lorsque vous supprimez des cartes réseau physiques de machines virtuelles actives, il peut arriver que les cartes réseau figurent toujours dans le . Reportez-vous à la section [Suppression des cartes réseau des machines virtuelles actives](#).

Suppression des cartes réseau des machines virtuelles actives

Lorsque vous supprimez des cartes réseau d'une machine virtuelle active, elles s'affichent toujours dans vSphere Client.

Suppression des cartes réseau d'une machine virtuelle active sans système d'exploitation invité

Vous ne pouvez pas supprimer les cartes réseau d'une machine virtuelle active si cette dernière ne dispose pas d'un système d'exploitation.

vSphere Client peut signaler que la carte réseau a été supprimée, mais elle continue d'être attachée à la machine virtuelle.

Suppression des cartes réseau d'une machine virtuelle active dotée d'un système d'exploitation invité

Vous pouvez supprimer une carte réseau d'une machine virtuelle active, mais cela n'est parfois pas signalé à vSphere Client. Si vous cliquez sur la boîte de dialogue **Modifier les paramètres** de la machine virtuelle, il se peut que la carte réseau supprimée soit toujours affichée, même si la tâche est terminée. La boîte de dialogue Modifier les paramètres de la machine virtuelle n'affiche pas immédiatement la carte réseau supprimée.

Il se peut également que vous la voyiez attachée à la machine virtuelle si le système d'exploitation invité de la machine virtuelle ne permet pas de supprimer à chaud les cartes réseau.

Groupes de ports distribués

Un groupe de ports distribués définit les options de configuration de chaque port membre d'un vSphere Distributed Switch. Les groupes de ports distribués définissent la manière dont une connexion à un réseau est établie.

Ajouter un groupe de ports distribués

Pour créer un réseau de commutateurs distribués pour vos machines virtuelles et pour associer des adaptateurs VMkernel, vous pouvez ajouter un groupe de ports distribués à un commutateur vSphere Distributed Switch.

En complément de l'ajout d'un groupe de ports, le balisage VLAN est appliqué globalement sur tous les ports distribués. À l'aide des options de VLAN, vous pouvez sélectionner des balises VLAN. Pour en savoir plus, consultez [Configurer le balisage VLAN sur un port distribué ou un groupe de ports distribués](#)

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le commutateur distribué et sélectionnez **Groupe de ports distribués > Nouveau groupe de ports distribués**.
- 3 Sur la page Nom et emplacement, entrez le nom du nouveau groupe de ports distribués ou acceptez le nom généré, puis cliquez sur **Suivant**.
- 4 Dans la page Configurer les paramètres, établissez les propriétés générales pour le nouveau groupe de ports distribués.

Paramètre	Description
Liaison de port	<p>Sélectionnez les ports attribués aux machines virtuelles connectées à ce groupe de ports distribués.</p> <ul style="list-style-type: none"> ■ Liaison statique : affectez un port à une machine virtuelle quand la machine virtuelle se connecte au groupe de ports distribués. ■ Éphémère - aucune attache : aucune liaison de port. Vous pouvez assigner une machine virtuelle à un groupe de ports distribués, avec également une liaison de port temporaire lors d'une connexion à l'hôte.
Allocation de port	<ul style="list-style-type: none"> ■ Élastique : le nombre de ports par défaut est de huit. Lorsque tous les ports sont attribués, un nouvel ensemble de huit ports est créé. ■ Fixe : le nombre de ports par défaut est de huit. Tous les ports sont attribués. Aucun port supplémentaire n'est créé.
Nombre de ports	Entrez le nombre de ports dans le groupe de ports distribués.
Pool de ressources réseau	<p>Pour attribuer le nouveau groupe de ports distribués à un pool de ressources réseau défini par l'utilisateur, utilisez le menu déroulant. Si vous n'avez pas créé de pool de ressources réseau, ce menu est vide.</p> <p>Note Vous ne pouvez pas attribuer un pool de ressources réseau si les déchargements réseau sont activés.</p>

Paramètre	Description
<p>VLAN</p>	<p>Utilisez le menu déroulant Type de VLAN pour spécifier le type de filtrage et de marquage du trafic VLAN :</p> <ul style="list-style-type: none"> ■ Aucun : ne pas utiliser de VLAN. Sélectionnez Aucun si vous utilisez le balisage de commutateur externe. ■ VLAN : dans la zone de texte ID VLAN, entrez un nombre compris entre 1 et 4 094 pour le balisage de commutateur virtuel. ■ Liaison de jonction VLAN : entrez une plage de jonction VLAN. <p>Transmettez le trafic VLAN avec un ID au système d'exploitation invité. Vous pouvez définir plusieurs plages et VLAN individuels à l'aide d'une liste séparée par des virgules. Par exemple : 1702-1705, 1848-1849</p> <p>Utilisez cette option pour l'identification de l'invité virtuel.</p> <ul style="list-style-type: none"> ■ VLAN privé : associez le trafic à un VLAN privé créé sur le commutateur distribué. Si vous n'avez pas créé de réseaux VLAN privés, ce menu est vide.
<p>Avancé</p>	<p>Pour personnaliser les configurations de stratégie pour le nouveau groupe de ports distribués, cochez cette case.</p>

5 Cliquez sur **Suivant**.

6 (Facultatif) Dans la page Sécurité, modifiez les exceptions de sécurité et cliquez sur **Suivant**.

Paramètre	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ Rejeter : l'activation du mode promiscuité sur un adaptateur à partir du système d'exploitation invité ne permet pas la réception de trames destinées à d'autres machines virtuelles. ■ Accepter : si le mode promiscuité est activé sur un adaptateur à partir du système d'exploitation invité, le commutateur autorise l'adaptateur de l'invité à recevoir toutes les trames transmises au commutateur, conformément à la stratégie VLAN active du port auquel l'adaptateur est connecté. <p>Les pare-feu, scanners de ports, systèmes de détection d'intrusion, etc., doivent s'exécuter en mode promiscuité.</p>
Modifications d'adresse MAC	<p>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.</p> <ul style="list-style-type: none"> ■ Rejeter : si l'option est définie sur Rejeter et que le système d'exploitation invité remplace l'adresse MAC de l'adaptateur par une valeur différente de l'adresse indiquée dans le fichier de configuration <code>.vmtx</code>, alors le commutateur rejette toutes les trames entrantes de l'adaptateur de la machine virtuelle. <p>Si le système d'exploitation invité annule les modifications apportées à l'adresse MAC, la machine virtuelle reçoit à nouveau les trames.</p> <ul style="list-style-type: none"> ■ Accepter : si le système d'exploitation invité remplace l'adresse MAC de l'adaptateur réseau, ce dernier reçoit les trames à sa nouvelle adresse.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter : le commutateur rejette toute trame sortante dont l'adresse MAC source est différente de celle indiquée dans le fichier de configuration <code>.vmtx</code>. ■ Accepter : le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

7 (Facultatif) Sur la page Sécurité, modifiez la stratégie d'apprentissage MAC et cliquez sur **Suivant**.

Paramètre	Description
État	Activez ou désactivez la fonctionnalité d'apprentissage MAC. La valeur par défaut est Désactivé.
Autoriser la saturation monodiffusion	Lorsqu'un paquet reçu par un port a une adresse MAC de destination inconnue, le paquet 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 si l'apprentissage MAC est activé.

Paramètre	Description
Limite MAC	Le nombre d'adresses MAC pouvant être apprises est configurable. La valeur maximale est 4 096, selon le port, cette valeur est prise par défaut.
Stratégie de limite MAC	Stratégie à appliquer lorsque la limite MAC est atteinte. Les options sont : <ul style="list-style-type: none"> ■ 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.

- 8 (Facultatif) Dans la page Formation du trafic, activez ou désactivez l'entrée ou la formation du trafic de sortie puis cliquez sur **Suivant**.

Paramètre	Description
État	Si vous activez soit la Formation du trafic d'entrée , soit la Formation du trafic de sortie , vous limitez l'allocation de bande passante réseau allouée à chaque adaptateur virtuel associé avec ce groupe de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique par défaut. Note Vous ne pouvez pas attribuer de stratégies de formation du trafic si l'option Compatibilité des déchargements réseau est activée.
Bande passante moyenne	Cette fonctionnalité établit le nombre moyen de bits par seconde à autoriser dans le temps. Il s'agit de la charge moyenne autorisée.
Bande passante maximale	Nombre maximal de bits par seconde à autoriser à travers un port quand il reçoit/envoie une rafale de trafic. Ce paramètre limite la bande passante utilisée par un port lorsqu'il utilise son bonus de rafale.
Taille de rafale	Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin de plus de bande passante que la quantité spécifiée par Bande passante moyenne , il pourra transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre s'ajoute au nombre d'octets qui peuvent être accumulés dans le bonus de rafale et par conséquent transférés à une vitesse plus élevée.

9 (Facultatif) Dans la page Association et basculement, modifiez les paramètres et cliquez sur **Suivant**.

Paramètre	Description
Équilibrage de charge	<p>Spécifiez la manière dont une liaison montante est sélectionnée.</p> <ul style="list-style-type: none"> ■ Route basée sur le port virtuel d'origine : sélectionnez une liaison montante selon le port virtuel par lequel est entré le trafic dans le commutateur distribué. ■ Route basée sur le hachage IP : sélectionnez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ Route basée sur le hachage MAC source : sélectionnez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ Route basée sur la charge NIC physique : sélectionnez une liaison montante basée sur les charges actuelles des NIC physiques. ■ Utiliser la commande de basculement explicite : utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. <p>Note L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel. Pour toutes les autres options, désactivez EtherChannel.</p>
Détection de panne réseau	<p>Spécifiez la méthode pour l'utiliser pour la détection de basculement.</p> <ul style="list-style-type: none"> ■ État de lien seulement : repose uniquement sur l'état du lien que l'adaptateur réseau fournit. Cette option détecte les pannes, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ Sondage balise : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. <p>Note Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.</p>

Paramètre	Description
Notifier les commutateurs	<p>Sélectionnez Oui ou Non pour notifier les commutateurs en cas de basculement. Si vous sélectionnez Oui, chaque fois qu'une carte réseau virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte réseau physique différente dans l'association suite à un basculement, une notification est envoyée sur le réseau pour mettre à jour les tables de recherche des commutateurs physiques. Dans presque tous les cas, ce processus est souhaitable pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion.</p> <p>Note N'utilisez pas cette option quand les machines virtuelles utilisant le groupe de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.</p>
Retour arrière	<p>Sélectionnez Oui ou Non pour mettre hors tension ou activer le retour arrière.</p> <p>Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur Oui, la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur Non, un adaptateur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.</p>
Ordre de basculement	<p>Spécifiez comment répartir la charge de travail pour les liaisons montantes. Pour utiliser certaines liaisons montantes mais en réserver d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes :</p> <ul style="list-style-type: none"> ■ Liaisons montantes actives : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ Liaisons montantes en veille : utilisez cette liaison montante si la connectivité de l'adaptateur actif est interrompue. ■ Liaisons montantes inutilisées : n'utilisez pas cette liaison montante. <p>Note En utilisant l'équilibrage de charge avec hachage IP, ne configurez pas les liaisons montantes en veille.</p>

10 (Facultatif) Dans la page Surveillance, activez ou désactivez NetFlow et cliquez sur **Suivant**.

Paramètre	Description
Désactivé	NetFlow est désactivé sur le groupe de ports distribués.
Activé	NetFlow est activé sur le groupe de ports distribués. Vous pouvez définir les paramètres NetFlow au niveau du vSphere Distributed Switch.

11 (Facultatif) Dans la page Divers, sélectionnez **Oui** ou **Non** et cliquez sur **Suivant**.

Sélectionner **Oui** arrête tous les ports dans le groupe de ports. Cette action peut perturber les opérations réseau normales des hôtes ou des machines virtuelles utilisant les ports.

12 Dans la page Prêt à terminer, vérifiez les paramètres et cliquez sur **Terminer**.

Pour modifier les paramètres, cliquez sur le bouton **Retour**.

Modifier les paramètres généraux d'un groupe de ports distribués

Vous pouvez modifier les paramètres généraux d'un groupe de ports distribués tels que le nom du groupe de ports distribués, les paramètres des ports et le pool de ressources réseau.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Général** pour modifier les paramètres de groupe de ports distribués suivants.

Option	Description
Nom	Le nom du groupe de ports distribués. Vous pouvez modifier le nom dans le champ de texte.
Liaison de port	Choisissez quand les ports sont affectés aux machines virtuelles connectées au groupe de ports distribués. <ul style="list-style-type: none"> ■ Liaison statique : affectez un port à une machine virtuelle quand la machine virtuelle se connecte au groupe de ports distribués. ■ Éphémère : aucune liaison de port. Vous pouvez attribuer une machine virtuelle à un groupe de ports distribués avec une liaison de port éphémère lors d'une connexion à l'hôte.
Allocation de port	<ul style="list-style-type: none"> ■ Élastique : le nombre de ports par défaut est défini sur huit. Lorsque tous les ports sont assignés, une nouvelle série de huit ports est créé. Ceci est la configuration par défaut. ■ Fixe : le nombre de ports par défaut est de huit. Lorsque tous les ports sont assignés, aucun port additionnel n'est créé.
Nombre de ports	Entrez le nombre de ports dans le groupe de ports distribués.
Pool de ressources réseau	Utilisez le menu déroulant pour attribuer le nouveau groupe de ports distribués à un pool de ressources réseau définie par l'utilisateur. Si vous n'avez pas créé de pool de ressources réseau, ce menu reste vide.
Description	Entrez toute l'information sur le groupe de ports distribués dans le champ de description.

- 4 Cliquez sur **OK**.

Supprimer un groupe de ports distribués

Supprimez un groupe de ports distribués lorsque vous n'avez plus besoin du réseau étiqueté correspondant pour fournir une connectivité et pour configurer les paramètres de connexion des machines virtuelles ou de la mise en réseau VMkernel.

Conditions préalables

- Vérifiez que toutes les machines connectées au réseau étiqueté correspondant sont migrées vers un autre réseau étiqueté.
- Vérifiez que tous les adaptateurs VMkernel connectés au groupe de ports distribués sont migrés vers un autre groupe de ports ou sont supprimés.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Sélectionnez le groupe de ports distribués.
- 3 Dans le menu **Actions**, sélectionnez **Supprimer**.

Utilisation des ports distribués

Un port distribué est un port sur un commutateur distribué vSphere qui se connecte à VMkernel ou à un adaptateur réseau de machine virtuelle.

La configuration de port distribué par défaut est déterminée par les paramètres du groupe de ports distribués, mais certains paramètres de ports distribués individuels peuvent être remplacés.

Surveiller l'état des ports distribués

vSphere peut surveiller les ports distribués et fournir des informations sur leur état actuel et des statistiques sur l'exécution de chaque port

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez sur un groupe de ports distribués.
- 3 Cliquez sur l'onglet **Ports** et sélectionnez un port dans la liste.

Le tableau des ports du groupe de ports distribués affiche les statistiques d'exécution pour chaque port distribué.

La colonne **État** affiche l'état actuel de chaque port distribué.

Option	Description
Raccorder	La liaison du port distribué est activé.
Lien bas	La liaison du port distribué est inactive.
Bloqué	Ce port distribué est bloqué.
--	L'état de ce port distribué n'est pas disponible actuellement.

Définir les paramètres de ports distribués

Vous pouvez changer les paramètres généraux des ports distribués, tels que le nom et la description des ports.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez sur un groupe de ports distribués dans la liste.
- 3 Cliquez sur l'onglet **Ports** et sélectionnez un port distribué dans le tableau.
Les informations sur le port distribué s'affichent au bas de l'écran.
- 4 Cliquez sur l'icône **Modifier les paramètres**.
- 5 Sur la page Propriétés et sur les pages de règles, modifiez les informations sur le port distribué et cliquez sur **OK**.

Si les remplacements ne sont pas autorisés, les options de stratégies sont désactivées.

Vous pouvez autoriser des remplacements au niveau du port en changeant les paramètres **Avancés** du groupe de ports distribués. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Configurer la mise en réseau de machines virtuelles sur un vSphere Distributed Switch

Connectez les machines virtuelles à un vSphere Distributed Switch en configurant une carte NIC de machine virtuelle individuelle ou en migrant des groupes de machines virtuelles depuis le vSphere Distributed Switch.

Connectez les machines virtuelles aux commutateurs distribués vSphere en connectant leurs adaptateurs réseau virtuels associés aux groupes de ports distribués. Vous pouvez le faire pour une machine virtuelle individuelle en modifiant la configuration de sa carte réseau ou pour un groupe de machines virtuelles en migrant les machines virtuelles depuis un réseau virtuel existant vers un vSphere Distributed Switch.

Migrer des machines virtuelles vers ou depuis vSphere Distributed Switch

Outre la connexion des machines virtuelles à un commutateur distribué au niveau de la machine virtuelle, vous pouvez migrer un groupe de machines virtuelles entre un réseau vSphere Distributed Switch et un réseau commutateur standard vSphere.

Procédure

- 1 Dans vSphere Client, accédez à un centre de données.
- 2 Cliquez avec le bouton droit sur le centre de données dans le navigateur et sélectionnez **Migrer les VM vers un autre réseau**.
- 3 Sélectionnez un réseau source.
 - Sélectionnez **Réseau spécifique** et utilisez le bouton **Parcourir** pour sélectionner un réseau source spécifique.
 - Sélectionnez **Pas de réseau** pour migrer tous les adaptateurs réseau de VM qui ne sont connectés à aucun autre réseau.
- 4 Utilisez **Parcourir** pour sélectionner un réseau de destination et cliquez sur **Suivant**.
- 5 Sélectionnez dans la liste les VM à migrer du réseau source vers le réseau de destination et cliquez sur **Suivant**.
- 6 Passez vos sélections en revue et cliquez sur **Terminer**.
Cliquez sur **Précédent** pour changer des paramètres.

Connecter une machine virtuelle individuelle à un groupe de ports distribués

Connectez une machine virtuelle individuelle à un vSphere Distributed Switch en modifiant la configuration de la carte réseau de la machine virtuelle.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 3 Développez la section **Adaptateur réseau** et sélectionnez **Parcourir** dans le menu déroulant **Adaptateur réseau**.
- 4 Dans la boîte de dialogue Sélectionner un réseau, sélectionnez un groupe de ports et cliquez sur **OK**.
- 5 Cliquez sur **OK**.

Diagrammes de la topologie d'un vSphere Distributed Switch

Les diagrammes de la topologie d'un vSphere Distributed Switch dans vSphere Client montrent la structure des adaptateurs de machine virtuelle, des adaptateurs VMkernel et des adaptateurs physiques dans le commutateur.

Vous pouvez examiner les composants, disposés par groupes de ports, dont le trafic est géré par le commutateur, ainsi que les connexions entre eux. Le diagramme affiche des informations sur l'adaptateur physique qui connecte les adaptateurs virtuels au réseau externe.

Vous pouvez afficher les composants qui s'exécutent sur tout le commutateur distribué et sur chaque hôte y participant.

Regardez la vidéo consacrée aux opérations que vous pouvez réaliser dans le diagramme de topologie de vSphere Distributed Switch.



(Gestion de la mise à niveau virtuelle en utilisant le diagramme de topologie de VDS)

Diagramme de la topologie centrale

Vous pouvez utiliser les diagrammes de la topologie centrale du commutateur pour localiser et modifier les paramètres de groupes de ports distribués et de groupes de liaisons montantes associés à plusieurs hôtes. Vous pouvez initier la migration d'adaptateurs de machine virtuelle d'un groupe de ports vers une destination sur le même commutateur ou sur un autre. Vous pouvez également réorganiser les hôtes et leur mise en réseau sur le commutateur à l'aide de l'assistant **Ajouter et gérer des hôtes**.

Diagramme de la topologie d'un commutateur de proxy hôte

Le diagramme de la topologie d'un commutateur de proxy hôte montre les adaptateurs attachés aux ports du commutateur sur l'hôte. Vous pouvez modifier les paramètres des adaptateurs VMkernel et des adaptateurs physiques.

Diagramme de la topologie d'un commutateur de déchargement réseau

Le diagramme de topologie d'un commutateur de déchargement réseau montre les adaptateurs attachés aux ports de commutateur sur l'hôte. Vous pouvez modifier les paramètres des adaptateurs VMkernel et des adaptateurs physiques.

Filtres de diagramme

Vous pouvez utiliser des filtres de diagramme pour limiter les informations affichées dans des diagrammes de la topologie. Le filtre par défaut limite le diagramme de la topologie à afficher 32 groupes de ports, 32 hôtes et 1 024 machines virtuelles.

Vous pouvez changer l'étendue du diagramme en n'utilisant aucun filtre ou en appliquant des filtres personnalisés. En utilisant un filtre personnalisé, vous pouvez afficher des informations portant uniquement sur un ensemble de machines virtuelles, sur un ensemble de groupes de ports sur certains hôtes ou sur un port. Vous pouvez créer des filtres à partir du diagramme de la topologie centrale du commutateur distribué.

Afficher la topologie d'un vSphere Distributed Switch

Examinez l'organisation des composants qui sont connectés aux commutateurs distribués sur les hôtes dans vCenter Server.

Procédure

- 1 Accédez au vSphere Distributed Switch dans vSphere Client.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **Topologie**.

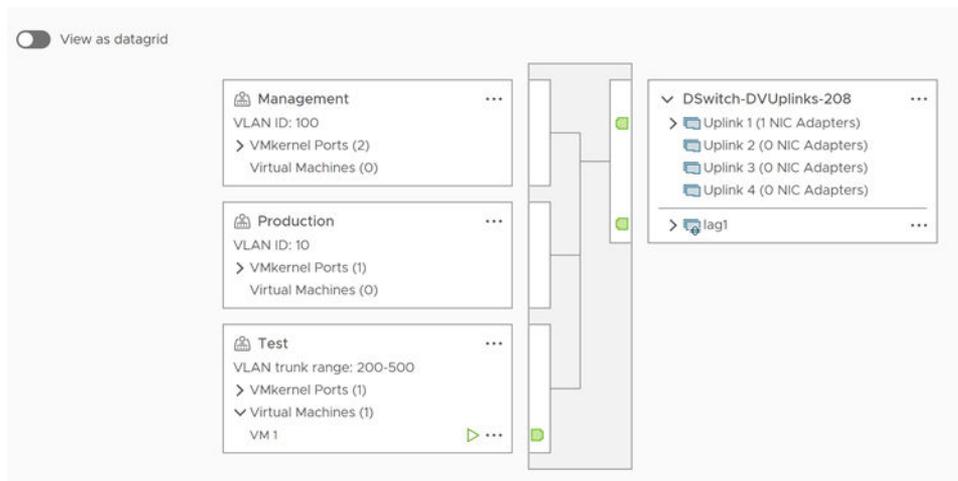
Résultats

Par défaut le diagramme montre jusqu'à 32 groupes de ports distribués, 32 hôtes et 1 024 machines virtuelles.

Exemple : Diagramme d'un commutateur distribué qui connecte VMkernel et les machines virtuelles au réseau

Dans votre environnement virtuel, un vSphere Distributed Switch gère les adaptateurs VMkernel pour vSphere vMotion et pour le réseau de gestion, et les machines virtuelles regroupées. Le diagramme de la topologie centrale permet notamment de déterminer si une machine virtuelle ou un adaptateur VMkernel est connecté au réseau externe et d'identifier l'adaptateur physique qui transmet les données.

Figure 3-4. Diagramme de la topologie d'un commutateur distribué qui gère la mise en réseau des adaptateurs VMkernel et des machines virtuelles



Étape suivante

Vous pouvez effectuer les tâches courantes suivantes dans la topologie du commutateur distribué :

- Utiliser des filtres pour afficher les composants de mise en réseau correspondant uniquement aux groupes de ports sélectionnés sur certains hôtes, à des machines virtuelles sélectionnées ou à un port spécifique.
- Localiser, configurer et migrer des composants de mise en réseau de machines virtuelles sur des hôtes et des groupes de ports à l'aide de l'assistant **Migrer la mise en réseau de machines virtuelles**.
- Détecter les adaptateurs de machine virtuelle ne disposant pas d'un réseau attribué et les déplacer vers le groupe de ports sélectionné à l'aide de l'assistant **Migrer la mise en réseau de machines virtuelles**.
- Gérer les composants de mise en réseau sur plusieurs hôtes à l'aide de l'assistant **Ajouter et gérer les hôtes**.
- Afficher la carte réseau physique ou l'association de cartes réseau qui transporte le trafic associé à un adaptateur de machine virtuelle ou un adaptateur VMkernel sélectionné.
De cette manière, vous pouvez également voir l'hôte sur lequel réside un adaptateur VMkernel sélectionné. Sélectionnez l'adaptateur, tracez la route vers la carte réseau physique associée, et affichez l'adresse IP ou le nom de domaine en regard de la carte réseau.
- Déterminer le mode VLAN et l'ID d'un groupe de ports. Pour plus d'informations sur les modes VLAN, reportez-vous à [Configuration VLAN](#).

Afficher la topologie d'un commutateur de proxy hôte

Examinez et réorganisez la mise en réseau de l'adaptateur VMkernel et des machines virtuelles gérées par le vSphere Distributed Switch sur un hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur distribué dans la liste.

Résultats

La topologie du commutateur de proxy hôte s'affiche sous la liste.

Afficher la topologie du commutateur de déchargements réseau

Examinez l'organisation du Distributed Switch avec des déchargements réseau.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 L'icône  indique que les déchargements réseau sont pris en charge pour ce Distributed Switch.

Comment configurer la mise en réseau d'adaptateurs VMkernel ?

4

Découvrez comment configurer les adaptateurs VMkernel pour fournir la connectivité réseau aux hôtes afin de gérer le trafic système de vMotion, de stockage IP, de journalisation de Fault Tolerance et de vSAN, entre autres.

- [Couche de mise en réseau VMkernel](#)

La couche de mise en réseau VMkernel assure la connectivité des hôtes et gère le trafic système standard de vSphere vMotion, du stockage IP, de Fault Tolerance et de vSAN, entre autres. Vous pouvez également créer des adaptateurs VMkernel sur les hôtes vSphere Replication source et cible dans le but d'isoler le trafic des données de réplication.

- [Créer un adaptateur VMkernel dans un commutateur vSphere standard](#)

Créez un adaptateur réseau VMkernel sur un commutateur vSphere standard pour fournir la connectivité réseau aux hôtes et gérer le trafic système dans vSphere vMotion, le stockage IP, la journalisation de Fault Tolerance, vSAN, etc. Vous pouvez également créer des adaptateurs VMkernel sur les hôtes vSphere Replication source et cible dans le but d'isoler le trafic des données de réplication. Chaque adaptateur VMkernel ne doit être associé qu'à un seul de type de trafic.

- [Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch](#)

Créez un adaptateur VMkernel sur un hôte associé à un Distributed Switch afin de fournir la connectivité réseau à l'hôte et de gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance et de vSAN, entre autres. Vous pouvez configurer des adaptateurs VMkernel pour le trafic système standard sur des commutateurs vSphere standard et sur des vSphere Distributed Switches.

- [Modifier la configuration d'un adaptateur VMkernel](#)

Vous pouvez être amené à modifier le type de trafic pris en charge pour un adaptateur VMkernel ou le mode d'obtention des adresses IPv4 ou IPv6.

- [Remplacer la passerelle par défaut d'un adaptateur VMkernel](#)

Vous devrez peut-être remplacer la passerelle par défaut d'un adaptateur VMkernel par une autre passerelle de vSphere vMotion.

- [Configurer la passerelle de l'adaptateur VMkernel avec les commandes esxcli](#)

Vous pouvez remplacer la passerelle par défaut d'un adaptateur VMkernel afin de fournir une passerelle différente pour vSphere vMotion avec les commandes esxcli.

- [Configurer le fichier `resolv.conf` à l'aide de commandes `esxcli`](#)

Le fichier `resolv.conf` est utilisé pour configurer des serveurs DNS gérés de manière centralisée. Vous pouvez configurer des entrées dans le fichier `/etc/resolv.conf` à l'aide de commandes `esxcli`, ce qui permet de conserver la modification lors du redémarrage de l'hôte ESXi. La propriété peut être définie explicitement si DHCP n'est pas activé.

- [Configurer le fichier d'hôtes DNS à l'aide des commandes `ESXCLI`](#)

Le fichier `hosts` est utilisé pour mapper des noms d'hôte ou des noms de domaine à des adresses IP. Vous pouvez configurer des entrées du fichier `/etc/hosts` à l'aide de commandes `esxcli`, ce qui permet de conserver la modification lors du redémarrage de l'hôte ESXi.

- [Afficher la configuration de la pile TCP/IP sur un hôte](#)

Vous pouvez également afficher le DNS et la configuration de routage de la pile TCP/IP d'un hôte, de même que les tables de routage IPv4 et IPv6, l'algorithme de contrôle d'encombrement et le nombre maximal de connexions autorisées.

- [Modifier la configuration de la pile TCP/IP d'un hôte](#)

Vous pouvez modifier le DNS et la configuration de passerelle par défaut de la pile TCP/IP d'un hôte, de même que l'algorithme de contrôle d'encombrement, le nombre maximal de connexions autorisées et le nom des piles TCP/IP personnalisées.

- [Créer une pile TCP/IP personnalisée](#)

Vous pouvez créer une pile TCP/IP personnalisée sur un hôte pour transférer le trafic de mise en réseau via une application personnalisée.

- [Supprimer un adaptateur VMkernel](#)

Lorsque vous n'utilisez plus un adaptateur VMkernel, vous pouvez le supprimer d'un commutateur vSphere standard ou distribué. Veuillez à conserver au moins un adaptateur VMkernel dédié au trafic de gestion sur l'hôte afin de maintenir la connectivité réseau.

Couche de mise en réseau VMkernel

La couche de mise en réseau VMkernel assure la connectivité des hôtes et gère le trafic système standard de vSphere vMotion, du stockage IP, de Fault Tolerance et de vSAN, entre autres. Vous pouvez également créer des adaptateurs VMkernel sur les hôtes vSphere Replication source et cible dans le but d'isoler le trafic des données de réplication.

Piles TCP/IP au niveau de VMkernel

Pile TCP/IP par défaut

Prend en charge la mise en réseau pour le trafic de gestion entre vCenter Server et les hôtes ESXi ainsi que pour le trafic système (vMotion, stockage IP, Fault Tolerance, etc.).

Pile TCP/IP vMotion

Prend en charge le trafic de la migration en direct des machines virtuelles. Utilisez la pile TCP/IP vMotion pour une meilleure isolation du trafic vMotion. Dès que vous avez créé un adaptateur VMkernel sur la pile TCP/IP vMotion, vous ne pouvez utiliser que cette pile pour vMotion sur cet hôte. Les adaptateurs VMkernel de la pile TCP/IP par défaut sont désactivés pour le service vMotion. Si la pile TCP/IP par défaut est utilisée au cours d'une migration en direct alors que vous configurez des adaptateurs VMkernel avec la pile TCP/IP vMotion, la migration s'effectue correctement. Toutefois, les adaptateurs VMkernel de la pile TCP/IP par défaut sont désactivés pour les sessions vMotion à venir.

Pile TCP/IP de provisionnement

Prend en charge le trafic de migration de snapshots, de clonage ou de migration à froid des machines virtuelles. Vous pouvez utiliser la pile TCP/IP de provisionnement pour gérer le trafic NFC (Network File Copy) lors des processus vMotion longue distance. Le trafic NFC fournit un service de FTP spécifique au fichier pour vSphere. ESXi utilise le trafic NFC pour copier et déplacer des données entre les banque de données. Les adaptateurs VMkernel configurés avec la pile TCP/IP de provisionnement gèrent le trafic issu du clonage des disques virtuels de machines virtuelles migrées dans vMotion longue distance. L'utilisation de la pile TCP/IP de provisionnement permet d'isoler le trafic issu des opérations de clonage en le faisant traverser une passerelle séparée. Une fois que vous avez configuré un adaptateur VMkernel avec la pile TCP/IP de provisionnement, tous les adaptateurs sur la pile TCP/IP par défaut sont désactivés pour le trafic de provisionnement.

Piles TCP/IP personnalisées

Vous pouvez ajouter des piles TCP/IP personnalisées au niveau de VMkernel afin de gérer le trafic de mise en réseau des applications personnalisées.

Pile TCP/IP miroir

Vous pouvez créer une vmknic sur une pile TCP/IP miroir lorsque vous sélectionnez une pile miroir pour ERSPAN.

Sécurisation du trafic système

Afin de prévenir l'accès non autorisé au trafic de gestion et au trafic système dans votre environnement vSphere, prenez les mesures de sécurité appropriées. Vous devez, par exemple, isoler le trafic vMotion et le placer dans un réseau séparé qui inclut les hôtes ESXi participant à la migration uniquement. Vous devez également isoler le trafic de gestion et le placer dans un réseau auquel seuls les administrateurs réseau et sécurité peuvent accéder. Pour plus d'informations, reportez-vous à *Sécurité de vSphere* et *Installation et configuration de vSphere*.

Types de trafic système

Vous devez dédier un adaptateur VMkernel distinct pour chaque type de trafic. Pour les commutateurs distribués, dédiez un groupe de ports distribués distinct pour chaque adaptateur VMkernel.

Trafic de gestion

Ce type de trafic transporte les communications de configuration et de gestion des hôtes ESXi et de vCenter Server, ainsi que le trafic High Availability entre les hôtes. Par défaut, lorsque vous installez le logiciel ESXi, un commutateur vSphere standard est créé sur l'hôte en même temps que l'adaptateur VMkernel pour le trafic de gestion. Pour assurer la redondance, vous pouvez, pour le trafic de gestion, connecter deux cartes réseau (ou plus) à un adaptateur VMkernel.

Trafic vMotion

Ce type de trafic reçoit les données vMotion. Les hôtes source et cible requièrent un adaptateur VMkernel pour vMotion. Configurez les adaptateurs VMkernel pour vMotion afin qu'ils gèrent uniquement le trafic vMotion. Pour obtenir de meilleures performances, vous pouvez configurer vMotion de plusieurs cartes réseau. Pour ce faire, dédiez au moins deux groupes de ports au trafic vMotion (un adaptateur VMkernel vMotion doit être associé à chaque groupe de ports). Connectez ensuite au moins une carte réseau physique à chaque groupe de ports. Plusieurs cartes réseau physiques sont alors utilisées pour vMotion, offrant ainsi une plus grande bande passante.

Note Le trafic réseau vMotion n'est pas chiffré. Il est conseillé de fournir des réseaux privés sécurisés réservés à vMotion.

Trafic de provisionnement

Ce type de trafic gère les données transférées dans le cadre de la migration de snapshots, du clonage et de la migration à froid des machines virtuelles.

Découverte et trafic de stockage IP

Ce type de trafic gère la connexion des types de stockage qui utilisent des réseaux TCP/IP standard et dépendent de la mise en réseau VMkernel. Ces types de stockage incluent iSCSI logiciel, iSCSI matériel dépendant et NFS. Si vous disposez de plusieurs cartes réseau physiques pour iSCSI, vous pouvez configurer le multichemin iSCSI. Les hôtes ESXi prennent en charge NFS 3 et 4.1.

Trafic Fault Tolerance

Ce type de trafic gère les données que la machine virtuelle avec Fault Tolerance principale envoie à la machine virtuelle avec Fault Tolerance secondaire à travers la couche de mise en réseau VMkernel. Un adaptateur VMkernel distinct dédié à la journalisation de Fault Tolerance est requis sur tous les hôtes appartenant à un cluster vSphere HA.

Trafic de vSphere Replication

Ce type de trafic gère les données de réplication sortantes que l'hôte ESXi source transfère vers le serveur vSphere Replication. Dédiez un adaptateur VMkernel sur le site source afin d'isoler le trafic de réplication sortant.

Trafic NFC de vSphere Replication

Gère les données de réplication entrantes sur le site de réplication cible.

trafic vSAN

Tous les hôtes faisant partie d'un cluster vSAN doivent disposer d'un adaptateur VMkernel pour la gestion du trafic vSAN.

vSphere Backup NFC

Paramètre de port VMkernel pour le trafic NFC de sauvegarde dédié. Le trafic NFC passe par l'adaptateur VMkernel lorsque le service NFC vSphereBackup est activé.

NVMe over TCP

Paramètre de port VMkernel pour le trafic de stockage NVMe over TCP dédié. Le trafic de stockage NVMe over TCP passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over TCP est activé. Pour plus d'informations, consultez le *Guide de stockage vSphere*.

NVMe over RDMA

Paramètre de port VMkernel pour le trafic de stockage NVMe over RDMA dédié. Le trafic de stockage NVMe over RDMA passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over RDMA est activé. Pour plus d'informations, consultez le *Guide de stockage vSphere*.

Afficher les informations sur les adaptateurs VMkernel d'un hôte

Vous pouvez afficher, pour chaque adaptateur VMkernel, les services attribués, le commutateur associé, les paramètres de port, les paramètres IP, la pile TCP/IP, l'ID VLAN et les stratégies.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Cliquez sur l'onglet **Configurer** et développez le menu **Mise en réseau**.
- 3 Pour afficher les informations sur les adaptateurs VMkernel de l'hôte, sélectionnez **Adaptateurs VMkernel**.

- Sélectionnez un adaptateur dans la liste des adaptateurs VMkernel pour afficher les paramètres correspondants.

Onglet	Description
Toutes	Affiche toutes les informations de configuration concernant l'adaptateur VMkernel. Elles incluent notamment les paramètres de port et de carte réseau, les paramètres IPv4 et IPv6, la formation du trafic, l'association et le basculement ainsi que les stratégies de sécurité.
Propriétés	Affiche les propriétés de port et les paramètres de carte réseau de l'adaptateur VMkernel. Les propriétés de port incluent le groupe de ports (étiquette réseau) auquel l'adaptateur est associé, l'ID VLAN, ainsi que les services activés. Les paramètres de carte réseau incluent l'adresse MAC et la taille de MTU configurée.
Paramètres IP	Affiche tous les paramètres IPv4 et IPv6 pour l'adaptateur VMkernel. Les informations IPv6 ne s'affiche pas si IPv6 n'a pas été activé sur l'hôte.
Stratégies	Affiche les paramètres configurés pour la formation du trafic, l'association et le basculement ainsi que les stratégies de sécurité qui s'appliquent au groupe de ports auquel l'adaptateur VMkernel est connecté.

Créer un adaptateur VMkernel dans un commutateur vSphere standard

Créez un adaptateur réseau VMkernel sur un commutateur vSphere standard pour fournir la connectivité réseau aux hôtes et gérer le trafic système dans vSphere vMotion, le stockage IP, la journalisation de Fault Tolerance, vSAN, etc. Vous pouvez également créer des adaptateurs VMkernel sur les hôtes vSphere Replication source et cible dans le but d'isoler le trafic des données de réplication. Chaque adaptateur VMkernel ne doit être associé qu'à un seul de type de trafic.

Procédure

- Dans vSphere Client, accédez à l'hôte.
- Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- Cliquez sur **Ajouter une mise en réseau**.
- Dans la page Sélectionner un type de connexion, sélectionnez **Adaptateur réseau VMkernel** et cliquez sur **Suivant**.
- Dans la page Sélectionner un périphérique cible, choisissez un commutateur standard existant ou sélectionnez **Nouveau commutateur standard**.

- 6 (Facultatif) Dans la page Créer un commutateur standard, attribuez des cartes réseau physiques au commutateur.

Vous pouvez créer le commutateur standard sans les cartes réseau physiques et les configurer ultérieurement. Lorsque aucune carte réseau physique n'est attachée à l'hôte, ce dernier n'a pas de connectivité réseau avec les autres hôtes du réseau physique. Les machines virtuelles de l'hôte peuvent communiquer entre elles.

- a Cliquez sur **Ajouter des adaptateurs** et sélectionnez autant de cartes réseau physiques que nécessaire.
 - b Utilisez les flèches vers le haut et le bas pour configurer les cartes réseau actives et en veille.
- 7 Dans la page Propriétés du port, configurez les paramètres de l'adaptateur VMkernel.

Option	Description
Étiquette réseau	L'étiquette réseau est héritée de l'étiquette du groupe de ports distribués.
Paramètres IP	Sélectionnez IPv4, IPv6 ou les deux. Note L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.
MTU	Indiquez si vous souhaitez obtenir le MTU pour l'adaptateur réseau à partir du commutateur ou définir une taille personnalisée. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9 000 octets.

Option	Description
Pile TCP/IP	<p>Sélectionnez une pile TCP/IP dans la liste. Dès que vous configurez une pile TCP/IP pour l'adaptateur VMkernel, vous ne pouvez pas la modifier ultérieurement. Si vous sélectionnez vMotion ou la pile TCP/IP de provisionnement, vous ne pourrez utiliser que ces piles pour gérer le trafic vMotion ou de provisionnement sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés pour les prochaines sessions vMotion. Si vous configurez la pile TCP/IP de provisionnement, les adaptateurs VMkernel de la pile TCP/IP par défaut seront désactivés pour les opérations qui incluent du trafic de provisionnement, par exemple, la migration à froid, le clonage et la migration de snapshot de machine virtuelle.</p>
Services disponibles	<p>Vous pouvez activer des services pour la pile TCP/IP par défaut de l'hôte. Sélectionnez les services souhaités dans la liste des services disponibles :</p> <ul style="list-style-type: none"> ■ vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. La migration avec vMotion vers l'hôte sélectionné est impossible si le service vMotion n'est pas activé pour un adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion. ■ Provisionnement. Gère les données transférées pour la migration à froid, le clonage et la migration de snapshot de machine virtuelle. ■ Journalisation de la tolérance aux pannes. Active la journalisation de Fault Tolerance sur l'hôte. Vous ne pouvez utiliser qu'un seul adaptateur VMkernel pour le trafic FT par hôte. ■ Gestion. Active le trafic de gestion pour l'hôte et vCenter Server. En règle général, ce type d'adaptateur VMkernel est créé pour les hôtes lors de l'installation du logiciel ESXi. Vous pouvez créer un autre adaptateur VMkernel pour le trafic de gestion sur l'hôte afin d'assurer la redondance. ■ vSphere Replication. Gère les données de réplication sortantes envoyées depuis l'hôte ESXi source vers le serveur vSphere Replication. ■ NFC de vSphere Replication. Gère les données de réplication entrantes sur le site de réplication cible. ■ vSAN. Active le trafic vSAN sur l'hôte. Chaque hôte faisant partie d'un cluster de vSAN doit disposer de ce type d'adaptateur VMkernel. ■ vSphere Backup NFC. Paramètre de port VMkernel pour le trafic NFC de sauvegarde dédié. Le trafic NFC passe par l'adaptateur VMkernel lorsque le service NFC vSphereBackup est activé. ■ NVMe over TCP. Paramètre de port VMkernel pour le trafic de stockage NVMe over TCP dédié. Le trafic de stockage NVMe over TCP passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over TCP est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>. ■ NVMe over RDMA. Paramètre de port VMkernel pour le trafic de stockage NVMe over RDMA dédié. Le trafic de stockage NVMe over RDMA passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over RDMA est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>.

- 8 (Facultatif) Sur la page des paramètres IPv4, sélectionnez une option pour l'obtention des adresses IP.

Option	Description
Obtenir automatiquement les paramètres IPv4	Utilisez DHCP pour obtenir les paramètres IP. Un serveur DHCP doit être présent sur le réseau.
Utiliser des paramètres IPv4 statiques	Entrez l'adresse IP IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel. Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la tâche TCP/IP sélectionnée. Cochez la case Remplacer la passerelle par défaut pour l'adaptateur et entrez une adresse de passerelle, si vous souhaitez spécifier une passerelle différente pour l'adaptateur VMkernel.

- 9 (Facultatif) Sur la page Paramètres IPv6, sélectionnez une option pour l'obtention des adresses IPv6.

Option	Description
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6. Dans ESXi 6.5 et versions ultérieures, l'annonce du routeur est activée par défaut et prend en charge les indicateurs M et O, conformément à la norme RFC 4861.
Adresses IPv6 statiques	<ol style="list-style-type: none"> Cliquez sur Ajouter adresse IPv6 pour ajouter une nouvelle adresse IPv6. Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur OK. Pour modifier la passerelle par défaut de VMkernel, cliquez sur Remplacer la passerelle par défaut pour l'adaptateur. <p>L'adresse de passerelle par défaut de VMkernel pour IPv6 est obtenue à partir de la pile TCP/IP sélectionnée.</p>

- 10 Vérifiez vos sélections dans la page Prêt à terminer et cliquez sur **Terminer**.

Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch

Créez un adaptateur VMkernel sur un hôte associé à un Distributed Switch afin de fournir la connectivité réseau à l'hôte et de gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance et de vSAN, entre autres. Vous pouvez configurer des adaptateurs VMkernel pour le trafic système standard sur des commutateurs vSphere standard et sur des vSphere Distributed Switches.

Vous devez dédier un groupe de ports distribués pour chaque adaptateur VMkernel. Pour une meilleure isolation, configurez un type de trafic par adaptateur VMkernel.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- 3 Cliquez sur **Ajouter une mise en réseau**.
- 4 Dans la page Sélectionner un type de connexion, sélectionnez **Adaptateur réseau VMkernel** et cliquez sur **Suivant**.
- 5 Sélectionnez un groupe de ports distribués dans **Sélectionner un réseau existant** et cliquez sur **Suivant**.
- 6 Dans la page Propriétés du port, configurez les paramètres de l'adaptateur VMkernel.

Option	Description
Étiquette réseau	L'étiquette réseau est héritée de l'étiquette du groupe de ports distribués.
Paramètres IP	Sélectionnez IPv4, IPv6 ou les deux. Note L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.
MTU	Indiquez si vous souhaitez obtenir le MTU pour l'adaptateur réseau à partir du commutateur ou définir une taille personnalisée. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9 000 octets.

Option	Description
Pile TCP/IP	<p>Sélectionnez une pile TCP/IP dans la liste. Dès que vous configurez une pile TCP/IP pour l'adaptateur VMkernel, vous ne pouvez pas la modifier ultérieurement. Si vous sélectionnez vMotion ou la pile TCP/IP de provisionnement, vous ne pourrez utiliser que ces piles pour gérer le trafic vMotion ou de provisionnement sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés pour les prochaines sessions vMotion. Si vous configurez la pile TCP/IP de provisionnement, les adaptateurs VMkernel de la pile TCP/IP par défaut seront désactivés pour les opérations qui incluent du trafic de provisionnement, par exemple, la migration à froid, le clonage et la migration de snapshot de machine virtuelle.</p>
Services disponibles	<p>Vous pouvez activer des services pour la pile TCP/IP par défaut de l'hôte. Sélectionnez les services souhaités dans la liste des services disponibles :</p> <ul style="list-style-type: none"> ■ vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. La migration avec vMotion vers l'hôte sélectionné est impossible si le service vMotion n'est pas activé pour un adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion. ■ Provisionnement. Gère les données transférées pour la migration à froid, le clonage et la migration de snapshot de machine virtuelle. ■ Journalisation de la tolérance aux pannes. Active la journalisation de Fault Tolerance sur l'hôte. Vous ne pouvez utiliser qu'un seul adaptateur VMkernel pour le trafic FT par hôte. ■ Gestion. Active le trafic de gestion pour l'hôte et vCenter Server. En règle général, ce type d'adaptateur VMkernel est créé pour les hôtes lors de l'installation du logiciel ESXi. Vous pouvez créer un autre adaptateur VMkernel pour le trafic de gestion sur l'hôte afin d'assurer la redondance. ■ vSphere Replication. Gère les données de réplication sortantes envoyées depuis l'hôte ESXi source vers le serveur vSphere Replication. ■ NFC de vSphere Replication. Gère les données de réplication entrantes sur le site de réplication cible. ■ vSAN. Active le trafic vSAN sur l'hôte. Chaque hôte faisant partie d'un cluster de vSAN doit disposer de ce type d'adaptateur VMkernel. ■ vSphere Backup NFC. Paramètre de port VMkernel pour le trafic NFC de sauvegarde dédié. Le trafic NFC passe par l'adaptateur VMkernel lorsque le service NFC vSphereBackup est activé. ■ NVMe over TCP. Paramètre de port VMkernel pour le trafic de stockage NVMe over TCP dédié. Le trafic de stockage NVMe over TCP passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over TCP est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>. ■ NVMe over RDMA. Paramètre de port VMkernel pour le trafic de stockage NVMe over RDMA dédié. Le trafic de stockage NVMe over RDMA passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over RDMA est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>.

- 7 (Facultatif) Sur la page des paramètres IPv4, sélectionnez une option pour l'obtention des adresses IP.

Option	Description
Obtenir automatiquement les paramètres IPv4	Utilisez DHCP pour obtenir les paramètres IP. Un serveur DHCP doit être présent sur le réseau.
Utiliser des paramètres IPv4 statiques	Entrez l'adresse IP IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel. Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la tâche TCP/IP sélectionnée. Cochez la case Remplacer la passerelle par défaut pour l'adaptateur et entrez une adresse de passerelle, si vous souhaitez spécifier une passerelle différente pour l'adaptateur VMkernel.

- 8 (Facultatif) Sur la page Paramètres IPv6, sélectionnez une option pour l'obtention des adresses IPv6.

Option	Description
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6. Dans ESXi 6.5 et versions ultérieures, l'annonce du routeur est activée par défaut et prend en charge les indicateurs M et O, conformément à la norme RFC 4861.
Adresses IPv6 statiques	<ul style="list-style-type: none"> a Cliquez sur Ajouter adresse IPv6 pour ajouter une nouvelle adresse IPv6. b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur OK. c Pour modifier la passerelle par défaut de VMkernel, cliquez sur Remplacer la passerelle par défaut pour l'adaptateur. L'adresse de passerelle par défaut de VMkernel pour IPv6 est obtenue à partir de la pile TCP/IP sélectionnée.

- 9 Vérifiez vos sélections dans la page Prêt à terminer et cliquez sur **Terminer**.

Modifier la configuration d'un adaptateur VMkernel

Vous pouvez être amené à modifier le type de trafic pris en charge pour un adaptateur VMkernel ou le mode d'obtention des adresses IPv4 ou IPv6.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- 3 Sélectionnez l'adaptateur VMkernel se trouvant sur le commutateur standard ou distribué cible, puis cliquez sur **Modifier**.

4 Dans la page Propriétés du port, modifiez les paramètres de l'adaptateur VMkernel.

Option	Description
MTU	Indiquez si vous souhaitez obtenir le MTU pour l'adaptateur réseau à partir du commutateur ou définir une taille personnalisée. La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9 000 octets.
Pile TCP/IP	Sélectionnez une pile TCP/IP dans la liste. Dès que vous configurez une pile TCP/IP pour l'adaptateur VMkernel, vous ne pouvez pas la modifier ultérieurement. Si vous sélectionnez vMotion ou la pile TCP/IP de provisionnement, vous ne pourrez utiliser que ces piles pour gérer le trafic vMotion ou de provisionnement sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés pour de futures sessions vMotion. Si vous configurez la pile TCP/IP de provisionnement, les adaptateurs VMkernel de la pile TCP/IP par défaut seront désactivés pour les opérations qui incluent du trafic de provisionnement, par exemple, la migration à froid, le clonage et la migration de snapshot de machine virtuelle.
Services disponibles	<p>Vous pouvez activer des services pour la pile TCP/IP par défaut de l'hôte. Sélectionnez les services souhaités dans la liste des services disponibles :</p> <ul style="list-style-type: none"> ■ vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. La migration avec vMotion vers l'hôte sélectionné est impossible si le service vMotion n'est pas activé pour un adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion. ■ Provisionnement. Gère les données transférées pour la migration à froid, le clonage et la migration de snapshot de machine virtuelle. ■ Journalisation de la tolérance aux pannes. Active la journalisation de Fault Tolerance sur l'hôte. Vous ne pouvez utiliser qu'un seul adaptateur VMkernel pour le trafic FT par hôte. ■ Gestion. Active le trafic de gestion pour l'hôte et vCenter Server. En règle général, ce type d'adaptateur VMkernel est créé pour les hôtes lors de l'installation du logiciel ESXi. Vous pouvez créer un autre adaptateur VMkernel pour le trafic de gestion sur l'hôte afin d'assurer la redondance. ■ vSphere Replication. Gère les données de réplication sortantes envoyées depuis l'hôte ESXi source vers le serveur vSphere Replication. ■ NFC de vSphere Replication. Gère les données de réplication entrantes sur le site de réplication cible. ■ vSAN. Active le trafic vSAN sur l'hôte. Chaque hôte faisant partie d'un cluster de vSAN doit disposer de ce type d'adaptateur VMkernel. ■ vSphere Backup NFC. Paramètre de port VMkernel pour le trafic NFC de sauvegarde dédié. Le trafic NFC passe par l'adaptateur VMkernel lorsque le service NFC vSphereBackup est activé. ■ NVMe over TCP. Paramètre de port VMkernel pour le trafic de stockage NVMe over TCP dédié. Le trafic de stockage NVMe over TCP passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over TCP est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>. ■ NVMe over RDMA. Paramètre de port VMkernel pour le trafic de stockage NVMe over RDMA dédié. Le trafic de stockage NVMe over RDMA passe par l'adaptateur VMkernel lorsque l'adaptateur NVMe over RDMA est activé. Pour plus d'informations, consultez le <i>Guide de stockage vSphere</i>.

- 5 (Facultatif) Sur la page Paramètres IPv4, sélectionnez la méthode par laquelle les adresses IP sont obtenues.

Option	Description
Obtenir automatiquement les paramètres IPv4	Utilisez DHCP pour obtenir les paramètres IP. Un serveur DHCP doit être présent sur le réseau.
Utiliser des paramètres IPv4 statiques	Entrez l'adresse IP IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel. Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la tâche TCP/IP sélectionnée. Cochez la case Remplacer la passerelle par défaut pour l'adaptateur et entrez une adresse de passerelle, si vous souhaitez spécifier une passerelle différente pour l'adaptateur VMkernel.

- 6 (Facultatif) Sur la page Paramètres IPv6, sélectionnez une option pour l'obtention des adresses IPv6.

Note L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.

Option	Description
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6. Dans ESXi 6.5 et versions ultérieures, l'annonce du routeur est activée par défaut et prend en charge les indicateurs M et O, conformément à la norme RFC 4861.
Adresses IPv6 statiques	<ul style="list-style-type: none"> a Cliquez sur Ajouter adresse IPv6 pour ajouter une nouvelle adresse IPv6. b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur OK. c Pour modifier la passerelle par défaut de VMkernel, cliquez sur Remplacer la passerelle par défaut pour l'adaptateur. <p>L'adresse de passerelle par défaut de VMkernel pour IPv6 est obtenue à partir de la pile TCP/IP sélectionnée.</p>

- 7 Cliquez sur **OK**.

Remplacer la passerelle par défaut d'un adaptateur VMkernel

Vous devrez peut-être remplacer la passerelle par défaut d'un adaptateur VMkernel par une autre passerelle de vSphere vMotion.

Toute pile TCP/IP d'un hôte donné ne peut avoir qu'une seule passerelle par défaut. Cette passerelle par défaut fait partie de la table de routage et tous les services qui s'exécutent sur la pile TCP/IP l'utilisent.

Par exemple, les adaptateurs VMkernel vmk0 et vmk1 peuvent être configurés sur un hôte.

- vmk0 sert au trafic de gestion sur le sous-réseau 10.162.10.0/24, avec la passerelle par défaut 10.162.10.1
- vmk1 est utilisé pour le trafic vMotion sur le sous-réseau 172.16.1.0/24

Si vous définissez 172.16.1.1 en tant que passerelle par défaut pour vmk1, vMotion utilise vmk1 comme interface de sortie avec la passerelle 172.16.1.1. La passerelle 172.16.1.1 fait partie de la configuration vmk1 et n'est pas incluse dans la table de routage. Seuls les services qui spécifient vmk1 en tant qu'interface de sortie utilisent cette passerelle. Ce processus offre des options supplémentaires de connectivité de couche 3 pour les services nécessitant plusieurs passerelles.

Vous pouvez utiliser vSphere Client ou une commande ESXCLI pour configurer la passerelle par défaut d'un adaptateur VMkernel.

Reportez-vous à [Créer un adaptateur VMkernel dans un commutateur vSphere standard](#), [Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch](#), et [Configurer la passerelle de l'adaptateur VMkernel avec les commandes esxcli](#).

Configurer la passerelle de l'adaptateur VMkernel avec les commandes esxcli

Vous pouvez remplacer la passerelle par défaut d'un adaptateur VMkernel afin de fournir une passerelle différente pour vSphere vMotion avec les commandes esxcli.

Procédure

- 1 Ouvrez une connexion SSH à l'hôte.
- 2 Connectez-vous en tant qu'utilisateur racine.

3 Exécutez la commande suivante.

Option	Description
IPv4	<pre>esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4 gateway -I IPv4 address -N mask</pre>
IPv6	<p>Important Vous devez désactiver DHCPv6 ou l'annonce du routeur avant de définir la passerelle vmknic IPv6.</p> <pre>esxcli network ip interface ipv6 set -i vmknic -d off -r off</pre> <p>Pour ajouter une adresse IPv6 statique :</p> <pre>esxcli network ip interface ipv6 address add -i vmknic -I IPv6 address</pre> <p>Pour définir la passerelle vmknic IPv6 :</p> <pre>esxcli network ip interface ipv6 set -i vmknic -g IPv6 gateway</pre>

Où *vmknic* est le nom de l'adaptateur VMkernel, *gateway* l'adresse IP de la passerelle, *IP address* l'adresse de l'adaptateur VMkernel et *mask* le masque de réseau.

Configurer le fichier `resolv.conf` à l'aide de commandes `esxcli`

Le fichier `resolv.conf` est utilisé pour configurer des serveurs DNS gérés de manière centralisée. Vous pouvez configurer des entrées dans le fichier `/etc/resolv.conf` à l'aide de commandes `esxcli`, ce qui permet de conserver la modification lors du redémarrage de l'hôte ESXi. La propriété peut être définie explicitement si DHCP n'est pas activé.

Procédure

- 1 Ouvrez une connexion SSH à l'hôte.
- 2 Connectez-vous en tant qu'utilisateur racine.

3 Exécutez la commande suivante.

Option	Description
<p>Ajouter un serveur DNS</p>	<p>Pour ajouter un nouveau serveur DNS à la fin de la liste des serveurs DNS à utiliser pour cet hôte ESXi.</p> <pre data-bbox="625 352 1423 411">esxcli network ip dns server add</pre> <p>Options de commande</p> <pre data-bbox="625 466 1423 525">-N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p> <pre data-bbox="625 609 1423 667">-s --server=<str></pre> <p>Adresse IPV4 ou IPV6 du serveur DNS que vous souhaitez ajouter à la liste de serveurs DNS.</p> <hr/> <p>Note Cette commande est obligatoire.</p> <pre data-bbox="625 819 1423 894">For example: esxcli network ip dns server add -N vmotion -s xx.xx.xx.xx</pre>
<p>Ajouter une recherche DNS</p>	<p>Pour ajouter un domaine de recherche à la liste des domaines à rechercher lors de la tentative de résolution d'un nom d'hôte sur l'hôte ESXi.</p> <pre data-bbox="625 991 1423 1041">esxcli network ip dns search add</pre> <p>Options de commande</p> <pre data-bbox="625 1096 1423 1155">-d --domain=<str></pre> <p>Nom de chaîne d'un domaine que vous souhaitez ajouter à la liste des domaines de recherche.</p> <hr/> <p>Note Cette commande est obligatoire.</p> <pre data-bbox="625 1306 1423 1356">-N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p>
<p>Supprimer le serveur DNS</p>	<p>Pour supprimer un serveur DNS de la liste des serveurs DNS à utiliser pour cet hôte ESXi.</p> <pre data-bbox="625 1524 1423 1575">esxcli network ip dns server remove IP address</pre> <p>Options de commande</p> <pre data-bbox="625 1629 1423 1680">-a --all</pre> <pre data-bbox="625 1705 1423 1755">-N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p> <pre data-bbox="625 1848 1423 1898">-s --server=<str></pre>

Option	Description
<p>Supprimer la recherche DNS</p>	<p>Pour supprimer un domaine de recherche de la liste des domaines à rechercher lors de la tentative de résolution d'un nom d'hôte sur l'hôte ESXi.</p> <pre data-bbox="625 289 1423 342">esxcli network ip dns search remove</pre> <p>Options de commande</p> <pre data-bbox="625 401 1423 453">-d --domain=<str></pre> <p>Nom de chaîne d'un domaine que vous souhaitez supprimer de la liste des domaines de recherche.</p> <hr/> <p>Note Cette commande est obligatoire.</p> <pre data-bbox="625 604 1423 657">-N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p>
<p>Liste de recherche DNS</p>	<p>Pour imprimer la liste des serveurs DNS actuellement configurés sur le système dans l'ordre dans lequel ils seront utilisés.</p> <pre data-bbox="625 821 1423 873">esxcli network ip dns server list</pre> <p>Options de commande</p> <pre data-bbox="625 932 1423 984">-N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p> <pre data-bbox="625 1073 1423 1125">For example: esxcli network ip dns server list -N vmotion</pre>
<p>Répertorier le domaine de recherche DNS</p>	<p>Pour répertorier les domaines de recherche actuellement configurés sur l'hôte ESXi dans l'ordre dans lequel ils seront utilisés lors de la recherche.</p> <pre data-bbox="625 1220 1423 1272">esxcli network ip dns search list -N</pre> <p>Options de commande</p> <pre data-bbox="625 1331 1423 1383">---N --netstack=<str></pre> <p>Instance de pile réseau. Si elle n'est pas spécifiée, utilisez l'instance de netstack par défaut.</p> <pre data-bbox="625 1472 1423 1524">For example: esxcli network ip dns search list -N vmotion</pre>

Configurer le fichier d'hôtes DNS à l'aide des commandes ESXCLI

Le fichier hosts est utilisé pour mapper des noms d'hôte ou des noms de domaine à des adresses IP. Vous pouvez configurer des entrées du fichier `/etc/hosts` à l'aide de commandes `esxcli`, ce qui permet de conserver la modification lors du redémarrage de l'hôte ESXi.

Procédure

- 1 Ouvrez une connexion SSH à l'hôte.
- 2 Connectez-vous en tant qu'utilisateur racine.
- 3 Exécutez la commande suivante.

Option	Description
ajouter	<p>Pour ajouter le mappage de nom d'hôte et d'adresse IP, exécutez la commande suivante.</p> <pre>esxcli network ip hosts add --ip</pre>
supprimer	<p>Pour supprimer un mappage de nom d'hôte de la configuration, exécutez la commande suivante.</p> <pre>esxcli network ip hosts remove --hostname</pre> <p>For example: <code>esxcli network ip hosts remove --hostname www.samplehostname.com --ip xx.xx.xx.xx</code></p>
liste	<p>Pour répertorier les adresses IP et leurs entrées DNS associées, exécutez la commande suivante.</p> <pre>esxcli network ip hosts list</pre>

Où *IP address* est l'adresse IP de l'adaptateur VMkernel, *hostname* est l'entrée DNS que vous souhaitez associer à l'adresse IP, *aliases* correspond à toutes les personnes que vous souhaitez associer et *comment* est une ligne sur cette entrée.

Afficher la configuration de la pile TCP/IP sur un hôte

Vous pouvez également afficher le DNS et la configuration de routage de la pile TCP/IP d'un hôte, de même que les tables de routage IPv4 et IPv6, l'algorithme de contrôle d'encombrement et le nombre maximal de connexions autorisées.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Mise en réseau** et sélectionnez **Configuration TCP/IP**.
- 3 Sélectionnez une pile dans la table de piles TCP/IP.

Si aucune pile TCP/IP personnalisée n'est configurée sur l'hôte, ce sont les piles TCP/IP de provisionnement, vMotion et par défaut de l'hôte qui s'affichent.

Résultats

Les informations concernant le DNS et le routage de la pile TCP/IP sélectionnée s'affichent sous la table de piles TCP/IP. Les tables de routage IPv4 et IPv6, ainsi que la configuration DNS et de routage de la pile, s'affichent également.

Note La table de routage IPv6 s'affiche uniquement si le protocole IPv6 est activé sur l'hôte.

L'onglet **Avancé** regroupe les informations relatives à l'algorithme de contrôle d'encombrement configuré et au nombre maximal de connexions autorisées pour la pile.

Modifier la configuration de la pile TCP/IP d'un hôte

Vous pouvez modifier le DNS et la configuration de passerelle par défaut de la pile TCP/IP d'un hôte, de même que l'algorithme de contrôle d'encombrement, le nombre maximal de connexions autorisées et le nom des piles TCP/IP personnalisées.

Note Vous pouvez modifier la configuration de passerelle DNS et par défaut de la pile TCP/IP par défaut uniquement. Plusieurs configurations de DNS et de passerelles sont prises en charge lors de l'utilisation de piles TCP/IP séparées.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Mise en réseau** et sélectionnez **Configuration TCP/IP**.
- 3 Sélectionnez une pile dans la table, cliquez sur **Modifier**, puis apportez les modifications appropriées.

Page	Option
Configuration DNS	<p>Sélectionnez une méthode pour obtenir les données du serveur DNS.</p> <ul style="list-style-type: none"> ■ Sélectionnez Obtenir les paramètres automatiquement à partir d'un adaptateur réseau VMkernel, puis choisissez un adaptateur réseau dans le menu déroulant Adaptateur réseau VMKernel. ■ Sélectionnez Saisissez les paramètres manuellement, puis modifiez les paramètres de configuration DNS. <ol style="list-style-type: none"> a Modifiez le nom de l'hôte. b Modifier le nom du domaine. c Entrez l'adresse IP du serveur DNS privilégié. d Entrez l'adresse IP d'un autre serveur DNS. e (Facultatif) Dans la zone de texte Recherches les domaines, indiquez les suffixes DNS à utiliser lors de la recherche de DNS pour résoudre les noms de domaine non qualifiés.
Routage	<p>Modifiez les informations de passerelle VMkernel.</p> <p>Note La suppression de la passerelle par défaut peut provoquer la perte de connectivité du client avec l'hôte.</p>

Page	Option
Nom	Modifiez le nom d'une pile TCP/IP personnalisée.
Avancé	Modifiez le nombre maximal de connexions et l'algorithme de contrôle d'encombrement de la pile.

4 Cliquez sur **OK** pour appliquer vos modifications.

Étape suivante

Vous pouvez ajouter des routes statiques à des passerelles supplémentaires à l'aide de commandes d'interface de ligne de commande. Pour plus d'informations, reportez-vous à l'article <http://kb.vmware.com/kb/2001426>

Notification explicite de congestion

La notification explicite de congestion (ECN, Explicit Congestion Notification) permet à un expéditeur TCP de réduire le taux de transmission afin d'éviter les abandons de paquets. La fonctionnalité ECN est spécifiée dans RFC 3168. vSphere 7.0 et versions ultérieures prend en charge la fonctionnalité ECN qui est activée par défaut.

Vous pouvez obtenir l'état ECN de n'importe quelle pile réseau à l'aide de la commande `esxcli`.

Procédure

1 Dans le shell ESXi, sur l'hôte, utilisez la commande suivante.

```
esxcli network ip netstack set -N <NetStack-Name> --ecn=<str>
```

2 Vous pouvez définir l'état ECN. Le paramètre comporte les valeurs possibles suivantes dans ESXi.

```
... --ecn=<str> État ECN. disabled : fonctionnalité ECN complètement désactivée echo-only : écho d'ECN, la fonctionnalité n'est pas lancée. enabled : fonctionnalité ECN entièrement activée
```

La valeur par défaut de ce paramètre est `enabled`. ESXi est susceptible d'utiliser ECN si la valeur de ce paramètre est `enabled`. Si un routeur ou un dispositif réseau dans l'environnement ne peut pas gérer avec précision les paquets IP avec des bits ECN, la fonctionnalité ECN peut être définie sur `disabled`.

Créer une pile TCP/IP personnalisée

Vous pouvez créer une pile TCP/IP personnalisée sur un hôte pour transférer le trafic de mise en réseau via une application personnalisée.

Dès que vous configurez une pile TCP/IP pour l'adaptateur VMkernel, vous ne pouvez pas la modifier ultérieurement. Si vous sélectionnez la pile TCP/IP de provisionnement ou vMotion, seules ces piles pourront être utilisées pour gérer le trafic de provisionnement ou vMotion sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés

pour de futures sessions vMotion. Si vous configurez la pile TCP/IP de provisionnement, les adaptateurs VMkernel de la pile TCP/IP par défaut seront désactivés pour les opérations qui incluent du trafic de provisionnement, par exemple, la migration à froid, le clonage et la migration de snapshot de machine virtuelle.

Si vous devez modifier la configuration de la pile TCP/IP, supprimez l'adaptateur VMkernel existant et créez-en un nouveau. Vous pouvez ensuite créer une pile TCP/IP pour cet adaptateur.

Procédure

- 1 Ouvrez une connexion SSH à l'hôte.
- 2 Connectez-vous en tant qu'utilisateur racine.
- 3 Exécutez la commande ESXCLI.

```
esxcli network ip netstack add -N="stack_name"
```

Résultats

La pile TCP/IP personnalisée est créée sur l'hôte. Vous pouvez affecter des adaptateurs VMkernel à la pile.

Supprimer un adaptateur VMkernel

Lorsque vous n'utilisez plus un adaptateur VMkernel, vous pouvez le supprimer d'un commutateur vSphere standard ou distribué. Veuillez à conserver au moins un adaptateur VMkernel dédié au trafic de gestion sur l'hôte afin de maintenir la connectivité réseau.

Procédure

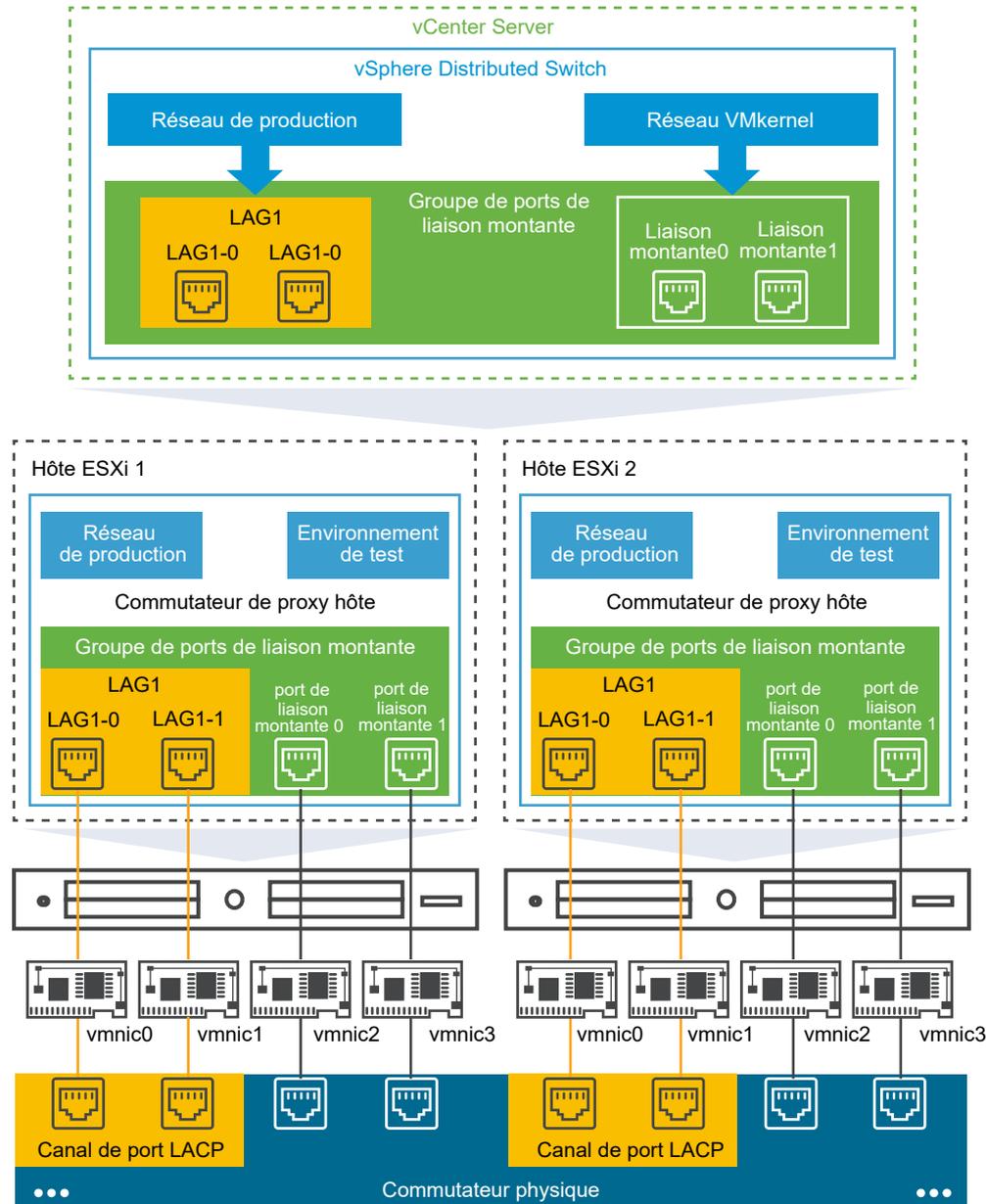
- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- 3 Sélectionnez un adaptateur VMkernel dans la liste et cliquez sur l'icône **Supprimer l'adaptateur réseau sélectionné**.
- 4 Cliquez sur **Supprimer**.

Prise en charge de LACP sur vSphere Distributed Switch

5

Grâce à la prise en charge du protocole LACP (Link Aggregation Control Protocol) sur un vSphere Distributed Switch, vous pouvez connecter des hôtes ESXi à des commutateurs physiques à l'aide de l'agrégation de liens dynamique. Vous pouvez créer plusieurs groupes d'agrégation de liens (LAG) sur un commutateur distribué pour agréger la bande passante de cartes réseau physiques sur des hôtes ESXi connectés aux canaux de port LACP.

Figure 5-1. Prise en charge étendue du protocole LACP sur un vSphere Distributed Switch



Configuration de LACP sur le Distributed Switch

Vous configurez un LAG avec au moins deux ports et connectez des cartes réseau physiques à ces ports. Les ports LAG sont associés au sein du LAG et la charge du trafic réseau est équilibrée entre les ports via un algorithme de hachage LACP. Vous pouvez utiliser un LAG pour gérer le trafic de groupes de ports distribués pour que ces derniers bénéficient d'une optimisation de la bande passante réseau, de la redondance et de l'équilibrage de charge.

Lorsque vous créez un LAG sur un commutateur distribué, un objet LAG est également créé sur le commutateur proxy de chaque hôte connecté au commutateur distribué. Par exemple, si vous créez un LAG1 avec deux ports, un LAG1 avec le même nombre de ports est créé sur chaque hôte connecté au commutateur distribué.

Sur un commutateur proxy hôte, vous ne pouvez connecter une carte réseau physique qu'à un seul port LAG. Sur le commutateur distribué, un port LAG peut avoir plusieurs cartes réseau physiques de différents hôtes qui lui sont connectés. Les cartes réseau physiques d'un hôte que vous connectez aux ports LAG doivent être connectées aux liens participant à un canal de port LACP sur le commutateur physique.

Vous pouvez créer jusqu'à 64 LAG sur un commutateur distribué. Un hôte peut prendre en charge un maximum de 32 LAG. Cependant, le nombre de LAG que vous pouvez réellement utiliser dépend des capacités de l'environnement physique sous-jacent et de la topologie du réseau virtuel. Par exemple, si le commutateur physique prend en charge un maximum de quatre ports dans un canal de port LACP, vous pouvez connecter à un LAG jusqu'à quatre cartes réseau physiques par hôte.

Vous pouvez configurer la valeur du délai d'expiration LACP. Le protocole LACP fonctionne en envoyant des trames à tous les liens sur lesquels le protocole est activé. S'il trouve un périphérique à l'autre extrémité du lien sur lequel LACP est également activé, il envoie des trames indépendamment sur les mêmes liens, ce qui permet aux deux unités de détecter plusieurs liens entre eux, puis de les combiner en un seul lien logique. La valeur du délai d'expiration est la durée pendant laquelle une interface LAG attend une unité de données de protocole (PDU) du système distant avant de mettre la session LACP hors service. Les transmissions périodiques des PDU LACP se produisent à un taux de transmission lent ou rapide.

Configuration du canal de port sur le commutateur physique

Pour chaque hôte sur lequel vous souhaitez utiliser LACP, vous devez créer un canal de port LACP distinct sur le commutateur physique. Vous devez tenir compte des conditions suivantes lorsque vous configurez LACP sur le commutateur physique :

- Le nombre de ports sur le canal de port LACP doit être égal au nombre de cartes réseau physiques que vous souhaitez regrouper sur l'hôte. Par exemple, si vous souhaitez agréger la bande passante de deux cartes réseau physiques sur un hôte, vous devez créer un canal de port LACP avec deux ports sur le commutateur physique. Le LAG sur le commutateur distribué doit être configuré avec au moins deux ports.
- L'algorithme de hachage du canal de port LACP sur le commutateur physique doit être le même que l'algorithme de hachage configuré sur le LAG du commutateur distribué.
- Toutes les cartes réseau physiques que vous souhaitez connecter au canal de port LACP doivent être configurées avec la même vitesse et le même duplex.

Ce chapitre contient les rubriques suivantes :

- [Configurer l'association et le basculement LACP pour les groupes de ports distribués](#)

- Configurer un groupe d'agrégation de liens afin de gérer le trafic pour des groupes de ports distribués
- Modifier un groupe d'agrégation de liens
- Limitations de la prise en charge de LACP sur un vSphere Distributed Switch

Configurer l'association et le basculement LACP pour les groupes de ports distribués

Pour gérer le trafic réseau des groupes de ports distribués à l'aide d'un LAG, vous devez affecter des cartes réseau physiques aux ports LAG et définir le LAG en mode actif dans l'association et l'ordre de basculement des groupes de ports distribués.

Tableau 5-1. Configuration de l'association et du basculement LACP pour des groupes de ports distribués

ordre de basculement	Liaisons montantes	Description
Active	LAG unique	Vous ne pouvez utiliser qu'un seul LAG actif ou plusieurs liaisons montantes autonomes pour gérer le trafic des groupes de ports distribués . Vous ne pouvez pas configurer plusieurs LAG actifs ou combiner des LAG actifs et des liaisons montantes autonomes.
En attente	Vide	La combinaison d'un LAG actif et de liaisons montantes en attente (ou inversement) n'est pas prise en charge. La combinaison d'un LAG et d'un autre LAG en attente n'est pas prise en charge.
Inutilisé	Toutes les liaisons montantes autonomes et d'autres LAG (le cas échéant)	Étant donné qu'un seul LAG doit être actif et que la liste des éléments en attente doit être vide, vous devez définir toutes les liaisons montantes autonomes et les autres LAG comme étant inutilisés.

Configurer un groupe d'agrégation de liens afin de gérer le trafic pour des groupes de ports distribués

Pour agréger la bande passante de plusieurs cartes réseau physiques sur les hôtes, vous pouvez créer un groupe d'agrégation de liens (LAG) sur le Distributed Switch et l'utiliser pour gérer le trafic des groupes de ports distribués.

Les LAG récemment créés ne disposent pas de carte réseau physique attribuée à leurs ports et ne sont pas utilisés pour l'association et l'ordre de basculement des groupes de ports distribués. Pour gérer le trafic réseau des groupes de ports distribués avec un LAG, vous devez migrer le trafic des liaisons montantes autonomes vers le LAG.

Conditions préalables

- Pour chacun des hôtes sur lesquels vous souhaitez utiliser LACP, vérifiez qu'un canal de port LACP séparé existe sur le commutateur physique. Reportez-vous à la section [Chapitre 5 Prise en charge de LACP sur vSphere Distributed Switch](#).
- Vérifiez que la version du vSphere Distributed Switch sur lequel vous configurez le LAG est 6.5 ou version ultérieure.
- Vérifiez que le commutateur distribué intègre la prise en charge étendue du protocole LACP.

Procédure

1 Créer un groupe d'agrégation de liens

Pour migrer le trafic réseau de plusieurs groupes de ports distribués vers un groupe d'agrégation de liens (LAG), vous devez créer un LAG sur le commutateur distribué.

2 Définir un groupe d'agrégation de liens sur En veille dans l'association et l'ordre de basculement des groupe de ports distribués

Le nouveau groupe d'agrégation de liens (LAG) par défaut n'est pas utilisé pour l'association et l'ordre de basculement des groupes de ports distribués. Étant donné que seul un LAG ou des liaisons montantes autonomes peuvent être actifs pour des groupes de ports distribués, vous devez créer une configuration d'association et de basculement intermédiaire dans laquelle le LAG est en veille. Cette configuration vous permet de migrer des cartes réseau physiques vers les ports LAG en maintenant la connectivité réseau.

3 Attribuer des cartes réseau physiques aux ports du groupe d'agrégation de liens

Vous avez défini le nouveau groupe d'agrégation de liens (LAG) en attente dans l'association et l'ordre de basculement des groupes de ports distribués. Lorsque le LAG est en attente, vous pouvez migrer en toute sécurité les cartes réseau physiques depuis des liaisons montantes autonomes vers des ports LAG sans perte de connectivité réseau.

4 Définir Groupe d'agrégation de liens sur Actif dans l'association et l'ordre de basculement du groupe de ports distribués

Vous avez migré des cartes réseau physiques vers les ports du groupe d'agrégation de liens (LAG). Définissez le LAG en mode Actif et mettez toutes les liaisons montantes autonomes en mode Inutilisé dans l'ordre d'association et de basculement des groupes de ports distribués.

Créer un groupe d'agrégation de liens

Pour migrer le trafic réseau de plusieurs groupes de ports distribués vers un groupe d'agrégation de liens (LAG), vous devez créer un LAG sur le commutateur distribué.

Procédure

- 1 Dans vSphere Client, accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **LACP**.
- 3 Cliquez sur l'icône **Nouveau groupe d'agrégation de liens**.

- 4 Nommez le nouveau LAG.
- 5 Définissez le nombre de ports sur le LAG.

Définissez le même nombre de ports sur le LAG que le nombre de ports du canal de port LACP sur le commutateur physique. Un port LAG joue le même rôle qu'une liaison montante sur le commutateur distribué. Tous les ports LAG forment une association de cartes réseau dans le contexte du LAG.

- 6 Sélectionnez le mode négociation LACP du LAG.

Option	Description
Active	Tous les ports LAG sont en mode de négociation active. Les ports LAG lancent les négociations avec le canal de port LACP sur le commutateur physique en envoyant des paquets LACP.
Passif	Les ports LAG sont en mode de négociation passive. Les ports LAG répondent aux paquets LACP qu'ils reçoivent, mais ne lancent pas de négociation LACP.

Sur le commutateur physique, si les ports sur lesquels LACP est activé sont en mode de négociation active, vous pouvez définir les ports LAG en mode de négociation passive, et inversement.

- 7 Sélectionnez un mode d'équilibrage de charge dans les algorithmes de hachage définis par LACP.

Note L'algorithme de hachage doit être identique à celui qui a été défini pour le canal du port LACP du commutateur physique.

- 8 Sélectionnez le mode de délai d'expiration de l'agrégation de liens.

Les transmissions périodiques des PDU LACP se produisent à un taux de transmission lent ou rapide, selon les préférences de délai d'expiration LACP que vous sélectionnez. Dans un délai d'expiration rapide, les PDU sont envoyées toutes les secondes et, dans un délai d'expiration lent, les PDU sont envoyées toutes les 30 secondes. Un délai d'expiration lent est le paramètre par défaut.

Note Un délai d'expiration rapide est pris en charge uniquement sur la version 7.0.2 ou version ultérieure d'un Distributed Switch.

- 9 Définissez les stratégies de VLAN et NetFlow du LAG.

Cette option est active lorsque le remplacement des stratégies de VLAN et NetFlow sur chaque port de liaison montante est activé sur le groupe de ports de liaison montante. Si vous définissez les stratégies de VLAN et NetFlow sur le LAG, celles-ci remplacent les stratégies définies au niveau du groupe de ports de liaison montante.

- 10 Cliquez sur **OK**.

Résultats

Le nouveau LAG n'est pas utilisé pour l'association et l'ordre de basculement des groupes de ports distribués. Aucune carte de réseau physique n'est attribuée aux ports LAG.

Tout comme pour les liaisons montantes autonomes, le LAG est représenté sur tous les hôtes associés au commutateur distribué. Par exemple, si vous créez un LAG1 avec deux ports sur le commutateur distribué, un LAG1 avec deux ports est créé sur chaque hôte associé au commutateur distribué.

Étape suivante

Définissez le LAG en mode veille pour l'association et l'ordre de basculement des groupes de ports distribués. De cette manière, vous créez une configuration intermédiaire qui vous permet de migrer le trafic réseau vers le LAG sans subir de perte de connectivité réseau.

Définir un groupe d'agrégation de liens sur En veille dans l'association et l'ordre de basculement des groupe de ports distribués

Le nouveau groupe d'agrégation de liens (LAG) par défaut n'est pas utilisé pour l'association et l'ordre de basculement des groupes de ports distribués. Étant donné que seul un LAG ou des liaisons montantes autonomes peuvent être actifs pour des groupes de ports distribués, vous devez créer une configuration d'association et de basculement intermédiaire dans laquelle le LAG est en veille. Cette configuration vous permet de migrer des cartes réseau physiques vers les ports LAG en maintenant la connectivité réseau.

Procédure

- 1 Accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Groupe de ports distribués > Gérer des groupes de ports distribués**.
- 3 Sélectionnez **Association et basculement** et cliquez sur **Suivant**.
- 4 Sélectionnez les groupes de ports pour lesquels vous souhaitez utiliser le LAG.
- 5 Dans l'ordre de basculement, sélectionnez le LAG et utilisez la flèche vers le haut pour le placer dans la liste Liaisons montantes en veille.
- 6 Cliquez sur **Suivant**, lisez le message vous informant de l'utilisation de la configuration d'association et de basculement intermédiaire, puis cliquez sur **OK**.
- 7 Sur la page Prêt à terminer, cliquez sur **Terminer**.

Étape suivante

Migrez les cartes réseau physiques à partir de liaisons montantes autonomes vers les ports LAG.

Attribuer des cartes réseau physiques aux ports du groupe d'agrégation de liens

Vous avez défini le nouveau groupe d'agrégation de liens (LAG) en attente dans l'association et l'ordre de basculement des groupes de ports distribués. Lorsque le LAG est en attente, vous pouvez migrer en toute sécurité les cartes réseau physiques depuis des liaisons montantes autonomes vers des ports LAG sans perte de connectivité réseau.

Conditions préalables

- Vérifiez que tous les ports LAG ou tous les ports sur lesquels LACP a été activé sur le commutateur physique, sont en mode de négociation LACP active.
- Vérifiez que toutes les cartes réseau physiques à affecter aux ports LAG sont définies sur la même vitesse et configurées en duplex intégral.

Procédure

- 1 Dans vSphere Client, accédez au commutateur distribué dans lequel se trouve le LAG.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**.
- 4 Sélectionnez l'hôte dont vous souhaitez affecter les cartes réseau physiques aux ports LAG, puis cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les tâches de l'adaptateur réseau, sélectionnez **Gérer adaptateurs physiques**, puis cliquez sur **Suivant**.
- 6 Sur la page Gérer les adaptateurs physiques, sélectionnez une carte réseau, puis cliquez sur **Attribuer une liaison montante**.
- 7 Sélectionnez un port LAG, puis cliquez sur **OK**.
- 8 Répétez l'**Étape 6** et l'**Étape 7** pour toutes les cartes réseau physiques à affecter aux ports LAG.
- 9 Terminez l'assistant.

Exemple : Configurer deux cartes réseau physiques sur un LAG dans l'assistant **Ajouter et gérer les hôtes**

Par exemple, si vous disposez d'un LAG disposant de deux ports, vous pouvez configurer une carte réseau physique sur chacun de ces ports dans l'assistant **Ajouter et gérer des hôtes**.

Étape suivante

Définissez le LAG en mode Actif et toutes les liaisons montantes autonomes en mode Inutilisé dans l'ordre d'association et de basculement des groupes de ports distribués.

Définir Groupe d'agrégation de liens sur Actif dans l'association et l'ordre de basculement du groupe de ports distribués

Vous avez migré des cartes réseau physiques vers les ports du groupe d'agrégation de liens (LAG). Définissez le LAG en mode Actif et mettez toutes les liaisons montantes autonomes en mode Inutilisé dans l'ordre d'association et de basculement des groupes de ports distribués.

Procédure

- 1 Accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Groupe de ports distribués > Gérer des groupes de ports distribués**.
- 3 Sélectionnez **Association et basculement** et cliquez sur **Suivant**.
- 4 Sélectionnez les groupes de ports pour lesquels vous souhaitez mettre le LAG en attente, puis cliquez sur **Suivant**.
- 5 Dans la section Ordre de basculement, déplacez le LAG dans la liste Actif(ve) à l'aide des flèches vers le haut et vers le bas, déplacez toutes les liaisons montantes autonomes dans la liste Inutilisé, et ne placez aucun élément dans la liste En attente.
- 6 Cliquez sur **Suivant**, puis sur **Terminer**.

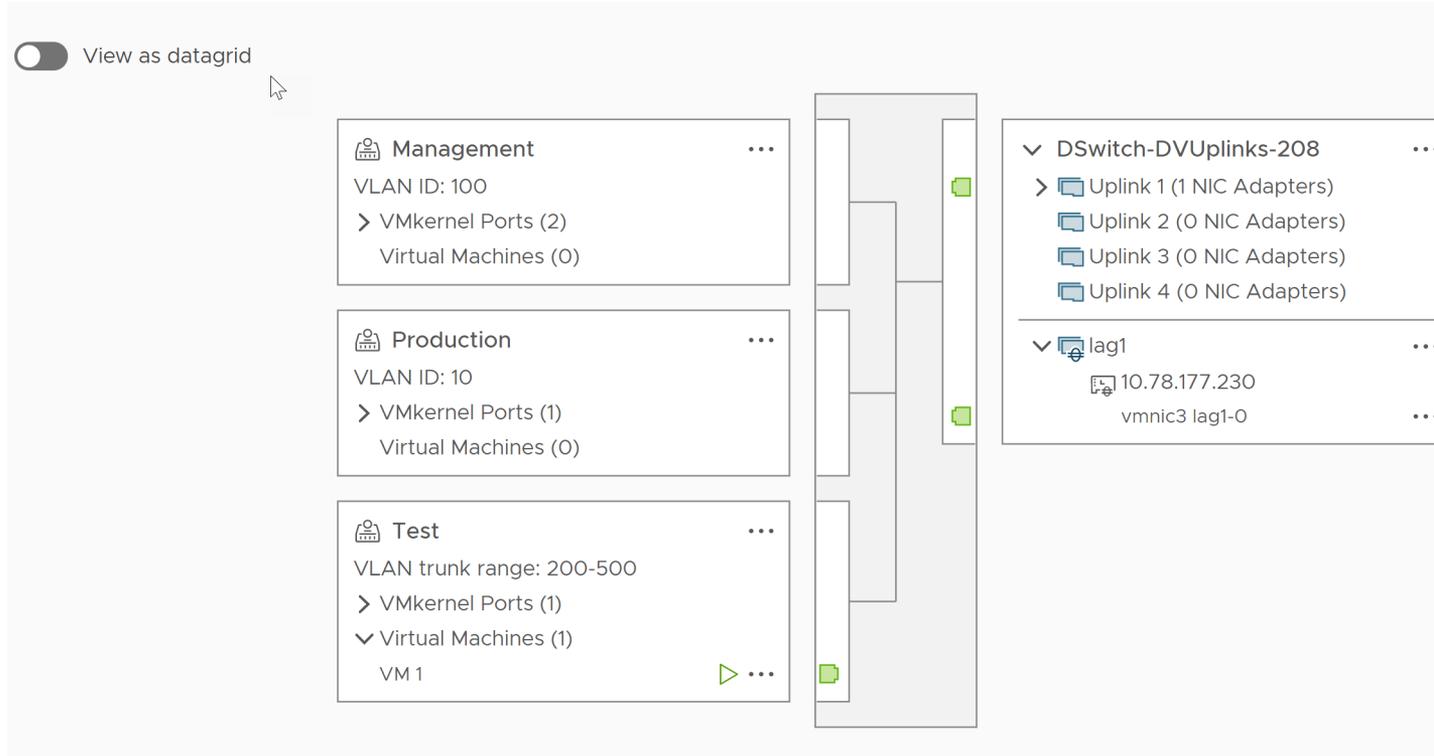
Résultats

Vous avez migré en toute sécurité le trafic réseau des liaisons montantes autonomes vers un LAG pour les groupes de ports distribués et créé une configuration d'association et de basculement LACP valide pour ces groupes.

Exemple : Topologie d'un commutateur distribué utilisant un LAG

Si vous configurez un LAG avec deux ports pour la gestion du trafic d'un groupe de ports distribués, vous pouvez afficher la topologie du commutateur distribué pour vérifier l'impact de la nouvelle configuration.

Figure 5-2. Topologie d'un commutateur distribué avec un LAG



Modifier un groupe d'agrégation de liens

Modifiez les paramètres d'un groupe d'agrégation de liens (LAG) si vous devez ajouter des ports supplémentaires au groupe ou modifier le mode de négociation LACP, l'algorithme d'équilibrage de charge ou les stratégies VLAN et NetFlow.

Procédure

- 1 Dans vSphere Client, accédez au vSphere Distributed Switch.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **LACP**.
- 3 Cliquez sur l'icône **Nouveau groupe d'agrégation de liens**.
- 4 Dans la zone de texte **Nom**, entrez le nouveau nom du LAG.
- 5 Modifiez le nombre de ports du LAG si vous souhaitez ajouter des cartes réseau physiques.

Les nouvelles cartes réseau doivent être connectées à des ports faisant partie d'un canal de port LACP sur le commutateur physique.

- 6 Modifiez le mode de négociation LACP du LAG.

Si tous les ports du canal de port du LACP physique sont en mode LACP actif, vous pouvez définir le mode LACP du LAG sur Passif, et inversement.

- 7 Modifiez le mode d'équilibrage de charge du LAG.

Vous pouvez sélectionner l'un des algorithmes d'équilibrage de charge que LACP définit.

8 Sélectionnez le mode de délai d'expiration de l'agrégation de liens.

Les transmissions périodiques des PDU LACP se produisent à un taux de transmission lent ou rapide, selon les préférences de délai d'expiration LACP que vous sélectionnez. Dans un délai d'expiration rapide, les PDU sont envoyées toutes les secondes et, dans un délai d'expiration lent, les PDU sont envoyées toutes les 30 secondes. Un délai d'expiration lent est le paramètre par défaut.

Note Vous pouvez définir un délai d'expiration LACP rapide en exécutant la commande ESXCLI suivante. Toutefois, le paramètre n'est pas disponible pour un DVS compatible NSX ou un N-VDS (vSwitch distribué NSX opaque).

```
esxcli network vswitch dvs vmware lacp timeout set --vds DVS-name --lag-id <integer> --
timeout 1
```

9 Modifiez les stratégies de VLAN et NetFlow.

Cette option est active lorsque l'option de remplacement des stratégies VLAN et NetFlow des ports individuels est activée sur le groupe de ports de liaison montante. Si vous modifiez les stratégies VLAN et NetFlow du LAG, elles remplacent les stratégies définies au niveau du groupe de ports de liaison montante.

10 Cliquez sur **OK**.

Limitations de la prise en charge de LACP sur un vSphere Distributed Switch

La prise en charge du protocole LACP sur un vSphere Distributed Switch permet aux périphériques réseau de négocier le regroupement automatique des liaisons en envoyant des paquets LACP à un homologue. Toutefois, la prise en charge du protocole LACP sur un vSphere Distributed Switch comporte des limitations.

- Le protocole LACP n'est pas pris en charge avec la liaison de port des adaptateurs iSCSI logiciels. La gestion multivoie iSCSI via LAG est prise en charge si la liaison de port n'est pas utilisée.
- Les paramètres de prise en charge du protocole LACP ne sont pas disponibles dans les profils d'hôte.
- La prise en charge du protocole LACP n'est pas possible entre des hôtes ESXi imbriqués.
- La prise en charge du protocole LACP ne fonctionne pas avec ESXi Dump Collector.
- Les paquets de contrôle LACP (LACP PDU) ne sont pas mis en miroir lorsque la fonction de mise en miroir de port est activée.
- Le contrôle de l'intégrité d'association et de basculement ne fonctionne pas sur les ports LAG. Le protocole LACP vérifie la connectivité des ports LAG.

- La prise en charge étendue du protocole LACP fonctionne correctement lorsqu'un seul LAG gère le trafic par port distribué ou par groupe de ports.

Configurations réseau de sauvegarde et de restauration

6

vSphere vous permet de sauvegarder et de rétablir la configuration d'un vSphere Distributed Switch, les groupes de ports de liaison montante et distribués en cas de modifications non valides ou encore un transfert vers un autre déploiement.

Ce chapitre contient les rubriques suivantes :

- [Sauvegarder et restaurer une configuration vSphere Distributed Switch](#)
- [Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere](#)
- [Intégration du gestionnaire de configuration ESXi](#)

Sauvegarder et restaurer une configuration vSphere Distributed Switch

vCenter Server vous permet de sauvegarder et de restaurer la configuration d'un vSphere Distributed Switch. Découvrez comment restaurer la configuration du réseau virtuel en cas d'échec de la mise à niveau ou de défaillance de la base de données. Vous pouvez également utiliser en tant que modèle une configuration de commutateur que vous aurez enregistrée afin de créer une copie du commutateur dans le même environnement vSphere ou dans un autre.

Vous pouvez importer ou exporter une configuration d'un commutateur distribué y compris ses groupes de ports. Pour obtenir des informations sur l'exportation, l'importation et la restauration d'une configuration de groupe de ports, reportez-vous à [Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere](#).

Note Vous pouvez utiliser un fichier de configuration enregistrée pour restaurer les stratégies et les associations d'hôtes sur le commutateur distribué. Vous ne pouvez pas restaurer la connexion de cartes réseau physiques à des ports de liaison montante ou des ports de groupes d'agrégation de liens.

Exporter les configurations de vSphere Distributed Switch

Vous pouvez exporter les configurations de groupes de ports distribués et de vSphere Distributed Switch dans un fichier. Le fichier conserve les configurations réseau valides, ce qui permet de transférer ces configurations vers d'autres environnements.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur Distributed Switch, puis sélectionnez **Paramètres > Exporter une configuration**.
- 3 Choisissez d'exporter la configuration du commutateur distribué, ou d'exporter la configuration du commutateur distribué et tous les groupes de ports.
- 4 (Facultatif) Tapez des notes au sujet de cette configuration dans le champ **Descriptions**
- 5 Cliquez sur **OK**.
- 6 Cliquez sur **Oui** pour enregistrer le fichier de configuration sur votre système local.

Étape suivante

Utilisez le fichier de configuration exporté pour effectuer les tâches suivantes :

- Créez une copie du Distributed Switch exporté dans un environnement vSphere. Reportez-vous à la section [Importer la configuration d'un vSphere Distributed Switch](#).
- Remplacez les paramètres sur un Distributed Switch existant. Reportez-vous à la section [Restaurer une configuration de vSphere Distributed Switch](#).

Vous ne pouvez exporter, importer, et restaurer que les configurations de groupe de ports. Reportez-vous à la section [Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere](#).

Importer la configuration d'un vSphere Distributed Switch

Importez un fichier de configuration stocké pour créer un nouveau vSphere Distributed Switch ou pour restaurer un commutateur précédemment supprimé.

Le fichier de configuration contient les paramètres de mise en réseau du commutateur. À l'aide de ce fichier, vous pouvez également répliquer le commutateur dans d'autres environnements virtuels.

Note Vous pouvez utiliser un fichier de configuration sauvegardé pour répliquer l'instance du commutateur, ses associations d'hôtes et les stratégies. Vous ne pouvez pas répliquer la connexion des cartes réseau physiques sur les ports de liaison montante ou les ports situés sur des groupes d'agrégation de liens.

Procédure

- 1 Dans vSphere Client, accédez à un centre de données.
- 2 Cliquez avec le bouton droit sur le Distributed Switch et sélectionnez **Distributed Switch > Importer Distributed Switch**.
- 3 Accédez à l'emplacement du fichier de configuration.

- 4 Pour attribuer les clés du fichier de configuration au commutateur et à ses groupes de ports, cochez la case **Conserver les identifiants d'origine du commutateur distribué et de tous les groupes de ports** et cliquez sur **Suivant**.

Vous pouvez utiliser l'option **Conserver les identifiants d'origine du commutateur distribué et de tous les groupes de ports** dans les cas suivants :

- Recréation d'un commutateur ayant été supprimé.
- Restauration d'un commutateur dont la mise à niveau a échoué.

Tous les groupes de ports sont recréés, et les hôtes ayant été connectés au commutateur sont ajoutés de nouveau.

- 5 Vérifiez les paramètres du commutateur et cliquez sur **Terminer**.

Résultats

Un nouveau commutateur distribué est créé avec les paramètres du fichier de configuration. Si vous aviez inclus dans le fichier de configuration des informations sur les groupes de ports distribués, les groupes de ports distribués sont également créés.

Restaurer une configuration de vSphere Distributed Switch

Utilisez l'option de restauration pour rétablir la configuration d'un groupe de ports distribués existante au paramètres dans un fichier de configuration. La restauration d'un commutateur distribué modifie les paramètres sur le commutateur sélectionné de retour aux paramètres enregistrés dans le fichier de configuration.

Note Vous pouvez utiliser un fichier de configuration enregistrée pour restaurer les stratégies et les associations d'hôtes sur le commutateur distribué. Vous ne pouvez pas restaurer la connexion de cartes réseau physiques à des ports de liaison montante ou des ports de groupes d'agrégation de liens.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le Distributed Switch dans le navigateur, puis sélectionnez **Paramètres > Restaurer une configuration**.
- 3 Recherchez le fichier de sauvegarde de la configuration à utiliser.
- 4 Sélectionnez **Restaurer un commutateur distribué et tous les groupes de ports** ou **Restaurer un commutateur distribué seulement** et cliquez sur **Suivant**.
- 5 Vérifiez les informations récapitulatives pour la restauration.

La restauration d'un commutateur distribué écrasera les paramètres actuels du commutateur distribué et ses groupes de ports. Il ne supprimera pas les groupes de ports existants qui ne font pas partie du fichier de configuration.

6 Cliquez sur **Terminer**.

La configuration du commutateur distribué a été restauré aux paramètres dans le fichier de configuration.

Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere

Vous pouvez exporter les configurations de groupes de ports distribués dans un fichier. Le fichier de configuration permet de conserver les configurations des groupes de ports valides, permettant de répartir ces configurations vers d'autres déploiements.

Vous pouvez exporter les informations relatives au groupe de ports tout en exportant les configurations de commutateurs distribués. Reportez-vous à [Sauvegarder et restaurer une configuration vSphere Distributed Switch](#).

Exporter les configurations de groupe de ports distribués vSphere

Vous pouvez exporter les configurations de groupes de ports distribués dans un fichier. La configuration conserve les configurations de réseau valides, permettant de répartir ces configurations vers d'autres déploiements.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit sur le groupe de ports distribués et sélectionnez **Exporter la configuration**.
- 3 (Facultatif) Dans le champ **Descriptions**, tapez quelques remarques concernant cette configuration.
- 4 Cliquez sur **OK**.

Cliquez sur **Oui** pour enregistrer le fichier de configuration sur votre système local.

Résultats

Vous avez maintenant un fichier de configuration qui contient tous les paramètres pour le groupe de ports distribués sélectionné. Vous pouvez utiliser ce fichier pour créer plusieurs copies de cette configuration sur un déploiement existant, ou pour écraser les paramètres de groupes de ports distribués existants pour qu'ils se conforment aux paramètres sélectionnés.

Étape suivante

Vous pouvez utiliser le fichier de configuration exporté pour effectuer les tâches suivantes:

- Pour créer une copie du groupe de ports distribués exportés, consulter [Importer une configuration de groupe de ports distribués vSphere](#) .
- Pour remplacer les paramètres sur un groupe de ports distribués existant, consulter [Restaurer une configuration de groupe de ports distribués vSphere](#) .

Importer une configuration de groupe de ports distribués vSphere

Utilisez l'importation pour créer un groupe de ports distribués à partir d'un fichier de configuration.

Si un groupe de ports existant porte le même nom que le groupe de ports importé, le nouveau nom du groupe de ports est suivi d'un nombre entre parenthèses. Les paramètres de la configuration importée sont appliqués au nouveau groupe de ports et ceux du groupe de ports d'origine restent inchangés.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le Distributed Switch et sélectionnez **Groupe de ports distribués > Importer un groupe de ports distribués**.
- 3 Accédez à l'emplacement de votre fichier de configuration sauvegardé et cliquez sur **Suivant**.
- 4 Vérifiez les paramètres d'importation avant de compléter l'importation.
- 5 Cliquez sur **Terminer**

Restaurer une configuration de groupe de ports distribués vSphere

Utilisez l'option de restauration pour rétablir la configuration d'un groupe de ports distribués existante pour les paramètres dans un fichier de configuration.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit sur le groupe de ports distribués et sélectionnez **Restaurer la configuration**.

3 Sélectionnez une des options suivantes et cliquez sur **Suivant** :

- ◆ Sélectionnez **Restaurer vers une configuration antérieure** pour revenir à l'étape précédente de votre configuration de groupe de ports. Si vous avez effectué plusieurs étapes, vous ne pouvez pas restaurer complètement la configuration de groupe de ports.
- ◆ Sélectionnez **Restaurer une configuration depuis un fichier** pour restaurer la configuration de groupe de ports à partir d'un fichier de sauvegarde exporté. Vous pouvez également utiliser un fichier de sauvegarde de commutateur distribué, à condition qu'il contienne les informations de configuration du groupe de ports.

4 Vérifiez les informations récapitulatives pour la restauration.

L'opération de restauration remplace les paramètres actuels du groupe de ports distribués par ceux de la sauvegarde. Si vous restaurez la configuration du groupe de ports à partir d'un fichier de sauvegarde de commutateur, l'opération de restauration ne supprime pas les groupes de ports existants qui ne figurent pas dans le fichier.

5 Cliquez sur **Terminer**.

Intégration du gestionnaire de configuration ESXi

Vous pouvez gérer les principales configurations de mise en réseau vSphere dans le gestionnaire de configuration au niveau du cluster vSphere Lifecycle Manager. Les configurations de mise en réseau vSphere incluent *vmknic*, *netstacks*, *vswitches*, *pnics*, *netdump*, *firewall*, *ipsec*, */etc/hosts*, */etc/resolv.conf*.

Exporter la configuration de l'hôte

La configuration de l'état souhaité vous permet de gérer de manière transparente vos configurations de mise en réseau vSphere dans des zones géographiques et des domaines différents.

Dans cette tâche, nous exportons un fichier JSON contenant la spécification d'état souhaitée pour un adaptateur vmknic.

Conditions préalables

- Vous devez disposer d'un cluster sur lequel vSphere Life Cycle Manager est activé.
- Assurez-vous que vous disposez d'hôtes dans le cluster.

Procédure

- 1 Dans vSphere Client, accédez au cluster.
- 2 Cliquez sur **État souhaité** > **Paramètres de l'hôte** > **Extraire de l'hôte de référence**. La boîte de dialogue **Extraire les paramètres** s'affiche.
- 3 Choisissez l'hôte dans le cluster existant.
- 4 Cliquez sur **Suivant**

5 Cliquez sur **Paramètres de téléchargement** pour télécharger le fichier.

Résultats

Le fichier JSON est téléchargé.

Étape suivante

Vous pouvez ensuite réutiliser le fichier JSON pour appliquer l'état souhaité qu'il contient à un autre cluster dans la même instance ou dans une instance différente de vCenter Server.

Note La configuration de la solution n'est pas incluse. Les informations mises en cache ne sont pas incluses. Seule une propriété spécifique à l'hôte est incluse.

Note Si vous disposez d'un cluster sur lequel vSphere Life Cycle Manager est activé, vous ne pouvez pas joindre l'hôte du cluster à un vSphere Distributed Switch.

Importer la configuration de l'hôte

Importez un état souhaité en tant que fichier JSON.

Découvrez comment importer un fichier JSON avec la configuration de l'hôte. Avant d'appliquer un état souhaité à un cluster, vous pouvez analyser tous les hôtes du cluster par rapport à l'état souhaité et vérifier la conformité du cluster par rapport à l'état souhaité. Vous pouvez exécuter des vérifications de conformité pour détecter instantanément les dérives.

Conditions préalables

- Vous devez disposer d'un cluster sur lequel vSphere Life Cycle Manager est activé.
- Assurez-vous que vous disposez d'hôtes dans le cluster.
- Assurez-vous que vous disposez d'un fichier JSON de configuration d'hôte valide.

Procédure

- 1 Dans vSphere Client, accédez au cluster.
- 2 Cliquez sur **État souhaité > Paramètres de l'hôte > Importer les paramètres**. La boîte de dialogue **Importer les paramètres de l'hôte** s'affiche.
- 3 Cliquez sur **Parcourir** pour sélectionner un fichier. La conformité est validée.
S'il existe des hôtes non-conformes, un message d'erreur s'affiche.
- 4 Cliquez sur **Corriger** pour corriger le problème de conformité d'hôte. La boîte de dialogue **Corriger les paramètres** s'affiche. La **Vérification préalable** est en cours.
- 5 La **Vérification préalable** est terminée. Les détails de la correction au niveau de l'hôte s'affichent sous **Examiner l'impact**.
- 6 Cliquez sur **Corriger** pour corriger les paramètres de configuration.

Résultats

Vous pouvez afficher les paramètres importés sur l'hôte.

Exemple :

Récupération et restauration du réseau de gestion

7

Vous pouvez empêcher une mauvaise configuration de la gestion réseau et récupérer des incidents qu'elle provoque à l'aide de la prise en charge de récupération et de restauration du vSphere Distributed Switch et du commutateur vSphere Standard.

La restauration peut être utilisée sur des commutateurs standards et distribués. Pour réparer une configuration non valide du réseau de gestion, vous pouvez vous connecter directement à un hôte pour corriger les problèmes via DCUI.

Ce chapitre contient les rubriques suivantes :

- [Restauration de mise en réseau vSphere](#)
- [Résoudre les erreurs dans la configuration du réseau de gestion sur un vSphere Distributed Switch](#)

Restauration de mise en réseau vSphere

Au moyen de l'annulation des changements de configuration, vSphere protège les hôtes contre la perte de connexion à vCenter Server qui serait due à une mauvaise configuration du réseau de gestion.

Dans vSphere, la restauration de mise en réseau est activée par défaut. Toutefois, vous pouvez activer ou désactiver les restaurations au niveau de vCenter Server.

Restaurations réseau d'hôtes

Des restaurations réseau d'hôtes se produisent lorsqu'une modification non valide est apportée à la configuration de mise en réseau pour la connexion avec vCenter Server. Chaque modification réseau qui déconnecte un hôte déclenche également une restauration. Les exemples suivants de modifications à la configuration de la mise en réseau des hôtes peuvent déclencher une restauration :

- Mettre à jour la vitesse ou le duplex d'une carte réseau physique.
- Mettre à jour DNS et paramètres de routage.
- Mettre à jour les stratégies d'association et de basculement ou les stratégies de formation du trafic d'un groupe de ports qui contient l'adaptateur réseau VMkernel de gestion.

- Mettre à jour le VLAN d'un groupe de port standard qui contient l'adaptateur réseau VMkernel de gestion.
- Augmenter la valeur de l'unité de transmission maximale (MTU) de l'adaptateur réseau VMkernel de gestion et de ses commutateurs à des valeurs non prises en charge par l'infrastructure physique.
- Modifier les paramètres IP des adaptateurs réseau VMkernel de gestion.
- Retirer l'adaptateur réseau VMkernel de gestion d'un commutateur distribué ou standard.
- Retirer une carte réseau physique d'un commutateur distribué ou standard contenant l'adaptateur réseau VMkernel de gestion.
- Migration de l'adaptateur VMkernel de gestion d'un commutateur vSphere standard vers un commutateur distribué.

Si un réseau se déconnecte pour une raison quelconque, la tâche échoue et l'hôte retourne à la dernière configuration valide.

Restaurations de vSphere Distributed Switch

Des restaurations de commutateurs distribués se produisent lorsque des mises à jour non valides sont apportées aux commutateurs distribués, aux groupes de ports distribués ou aux ports distribués. Les modifications suivantes apportées à la configuration du commutateur distribué déclenchent une restauration :

- Changer le MTU d'un commutateur distribué.
- Changer les paramètres suivants dans le groupe de ports distribués de l'adaptateur réseau VMkernel de gestion :
 - Association et basculement
 - VLAN
 - Formation du trafic
- Bloquer tous les ports dans le groupe de ports distribués contenant l'adaptateur réseau VMkernel de gestion.
- Remplacer les stratégies au niveau du port distribué pour l'adaptateur réseau VMkernel de gestion.

Si une configuration devient non valide à la suite d'une modification, un ou plusieurs hôtes peuvent ne plus être synchronisés avec le commutateur distribué.

Si vous savez où le paramètre de configuration conflictuel se trouve, vous pouvez le corriger manuellement. Par exemple, si vous avez migré un adaptateur réseau VMkernel de gestion vers un nouveau VLAN, il se peut que ce dernier ne soit pas joint sur le commutateur physique. Lorsque vous corrigez la configuration du commutateur physique, la prochaine synchronisation commutateur distribué vers hôte résout le problème de configuration.

En cas de doute sur la localisation du problème, vous pouvez restaurer l'état du commutateur distribué ou du groupe de ports distribués à une configuration antérieure. Reportez-vous à la section [Restaurer une configuration de groupe de ports distribués vSphere](#).

Désactiver la restauration de la mise en réseau

La restauration est activée par défaut dans vSphere. Vous pouvez désactiver la restauration dans vCenter Server à l'aide de vSphere Client.

Procédure

- 1 Dans vSphere Client, accédez à une instance de vCenter Server.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **Paramètres avancés**.
- 3 Cliquez sur **Modifier les paramètres**.
- 4 Sélectionnez la clé `config.vpxd.network.rollback` et modifiez la valeur à `false`.
Si la clé n'est pas présente, vous pouvez l'ajouter et définir la valeur à `false`.
- 5 Cliquez sur **OK**.
- 6 Redémarrez vCenter Server pour appliquer les modifications.

Désactiver la restauration réseau à l'aide du fichier de configuration de vCenter Server

La restauration est activée par défaut dans vSphere. Vous pouvez désactiver la restauration en modifiant directement le fichier de configuration `vpxd.cfg` de vCenter Server.

Procédure

- 1 Sur la machine hôte de vCenter Server, accédez au répertoire `/etc/vmware-vpx`.
- 2 Ouvrez le fichier `vpxd.cfg` pour modification.
- 3 Dans l'élément `<network>`, définissez l'élément `<rollback>` sur **false** :

```
<config>
  <vpxd>
    <network>
      <rollback>false</rollback>
    </network>
  </vpxd>
</config>
```

- 4 Enregistrez et fermez le fichier.
- 5 Redémarrez le système vCenter Server.

Résoudre les erreurs dans la configuration du réseau de gestion sur un vSphere Distributed Switch

Vous pouvez utiliser l'interface utilisateur de la console directe (DCUI) pour restaurer la connexion entre vCenter Server et un hôte qui accède au réseau de gestion via un Distributed Switch.

Si la restauration réseau est désactivée, une configuration erronée du groupe de ports du réseau de gestion sur le commutateur distribué provoque une perte de connexion entre vCenter Server et les hôtes qui sont ajoutés au commutateur. Vous devez utiliser l'interface DCUI pour connecter chaque hôte individuellement.

Si les liaisons montantes que vous utilisez pour restaurer le réseau de gestion sont également utilisées par des adaptateurs VMkernel qui gèrent d'autres types de trafic (vMotion, Fault Tolerance, etc.), ces adaptateurs perdent la connectivité du réseau après la restauration.

Pour plus d'informations sur l'accès à l'interface DCUI et son utilisation, consultez la documentation *Sécurité vSphere*.

Note La récupération de la connexion de gestion sur un commutateur distribué n'est pas prise en charge sur les instances ESXi sans état.

Conditions préalables

Vérifiez que le réseau de gestion du commutateur distribué est configuré sur un groupe de ports.

Procédure

- 1 Connectez-vous à l'interface DCUI de l'hôte.
- 2 Depuis le menu **Options de restauration réseau**, sélectionnez **Restaurer vDS**.
- 3 Configurez les liaisons montantes et éventuellement le VLAN du réseau de gestion.
- 4 Appliquez la configuration.

Résultats

L'interface DCUI crée un port éphémère local et applique les valeurs que vous avez fournies au VLAN et aux liaisons montantes. L'interface DCUI déplace l'adaptateur VMkernel du réseau de gestion vers le nouveau port local pour restaurer la connectivité à vCenter Server.

Étape suivante

Une fois que la connexion de l'hôte à vCenter Server est restaurée, corrigez la configuration du groupe de ports distribués et rajoutez l'adaptateur VMkernel au groupe.

Stratégies de mise en réseau vSphere



Les règles définies au niveau du commutateur standard ou du groupe de ports distribués s'appliquent à tous les groupes de ports du commutateur standard ou aux ports du groupe de ports distribués. Les exceptions sont les options de configuration qui sont remplacées au niveau du groupe de ports standard ou du port distribué.

Regardez cette vidéo consacrée à l'application des stratégies de mise en réseau sur les commutateurs standard vSphere et les commutateurs distribués.



(Utilisation des stratégies de mise en réseau)

- [Appliquer les stratégies de mise en réseau sur vSphere Standard ou Distributed Switch](#)

Vous appliquez des stratégies de mise en réseau différemment sur les commutateurs standard vSphere et les commutateurs vSphere Distributed Switch. Certaines stratégies disponibles pour un vSphere Distributed Switch ne le sont pas pour un commutateur standard vSphere.

- [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#)

Pour appliquer des stratégies différentes aux ports distribués, vous devez configurer le remplacement port par port des stratégies définies au niveau du groupe de ports. Vous pouvez également activer la réinitialisation d'une configuration quelle qu'elle soit définie au niveau d'un port lorsqu'un port distribué se déconnecte d'une machine virtuelle.

- [Présentation de la stratégie d'association et de basculement](#)

L'association de cartes réseau permet d'augmenter la capacité réseau d'un commutateur virtuel en incluant plusieurs cartes réseau physiques dans une association. Pour déterminer comment le trafic est réacheminé en cas de panne d'un adaptateur, vous incluez des cartes réseau physiques dans un ordre de basculement. Pour déterminer comment le commutateur virtuel distribue le trafic entre les cartes réseau physiques d'une association, vous sélectionnez des algorithmes d'équilibrage de charge selon les besoins et les capacités de votre environnement.

- [Présentation de la stratégie VLAN](#)

Les règles VLAN déterminent le fonctionnement des VLAN dans l'ensemble de votre environnement réseau.

- [Présentation de la stratégie de sécurité](#)

Une règle de sécurité réseau assure la protection du trafic contre l'emprunt d'identité d'adresse MAC et le balayage de port indésirable.

- [Qu'est-ce que la stratégie de formation de trafic ?](#)

Une stratégie de formation de trafic est définie par la bande passante moyenne, le pic de bande passante et la taille de rafale. Vous pouvez établir une règle de formation de trafic pour chaque groupe de ports et chaque port distribué ou groupe de ports distribués.

- [Présentation de la stratégie d'allocation des ressources](#)

La stratégie d'allocation des ressources vous permet d'associer un port distribué ou un groupe de ports à un pool de ressources réseau créé par l'utilisateur. Cette règle vous permet de contrôler plus efficacement la bande passante affectée au port ou au groupe de ports.

- [Présentation de la stratégie de surveillance](#)

La règle de surveillance permet d'activer ou de désactiver la surveillance NetFlow d'un port distribué ou d'un groupe de ports distribués.

- [Qu'est-ce que la stratégie de filtrage et de balisage du trafic ?](#)

Dans un vSphere Distributed Switch, les stratégies de filtrage et de balisage du trafic permettent de protéger le réseau virtuel contre le trafic indésirable et les attaques de sécurité, ou d'appliquer une balise QoS à un type de trafic spécifique.

- [Gérer les règles pour plusieurs groupes de ports sur vSphere Distributed Switch](#)

Vous pouvez modifier les stratégies de mise en réseau de plusieurs groupes de ports sur vSphere Distributed Switch.

- [Règles de blocage des ports](#)

Les règles de blocage des ports vous permettent d'empêcher les ports de votre choix d'envoyer ou de recevoir des données.

- [Présentation de la stratégie d'apprentissage MAC](#)

L'apprentissage MAC fournit une connectivité réseau aux déploiements où plusieurs adresses MAC sont utilisées à partir d'une vNIC.

Appliquer les stratégies de mise en réseau sur vSphere Standard ou Distributed Switch

Vous appliquez des stratégies de mise en réseau différemment sur les commutateurs standard vSphere et les commutateurs vSphere Distributed Switch. Certaines stratégies disponibles pour un vSphere Distributed Switch ne le sont pas pour un commutateur standard vSphere.

Tableau 8-1. Objets commutateur virtuel auxquels des stratégies s'appliquent

Commutateur virtuel	Objet de commutateur virtuel	Description
Commutateur standard vSphere	Intégralité du commutateur	Lorsque vous appliquez des stratégies sur l'intégralité du commutateur standard, les stratégies sont propagées à tous les groupes de ports standard sur le commutateur.
	Groupe de ports standard	Vous pouvez appliquer différentes stratégies sur des groupes de ports individuels en remplaçant les stratégies héritées du commutateur.
vSphere Distributed Switch	Groupe de ports distribués	Lorsque vous appliquez des stratégies sur un groupe de ports distribués, les stratégies sont propagées à tous les ports du groupe.
	Port distribué	Vous pouvez appliquer différentes stratégies sur des ports distribués individuels en remplaçant les stratégies héritées du groupe de ports distribués.
	Groupe de ports de liaison montante	Vous pouvez appliquer des stratégies au niveau du groupe de ports de liaison montante, les stratégies se propagent alors à tous les ports du groupe.
	Port de liaison montante	Vous pouvez appliquer différentes stratégies sur les ports de liaison montante individuels en remplaçant les stratégies héritées du groupe de ports de liaison montante.

Tableau 8-2. Stratégies disponibles pour un commutateur standard vSphere et pour vSphere Distributed Switch

Règle	Commutateur standard	Distributed Switch	Description
Association et basculement	Oui	Oui	Permet de configurer les cartes réseau physiques qui gèrent le trafic réseau pour un commutateur standard, un groupe de ports standard, un groupe de ports distribués ou un port distribué. Vous disposez les cartes réseau physiques dans un ordre de basculement et leur appliquez différentes stratégies d'équilibrage de charge.
Sécurité	Oui	Oui	Assure la protection du trafic contre l'usurpation d'adresses MAC et l'analyse de port indésirable. La stratégie de sécurité de mise en réseau est mise en œuvre dans la couche 2 de la pile de protocole de mise en réseau.
Formation du trafic	Oui	Oui	Vous permet de restreindre la bande passante réseau dont disposent les ports, mais aussi de transférer des rafales de trafic à des vitesses plus élevées. ESXi formate le trafic réseau sortant sur les commutateurs standard et le trafic entrant et sortant sur les commutateurs distribués.
VLAN	Oui	Oui	Vous permet de configurer le balisage VLAN pour un commutateur standard ou distribué. Vous pouvez configurer le balisage du commutateur externe (EST), le balisage du commutateur virtuel (VST) et le balisage d'invité virtuel (VGT).

Tableau 8-2. Stratégies disponibles pour un commutateur standard vSphere et pour vSphere Distributed Switch (suite)

Règle	Commutateur standard	Distributed Switch	Description
Surveillance	Non	Oui	Active et désactive la surveillance NetFlow sur un port distribué ou un groupe de ports.
Filtrage et balisage du trafic	Non	Oui	Permet de protéger le réseau virtuel contre le trafic indésirable et les attaques de sécurité, ou d'appliquer une balise QoS à un certain type de trafic.
Allocation de ressources	Non	Oui	Vous permet d'associer un port distribué ou un groupe de ports à un pool de ressources réseau défini par l'utilisateur. De cette manière, vous pouvez mieux contrôler la bande passante dont dispose le port ou le groupe de ports. Vous pouvez utiliser la stratégie d'allocation de ressources avec vSphere Network I/O Control version 2 et 3.
Blockage des ports	Non	Oui	Permet de sélectionner des ports pour y bloquer l'envoi et la réception de données.

Configurer le remplacement des stratégies de mise en réseau au niveau des ports

Pour appliquer des stratégies différentes aux ports distribués, vous devez configurer le remplacement port par port des stratégies définies au niveau du groupe de ports. Vous pouvez également activer la réinitialisation d'une configuration quelle qu'elle soit définie au niveau d'un port lorsqu'un port distribué se déconnecte d'une machine virtuelle.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez la page **Avancé**.

Option	Description
Configurez la réinitialisation à la déconnexion	Dans le menu déroulant, activez ou désactivez la réinitialisation à la déconnexion. Quand un port distribué est déconnecté d'une machine virtuelle, la configuration de ports distribués devient identique au paramétrage de groupe de ports distribués. Tous les remplacements par port sont ignorés.
Remplacer les règles de port	Sélectionnez les règles de groupes de ports distribués au niveau de chaque port à remplacer.

- 4 (Facultatif) Utilisez les pages de règles pour établir des remplacements pour chaque règle de port.
- 5 Cliquez sur **OK**.

Présentation de la stratégie d'association et de basculement

L'association de cartes réseau permet d'augmenter la capacité réseau d'un commutateur virtuel en incluant plusieurs cartes réseau physiques dans une association. Pour déterminer comment le trafic est réacheminé en cas de panne d'un adaptateur, vous incluez des cartes réseau physiques dans un ordre de basculement. Pour déterminer comment le commutateur virtuel distribue le trafic entre les cartes réseau physiques d'une association, vous sélectionnez des algorithmes d'équilibrage de charge selon les besoins et les capacités de votre environnement.

Stratégie d'association de cartes réseau

Vous pouvez utiliser l'association de cartes réseau pour connecter un commutateur virtuel à plusieurs cartes réseau physiques sur un hôte afin d'augmenter la bande passante réseau du commutateur et fournir de la redondance. Une association de cartes réseau peut distribuer le trafic entre ses membres et fournir un basculement passif en cas de panne d'adaptateur ou d'indisponibilité du réseau. Vous définissez les stratégies d'association de cartes réseau au niveau du commutateur virtuel ou du groupe de ports pour un commutateur standard vSphere et au niveau du groupe de ports ou du port pour un vSphere Distributed Switch.

Note Tous les ports sur le commutateur physique dans la même association doivent se trouver dans le même domaine de diffusion de couche 2.

Stratégie d'équilibrage de charge

La stratégie d'équilibrage de charge détermine la distribution du trafic réseau entre les adaptateurs réseau dans une association de cartes réseau. La charge des commutateurs virtuels vSphere équilibre uniquement la charge du trafic sortant. Le trafic entrant est contrôlé par la stratégie d'équilibrage de charge sur le commutateur physique.

Pour plus d'informations sur chaque algorithme d'équilibrage de charge, reportez-vous à la section [Algorithmes d'équilibrage de charge disponibles pour les commutateurs virtuels](#).

Stratégie de détection de panne réseau

Vous pouvez spécifier l'une des méthodes suivantes à utiliser par un commutateur virtuel pour la détection de basculement.

État de lien seulement

Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Détecte des pannes (par exemple, des câbles retirés et des coupures d'alimentation de commutateur physique). Cependant, l'état du lien ne détecte pas les erreurs de configuration suivantes :

- Port de commutateur physique bloqué par l'arborescence ou configuré sur un VLAN incorrect.
- Câble débranché reliant un commutateur physique à d'autres périphériques de mise en réseau, par exemple, un commutateur en amont.

Sondage de balise

Envoie et écoute les trames de diffusion Ethernet, ou les sondes de balise, que les cartes réseau physiques envoient pour détecter une panne de liaison dans toutes les cartes réseau physiques d'une association. Les hôtes ESXi envoient des paquets de balises chaque seconde. Le sondage de balise est très utile pour détecter les pannes du commutateur physique le plus proche de l'hôte ESXi, lorsque la panne ne provoque pas un événement de liaison interrompue pour l'hôte.

Utilisez le sondage de balise pour une association comportant au moins trois cartes réseau, car ESXi peut détecter les pannes d'une carte unique. Si seulement deux cartes réseau sont attribuées et que l'une d'elles perd la connectivité, le commutateur ne parvient pas à déterminer celle à mettre hors service, car aucune des deux ne reçoit de balise et tous les paquets sont par conséquent envoyés aux deux liaisons montantes. L'utilisation d'au moins trois cartes réseau dans ce type d'association autorise $n-2$ pannes, n étant le nombre de cartes réseau présentes dans l'association avant d'arriver à une situation ambiguë.

Stratégie de restauration automatique

Par défaut, une stratégie de restauration automatique est activée sur une association de cartes réseau. Si une carte réseau physique en panne revient en ligne, le commutateur virtuel réactive la carte réseau en remplaçant la carte réseau de secours qui a pris son emplacement.

Si la carte réseau physique occupant la première position dans l'ordre de basculement subit des pannes intermittentes, la stratégie de restauration automatique peut entraîner de fréquents changements de carte réseau utilisée. Le commutateur physique voit de fréquentes modifications des adresses MAC, et le port du commutateur physique peut ne pas accepter immédiatement le trafic lorsqu'une carte devient en ligne. Pour minimiser de tels retards, vous pouvez envisager de modifier les paramètres suivants sur le commutateur physique :

- Désactivez le protocole STP (Spanning Tree Protocol) sur les cartes réseau physiques connectées aux hôtes ESXi.
- Pour les réseaux Cisco, activez le mode PortFast afin d'accéder aux interfaces ou le mode PortFast Trunk pour les interfaces de jonction. Cela permet de gagner environ 30 secondes lors de l'initialisation du port du commutateur physique.
- Désactivez la négociation de jonction.

Stratégie de notification des commutateurs

En utilisant la stratégie de notification des commutateurs, vous pouvez déterminer comment l'hôte ESXi communique les événements de basculement. Lorsqu'une carte réseau physique se connecte au commutateur virtuel ou lorsque du trafic est réacheminé vers une autre carte réseau physique dans l'association, le commutateur virtuel envoie des notifications sur le réseau pour mettre à jour les tables de recherche des commutateurs physiques. Le fait d'avertir le commutateur physique permet d'obtenir la latence la plus faible en cas de basculement ou de migration dans vSphere vMotion.

Algorithmes d'équilibrage de charge disponibles pour les commutateurs virtuels

Vous pouvez configurer divers algorithmes d'équilibrage de charge sur un commutateur virtuel pour déterminer comment le trafic réseau est distribué entre les cartes réseau physiques d'une association.

- **Route basée sur le port virtuel d'origine**

Le commutateur virtuel sélectionne les liaisons montantes en fonction des ID de port de machine virtuelle sur un commutateur vSphere standard ou un vSphere Distributed Switch.

- **Route basée sur le hachage MAC source**

Le commutateur virtuel sélectionne une liaison montante pour une machine virtuelle en fonction de l'adresse MAC de la machine virtuelle. Pour calculer une liaison montante pour une machine virtuelle, le commutateur virtuel utilise l'adresse MAC de la machine virtuelle et le nombre de liaisons montantes figurant dans l'association de cartes réseau.

- **Route basée sur le hachage IP**

Le commutateur virtuel sélectionne les liaisons montantes pour les machines virtuelles selon les adresses IP source et de destination de chaque paquet.

- **Route basée sur la charge NIC physique**

La route basée sur la charge NIC physique est basée sur la route en fonction du port virtuel originel, dans laquelle le commutateur virtuel vérifie la charge réelle des liaisons montantes et prend des mesures pour la réduire sur les liaisons montantes surchargées. Uniquement disponible pour le vSphere Distributed Switch.

- **Utiliser la commande de basculement explicite**

Aucun équilibrage de charge n'est réellement disponible avec cette stratégie. Le commutateur virtuel examine les liaisons montantes de la liste des adaptateurs actifs fournie par la commande de basculement et utilise toujours la première de la liste qui satisfait les critères de détection de basculement. Si aucune liaison montante de la liste des adaptateurs actifs n'est disponible, le commutateur virtuel utilise les liaisons montantes de la liste des adaptateurs en veille.

Route basée sur le port virtuel d'origine

Le commutateur virtuel sélectionne les liaisons montantes en fonction des ID de port de machine virtuelle sur un commutateur vSphere standard ou un vSphere Distributed Switch.

La route basée sur le port virtuel d'origine est la méthode d'équilibrage de charge par défaut sur un commutateur vSphere standard ou un vSphere Distributed Switch.

Un ID de port virtuel défini sur le commutateur virtuel est associé à chaque machine virtuelle qui s'exécute sur un hôte ESXi. Pour calculer une liaison montante pour une machine virtuelle, le commutateur virtuel utilise l'ID de port de la machine virtuelle et le nombre de liaisons montantes figurant dans l'association de cartes réseau. Une fois que le commutateur virtuel a sélectionné une liaison montante pour une machine virtuelle, il transfère toujours le trafic via la même liaison montante pour cette machine virtuelle, tant que celle-ci s'exécute sur le même port. Le commutateur virtuel calcule les liaisons montantes correspondant aux machines virtuelles une seule fois, sauf si des liaisons montantes sont ajoutées ou supprimées dans l'association de cartes réseau.

L'ID de port d'une machine virtuelle reste inchangé tant que la machine virtuelle s'exécute sur le même port. Si vous migrez, mettez hors tension ou supprimez la machine virtuelle, son ID de port est libéré sur le commutateur virtuel. Le commutateur virtuel cesse d'envoyer du trafic vers ce port, ce qui réduit le trafic global pour la liaison montante associée. En cas de migration ou de mise sous tension d'une machine virtuelle, elle peut apparaître sur un autre port et utiliser la liaison montante associée à ce nouveau port.

Tableau 8-3. Remarques concernant l'utilisation d'une route basée sur le port virtuel d'origine

Considérations	Description
Avantages	<ul style="list-style-type: none"> ■ Distribution homogène du trafic si l'association comprend plus de cartes réseau virtuelles que de cartes réseau physiques. ■ Consommation réduite des ressources, car en général, le commutateur virtuel calcule une seule fois les liaisons montantes associées aux machines virtuelles. ■ Aucune modification n'est requise sur le commutateur physique.
Inconvénients	<ul style="list-style-type: none"> ■ Le commutateur virtuel n'a pas connaissance de la charge du trafic sur les liaisons montantes et n'équilibre pas la charge du trafic en la répartissant sur les liaisons montantes moins utilisées. ■ La bande passante disponible pour une machine virtuelle est limitée à la vitesse de la liaison montante associée à l'ID de port pertinent, sauf si la machine virtuelle est dotée de plusieurs cartes réseau virtuelles.

Route basée sur le hachage MAC source

Le commutateur virtuel sélectionne une liaison montante pour une machine virtuelle en fonction de l'adresse MAC de la machine virtuelle. Pour calculer une liaison montante pour une machine

virtuelle, le commutateur virtuel utilise l'adresse MAC de la machine virtuelle et le nombre de liaisons montantes figurant dans l'association de cartes réseau.

Tableau 8-4. Remarques concernant l'utilisation d'une route basée sur le hachage MAC source

Considérations	Description
Avantages	<ul style="list-style-type: none"> ■ Distribution plus homogène du trafic, par rapport à une route basée sur le port virtuel d'origine, car le commutateur virtuel calcule une liaison montante pour chaque paquet. ■ Les machines virtuelles utilisent la même liaison montante, car l'adresse MAC est statique. La liaison montante utilisée par une machine virtuelle ne change pas lorsque celle-ci est mise sous tension ou hors tension. ■ Aucune modification n'est requise sur le commutateur physique.
Inconvénients	<ul style="list-style-type: none"> ■ La bande passante disponible pour une machine virtuelle est limitée à la vitesse de la liaison montante associée à l'ID de port pertinent, sauf si la machine virtuelle utilise plusieurs adresses MAC source. ■ Plus grande consommation de ressources, par rapport à une route basée sur le port virtuel d'origine, car le commutateur virtuel calcule une liaison montante pour chaque paquet. ■ Le commutateur virtuel n'a pas connaissance de la charge des liaisons montantes, donc les liaisons montantes peuvent finir par être surchargées.

Route basée sur le hachage IP

Le commutateur virtuel sélectionne les liaisons montantes pour les machines virtuelles selon les adresses IP source et de destination de chaque paquet.

Pour calculer une liaison montante pour une machine virtuelle, le commutateur virtuel extrait du paquet le dernier octet de l'adresse IP source et de l'adresse IP de destination, les soumet à une opération XOR et obtient le résultat par le biais d'un autre calcul basé sur le nombre de liaisons montantes figurant dans l'association de cartes réseau. Le résultat est un numéro compris entre 0 et le nombre de liaisons montantes figurant dans l'association, moins un. Par exemple, si une association de cartes réseau comprend quatre liaisons montantes, le résultat est un numéro compris entre 0 et 3, puisque chaque numéro est associé à une carte réseau de l'association. Pour les paquets non-IP, le commutateur virtuel extrait deux valeurs binaires de 32 bits de la trame ou du paquet qui contiendrait l'adresse IP.

Toute machine virtuelle peut utiliser toute liaison montante de l'association de cartes réseau, selon les adresses IP source et de destination. Ainsi, chaque machine virtuelle peut utiliser indifféremment la bande passante de l'une ou l'autre des liaisons montantes de l'association. Si une machine virtuelle s'exécute dans un environnement contenant un grand nombre de machines virtuelles indépendantes, l'algorithme de hachage IP permet de répartir le trafic de

façon homogène entre les différentes cartes réseau de l'association. Lorsqu'une machine virtuelle communique avec plusieurs adresses IP de destination, le commutateur virtuel peut générer un hachage différent pour chaque IP de destination. Ainsi, les paquets peuvent utiliser différentes liaisons montantes sur le commutateur virtuel qui permet d'obtenir le débit potentiel le plus élevé.

Toutefois, si votre environnement contient un nombre limité d'adresses IP, le commutateur virtuel peut faire passer le trafic uniformément via une liaison montante de l'association. Par exemple, dans le cas d'un serveur de base de données auquel accède un seul serveur d'applications, le commutateur virtuel calcule toujours la même liaison montante, car il existe une seule paire source-destination.

Configuration du commutateur physique

Pour garantir que l'équilibrage de charge basé sur le hachage IP fonctionne correctement, vous devez configurer Etherchannel sur le commutateur physique. Etherchannel rassemble plusieurs adaptateurs réseau dans un lien logique unique. Lorsque les ports sont liés dans une configuration Etherchannel, à chaque fois que le commutateur physique reçoit un paquet provenant de la même adresse MAC de machine virtuelle sur différents ports, le commutateur met à jour sa table de mémoire adressable par contenu (CAM) avec les données pertinentes.

Par exemple, si le commutateur physique reçoit des paquets provenant de l'adresse MAC A sur les ports O1 et O2, le commutateur crée les entrées O1-A et O2-A dans sa table CAM. Ainsi, le commutateur physique distribue le trafic entrant aux ports adéquats. Sans Etherchannel, le commutateur physique commence par créer un enregistrement répertoriant qu'un paquet provenant de l'adresse MAC A a été reçu sur le port O1, puis met à jour cet enregistrement pour signaler qu'un paquet provenant de l'adresse MAC A a été reçu sur le port O2. Par conséquent, le commutateur physique ne transfère que le trafic entrant sur le port O2 et certains paquets risquent de ne pas atteindre leur destination et de surcharger la liaison montante correspondante.

Exigences de configuration et limitations

- Les hôtes ESXi prennent en charge l'association basée sur le hachage IP sur un commutateur physique ou sur des commutateurs empilés.
- Les hôtes ESXi prennent uniquement en charge l'agrégation de liens 802.3ad en mode statique. Vous pouvez seulement utiliser une configuration Etherchannel statique avec des commutateurs vSphere standard. LACP n'est pas pris en charge. Si vous activez l'équilibrage de charge basée sur le hachage IP sans l'agrégation de liens 802.3ad ou vice-versa, vous risquez de subir des interruptions de mise en réseau.
- Avec l'équilibrage de charge basée sur le hachage IP, vous devez utiliser la détection de panne de réseau État de lien seulement.
- Vous devez définir toutes les liaisons montantes de l'association dans la liste de basculement actif. Les listes des éléments en veille et inutilisés doivent être vides.
- Le nombre de ports dans Etherchannel doit être identique au nombre de liaisons montantes figurant dans l'association.

Remarques concernant l'utilisation d'une route basée sur le hachage IP

Considérations	Description
Avantages	<ul style="list-style-type: none"> ■ Distribution plus homogène de la charge, par rapport à une route basée sur le port virtuel d'origine ou sur le hachage MAC source, car le commutateur virtuel calcule la liaison montante pour chaque paquet. ■ Débit potentiel supérieur pour les machines virtuelles qui communiquent avec plusieurs adresses IP.
Inconvénients	<ul style="list-style-type: none"> ■ Consommation des ressources plus élevée qu'avec les autres algorithmes d'équilibrage de charge. ■ Le commutateur virtuel ne connaît pas la charge réelle des liaisons montantes. ■ Nécessite des changements sur le réseau physique. ■ Dépannage complexe.

Route basée sur la charge NIC physique

La route basée sur la charge NIC physique est basée sur la route en fonction du port virtuel originel, dans laquelle le commutateur virtuel vérifie la charge réelle des liaisons montantes et prend des mesures pour la réduire sur les liaisons montantes surchargées. Uniquement disponible pour le vSphere Distributed Switch.

Le commutateur distribué calcule les liaisons montantes pour les machines virtuelles en utilisant leur ID de port et le nombre de liaisons montantes dans l'association de cartes réseau. Le commutateur distribué teste les liaisons montantes toutes les 30 secondes. Si leur charge est supérieure à 75 pour cent d'utilisation, l'ID de port de la machine virtuelle dont les E/S sont les plus élevées est déplacé vers une autre liaison montante.

Tableau 8-5. Considérations sur l'utilisation de la route basée sur la charge NIC physique

Considérations	Description
Avantages	<ul style="list-style-type: none"> ■ Faible consommation de ressources parce que le commutateur distribué ne calcule qu'une fois les liaisons montantes pour les machines virtuelles et parce que la vérification des liaisons montantes n'a qu'un impact minime. ■ Le commutateur distribué a connaissance de la charge des liaisons montantes et veille à la réduire, le cas échéant. ■ Aucune modification n'est requise sur le commutateur physique.
Inconvénients	<ul style="list-style-type: none"> ■ La bande passante dont disposent les machines virtuelles est limitée aux liaisons montantes connectées au commutateur distribué.

Utiliser la commande de basculement explicite

Aucun équilibrage de charge n'est réellement disponible avec cette stratégie. Le commutateur virtuel examine les liaisons montantes de la liste des adaptateurs actifs fournie par la commande de basculement et utilise toujours la première de la liste qui satisfait les critères de détection de basculement. Si aucune liaison montante de la liste des adaptateurs actifs n'est disponible, le commutateur virtuel utilise les liaisons montantes de la liste des adaptateurs en veille.

Configurer l'association de cartes réseau, le basculement et l'équilibrage de charge sur un commutateur ou un groupe de ports vSphere standard

Pour accroître la capacité réseau d'un commutateur vSphere standard ou d'un groupe de ports standard, intégrez deux cartes réseau physiques ou plus à une association de cartes. Configurez l'ordre de basculement pour déterminer comment le trafic réseau est réacheminé en cas de panne d'adaptateur. Sélectionnez un algorithme d'équilibrage de charge pour déterminer comment le commutateur standard distribue le trafic entre les cartes réseau physiques de l'association.

Configurez l'association de cartes réseau, le basculement et l'équilibrage de charge en fonction de la configuration du réseau sur le commutateur physique et de la topologie du commutateur standard. Pour plus d'informations, reportez-vous aux sections [Présentation de la stratégie d'association et de basculement](#) et [Algorithmes d'équilibrage de charge disponibles pour les commutateurs virtuels](#).

Si vous configurez la stratégie d'association et de basculement sur un commutateur standard, la stratégie est propagée à tous les groupes de ports du commutateur. Si vous la configurez sur un groupe de ports standard, elle remplace la stratégie héritée du commutateur.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Accédez à la stratégie Association et basculement du commutateur standard ou du groupe de ports standard.

Option	Action
Commutateur standard	<ol style="list-style-type: none"> a Sélectionnez le commutateur dans la liste. b Cliquez sur Modifier les paramètres et sélectionnez Association et basculement.
Groupe de ports standard	<ol style="list-style-type: none"> a Sélectionnez le commutateur sur lequel réside le groupe de ports. b Dans le diagramme de topologie du commutateur, sélectionnez le groupe de ports standard et cliquez sur Modifier les paramètres. c Sélectionnez Association et basculement. d Sélectionnez Remplacer en regard des stratégies que vous souhaitez remplacer.

- 4 Dans le menu déroulant **Équilibrage de charge**, indiquez comment la charge du commutateur virtuel équilibre le trafic sortant entre les cartes réseau physiques d'une équipe.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionnez une liaison montante en fonction des ID de ports virtuels sur le commutateur. Une fois que le commutateur virtuel a sélectionné une liaison montante pour une machine virtuelle ou pour un adaptateur VMkernel, il transfère toujours le trafic par la même liaison montante pour cette machine virtuelle ou cet adaptateur VMkernel.
Route basée sur le hachage IP	Sélectionner une liaison montante en fonction d'un hachage des adresses IP de source et de destination de chaque paquet. Pour les paquets non IP, le commutateur utilise les données de ces champs pour calculer le hachage. L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel.
Router en fonction du hachage de l'adresse MAC source	Sélectionner une liaison montante en fonction d'un hachage de l'Ethernet source.
Utiliser la commande de basculement explicite	Dans la liste des adaptateurs actifs, toujours utiliser la liaison montante la plus élevée qui satisfait aux critères de détection de basculement. Aucun équilibrage de charge n'est réellement effectué avec cette option.

- 5 Dans le menu déroulant **Détection de panne réseau**, sélectionnez la méthode de détection du basculement utilisée par le commutateur virtuel.

Option	Description
État de lien seulement	Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les anomalies telles que les câbles retirés et les pannes d'alimentation des commutateurs physiques.
Sondage de balise	Envoie et détecte des sondes de balise sur toutes les cartes réseau de l'association et utilise ces informations, en plus de l'état du lien, pour déterminer la défaillance du lien. ESXi envoie des paquets de balises toutes les secondes. La configuration des cartes réseau doit être active/active ou active/en veille, car celles qui sont dans l'état Inutilisé ne participent pas au sondage de balise.

- 6 Dans le menu déroulant **Notifier les commutateurs**, indiquez si le commutateur standard ou distribué avertit le commutateur physique en cas de basculement.

Note Sélectionnez **Non** pour cette option si une machine virtuelle connectée utilise l'équilibrage de charge réseau Microsoft en mode monodiffusion. L'équilibrage de charge réseau exécuté en mode multidiffusion ne pose aucun problème.

- 7 Dans le menu déroulant **Restauration automatique**, indiquez si un adaptateur physique retourne à l'état actif après la récupération d'une panne.

Si le retour arrière est défini sur **Oui** (sélection par défaut) l'adaptateur est ramené au service actif immédiatement après la récupération, en déplaçant l'adaptateur en attente éventuel ayant repris son emplacement.

Si la restauration automatique est définie sur **Non** pour un port standard, un adaptateur défectueux reste inactif après la récupération jusqu'à ce qu'un autre adaptateur actif tombe en panne et doive être remplacé.

- 8 Indiquez la manière dont les liaisons montantes d'une association sont utilisées en cas de basculement en configurant la liste Ordre de basculement.

Si vous souhaitez utiliser certaines liaisons montantes et en réserver d'autres pour les urgences en cas de panne des liaisons montantes actives, déplacez-les dans différents groupes à l'aide des flèches de direction.

Option	Description
Adaptateurs actifs	Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est opérationnelle.
Adaptateurs en veille	Utilisez cette liaison montante si l'un des adaptateurs physiques actifs est en panne.
Adaptateurs inutilisés	N'utilisez pas cette liaison montante.

- 9 Cliquez sur **OK**.

Configurer l'association de cartes réseau, le basculement et l'équilibrage de charge sur un groupe de ports distribués ou un port distribué

Incluez plusieurs cartes réseau physiques dans une association pour augmenter la capacité réseau d'un groupe de ports distribués ou d'un port distribué. Configurez l'ordre de basculement pour déterminer comment le trafic réseau est réacheminé en cas de panne d'adaptateur. Sélectionnez un algorithme d'équilibrage de charge pour déterminer comment le Distributed Switch équilibre la charge du trafic entre les cartes réseau physiques dans une association.

Configurez l'association de cartes réseau, le basculement et l'équilibrage de charge conformément à la configuration réseau sur le commutateur physique et à la topologie du Distributed Switch. Pour plus d'informations, reportez-vous aux sections [Présentation de la stratégie d'association et de basculement](#) et [Algorithmes d'équilibrage de charge disponibles pour les commutateurs virtuels](#).

Si vous configurez la stratégie d'association et de basculement pour un groupe de ports distribués, la stratégie est propagée à tous les ports du groupe. Si vous configurez la stratégie pour un port distribué, cette configuration remplace la stratégie héritée du groupe.

Note La définition d'une option de retour arrière n'est pas prise en charge avec la stratégie d'association **Route basée sur la charge NIC physique**.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Accédez à la stratégie d'association et de basculement sur le groupe de ports distribués ou le port distribué.

Option	Action
Groupe de ports distribués	<ol style="list-style-type: none"> a Dans le menu Actions, sélectionnez Groupe de ports distribués > Gérer des groupes de ports distribués. b Sélectionnez le groupe de ports et cliquez sur Suivant. c Sélectionnez Association et basculement.
Port distribué	<ol style="list-style-type: none"> a Dans l'onglet Réseaux, cliquez sur Groupes de ports distribués et faites un double clic sur un groupe de ports distribués. b Dans l'onglet Ports, sélectionnez un port et cliquez sur Modifier les paramètres d'un port distribué. c Sélectionnez Association et basculement. d Sélectionnez Remplacer en regard des propriétés que vous souhaitez remplacer.

- 3 Dans le menu déroulant **Équilibrage de charge**, indiquez comment la charge du commutateur virtuel équilibre le trafic sortant entre les cartes réseau physiques d'une équipe.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionnez une liaison montante en fonction des ID de ports virtuels sur le commutateur. Une fois que le commutateur virtuel a sélectionné une liaison montante pour une machine virtuelle ou pour un adaptateur VMkernel, il transfère toujours le trafic par la même liaison montante pour cette machine virtuelle ou cet adaptateur VMkernel.
Route basée sur le hachage IP	Sélectionner une liaison montante en fonction d'un hachage des adresses IP de source et de destination de chaque paquet. Pour les paquets non IP, le commutateur utilise les données de ces champs pour calculer le hachage. L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel.
Router en fonction du hachage de l'adresse MAC source	Sélectionner une liaison montante en fonction d'un hachage de l'Ethernet source.

Option	Description
Route basée sur la charge NIC physique	<p>Disponible pour les groupes de ports distribués ou les ports distribués. Sélectionnez une liaison montante en fonction du nombre actuel d'adaptateurs réseau physiques connectés au groupe de ports ou au port. Si une liaison montante est occupée à 75 pour cent (ou plus) pendant 30 secondes, le commutateur de proxy hôte déplace une partie du trafic de machine virtuelle vers un adaptateur physique dont la capacité le permet.</p> <p>Note La sélection de Route basée sur la charge NIC physique vous empêche d'utiliser une option de retour arrière pour un groupe de ports distribués.</p>
Utiliser la commande de basculement explicite	<p>Dans la liste des adaptateurs actifs, toujours utiliser la liaison montante la plus élevée qui satisfait aux critères de détection de basculement. Aucun équilibrage de charge n'est réellement effectué avec cette option.</p>

- 4 Dans le menu déroulant **Détection de panne réseau**, sélectionnez la méthode de détection du basculement utilisée par le commutateur virtuel.

Option	Description
État de lien seulement	<p>Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les anomalies telles que les câbles retirés et les pannes d'alimentation des commutateurs physiques.</p>
Sondage de balise	<p>Envoie et détecte des sondes de balise sur toutes les cartes réseau de l'association et utilise ces informations, en plus de l'état du lien, pour déterminer la défaillance du lien. ESXi envoie des paquets de balises toutes les secondes.</p> <p>La configuration des cartes réseau doit être active/active ou active/en veille, car celles qui sont dans l'état Inutilisé ne participent pas au sondage de balise.</p>

- 5 Dans le menu déroulant **Notifier les commutateurs**, indiquez si le commutateur standard ou distribué avertit le commutateur physique en cas de basculement.

Note Sélectionnez **Non** pour cette option si une machine virtuelle connectée utilise l'équilibrage de charge réseau Microsoft en mode monodiffusion. L'équilibrage de charge réseau exécuté en mode multidiffusion ne pose aucun problème.

- 6 Dans le menu déroulant **Restauration automatique**, indiquez si un adaptateur physique retourne à l'état actif après la récupération d'une panne.

Si le retour arrière est défini sur **Oui** (sélection par défaut) l'adaptateur est ramené au service actif immédiatement après la récupération, en déplaçant l'adaptateur en attente éventuel ayant repris son emplacement.

Si la restauration automatique est définie sur **Non** pour un port distribué, un adaptateur défectueux reste inactif après la récupération uniquement si la machine virtuelle associée est en cours d'exécution. Lorsque l'option **Restauration automatique** est définie sur **Non** et qu'une machine virtuelle est mise hors tension, si tous les adaptateurs physiques actifs sont en panne et que l'un d'eux est récupéré, la carte réseau virtuelle est connectée à

l'adaptateur récupéré et non à un adaptateur en veille après la mise sous tension de la machine virtuelle. La mise hors tension, puis à nouveau sous tension d'une machine virtuelle entraîne la reconnexion de la carte réseau virtuelle au port distribué. Le commutateur distribué considère que le port vient d'être ajouté et lui attribue le port de liaison montante par défaut, c'est-à-dire, l'adaptateur de liaison montante actif.

- Indiquez la manière dont les liaisons montantes d'une association sont utilisées en cas de basculement en configurant la liste Ordre de basculement.

Si vous souhaitez utiliser certaines liaisons montantes et en réserver d'autres pour les urgences en cas de panne des liaisons montantes actives, déplacez-les dans différents groupes à l'aide des flèches de direction.

Option	Description
Adaptateurs actifs	Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est opérationnelle.
Adaptateurs en veille	Utilisez cette liaison montante si l'un des adaptateurs physiques actifs est en panne.
Adaptateurs inutilisés	N'utilisez pas cette liaison montante.

- Vérifiez vos paramètres et appliquez la configuration.

Présentation de la stratégie VLAN

Les règles VLAN déterminent le fonctionnement des VLAN dans l'ensemble de votre environnement réseau.

Un réseau local virtuel (VLAN) est un groupe d'hôtes ayant un ensemble de besoins commun, qui communiquent comme s'ils étaient attachés au même domaine de diffusion, quel que soit leur emplacement physique. Un VLAN utilise les mêmes attributs qu'un réseau local physique (LAN), mais il permet aux stations finales d'être regroupées même si elles ne sont pas sur le même commutateur réseau.

Les règles VLAN peuvent s'étendre aux groupes de ports distribués, aux ports distribués, ainsi qu'aux groupes de ports de liaison montante et aux ports de liaison montante.

Configurer le balisage VLAN sur un port distribué ou un groupe de ports distribués

Pour appliquer l'identification VLAN globalement sur tous les ports distribués, vous devez définir la règle VLAN sur un groupe de ports distribués. Pour intégrer le trafic virtuel à des VLAN physiques sur ce port, différemment du groupe de ports distribués parent, vous devez utiliser la règle VLAN sur un port distribué.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Accédez à la stratégie VLAN configurée sur le port distribué ou le groupe de ports distribués.

Option	Action
Groupe de ports distribués	<ol style="list-style-type: none"> a Dans le menu Actions, sélectionnez Groupe de ports distribués > Gérer des groupes de ports distribués. b Sélectionnez l'option VLAN et cliquez sur Suivant. c Sélectionnez le groupe de ports et cliquez sur Suivant.
Port distribué	<ol style="list-style-type: none"> a Dans l'onglet Réseaux, cliquez sur Groupes de ports distribués et faites un double clic sur un groupe de ports distribués. b Dans l'onglet Ports, sélectionnez un port et cliquez sur l'icône Modifier les paramètres d'un port distribué. c Sélectionnez VLAN. d Sélectionnez Remplacer en regard des propriétés à remplacer.

- 3 Dans le menu déroulant **Type VLAN**, sélectionnez le type de filtrage et de balisage du trafic VLAN, puis cliquez sur **Suivant**.

Option	Description
Aucun	N'utilise pas de VLAN. Utilisez cette option en cas de balisage de commutateur externe.
VLAN	Identifier le trafic avec l'ID du champ ID VLAN . Entrez un nombre entre 1 et 4 094 pour le balisage de commutateur virtuel.
jonction VLAN	Passez le trafic VLAN avec ID dans la Plage de jonction VLAN au système d'exploitation invité. Vous pouvez définir plusieurs plages et VLAN individuels à l'aide d'une liste séparée par des virgules. Par exemple : 1702-1705, 1848-1849 . Utilisez cette option pour l'identification de l'invité virtuel.
VLAN privé	Associez le trafic avec un VLAN privé créé sur le commutateur distribué.

- 4 Vérifiez vos paramètres et appliquez la configuration.

Configurer le balisage VLAN sur un port ou un groupe de ports de liaisons montantes

Pour configurer le traitement du trafic VLAN, en général pour toutes les liaisons montantes membres, vous devez définir la règle VLAN sur un groupe de ports de liaison montante. Pour

gérer le trafic VLAN via le port d'une façon différente du groupe de ports de liaison montante parent, vous devez définir la règle VLAN sur une liaison montante.

Utilisez la règle VLAN sur le port de liaison montante pour propager une plage de jonctions des ID VLAN vers l'adaptateur réseau physique pour le filtrage du trafic. Les adaptateurs réseau physique abandonnent les paquets provenant des autres VLAN s'ils prennent en charge le filtrage par VLAN. Le paramétrage d'une plage de jonctions améliore les performances de gestion de réseau car les adaptateurs réseau physique filtrent le trafic à la place des ports de liaison montante dans le groupe.

Si vous disposez d'un adaptateur réseau physique qui ne prend pas en charge le filtrage VLAN, les VLAN risquent de ne toujours pas être bloqués. Dans ce cas, configurez le filtrage VLAN sur un groupe de ports distribués ou sur un port distribué.

Pour plus d'informations sur la prise en charge du filtrage VLAN, consultez la documentation technique des fabricants des adaptateurs.

Conditions préalables

Pour remplacer la règle VLAN au niveau du port, permettez les remplacements au niveau du port. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Dans vSphere Client, accédez à un commutateur distribué.
- 2 Dans l'onglet **Réseaux**, cliquez sur **Groupe de ports de liaison montante**.
- 3 Accédez à la stratégie VLAN configurée sur le port ou le groupe de ports de liaison montante.

Option	Action
Groupe de ports de liaison montante	<ol style="list-style-type: none"> a Cliquez avec le bouton droit sur un groupe de ports de liaison montante dans la liste et sélectionnez Modifier les paramètres. b Cliquez sur VLAN.
Port de liaison montante	<ol style="list-style-type: none"> a Faites un double clic sur un groupe de ports de liaison montante. b Dans l'onglet Ports, sélectionnez un port et cliquez sur l'onglet Modifier les paramètres de port distribué. c Cliquez sur VLAN et sélectionnez Remplacer.

- 4 Entrez une valeur **Plage jonction VLAN** à propager aux adaptateurs réseau physiques.
Pour effectuer la jonction de plusieurs plages et de VLAN individuels, séparez les entrées par des virgules.
- 5 Cliquez sur **OK**.

Présentation de la stratégie de sécurité

Une règle de sécurité réseau assure la protection du trafic contre l'emprunt d'identité d'adresse MAC et le balayage de port indésirable.

La règle de sécurité d'un commutateur standard ou distribué est mise en œuvre au niveau de la couche 2 (couche de liaison de données) de la pile de protocole réseau. Les trois éléments de la stratégie de sécurité sont le mode Proximité, les changements d'adresse MAC et les Transmissions forgées. Pour plus d'informations sur les menaces réseau potentielles, consultez la documentation de *Sécurité vSphere*.

Configurer la stratégie de sécurité d'un groupe de ports standard ou d'un commutateur vSphere standard

Sur un commutateur standard vSphere, vous pouvez configurer la règle de sécurité permettant d'interdire les modifications d'adresse MAC et l'activation du mode promiscuité sur le système d'exploitation invité d'une machine virtuelle. Vous pouvez remplacer la règle de sécurité héritée du commutateur standard sur des groupes de ports individuels.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Accédez à la stratégie de sécurité sur le groupe de ports ou le commutateur standard.

Option	Action
Commutateur standard vSphere	<ol style="list-style-type: none"> a Sélectionnez un commutateur standard dans la liste. b Cliquez sur Edit settings. c Sélectionnez Sécurité.
Groupe de ports standard	<ol style="list-style-type: none"> a Sélectionnez le commutateur standard sur lequel réside le groupe de ports. b Dans le diagramme de topologie, sélectionnez un groupe de ports standard. c Cliquez sur Edit settings. d Sélectionnez Sécurité, puis Remplacer en regard des options que vous souhaitez remplacer.

- 4 Interdisez ou autorisez l'activation du mode promiscuité ou les modifications d'adresse MAC sur le système d'exploitation invité des machines virtuelles reliées au commutateur ou au groupe de ports standard.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ Rejeter. L'adaptateur réseau de la machine virtuelle ne reçoit que les trames adressées à la machine virtuelle. ■ Accepter. Le commutateur virtuel transmet toutes les trames à la machine virtuelle conformément à la stratégie VLAN active du port auquel l'adaptateur réseau de la machine virtuelle est connecté. <p>Note Le mode promiscuité est un mode de fonctionnement non sécurisé. Les pare-feu, scanners de ports, systèmes de détection d'intrusion, doivent s'exécuter en mode promiscuité.</p>
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ Rejeter. Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur rejette toutes les trames entrantes de l'adaptateur. <p>Si le système d'exploitation invité remplace à nouveau l'adresse MAC effective de la machine virtuelle par l'adresse MAC de l'adaptateur réseau de la machine virtuelle, la machine virtuelle reçoit de nouveau les trames.</p> <ul style="list-style-type: none"> ■ Accepter. Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur autorise la transmission des trames vers la nouvelle adresse.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter. Le commutateur ignore toutes les trames sortantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration <code>.vmx</code>. ■ Accepter. Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.
État	<p>Activez ou désactivez la fonctionnalité d'apprentissage MAC. La valeur par défaut est Désactivé.</p>
Autoriser la saturation monodiffusion	<p>Lorsqu'un paquet reçu par un port a une adresse MAC de destination inconnue, le paquet 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 si l'apprentissage MAC est activé.</p>

Option	Description
Limite MAC	Le nombre d'adresses MAC pouvant être apprises est configurable. La valeur maximale est 4 096, selon le port, cette valeur est prise par défaut.
Stratégie de limite MAC	Stratégie à appliquer lorsque la limite MAC est atteinte. Les options sont : <ul style="list-style-type: none"> ■ 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.

5 Cliquez sur **OK**.

Configurer la règle de sécurité d'un port distribué ou d'un groupe de ports distribués

Définissez une règle de sécurité sur un groupe de ports distribués pour autoriser ou interdire le mode de promiscuité et les modifications d'adresse MAC pour le système d'exploitation invité des machines virtuelles associées au groupe de ports. Vous pouvez remplacer la règle de sécurité héritée des groupes de ports distribués ou de ports individuels.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Accédez à la règle de sécurité configurée sur le port distribué ou le groupe de ports distribués.

Option	Action
Groupe de ports distribués	<ol style="list-style-type: none"> a Dans le menu Actions, sélectionnez Groupe de ports distribués > Gérer des groupes de ports distribués. b Sélectionnez Sécurité et cliquez sur Suivant. c Sélectionnez le groupe de ports et cliquez sur Suivant.
Port distribué	<ol style="list-style-type: none"> a Dans l'onglet Réseaux, cliquez sur Groupes de ports distribués et faites un double clic sur un groupe de ports distribués. b Dans l'onglet Ports, sélectionnez un port et cliquez sur l'icône Modifier les paramètres. c Sélectionnez Sécurité. d Sélectionnez Remplacer en regard des propriétés à remplacer.

3 Interdisez ou autorisez l'activation du mode promiscuité ou les modifications d'adresse MAC sur le système d'exploitation invité des machines virtuelles reliées au port distribué ou au groupe de ports distribués.

Option	Description
<p>Mode promiscuité</p>	<ul style="list-style-type: none"> ■ Rejeter. L'adaptateur réseau de la machine virtuelle ne reçoit que les trames adressées à la machine virtuelle. ■ Accepter. Le commutateur virtuel transmet toutes les trames à la machine virtuelle conformément à la stratégie VLAN active du port auquel l'adaptateur réseau de la machine virtuelle est connecté. <p>Note Le mode promiscuité est un mode de fonctionnement non sécurisé. Les pare-feu, scanners de ports, systèmes de détection d'intrusion, doivent s'exécuter en mode promiscuité.</p>
<p>Modifications d'adresse MAC</p>	<ul style="list-style-type: none"> ■ Rejeter. Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur rejette toutes les trames entrantes de l'adaptateur. <p>Si le système d'exploitation invité remplace à nouveau l'adresse MAC effective de la machine virtuelle par l'adresse MAC de l'adaptateur réseau de la machine virtuelle, la machine virtuelle reçoit de nouveau les trames.</p> <ul style="list-style-type: none"> ■ Accepter. Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur autorise la transmission des trames vers la nouvelle adresse.
<p>Transmissions forgées</p>	<ul style="list-style-type: none"> ■ Rejeter. Le commutateur ignore toutes les trames sortantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration <code>.vmx</code>. ■ Accepter. Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.
<p>État</p>	<p>Activez ou désactivez la fonctionnalité d'apprentissage MAC. La valeur par défaut est Désactivé.</p>
<p>Autoriser la saturation monodiffusion</p>	<p>Lorsqu'un paquet reçu par un port a une adresse MAC de destination inconnue, le paquet 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 si l'apprentissage MAC est activé.</p>

Option	Description
Limite MAC	Le nombre d'adresses MAC pouvant être apprises est configurable. La valeur maximale est 4 096, selon le port, cette valeur est prise par défaut.
Stratégie de limite MAC	Stratégie à appliquer lorsque la limite MAC est atteinte. Les options sont : <ul style="list-style-type: none"> ■ 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.

4 Vérifiez vos paramètres et appliquez la configuration.

Qu'est-ce que la stratégie de formation de trafic ?

Une stratégie de formation de trafic est définie par la bande passante moyenne, le pic de bande passante et la taille de rafale. Vous pouvez établir une règle de formation de trafic pour chaque groupe de ports et chaque port distribué ou groupe de ports distribués.

ESXi formate le trafic réseau sortant sur les commutateurs standard et le trafic entrant et sortant sur les commutateurs distribués. La formation du trafic limite la bande passante de réseau à la disposition d'un port, mais elle peut également être configurée pour permettre à des rafales de trafic de traverser à des vitesses plus élevées.

Bande passante moyenne

Établit le nombre de bits par seconde moyen à autoriser dans le temps. Ce nombre est la charge moyenne autorisée.

Bande passante maximale

Nombre maximal d'octets par seconde à autoriser à travers un port quand il reçoit ou envoie une rafale de trafic. Ce nombre limite la bande passante qu'utilise un port lorsqu'il utilise son bonus de rafale.

Taille de rafale

Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Lorsque le port a besoin de plus de bande passante que la quantité spécifiée par la bande passante moyenne, il peut être autorisé à transmettre temporairement les données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre limite le nombre d'octets qui peuvent être cumulés dans le bonus de rafale et transfère le trafic plus rapidement.

Configurer la formation du trafic d'un groupe de ports ou d'un commutateur vSphere standard

ESXi permet de mettre en forme le trafic sortant sur des commutateurs ou des groupes de ports standard. L'outil de formation du trafic limite la bande passante de réseau à la disposition d'un port, mais il peut également être configuré pour permettre temporairement à des rafales de trafic de traverser un port à des vitesses plus élevées.

Les stratégies de mise en forme du trafic que vous définissez au niveau du commutateur ou du groupe de ports sont appliquées à chaque port qui participe au commutateur ou au groupe de ports. Par exemple, si vous définissez une bande passante moyenne de 100 000 Kbit/s sur un groupe de ports standard, 100 000 Kbit/s calculés en moyenne dans le temps peuvent traverser chaque port associé au groupe de ports standard.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Accédez à la stratégie de formation du trafic sur le groupe de ports ou le commutateur standard.

Option	Action
Commutateur standard vSphere	<ol style="list-style-type: none"> a Sélectionnez un commutateur standard dans la liste. b Cliquez sur Edit settings. c Sélectionnez Formation du trafic.
Groupe de ports standard	<ol style="list-style-type: none"> a Sélectionnez le commutateur standard sur lequel réside le groupe de ports. b Dans le diagramme de topologie, sélectionnez un groupe de ports standard. c Cliquez sur Edit settings. d Sélectionnez Formation du trafic, puis Remplacer en regard des options que vous souhaitez remplacer.

- 4 Configurez les stratégies de formation du trafic.

Option	Description
État	Permet de définir des limites sur le niveau de bande passante allouée à chaque port associé au commutateur ou au groupe de ports standard.
Bande passante moyenne	Définit le nombre de bits moyen par seconde à autoriser sur un port dans le temps (charge moyenne autorisée).

Option	Description
Bande passante maximale	Correspond au nombre maximum de bits par seconde à autoriser sur un port lors de la transmission d'une rafale de trafic. Ce paramètre limite la bande passante utilisée par un port lorsqu'il utilise son bonus de rafale. Il doit toujours être supérieur à la bande passante moyenne.
Taille de rafale	Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin de plus de bande passante que la bande passante moyenne spécifiée, il pourra transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre s'ajoute au nombre d'octets qui peuvent s'accumuler dans le bonus de rafale et être transférés à une vitesse plus élevée.

- Entrez une valeur de bande passante pour chaque stratégie de formation du trafic (**Bande passante moyenne**, **Bande passante maximale** et **Ampleur du pic**).
- Cliquez sur **OK**.

Modifier la stratégie de formation du trafic sur un port distribué ou un groupe de ports distribués

Vous pouvez contrôler le trafic entrant et sortant sur des ports distribués ou des groupes de ports distribués vSphere. L'outil de formation du trafic limite la bande passante réseau pour un port dans le groupe, mais il peut également être configuré pour permettre temporairement à des « rafales » du trafic de traverser un port à des vitesses plus élevées.

Les stratégies de mise en forme du trafic que vous définissez au niveau du groupe de ports distribués sont appliquées à chaque port individuel qui participe au groupe de ports. Par exemple, si vous définissez une bande passante moyenne de 100 000 Kbits/s sur un groupe de ports distribués, une moyenne de 100 000 Kbits/s dans le temps peut transiter sur chaque port associé au groupe de ports distribués.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.

2 Accédez à la stratégie de formation du trafic sur le port ou le groupe de ports distribués.

Option	Action
Groupe de ports distribués	<ul style="list-style-type: none"> a Dans le menu Actions, sélectionnez Groupe de ports distribués > Gérer des groupes de ports distribués. b Sélectionnez Formation du trafic et cliquez sur Suivant. c Sélectionnez le groupe de ports et cliquez sur Suivant.
Port distribué	<ul style="list-style-type: none"> a Dans l'onglet Réseaux, cliquez sur Groupes de ports distribués et faites un double clic sur un groupe de ports distribués. b Dans l'onglet Ports, sélectionnez un port et cliquez sur l'icône Modifier les paramètres d'un port distribué. c Sélectionnez Formation du trafic. d Sélectionnez Remplacer en regard des propriétés à remplacer.

3 Configurez les stratégies de formation du trafic.

Note Le trafic est qualifié d'entrée ou de sortie d'après le sens du trafic dans le commutateur et non dans l'hôte.

Option	Description
État	Activez la Formation du trafic d'entrée ou la Formation du trafic de sortie en utilisant les menus déroulants État .
Bande passante moyenne	Définit le nombre moyen de bits par seconde à autoriser sur un port, c'est-à-dire la charge moyenne autorisée.
Bande passante maximale	Nombre maximal d'octets par seconde à autoriser à travers un port quand il envoie/reçoit une rafale de trafic. Ce paramètre limite la bande passante utilisée par un port lorsqu'il utilise son bonus de rafale.
Taille de rafale	Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin de plus de bande passante que la bande passante moyenne spécifiée, il pourra transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre s'ajoute au nombre d'octets qui peuvent s'accumuler dans le bonus de rafale et être transférés à une vitesse plus élevée.

4 Vérifiez vos paramètres et appliquez la configuration.

Présentation de la stratégie d'allocation des ressources

La stratégie d'allocation des ressources vous permet d'associer un port distribué ou un groupe de ports à un pool de ressources réseau créé par l'utilisateur. Cette règle vous permet de contrôler plus efficacement la bande passante affectée au port ou au groupe de ports.

Pour obtenir des informations sur la création et la configuration des pools de ressources réseau, reportez-vous au [Chapitre 11 vSphere Network I/O Control](#).

Modifier la règle d'allocation des ressources d'un groupe de ports distribués

Associez un groupe de ports distribués à un pool de ressources réseau pour contrôler plus efficacement la bande passante affectée au groupe de ports distribués.

Conditions préalables

- Activez Network I/O Control sur Distributed Switch. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).
- Créez et configurez des pools de ressources réseau. Reportez-vous à la section [Créer un pool de ressources réseau](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué dans le navigateur et sélectionnez **Groupes de ports distribués > Gérer des groupes de ports distribués**.
- 3 Cochez la case **Allocation des ressources** et cliquez sur **Suivant**.
- 4 Sélectionnez le groupe de ports distribués à configurer et cliquez sur **Suivant**.
- 5 Ajouter ou supprimer du pool de ressources réseau le groupe de ports distribués et cliquez sur **Suivant**.
 - Pour ajouter le groupe de ports distribués, sélectionnez un pool de ressources défini par l'utilisateur depuis le menu déroulant **Pool de ressources réseau**.
 - Pour supprimer le groupe de ports distribués, sélectionnez **par défaut** du menu déroulant **Pool de ressources réseaux**.
- 6 Vérifiez vos paramètres dans la section **Prêt à terminer** et cliquez sur **Terminer**.
Utilisez le bouton **Précédent** pour modifier les paramètres.

Présentation de la stratégie de surveillance

La règle de surveillance permet d'activer ou de désactiver la surveillance NetFlow d'un port distribué ou d'un groupe de ports distribués.

Vous pouvez définir les paramètres NetFlow au niveau du vSphere Distributed Switch. Reportez-vous à la section [Configurer les paramètres NetFlow d'un vSphere Distributed Switch](#).

Gérer la surveillance NetFlow sur un port distribué ou un groupe de ports distribués

Vous pouvez configurer NetFlow pour surveiller les paquets IP qui transitent par les ports d'un groupe de ports distribués ou par des ports distribués individuels.

Vous configurez les paramètres NetFlow sur vSphere Distributed Switch. Reportez-vous à la section [Configurer les paramètres NetFlow d'un vSphere Distributed Switch](#).

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Accédez à la règle de surveillance configurée sur le port distribué ou le groupe de ports distribués.

Option	Action
Groupe de ports distribués	<ol style="list-style-type: none"> a Dans le menu Actions, sélectionnez Groupe de ports distribués > Gérer des groupes de ports distribués. b Sélectionnez Surveillance et cliquez sur Suivant. c Sélectionnez le groupe de ports et cliquez sur Suivant.
Port distribué	<ol style="list-style-type: none"> a Dans l'onglet Réseaux, cliquez sur Groupes de ports distribués et faites un double clic sur un groupe de ports distribués. b Dans l'onglet Ports, sélectionnez un port et cliquez sur l'icône Modifier les paramètres d'un port distribué. c Sélectionnez Surveillance. d Sélectionnez Remplacer en regard des propriétés à remplacer.

- 3 Dans le menu déroulant **NetFlow**, sélectionnez **Activé** ou **Désactivé**, puis cliquez sur **Suivant**.
- 4 Vérifiez vos paramètres et appliquez la configuration.

Qu'est-ce que la stratégie de filtrage et de balisage du trafic ?

Dans un vSphere Distributed Switch, les stratégies de filtrage et de balisage du trafic permettent de protéger le réseau virtuel contre le trafic indésirable et les attaques de sécurité, ou d'appliquer une balise QoS à un type de trafic spécifique.

Les stratégies de filtrage et de balisage du trafic correspondent à un ensemble ordonné de règles de trafic réseau permettant d'assurer la sécurité et le balisage QoS des flux de données acheminés via les ports d'un commutateur distribué. Une règle est en principe constituée d'un qualificateur de trafic et d'une action visant à restreindre ou à hiérarchiser le trafic correspondant.

Le vSphere Distributed Switch applique des règles de trafic à différents niveaux du flux de données. Les stratégies de filtrage du trafic s'appliquent sur le chemin de données reliant l'adaptateur réseau de la machine virtuelle au port distribué. Les règles de liaison montante s'appliquent quant à elles entre le port de liaison montante et l'adaptateur réseau physique. La stratégie de filtrage et de balisage du trafic ne prend pas en charge vSphere Distributed Switch configuré avec la Compatibilité des déchargements réseau.

Filtrage et marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Définissez des règles de trafic au niveau des groupes de ports distribués ou des groupes de ports de liaison montante pour activer le filtrage et le balisage prioritaire pour l'accès du trafic sur les machines virtuelles, les adaptateurs VMkernel ou les adaptateurs physiques.

- [Activer le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

L'activation des règles de filtrage et de balisage du trafic dans un groupe de ports permet de configurer la sécurité et le balisage du trafic sur tous les adaptateurs réseau et de liaison montante des machines virtuelles faisant partie du groupe.

- [Marquer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Attribuez des balises prioritaires au trafic (par exemple, au trafic VoIP et au flux vidéo) nécessitant des capacités réseau supérieures en matière de bande passante, de faible latence, etc. Vous pouvez baliser le trafic en attribuant une balise CoS à la couche 2 de la pile de protocole réseau ou une balise DSCP à la couche 3.

- [Filtrer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Autorisez ou arrêtez le trafic pour sécuriser les données acheminées via les ports d'un groupe de ports distribués ou d'un groupe de ports de liaison montante.

- [Utilisation de règles de trafic réseau sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Définissez des règles de trafic dans un groupe de ports distribués ou un groupe de ports de liaison montante pour mettre en place une règle de traitement du trafic liée aux machines virtuelles ou aux adaptateurs physiques. Vous pouvez filtrer un type de trafic spécifique ou décrire ses demandes QoS.

- [Désactiver le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Autorisez l'acheminement du trafic vers les machines virtuelles ou les adaptateurs physiques sans contrôle supplémentaire de la sécurité ou de la qualité de service en désactivant les règles de filtrage et de balisage du trafic.

Activer le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

L'activation des règles de filtrage et de balisage du trafic dans un groupe de ports permet de configurer la sécurité et le balisage du trafic sur tous les adaptateurs réseau et de liaison montante des machines virtuelles faisant partie du groupe.

Note Vous pouvez désactiver la stratégie de filtrage et de balisage du trafic sur un port spécifique pour éviter de traiter le trafic acheminé via ce port. Reportez-vous à la section [Désactiver le filtrage et le marquage du trafic sur un port distribué ou un port de liaison montante](#).

Note La stratégie de filtrage et de balisage du trafic ne prend pas en charge vSphere Distributed Switch configuré avec la capacité de déchargements réseau.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Cliquez sur **Activer toutes les règles de trafic**.
- 6 Cliquez sur **OK**.

Étape suivante

Configurez le filtrage ou le balisage du trafic sur les données acheminées via les ports du groupe de ports distribués ou du groupe de ports de liaison montante. Reportez-vous aux sections [Marquer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#) et [Filtrer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#).

Marquer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Attribuez des balises prioritaires au trafic (par exemple, au trafic VoIP et au flux vidéo) nécessitant des capacités réseau supérieures en matière de bande passante, de faible latence, etc. Vous pouvez baliser le trafic en attribuant une balise CoS à la couche 2 de la pile de protocole réseau ou une balise DSCP à la couche 3.

Le balisage prioritaire est un mécanisme qui permet de baliser le trafic pour lequel les demandes QoS sont plus élevées. Le réseau peut ainsi reconnaître les différentes classes de trafic. Les périphériques réseau peuvent gérer le trafic de chaque classe en fonction de ses priorités et de ses critères.

Vous pouvez aussi baliser à nouveau le trafic afin d'augmenter ou de réduire l'importance du flux. L'utilisation d'une balise QoS faible vous permet de limiter les données balisées dans un système d'exploitation invité.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer et réorganiser > Activer toutes les règles de trafic > OK**.
- 5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.
- 6 Dans la boîte de dialogue de la règle de trafic réseau, sélectionnez l'option **Balise** dans le menu déroulant **Action**.
- 7 Définissez la balise de priorité du trafic dans l'étendue de la règle.

Option	Description
Valeur CoS	Marquez le trafic correspondant à la règle avec une balise de priorité CoS dans la couche réseau 2. Cochez la case et tapez une valeur comprise entre 0 et 7.
Valeur DSCP	Marquez le trafic associé à la règle avec une balise DSCP dans la couche réseau 3. Cocher la case et tapez une valeur comprise entre 0 et 63.

8 Indiquez le type de trafic auquel la règle s'applique.

Pour déterminer si un flux de données se trouve dans l'étendue d'une règle pour le balisage ou le filtrage, le vSphere Distributed Switch examine le sens du trafic, ainsi que des propriétés telles que la source et la destination, le VLAN, le protocole du niveau suivant, le type de trafic d'infrastructure, etc.

- a Dans le menu déroulant **Sens du trafic**, choisissez si le trafic doit entrer, sortir ou les deux, afin que la règle le reconnaisse comme une correspondance.

Le sens influence aussi la manière dont vous allez identifier la source et la destination du trafic.

- b En utilisant des qualificatifs pour le type de données système, les attributs de paquet de la couche 2 et les attributs de paquet de la couche 3, définissez les propriétés que les paquets doivent posséder pour correspondre à la règle.

Un qualificatif représente un ensemble de critères de correspondance liés à une couche réseau. Vous pouvez faire correspondre le trafic au type de données système, aux propriétés de trafic de la couche 2 et aux propriétés de trafic de la couche 3. Vous pouvez utiliser un qualificatif pour une couche réseau spécifique ou combiner des qualificatifs pour faire correspondre les paquets de manière plus précise.

- Utilisez le qualificatif de trafic système pour faire correspondre les paquets au type des données d'infrastructure virtuelle qui sont transmises via les ports du groupe. Par exemple, vous pouvez sélectionner NFS pour les transferts de données vers un stockage réseau.
- Utilisez le qualificatif de trafic MAC pour faire correspondre les paquets par adresse MAC, ID VLAN et protocole du niveau suivant.

La recherche du trafic avec un ID VLAN sur un groupe de ports distribués fonctionne avec le balisage d'invité virtuel (VGT). Pour faire correspondre le trafic à l'ID VLAN si le balisage de commutateur virtuel (VST) est actif, utilisez une règle sur un groupe de ports de liaison montante ou un port de liaison montante.

- Utilisez le qualificatif de trafic IP pour faire correspondre les paquets par version IP, adresse IP et protocole et port du niveau suivant.

- 9 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Exemple : Balisage du trafic Voice over IP

Les flux Voice over IP (VoIP) nécessitent des capacités QoS spécifiques en matière de réduction des pertes et de délai. Le trafic SIP (Session Initiation Protocol) des flux VoIP est généralement associé à une balise DSCP 26, ce qui correspond à un acheminement assuré de classe 3 à faible probabilité de perte (AF31).

Par exemple, pour baliser des paquets UDP SIP sortants vers un sous-réseau 192.168.2.0/24, vous pouvez utiliser la règle suivante :

Paramètre de règle	Valeur de paramètre
Action	Balise
Valeur DSCP	26
Direction de trafic	Sortie
Qualificateurs de trafic	Qualificateur IP
Protocole	UDP
Port de destination	5060
Adresse source	L'adresse IP correspond à 192.168.2.0 avec une longueur de préfixe de 24

Filtrer le trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Autorisez ou arrêtez le trafic pour sécuriser les données acheminées via les ports d'un groupe de ports distribués ou d'un groupe de ports de liaison montante.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer et réorganiser > Activer toutes les règles de trafic > OK**.
- 5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.
- 6 Dans la boîte de dialogue Règle de trafic réseau, définissez les options de la section Action pour autoriser ou interdire l'acheminement du trafic via les ports du groupe de ports distribués ou du groupe de ports de liaison montante.

7 Indiquez le type de trafic auquel la règle s'applique.

Pour déterminer si un flux de données se trouve dans l'étendue d'une règle pour le balisage ou le filtrage, le vSphere Distributed Switch examine le sens du trafic, ainsi que des propriétés telles que la source et la destination, le VLAN, le protocole du niveau suivant, le type de trafic d'infrastructure, etc.

- a Dans le menu déroulant **Sens du trafic**, choisissez si le trafic doit entrer, sortir ou les deux, afin que la règle le reconnaisse comme une correspondance.

Le sens influence aussi la manière dont vous allez identifier la source et la destination du trafic.

- b En utilisant des qualificateurs pour le type de données système, les attributs de paquet de la couche 2 et les attributs de paquet de la couche 3, définissez les propriétés que les paquets doivent posséder pour correspondre à la règle.

Un qualificateur représente un ensemble de critères de correspondance liés à une couche réseau. Vous pouvez faire correspondre le trafic au type de données système, aux propriétés de trafic de la couche 2 et aux propriétés de trafic de la couche 3. Vous pouvez utiliser un qualificateur pour une couche réseau spécifique ou combiner des qualificateurs pour faire correspondre les paquets de manière plus précise.

- Utilisez le qualificateur de trafic système pour faire correspondre les paquets au type des données d'infrastructure virtuelle qui sont transmises via les ports du groupe. Par exemple, vous pouvez sélectionner NFS pour les transferts de données vers un stockage réseau.
- Utilisez le qualificateur de trafic MAC pour faire correspondre les paquets par adresse MAC, ID VLAN et protocole du niveau suivant.

La recherche du trafic avec un ID VLAN sur un groupe de ports distribués fonctionne avec le balisage d'invité virtuel (VGT). Pour faire correspondre le trafic à l'ID VLAN si le balisage de commutateur virtuel (VST) est actif, utilisez une règle sur un groupe de ports de liaison montante ou un port de liaison montante.

- Utilisez le qualificateur de trafic IP pour faire correspondre les paquets par version IP, adresse IP et protocole et port du niveau suivant.

- 8 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Utilisation de règles de trafic réseau sur un groupe de ports distribués ou un groupe de ports de liaison montante

Définissez des règles de trafic dans un groupe de ports distribués ou un groupe de ports de liaison montante pour mettre en place une règle de traitement du trafic liée aux machines virtuelles

ou aux adaptateurs physiques. Vous pouvez filtrer un type de trafic spécifique ou décrire ses demandes QoS.

Note Vous pouvez remplacer les règles de filtrage et balisage du trafic au niveau du port. Reportez-vous à [Utilisation des règles de trafic réseau sur un port distribué ou un port de liaison montante](#).

- [Afficher les règles de trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Affichez les règles de trafic qui forment la règle de filtrage et de balisage du trafic dans un groupe de ports distribués ou un groupe de ports de liaisons montantes.

- [Modifier une règle de trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Créez ou modifiez des règles de trafic, et utilisez leurs paramètres pour configurer une règle de filtrage ou de balisage du trafic sur un groupe de ports distribués ou un groupe de ports de liaisons montantes.

- [Modifier les priorités de règles sur un groupe de ports distribués ou un groupe de ports de liaison montante](#)

Réorganisez les règles qui définissent la règle de filtrage et balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante afin de modifier l'ordre des actions réalisées lors du traitement du trafic.

- [Supprimer une règle de trafic sur un groupe de ports distribué ou un groupe de ports de liaison montante](#)

Supprimez une règle de trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante pour arrêter le traitement des paquets se dirigeant vers des machines virtuelles ou des adaptateurs physiques de manière spécifique.

Afficher les règles de trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Affichez les règles de trafic qui forment la règle de filtrage et de balisage du trafic dans un groupe de ports distribués ou un groupe de ports de liaisons montantes.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.

- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer et réorganiser > Activer toutes les règles de trafic > OK**.
- 5 Examinez **Action** pour voir si la règle filtre le trafic (autoriser ou annuler) ou marque le trafic (baliser) avec des demandes QoS spéciales.
- 6 Dans la liste supérieure, sélectionnez la règle pour laquelle vous souhaitez afficher les critères de recherche du trafic.

Les paramètres de qualification du trafic de la règle s'affichent dans la liste Qualificateurs de trafic.

Modifier une règle de trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Créez ou modifiez des règles de trafic, et utilisez leurs paramètres pour configurer une règle de filtrage ou de balisage du trafic sur un groupe de ports distribués ou un groupe de ports de liaisons montantes.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer et réorganiser > Activer toutes les règles de trafic > OK**.
- 5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.

Étape suivante

Attribuez un nom à la règle de trafic réseau, puis refusez, autorisez ou balisez le trafic cible.

Modifier les priorités de règles sur un groupe de ports distribués ou un groupe de ports de liaison montante

Réorganisez les règles qui définissent la règle de filtrage et balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante afin de modifier l'ordre des actions réalisées lors du traitement du trafic.

Le vSphere Distributed Switch applique les règles de trafic réseau dans un ordre strict. Si un paquet respecte déjà une règle, il peut ne pas être transmis à la règle suivante de la règle.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer toutes les règles de trafic** pour les activer.
- 6 Sélectionnez une règle et utilisez le bouton **Monter** ou **Descendre** pour modifier sa priorité.
- 7 Cliquez sur **OK** pour appliquer les modifications.

Supprimer une règle de trafic sur un groupe de ports distribué ou un groupe de ports de liaison montante

Supprimez une règle de trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante pour arrêter le traitement des paquets se dirigeant vers des machines virtuelles ou des adaptateurs physiques de manière spécifique.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic sont désactivés, cliquez sur **Activer et réorganiser > Activer toutes les règles de trafic > OK**.
- 5 Sélectionnez la règle et cliquez sur le bouton **Supprimer ..**

6 Cliquez sur **OK**.

Désactiver le filtrage et le marquage du trafic sur un groupe de ports distribués ou un groupe de ports de liaison montante

Autorisez l'acheminement du trafic vers les machines virtuelles ou les adaptateurs physiques sans contrôle supplémentaire de la sécurité ou de la qualité de service en désactivant les règles de filtrage et de balisage du trafic.

Note Vous pouvez activer et configurer les stratégies de filtrage et de balisage du trafic sur un port spécifique. Reportez-vous à [Activer le filtrage et le balisage du trafic d'un port distribué ou d'un port de liaison montante](#).

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupes de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez sur un groupe de ports distribués ou un groupe de ports de liaison montante, puis sélectionnez l'onglet **Configurer**.
- 3 Sous Paramètres, sélectionnez **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Utilisez le bouton bascule pour désactiver toutes les règles de trafic.
- 6 Cliquez sur **OK**.

Filtrage et marquage du trafic sur un port distribué ou un port de liaison montante

Vous pouvez filtrer le trafic ou décrire ses demandes QoS pour chaque machine virtuelle, adaptateur VMkernel ou adaptateur physique en configurant les règles de filtrage et de balisage du trafic sur un port distribué ou un port de liaison montante.

- [Activer le filtrage et le balisage du trafic d'un port distribué ou d'un port de liaison montante](#)

Activez la règle de filtrage et de balisage du trafic sur un port pour configurer la sécurité et le balisage du trafic sur un adaptateur réseau de la machine virtuelle, un adaptateur VMkernel ou un adaptateur de liaison montante. La stratégie de filtrage et de balisage du trafic ne prend pas en charge vSphere Distributed Switch configuré avec la Compatibilité des déchargements réseau.

- [Marquer le trafic sur un port distribué ou un port de liaison montante](#)

Attribuez des balises prioritaires dans une règle pour le trafic nécessitant un traitement spécial (par exemple, le trafic VoIP et le flux vidéo). Vous pouvez baliser le trafic d'une machine virtuelle, d'un adaptateur VMkernel ou d'un adaptateur physique en attribuant une balise CoS à la couche 2 de la pile de protocole réseau ou une balise DSCP à la couche 3.

- [Filtrer le trafic sur un port distribué ou un port de liaison montante](#)

À l'aide d'une règle, autorisez ou arrêtez le trafic pour sécuriser les flux de données via une machine virtuelle, un adaptateur VMkernel ou un adaptateur physique.

- [Utilisation des règles de trafic réseau sur un port distribué ou un port de liaison montante](#)

Définissez des règles de trafic dans un groupe de ports distribués ou de ports de liaison montante pour mettre en place une règle de traitement du trafic associé à une machine virtuelle ou à un adaptateur physique. Vous pouvez filtrer un type de trafic spécifique ou décrire ses demandes QoS.

- [Désactiver le filtrage et le marquage du trafic sur un port distribué ou un port de liaison montante](#)

Désactivez les règles de filtrage et de balisage du trafic sur un port pour autoriser l'acheminement du trafic à destination d'une machine virtuelle ou d'un adaptateur physique sans filtrage de sécurité, ni balisage de QoS.

Activer le filtrage et le balisage du trafic d'un port distribué ou d'un port de liaison montante

Activez la règle de filtrage et de balisage du trafic sur un port pour configurer la sécurité et le balisage du trafic sur un adaptateur réseau de la machine virtuelle, un adaptateur VMkernel ou un adaptateur de liaison montante. La stratégie de filtrage et de balisage du trafic ne prend pas en charge vSphere Distributed Switch configuré avec la Compatibilité des déchargements réseau.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.

- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Utilisez le bouton bascule pour remplacer les paramètres par défaut.
- 6 (Facultatif) Cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.

- 7 Cliquez sur **OK**.

Étape suivante

Configurez le filtrage et le balisage du trafic pour le flux de données via le port distribué ou le port de liaison montante. Reportez-vous aux sections [Marquer le trafic sur un port distribué ou un port de liaison montante](#) et [Filtrer le trafic sur un port distribué ou un port de liaison montante](#).

Marquer le trafic sur un port distribué ou un port de liaison montante

Attribuez des balises prioritaires dans une règle pour le trafic nécessitant un traitement spécial (par exemple, le trafic VoIP et le flux vidéo). Vous pouvez baliser le trafic d'une machine virtuelle, d'un adaptateur VMkernel ou d'un adaptateur physique en attribuant une balise CoS à la couche 2 de la pile de protocole réseau ou une balise DSCP à la couche 3.

Le balisage prioritaire est un mécanisme qui permet de baliser le trafic pour lequel les demandes QoS sont plus élevées. Le réseau peut ainsi reconnaître les différentes classes de trafic. Les périphériques réseau peuvent gérer le trafic de chaque classe en fonction de ses priorités et de ses critères.

Vous pouvez aussi baliser à nouveau le trafic afin d'augmenter ou de réduire l'importance du flux. L'utilisation d'une balise QoS faible vous permet de limiter les données balisées dans un système d'exploitation invité.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.

- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, cliquez sur le bouton Activer et réorganiser, remplacez les paramètres par défaut et cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.

- 5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.

Vous pouvez modifier une règle héritée du groupe de ports distribués ou du groupe de ports de liaison montante. Ainsi, la règle devient unique dans l'étendue du port.

- 6 Dans la boîte de dialogue de la règle de trafic réseau, sélectionnez l'option **Balise** dans le menu déroulant **Action**.
- 7 Définissez la balise de priorité du trafic dans l'étendue de la règle.

Option	Description
Valeur CoS	Marquez le trafic correspondant à la règle avec une balise de priorité CoS dans la couche réseau 2. Cochez la case et tapez une valeur comprise entre 0 et 7.
Valeur DSCP	Marquez le trafic associé à la règle avec une balise DSCP dans la couche réseau 3. Cocher la case et tapez une valeur comprise entre 0 et 63.

8 Indiquez le type de trafic auquel la règle s'applique.

Pour déterminer si un flux de données se trouve dans l'étendue d'une règle pour le balisage ou le filtrage, le vSphere Distributed Switch examine le sens du trafic, ainsi que des propriétés telles que la source et la destination, le VLAN, le protocole du niveau suivant, le type de trafic d'infrastructure, etc.

- a Dans le menu déroulant **Sens du trafic**, choisissez si le trafic doit entrer, sortir ou les deux, afin que la règle le reconnaisse comme une correspondance.

Le sens influence aussi la manière dont vous allez identifier la source et la destination du trafic.

- b En utilisant des qualificateurs pour le type de données système, les attributs de paquet de la couche 2 et les attributs de paquet de la couche 3, définissez les propriétés que les paquets doivent posséder pour correspondre à la règle.

Un qualificateur représente un ensemble de critères de correspondance liés à une couche réseau. Vous pouvez faire correspondre le trafic au type de données système, aux propriétés de trafic de la couche 2 et aux propriétés de trafic de la couche 3. Vous pouvez utiliser un qualificateur pour une couche réseau spécifique ou combiner des qualificateurs pour faire correspondre les paquets de manière plus précise.

- Utilisez le qualificateur de trafic système pour faire correspondre les paquets au type des données d'infrastructure virtuelle qui sont transmises via les ports du groupe. Par exemple, vous pouvez sélectionner NFS pour les transferts de données vers un stockage réseau.
- Utilisez le qualificateur de trafic MAC pour faire correspondre les paquets par adresse MAC, ID VLAN et protocole du niveau suivant.

La recherche du trafic avec un ID VLAN sur un groupe de ports distribués fonctionne avec le balisage d'invité virtuel (VGT). Pour faire correspondre le trafic à l'ID VLAN si le balisage de commutateur virtuel (VST) est actif, utilisez une règle sur un groupe de ports de liaison montante ou un port de liaison montante.

- Utilisez le qualificateur de trafic IP pour faire correspondre les paquets par version IP, adresse IP et protocole et port du niveau suivant.

- 9 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Filtrer le trafic sur un port distribué ou un port de liaison montante

À l'aide d'une règle, autorisez ou arrêtez le trafic pour sécuriser les flux de données via une machine virtuelle, un adaptateur VMkernel ou un adaptateur physique.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.

2 Sélectionnez un port de la liste.

3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.

4 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, cliquez sur le bouton Activer et réorganiser, remplacez les paramètres par défaut et cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.

5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.

Vous pouvez modifier une règle héritée du groupe de ports distribués ou du groupe de ports de liaison montante. Ainsi, la règle devient unique dans l'étendue du port.

6 Dans la boîte de dialogue de la règle de trafic réseau, sélectionnez l'action **Autoriser** pour autoriser le trafic à passer par le port distribué ou le port de liaison montante ou l'action **Annuler** pour le restreindre.

7 Indiquez le type de trafic auquel la règle s'applique.

Pour déterminer si un flux de données se trouve dans l'étendue d'une règle pour le balisage ou le filtrage, le vSphere Distributed Switch examine le sens du trafic, ainsi que des propriétés telles que la source et la destination, le VLAN, le protocole du niveau suivant, le type de trafic d'infrastructure, etc.

- a Dans le menu déroulant **Sens du trafic**, choisissez si le trafic doit entrer, sortir ou les deux, afin que la règle le reconnaisse comme une correspondance.

Le sens influence aussi la manière dont vous allez identifier la source et la destination du trafic.

- b En utilisant des qualificateurs pour le type de données système, les attributs de paquet de la couche 2 et les attributs de paquet de la couche 3, définissez les propriétés que les paquets doivent posséder pour correspondre à la règle.

Un qualificateur représente un ensemble de critères de correspondance liés à une couche réseau. Vous pouvez faire correspondre le trafic au type de données système, aux propriétés de trafic de la couche 2 et aux propriétés de trafic de la couche 3. Vous pouvez utiliser un qualificateur pour une couche réseau spécifique ou combiner des qualificateurs pour faire correspondre les paquets de manière plus précise.

- Utilisez le qualificateur de trafic système pour faire correspondre les paquets au type des données d'infrastructure virtuelle qui sont transmises via les ports du groupe. Par exemple, vous pouvez sélectionner NFS pour les transferts de données vers un stockage réseau.
- Utilisez le qualificateur de trafic MAC pour faire correspondre les paquets par adresse MAC, ID VLAN et protocole du niveau suivant.

La recherche du trafic avec un ID VLAN sur un groupe de ports distribués fonctionne avec le balisage d'invité virtuel (VGT). Pour faire correspondre le trafic à l'ID VLAN si le balisage de commutateur virtuel (VST) est actif, utilisez une règle sur un groupe de ports de liaison montante ou un port de liaison montante.

- Utilisez le qualificateur de trafic IP pour faire correspondre les paquets par version IP, adresse IP et protocole et port du niveau suivant.

- 8 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Utilisation des règles de trafic réseau sur un port distribué ou un port de liaison montante

Définissez des règles de trafic dans un groupe de ports distribués ou de ports de liaison montante pour mettre en place une règle de traitement du trafic associé à une machine virtuelle ou à un adaptateur physique. Vous pouvez filtrer un type de trafic spécifique ou décrire ses demandes QoS.

- [Afficher les règles de trafic sur un port distribué ou un port de liaison montante](#)

Vérifiez les règles de trafic qui forment la règle de filtrage et de balisage du trafic d'un port distribué ou d'un port de liaison montante.

- **Modifier une règle de trafic sur un port distribué ou un port de liaison montante**

Créez ou modifiez les règles de trafic, et utilisez leurs paramètres pour configurer une règle de filtrage ou de balisage du trafic sur un port distribué ou un port de liaison montante.

- **Modifier les priorités de règles sur un port distribué ou un port de liaison montante**

Réordonnez les règles qui forment la règle de filtrage et de balisage du trafic d'un port distribué ou d'un port de liaison montante afin de changer la séquence des actions d'analyse du trafic pour la sécurité et QoS.

- **Supprimer une règle de trafic sur un port distribué ou un port de liaison montante**

Supprimez une règle de trafic d'un port distribué ou d'un port de liaison montante pour arrêter le filtrage ou le balisage d'un certain type de paquets se dirigeant vers une machine virtuelle ou un adaptateur physique.

Afficher les règles de trafic sur un port distribué ou un port de liaison montante

Vérifiez les règles de trafic qui forment la règle de filtrage et de balisage du trafic d'un port distribué ou d'un port de liaison montante.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, cliquez sur le bouton Activer et réorganiser, remplacez les paramètres par défaut et cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.
- 5 Examinez **Action** pour voir si la règle filtre le trafic (autoriser ou annuler) ou marque le trafic (baliser) avec des demandes QoS spéciales.

- 6 Dans la liste supérieure, sélectionnez la règle pour laquelle vous souhaitez afficher les critères de recherche du trafic.

Les paramètres de qualification du trafic de la règle s'affichent dans la liste Qualificateurs de trafic.

Modifier une règle de trafic sur un port distribué ou un port de liaison montante

Créez ou modifiez les règles de trafic, et utilisez leurs paramètres pour configurer une règle de filtrage ou de balisage du trafic sur un port distribué ou un port de liaison montante.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, cliquez sur le bouton Activer et réorganiser, remplacez les paramètres par défaut et cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.

- 5 Cliquez sur **Ajouter** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour la modifier.

Vous pouvez modifier une règle héritée du groupe de ports distribués ou du groupe de ports de liaison montante. Ainsi, la règle devient unique dans l'étendue du port.

Étape suivante

Attribuez un nom à la règle de trafic réseau, puis refusez, autorisez ou balisez le trafic cible.

Modifier les priorités de règles sur un port distribué ou un port de liaison montante

Réordonnez les règles qui forment la règle de filtrage et de balisage du trafic d'un port distribué ou d'un port de liaison montante afin de changer la séquence des actions d'analyse du trafic pour la sécurité et QoS.

Le vSphere Distributed Switch applique les règles de trafic réseau dans un ordre strict. Si un paquet respecte déjà une règle, il peut ne pas être transmis à la règle suivante de la règle.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, remplacez les paramètres par défaut et cliquez sur Activer toutes les règles de trafic.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.
- 6 Sélectionnez une règle et utilisez le bouton **Monter** ou **Descendre** pour modifier sa priorité.
- 7 Cliquez sur **OK** pour appliquer les modifications.

Supprimer une règle de trafic sur un port distribué ou un port de liaison montante

Supprimez une règle de trafic d'un port distribué ou d'un port de liaison montante pour arrêter le filtrage ou le balisage d'un certain type de paquets se dirigeant vers une machine virtuelle ou un adaptateur physique.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic ne sont pas activés au niveau du port, cliquez sur le bouton Activer et réorganiser, remplacez les paramètres par défaut et cliquez sur **Activer toutes les règles de trafic**.

Si les règles de trafic sont activées au niveau du groupe, une fois que vous avez remplacé les paramètres par défaut du port, les règles de trafic sont automatiquement activées.
- 5 Sélectionnez la règle puis cliquez sur le bouton **Supprimer**.
- 6 Cliquez sur **OK**.

Désactiver le filtrage et le marquage du trafic sur un port distribué ou un port de liaison montante

Désactivez les règles de filtrage et de balisage du trafic sur un port pour autoriser l'acheminement du trafic à destination d'une machine virtuelle ou d'un adaptateur physique sans filtrage de sécurité, ni balisage de QoS.

Conditions préalables

Pour remplacer une stratégie au niveau d'un port distribué, activez l'option de remplacement au niveau du port de cette stratégie. Reportez-vous à la section [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#).

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.

- 2 Sélectionnez un port de la liste.
- 3 Sélectionnez l'onglet **Filtrage et balisage du trafic**.
- 4 Cliquez sur le bouton **Activer et réorganiser**.
- 5 Utilisez les boutons bascule pour remplacer les paramètres par défaut au niveau du port et désactiver toutes les règles de trafic.
- 6 Cliquez sur **OK**.

Qualification du trafic pour le filtrage et le balisage

Le trafic à filtrer ou à marquer à l'aide de balises QoS peut être mis en correspondance avec le type des données d'infrastructure transportées, telles que les données de stockage, la gestion vCenter Server, etc., et avec les propriétés des couches 2 et 3.

Pour faire correspondre le trafic dans l'étendue de la règle de manière plus précise, vous pouvez combiner des critères pour le type de données système, l'en-tête de la couche 2 et l'en-tête de la couche 3.

Qualificateur de trafic système

L'utilisation du qualificateur de trafic système dans une règle de port ou de groupe de ports permet de déterminer si un type de trafic de données système spécifique doit être associé à une balise QoS, autorisé ou abandonné.

Type de trafic système

Vous pouvez sélectionner le type de trafic devant transporter les données système acheminées via les ports du groupe, c'est-à-dire le trafic de gestion depuis vCenter Server, de stockage, VMware vSphere[®] vMotion[®] et vSphere Fault Tolerance. Vous pouvez baliser ou filtrer un type de trafic spécifique ou l'ensemble du trafic de données système, à l'exception du trafic d'une fonction d'infrastructure. Par exemple, vous pouvez appliquer une balise QoS ou un filtre au trafic de gestion depuis vCenter Server, au trafic de stockage et au trafic vMotion, mais pas aux données Fault Tolerance.

Qualificateur de trafic MAC

L'utilisation du qualificateur de trafic MAC dans une règle vous permet de définir des critères de correspondance de trafic pour les propriétés de la couche 2 (couche de liaison de données) des paquets, tels que l'adresse MAC, l'ID VLAN et le protocole de niveau suivant qui consomme la charge utile de trame.

Type de protocole

L'attribut **Type de protocole** du qualificateur de trafic MAC correspond au champ EtherType des trames Ethernet. EtherType désigne le type de protocole suivant qui va consommer la charge utile de la trame.

Vous pouvez sélectionner un protocole dans le menu déroulant ou entrer son code hexadécimal. Par exemple, pour capturer le trafic du protocole LLDP (Link Layer Discovery Protocol), tapez **88CC**.

ID VLAN

Vous pouvez utiliser l'attribut ID VLAN du qualificateur de trafic MAC pour baliser ou filtrer le trafic sur un VLAN spécifique.

Note Le qualificateur ID VLAN d'un groupe de ports distribués fonctionne avec le balisage d'invité virtuel (VGT).

Si un flux est balisé avec un ID VLAN via le balisage de commutateur virtuel (VST), il est impossible de le localiser en utilisant cet ID dans une règle sur un groupe de ports distribués ou un port distribué. En effet, le commutateur distribué vérifie les conditions de la règle, notamment l'ID VLAN, après que le commutateur a déjà annulé le balisage du trafic. En l'occurrence, pour réussir à faire correspondre le trafic en fonction de l'ID VLAN, vous devez utiliser une règle sur un groupe de ports de liaison montante ou sur un port de liaison montante.

Adresse source

L'utilisation du groupe d'attributs Adresse source vous permet de faire correspondre des paquets en fonction du réseau ou de l'adresse MAC source.

Vous pouvez utiliser un opérateur de comparaison pour baliser ou filtrer des paquets, qu'ils disposent ou non de l'adresse ou du réseau source spécifié.

Il existe différentes manières de faire correspondre la source du trafic.

Tableau 8-6. Modèles de filtrage ou de balisage du trafic en fonction de l'adresse source MAC

Paramètres de correspondance de l'adresse source du trafic	Opérateur de comparaison	Format d'argument de mise en réseau
Adresse MAC	est ou n'est pas	Indiquez l'adresse MAC à faire correspondre. Séparez les octets en utilisant deux points « : ».
Réseau MAC	correspond ou ne correspond pas	Indiquez l'adresse la plus petite du réseau et un masque. Définissez des uns à l'emplacement des bits de réseau et des zéros pour la partie hôte.

Par exemple, pour un réseau MAC associé au préfixe 05:50:56 et d'une longueur de 23 bits, définissez l'adresse sur **00:50:56:00:00:00** et le masque sur **ff:ff:fe:00:00:00**.

Adresse de destination

En utilisant le groupe d'attributs Adresse de destination, vous pouvez faire correspondre les paquets en fonction de leur adresse de destination. Le format des options d'adresse de destination MAC est identique à celui des options d'adresse source.

Opérateurs de comparaison

Pour personnaliser la correspondance du trafic d'un qualificateur MAC selon vos besoins, vous pouvez utiliser la comparaison affirmative ou la négation. Vous pouvez définir les opérateurs de sorte que tous les paquets à l'exception de ceux associés à certains attributs répondent aux critères d'une règle.

Qualificateur de trafic IP

L'utilisation du qualificateur de trafic IP dans une règle vous permet de définir des critères de correspondance du trafic pour les propriétés de la couche 3 (couche réseau), telles que la version IP, l'adresse IP, le protocole de niveau suivant et le port.

Protocole

L'attribut **Protocole** du qualificateur de trafic IP représente le protocole de niveau suivant consommant la charge utile du paquet. Vous pouvez sélectionner un protocole dans le menu déroulant ou taper son code décimal en fonction de la RFC 1700.

Pour les protocoles TCP et UDP, vous pouvez également faire correspondre le trafic en fonction des ports source et de destination.

Port source

À l'aide de l'attribut de port Source, vous pouvez faire correspondre des paquets TCP ou UDP en fonction du port source. Tenez compte de la direction du trafic lorsque vous faites correspondre le trafic à un port source.

Port de destination

À l'aide de l'attribut de port Destination, vous pouvez faire correspondre des paquets TCP ou UDP en fonction du port de destination. Tenez compte de la direction du trafic lorsque vous faites correspondre le trafic à un port de destination.

Adresse source

À l'aide de l'attribut Adresse source, vous pouvez faire correspondre des paquets en fonction de l'adresse ou du sous-réseau source. Tenez compte de la direction du trafic lorsque vous faites correspondre le trafic à une adresse ou un réseau source.

Il existe différentes manières de faire correspondre la source du trafic.

Tableau 8-7. Modèles de filtrage ou de balisage du trafic en fonction de l'adresse IP source

Paramètres de correspondance de l'adresse source du trafic	Opérateur de comparaison	Format d'argument de mise en réseau
Version IP	n'importe	Sélectionnez la version IP dans le menu déroulant.
adresse IP	est ou n'est pas	Tapez l'adresse IP à faire correspondre.
Sous-réseau IP	correspond ou ne correspond pas	Tapez l'adresse la plus basse du sous-réseau, ainsi que la longueur en bits du préfixe de sous-réseau.

Adresse de destination

Utilisez l'adresse de destination pour faire correspondre les paquets en fonction de l'adresse IP, du sous-réseau ou de la version IP. Le format de l'adresse de destination est le même que celui de l'adresse source.

Opérateurs de comparaison

Pour personnaliser la correspondance du trafic d'un qualificateur IP selon vos besoins, vous pouvez utiliser la comparaison affirmative ou la négation. Vous pouvez définir que tous les paquets, à l'exception de ceux associés à certains attributs, répondent aux critères d'une règle.

Gérer les règles pour plusieurs groupes de ports sur vSphere Distributed Switch

Vous pouvez modifier les stratégies de mise en réseau de plusieurs groupes de ports sur vSphere Distributed Switch.

Conditions préalables

Créez vSphere Distributed Switch avec un ou plusieurs groupes de ports.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le commutateur distribué dans le navigateur d'objets et sélectionnez **Groupe de ports distribués > Gérer des groupes de ports distribués**.

- 3 Sur la page Sélectionner les règles de groupe de ports, cochez la case à côté des catégories de stratégies à modifier et cliquez sur **Suivant**.

Option	Description
Sécurité	Définissez les modifications d'adresse MAC, les transmissions frauduleuses et le mode promiscuité des groupes de ports sélectionnés.
Formation du trafic	Définissez la bande passante moyenne, la bande passante maximale et la taille de rafale du trafic entrant et du trafic sortant dans les groupes de ports sélectionnés.
VLAN	Indiquez comment les groupes de ports sélectionnés se connectent aux réseaux VLAN physiques.
Association et basculement	Définissez l'équilibrage de charge, la détection du basculement, la notification de commutation et l'ordre de basculement des groupes de ports sélectionnés.
Allocation des ressources	Définissez l'association de pool de ressources réseau des groupes de ports sélectionnés.
Surveillance	Activez ou désactivez NetFlow sur les groupes de ports sélectionnés.
Divers	Activez ou désactivez le blocage de port dans les groupes de ports sélectionnés.

- 4 Sur la page Sélectionner groupes de ports, sélectionnez le(s) groupe(s) de ports distribués à modifier et cliquez sur **Suivant**.
- 5 (Facultatif) Sur la page Sécurité, utilisez les menus déroulants pour modifier les exceptions de sécurité et cliquez sur **Suivant**.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ Rejeter. Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit. ■ Accepter. L'activation du mode promiscuité sur un adaptateur invité permet de détecter toutes les trames transmises à vSphere Distributed Switch qui sont autorisées par la stratégie VLAN pour le groupe de ports auquel l'adaptateur est connecté.
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ Rejeter. S'il est défini sur Rejeter et si le système d'exploitation invité modifie l'adresse MAC de l'adaptateur par une autre ne figurant pas dans le fichier de configuration <code>.vmmx</code>, toutes les trames entrantes sont abandonnées. <p>Si le système d'exploitation invité recharge l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration <code>.vmmx</code>, les trames entrantes sont de nouveau transmises.</p> <ul style="list-style-type: none"> ■ Accepter. Le changement d'adresse MAC dans le SE invité a l'effet prévu. Les trames envoyées à la nouvelle adresse MAC sont reçues.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter. Toutes les trames sortantes dont l'adresse MAC source est différente de celle définie sur l'adaptateur sont abandonnées. ■ Accepter. Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

- 6 (Facultatif) Sur la page VLAN, utilisez les menus déroulants pour modifier la stratégie VLAN et cliquez sur **Suivant**.

Option	Description
Aucun	N'utilise pas de VLAN.
VLAN	Dans le champ ID VLAN , entrez un nombre entre 1 et 4094.
Jonction VLAN	Entrez une plage de jonctions VLAN dans Intervalle de joncteur réseau VLAN .
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

- 7 (Facultatif) Sur la page Formation du trafic, utilisez les menus déroulants pour activer ou désactiver la formation de trafic d'entrée ou de sortie et cliquez sur **Suivant**.

Option	Description
État	Si vous activez la Formation du trafic d'entrée ou la Formation du trafic de sortie , vous limitez l'allocation de bande passante de mise en réseau pour chaque adaptateur VMkernel ou adaptateur réseau virtuel associé à ce groupe de ports. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique par défaut.
Bande passante moyenne	Définit le nombre de bits moyen par seconde à autoriser sur un port, une moyenne sur une période donnée, c'est à dire la charge moyenne autorisée.
Bande passante maximale	Nombre maximal d'octets par seconde à autoriser à travers un port quand il reçoit ou envoie une rafale de trafic. Ce nombre maximal limite la bande passante utilisée par un port lorsqu'il utilise son bonus de rafale.
Taille de rafale	Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin de plus de bande passante que la quantité spécifiée par Bande passante moyenne , il peut être autorisé à transmettre des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre s'ajoute au nombre d'octets qui peuvent être accumulés dans le bonus de rafale et transféré à une vitesse plus élevée.

8 (Facultatif) Sur la page Association et basculement, utilisez les menus déroulants pour modifier les paramètres et cliquez sur **Suivant**.

Option	Description
Équilibrage de charge	<p>L'association basée sur IP exige que le commutateur physique soit configuré avec ether channel. Pour toutes les autres options, ether channel doit être désactivé. Indiquez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> ■ Route basée sur le port virtuel d'origine. Choisissez une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur distribué. ■ Route basée sur le hachage IP. Choisissez une liaison montante en fonction d'un hachage des adresses IP de source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ Route basée sur le hachage MAC source. Choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ Route basée sur la charge de carte réseau physique. Choisissez une liaison montante basée sur les charges actuelles des cartes réseau physiques. ■ Utiliser la commande de basculement explicite. Toujours utiliser la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui vérifient les critères de détection du basculement.
Détection de panne réseau	<p>Sélectionnez la méthode à utiliser pour la détection de basculement.</p> <ul style="list-style-type: none"> ■ État de lien seulement. Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les pannes, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ Sondage balise. Envoie et détecte des sondes d'incident sur toutes les cartes réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.
Notifier les commutateurs	<p>Sélectionnez Oui ou Non pour notifier les commutateurs en cas de basculement. N'utilisez pas cette option quand les machines virtuelles utilisant le groupe de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion.</p> <p>Si vous sélectionnez Oui, chaque fois qu'une carte réseau virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte réseau physique différente dans l'association suite à un basculement, une notification est envoyée sur le réseau pour mettre à jour les tables de recherche des commutateurs physiques. Utilisez ce processus pour obtenir la latence la plus faible des occurrences de basculement avec vMotion.</p>

Option	Description
Retour arrière	<p>Sélectionnez Oui ou Non pour mettre hors tension ou activer le retour arrière.</p> <p>Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec.</p> <ul style="list-style-type: none"> ■ Oui (par défaut). L'adaptateur est ramené au service actif immédiatement après la récupération, en déplaçant l'adaptateur en attente éventuel ayant repris son emplacement. ■ Non. Un adaptateur ayant échoué est laissé inactif même après la récupération jusqu'à ce qu'un autre adaptateur actuellement actif échoue, exigeant un remplacement.
Ordre de basculement	<p>Indiquez comment répartir la charge de travail pour les liaisons montantes. Pour utiliser certaines liaisons montantes mais en réserver d'autres si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes.</p> <ul style="list-style-type: none"> ■ Liaisons montantes actives. Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est disponible et en activité. ■ Liaisons montantes en veille. Utilisez cette liaison montante si la connectivité de l'un des adaptateurs actif est indisponible. En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve. ■ Liaisons montantes inutilisées. N'utilisez pas cette liaison montante.

9 (Facultatif) Sur la page Allocations des ressources, utilisez le menu déroulant **Pool de ressources réseau** pour ajouter ou retirer des allocations de ressources et cliquez sur **Suivant**.

10 (Facultatif) Sur la page Surveillance, utilisez le menu déroulant pour activer ou désactiver NetFlow et cliquez sur **Suivant**.

Option	Description
Désactivé	NetFlow est désactivé sur le groupe de ports distribués.
Activé	NetFlow est activé sur le groupe de ports distribués. Vous pouvez configurer les paramètres NetFlow au niveau de vSphere Distributed Switch.

11 (Facultatif) Sur la page Divers, sélectionnez **Oui** ou **Non** depuis le menu déroulant et cliquez sur **Suivant**.

Sélectionnez **Oui** pour éteindre tous les ports dans le groupe de ports. Cet arrêt risque de perturber les opérations normales du réseau des hôtes ou des machines virtuelles qui utilisent les ports

12 Passez en revue les paramètres sur la page Prêt à terminer et cliquez sur **Terminer**.

Utilisez le bouton **Précédent** pour modifier les paramètres.

Règles de blocage des ports

Les règles de blocage des ports vous permettent d'empêcher les ports de votre choix d'envoyer ou de recevoir des données.

Modifier la règle de blocage des ports d'un groupe de ports distribués

Vous pouvez bloquer tous les ports d'un groupe de ports distribués.

Le blocage des ports d'un groupe de ports distribués peut perturber les opérations réseau normales des hôtes ou des machines virtuelles qui utilisent les ports.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le commutateur distribué dans le navigateur d'objets et sélectionnez **Groupe de ports distribués > Gérer des groupes de ports distribués**.
- 3 Cochez la case **Divers** et cliquez sur **Suivant**.
- 4 Sélectionnez le ou les groupes de ports distribués à configurer et cliquez sur **Suivant**.
- 5 Dans le menu déroulant **Bloquer tous les ports**, activez ou désactivez le blocage des ports, puis cliquez sur **Suivant**.
- 6 Vérifiez les paramètres et cliquez sur **Terminer**.

Modifier la stratégie de blocage d'un port distribué ou d'un port de liaison montante

Vous pouvez bloquer un port distribué ou un port de liaison montante individuel.

Le blocage du flux d'un port peut perturber les opérations normales du réseau sur l'hôte ou la machine virtuelle utilisant le port.

Conditions préalables

Activer les remplacements à niveau du port Reportez-vous à [Configurer le remplacement des stratégies de mise en réseau au niveau des ports](#)

Procédure

- 1 Accédez à un commutateur distribué, puis accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Réseaux > Groupes de ports distribués**, cliquez sur un groupe de ports distribués dans la liste et enfin cliquez sur l'onglet **Ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Réseaux > Groupes de ports de liaison montante**, cliquez sur un groupe de ports de liaison montante dans la liste, puis cliquez sur l'onglet **Ports**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres du port distribué**.

- 4 Dans la section **Divers**, cochez la case **Remplacer**, puis activez ou désactivez le blocage de port dans le menu déroulant.
- 5 Cliquez sur **OK**.

Présentation de la stratégie d'apprentissage MAC

L'apprentissage MAC fournit une connectivité réseau aux déploiements où plusieurs adresses MAC sont utilisées à partir d'une vNIC.

Par exemple, dans un déploiement d'hyperviseur imbriqué où une machine virtuelle ESXi s'exécute sur un hôte ESXi et où plusieurs machines virtuelles s'exécutent à l'intérieur de la machine virtuelle ESXi. Sans l'apprentissage MAC, lorsque la vNIC de la machine virtuelle ESXi se connecte à un port de commutateur, elle contient uniquement une adresse MAC 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 dans sa table MAC et autorise le paquet à passer. Si une adresse MAC apprise n'est pas utilisée pendant un certain temps, elle est supprimée.

L'apprentissage MAC prend également en charge la propagation monodiffusion inconnue. Normalement, lorsqu'un paquet reçu par un port a une adresse MAC de destination inconnue, le paquet 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, selon le port, cette valeur est prise par défaut. Vous pouvez également définir la stratégie pour le moment auquel la limite est atteinte. Les options sont :

- **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.

Dans vSphere 6.7 et versions ultérieures, l'apprentissage MAC peut être activé sur un groupe de ports virtuels distribués à l'aide de vSphere API. Vous pouvez configurer la stratégie d'apprentissage MAC sur vSphere Distributed Switch, le groupe de ports virtuels distribués et le port virtuel distribué. Si une stratégie d'apprentissage MAC n'est pas définie sur le groupe de ports virtuels distribués, elle est héritée de vSphere Distributed Switch et, si elle n'est pas activée sur le DVport, elle est héritée du groupe de ports virtuels distribués. Consultez *Référence de l'API vSphere Web Services*.

Utilisation de VLAN pour isoler le trafic réseau

9

Les VLAN vous permettent de segmenter un réseau en plusieurs domaines de diffusion logiques sur la couche 2 de la pile de protocole réseau.

Ce chapitre contient les rubriques suivantes :

- [Configuration VLAN](#)
- [VLAN privés](#)

Configuration VLAN

Les réseaux VLAN (réseaux LAN virtuels) permettent à un segment LAN physique unique d'être davantage isolé, de sorte que des groupes de ports soient isolés les uns des autres comme s'ils se trouvaient sur des segments physiquement différents.

Avantages de l'utilisation des VLAN dans vSphere

La configuration VLAN dans un environnement vSphere procure certains avantages.

- Intègre des hôtes ESXi dans une topologie VLAN préexistante.
- Isole et sécurise le trafic réseau.
- Réduit la congestion du trafic réseau.

Regardez la vidéo sur les avantages et les principes essentiels de l'introduction de VLAN dans un environnement vSphere.



(Utilisation de VLAN dans un environnement vSphere)

Modes de balisage VLAN

vSphere prend en charge trois modes de balisage VLAN dans ESXi : le balisage de commutateur externe (EST, External Switch Tagging), le balisage de commutateur virtuel (VST, Virtual Switch Tagging) et le balisage d'invité virtuel (VGT, Virtual Guest Tagging).

Mode de balisage	ID VLAN sur groupes de ports de commutateur	Description
EST	0	Le commutateur physique effectue le balisage VLAN. Les adaptateurs réseau hôtes sont connectés aux ports d'accès sur le commutateur physique.
VST (balisage de commutateur virtuel)	Entre 1 et 4094	Le commutateur virtuel effectue le balisage VLAN avant que les paquets ne quittent l'hôte. Les adaptateurs réseau hôtes doivent être connectés aux ports de jonction sur le commutateur physique.
VGT	<ul style="list-style-type: none"> ■ 4095 pour un commutateur standard ■ Plage et VLAN individuel pour un commutateur distribué 	<p>La machine virtuelle effectue le balisage VLAN. Le commutateur virtuel conserve les balises VLAN lorsqu'il transfère les paquets entre la pile de mise en réseau de la machine virtuelle et le commutateur externe. Les adaptateurs réseau hôtes doivent être connectés aux ports de jonction sur le commutateur physique.</p> <p>vSphere Distributed Switch prend en charge la modification de VGT. Pour des raisons de sécurité, vous pouvez configurer un commutateur distribué pour transmettre uniquement les paquets qui appartiennent à des VLAN particuliers.</p> <p>Note Pour VGT, assurez-vous qu'un pilote de jonction VLAN 802.1Q est installé sur le système d'exploitation invité de la machine virtuelle.</p>

Regardez la vidéo qui explique les modes de balisage VLAN dans les commutateurs virtuels.



(Modes de balisage VLAN dans vSphere)

VLAN privés

Les VLAN privés servent à résoudre les restrictions d'ID VLAN en ajoutant une segmentation supplémentaire du domaine de diffusion logique à plusieurs sous-domaines de diffusion plus petits.

Un VLAN privé est identifié par son ID VLAN primaire. un ID VLAN primaire peut avoir plusieurs ID VLAN associées. Les VLAN primaires sont **Promiscuité**, afin que les ports sur un VLAN privé puissent communiquer avec des ports configurés en tant que VLAN primaire. Des ports sur un VLAN secondaire peuvent être **Isolé** et communiquer uniquement avec des ports de promiscuité, ou **Communauté** et communiquer avec des ports de promiscuité et d'autres ports sur le même VLAN secondaire.

Pour utiliser des VLAN privés entre un hôte et le reste du réseau physique, le commutateur physique connecté à l'hôte doit être un VLAN privé compatible et configuré avec les ID VLAN utilisés par ESXi pour la fonctionnalité VLAN privée. Pour les commutateurs physiques utilisant un apprentissage par ID VLAN+MAC dynamique, toutes les ID VLAN privé correspondantes doivent être d'abord entrées dans la base de données VLAN du commutateur.

Créer un VLAN privé

Créez les VLAN privés nécessaires sur le vSphere Distributed Switch pour pouvoir attribuer Les ports distribués à inclure dans un VLAN.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **VLAN privé**.
- 3 Cliquez sur **Modifier**.
- 4 Pour ajouter un VLAN primaire, au-dessus de l'ID du VLAN primaire, cliquez sur le bouton **signe plus (+)**.

Ce VLAN privé primaire apparaît également sous l'ID du VLAN privé secondaire.

- 5 Pour ajouter un VLAN secondaire, dans le volet de droite, cliquez sur le bouton **signe plus (+)**.
- 6 Dans le menu déroulant de la colonne **Type de VLAN secondaire**, sélectionnez **Isolé** ou **Communauté**.
- 7 Cliquez sur **OK**.

Étape suivante

Configurez un port distribué ou un groupe de ports distribués pour associer le trafic au réseau VLAN privé. Reportez-vous à la section [Configurer le balisage VLAN sur un port distribué ou un groupe de ports distribués](#).

Supprimer un VLAN privé principal

Supprimez les VLAN principaux inutilisés de la configuration d'un vSphere Distributed Switch.

Lorsque vous supprimez un VLAN privé principal, vous supprimez également les VLAN privés secondaires associés.

Conditions préalables

Vérifiez qu'aucun groupe de ports n'est configuré pour utiliser le VLAN principal et ses VLAN secondaires associés.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **VLAN privé**.
- 3 Cliquez sur **Modifier**.
- 4 Sélectionnez le VLAN privé principal à supprimer.
- 5 Cliquez sur le bouton **x dans cercle (x)** au-dessus de la liste des ID VLAN principaux.
- 6 Cliquez sur **OK**.

Supprimer un VLAN privé secondaire

Supprimez les VLAN privés secondaires inutilisés de la configuration d'un vSphere Distributed Switch.

Conditions préalables

Vérifiez qu'aucun groupe de ports n'est configuré pour utiliser le VLAN secondaire.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **VLAN privé**.
- 3 Cliquez sur **Modifier**.
- 4 Sélectionnez un VLAN privé principal.
Les VLAN privés secondaires associés avec lui s'affichent à droite.
- 5 Sélectionnez le VLAN privé secondaire à supprimer.
- 6 Supérieure la liste d'ID de VLAN secondaire, cliquez sur le bouton **x dans cercle (x)** . puis cliquez sur **OK**.

vSphere propose plusieurs méthodes différentes pour vous aider à gérer vos ressources réseau.

Ce chapitre contient les rubriques suivantes :

- DirectPath I/O
- Présentation de la virtualisation des E/S à racine unique (SR-IOV)
- Technologie RDMA (Remote Direct Memory Access) pour machines virtuelles
- Configurer des adaptateurs réseau RDMA
- Trames jumbo
- délestage de segmentation TCP
- LRO (Large Receive Offload)
- NetQueue et performances réseau

DirectPath I/O

DirectPath I/O permet à une machine virtuelle d'accéder aux fonctions physiques PCI sur les plates-formes avec une unité de gestion de mémoire E/S.

Les fonctionnalités suivantes ne sont pas disponibles pour les machines virtuelles configurées avec DirectPath :

- Retrait ou ajout à chaud de périphériques virtuels
- Interruption et reprise
- Enregistrement et lecture
- Tolérance aux pannes
- Haute disponibilité
- DRS (disponibilité limitée. La machine virtuelle peut faire partie d'un cluster, mais pas migrer à travers des hôtes)

- Snapshots
- [Activer le relais d'un périphérique réseau sur un hôte](#)
 Les périphériques de relais peuvent fournir les moyens nécessaires pour utiliser plus efficacement les ressources et améliorer la performances de votre environnement. Vous pouvez activer un relais DirectPath I/O pour un périphérique réseau sur un hôte.
- [Configurer un périphérique PCI sur une machine virtuelle](#)
 Les périphériques de relais peuvent fournir les moyens d'utiliser plus efficacement les ressources et d'améliorer la performance de votre environnement. Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle dans vSphere Client.

Activer le relais d'un périphérique réseau sur un hôte

Les périphériques de relais peuvent fournir les moyens nécessaires pour utiliser plus efficacement les ressources et améliorer la performances de votre environnement. Vous pouvez activer un relais DirectPath I/O pour un périphérique réseau sur un hôte.

Attention Si votre hôte ESXi est configuré afin de démarrer à partir d'un périphérique USB ou d'une carte SD connecté à un canal USB, veillez à ne pas activer de relais DirectPath I/O pour le contrôleur USB. Le fait de traverser un contrôleur USB sur un hôte ESXi qui démarre à partir d'un périphérique USB ou d'une carte SD peut placer l'hôte dans un état dans lequel sa configuration ne peut pas être conservée.

Procédure

- 1 Accédez à un hôte dans le navigateur vSphere Client.
- 2 Dans l'onglet **Configurer**, développez la section **Matériel** et sélectionnez **Périphériques PCI**.
- 3 Pour activer un relais DirectPath I/O pour un périphérique réseau PCI sur l'hôte, cliquez sur **Modifier**.

Une liste de périphériques de relais s'affiche.

Icône	Description
icône verte	Un dispositif est actif et peut être activé.
icône orange	L'état de l'appareil a changé et l'hôte doit être redémarré avant que le périphérique puisse être utilisé.

- 4 Sélectionnez le périphérique réseau à utiliser pour le relais et cliquez sur **OK**.
 Le périphérique PCI sélectionné apparaît dans le tableau. Les informations sur le périphérique s'affichent au bas de l'écran.

Configurer un périphérique PCI sur une machine virtuelle

Les périphériques de relais peuvent fournir les moyens d'utiliser plus efficacement les ressources et d'améliorer la performance de votre environnement. Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle dans vSphere Client.

Lors de l'utilisation de périphériques de relais avec un noyau Linux version 2.6.20 ou antérieure, évitez les modes MSI et MSI-X, car ces modes ont un impact important sur les performances.

Conditions préalables

Vérifiez qu'un périphérique de relais de mise en réseau est configuré sur l'hôte de la machine virtuelle. Reportez-vous à la section [Activer le relais d'un périphérique réseau sur un hôte](#).

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 4 Sélectionnez l'onglet **Matériel virtuel** dans la boîte de dialogue affichant les paramètres.
- 5 Développez la section **Mémoire** et établissez la **Limite** sur **Illimité**
- 6 Cliquez sur le bouton **Ajouter un nouveau périphérique** et, sous Autres périphériques, sélectionnez **Périphérique PCI**.

Le menu déroulant **Nouveau périphérique PCI** est ajouté à la liste dans l'onglet **Matériel virtuel**.
- 7 Dans le menu déroulant **Nouveau périphérique PCI**, sélectionnez le périphérique de relais à utiliser et cliquez sur **OK**.
- 8 Mettez la machine virtuelle sous tension.

Résultats

L'ajout d'un périphérique d'E/S DirectPath à une machine virtuelle configure la réservation de mémoire sur la taille de mémoire de la machine virtuelle.

Présentation de la virtualisation des E/S à racine unique (SR-IOV)

vSphere prend en charge la virtualisation des E/S à racine unique (SR-IOV) Vous pouvez utiliser SR-IOV pour la mise en réseau de machines virtuelles sensibles à la latence ou qui nécessitent plus de ressources de CPU.

Présentation de SR-IOV

SR-IOV est une spécification permettant à un périphérique PCIE (Peripheral Component Interconnect Express) physique unique sous un port racine unique d'apparaître comme plusieurs périphériques physiques distincts pour l'hyperviseur ou le système d'exploitation invité.

SR-IOV utilise des fonctions physiques (PF) et des fonctions virtuelles (VF) afin de gérer les fonctions globales des périphériques SR-IOV. Les fonctions PF sont des fonctions PCIe complètes permettant de configurer et de gérer la fonction SR-IOV. Il est possible de configurer ou de contrôler les périphériques PCIe à l'aide de PF, celles-ci ayant l'entière capacité de déplacer des données de et vers le périphérique. Les fonctions VF sont des fonctions PCIe légères qui prennent en charge le flux de données mais disposent d'un ensemble restreint de ressources de configuration.

Le nombre de fonctions virtuelles fournies à l'hyperviseur ou au système d'exploitation invité dépend du périphérique. Les périphériques PCIe compatibles SR-IOV nécessitent une prise en charge BIOS et matérielle appropriée, ainsi que la prise en charge de SR-IOV dans l'instance du pilote du système d'exploitation invité ou de l'hyperviseur. Reportez-vous à la section [Prise en charge SR-IOV](#).

Utilisation de SR-IOV dans vSphere

Dans vSphere, une machine virtuelle peut utiliser une fonction virtuelle SR-IOV pour la mise en réseau. La machine virtuelle et l'adaptateur physique échangent des données directement sans utiliser VMkernel comme intermédiaire. Le contournement de VMkernel pour la mise en réseau réduit la latence et améliore l'efficacité du CPU.

Dans vSphere, bien qu'un commutateur virtuel (commutateur standard ou commutateur distribué) ne gère pas le trafic réseau d'une machine virtuelle prenant en charge SR-IOV connectée au commutateur, vous pouvez contrôler les fonctions virtuelles attribuées en utilisant des règles de configuration de commutateur au niveau du groupe de ports ou du port.

Prise en charge SR-IOV

vSphere prend en charge SR-IOV dans un environnement disposant d'une configuration spécifique uniquement. Certaines fonctions de vSphere ne sont pas disponibles lorsque SR-IOV est activé.

Configurations prises en charge

Pour utiliser SR-IOV dans vSphere, votre environnement doit répondre à un certain nombre d'exigences de configuration.

Tableau 10-1. Configurations prises en charge pour l'utilisation de SR-IOV

Composant	Configuration requise
Hôte physique	<ul style="list-style-type: none"> ■ Doit être compatible avec la version d'ESXi. ■ Doit disposer d'un processeur Intel ou AMD. ■ Doit prendre en charge la technologie d'unité de gestion de mémoire E/S (IOMMU, I/O memory management unit) et doit avoir IOMMU activé dans le BIOS. ■ Doit prendre en charge SR-IOV, et doit avoir SR-IOV activé dans le BIOS. Contactez le fournisseur du serveur afin de déterminer si l'hôte prend en charge SR-IOV.
Carte réseau physique	<ul style="list-style-type: none"> ■ Doit être compatible avec la version d'ESXi. ■ Doit être prise en charge pour une utilisation par l'hôte et SR-IOV, conformément à la documentation technique du fournisseur du serveur. ■ Doit disposer d'un micrologiciel où SR-IOV est activé. ■ Doit utiliser des interruptions MSI-X.
Pilote PF dans ESXi pour l'adaptateur réseau physique	<ul style="list-style-type: none"> ■ Doit être certifié par VMware. ■ Doit être installé sur l'hôte ESXi. La version d'ESXi fournit un pilote par défaut pour certaines cartes réseau. Pour les autres cartes réseau, vous devez le télécharger et l'installer manuellement.
SE client	Doit être pris en charge par la carte réseau sur la version d'ESXi installée conformément à la documentation technique du fournisseur de la carte réseau.
Pilote VF sur le SE client	<ul style="list-style-type: none"> ■ Doit être compatible avec la carte réseau. ■ Doit être pris en charge sur le SE client, conformément à la documentation technique du fournisseur de la carte réseau. ■ Doit être certifié Microsoft WLK ou WHCK pour les machines virtuelles Windows. ■ Doit être installé sur le système d'exploitation. La version du système d'exploitation contient un pilote par défaut pour certaines cartes réseau. Pour les autres cartes réseau, vous devez le télécharger et l'installer à partir d'un emplacement fourni par le fournisseur de la carte réseau ou par l'hôte.

Pour vérifier la compatibilité de vos hôtes et cartes réseau physiques avec les versions d'ESXi, reportez-vous au *Guide de compatibilité VMware*.

Disponibilité des fonctionnalités

Les fonctionnalités suivantes ne sont pas disponibles pour les machines virtuelles configurées avec SR-IOV :

- vSphere vMotion

- Storage vMotion
- vShield
- NetFlow
- Câble virtuel VXLAN
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- Interruption et reprise de machine virtuelle
- Snapshots de machine virtuelle
- VLAN basé sur adresse MAC pour fonctions relai virtuelles
- Insertion et extraction à chaud des périphériques virtuels, de la mémoire et du vCPU
- Participation à un environnement de cluster
- Statistiques réseau pour une carte réseau de machine virtuelle utilisant un relais SR-IOV

Note Les tentatives d'activation ou de configuration des fonctionnalités non prises en charge par SR-IOV entraînent des comportements inattendus dans votre environnement.

Cartes réseau prises en charge

Toutes les cartes réseau doivent être équipées de pilotes et de microprogrammes qui prennent en charge SR-IOV. Certaines cartes réseau peuvent nécessiter que SR-IOV soit activé dans le micrologiciel. Pour savoir quelles NIC sont compatibles avec les machines virtuelles configurées avec SR-IOV, consultez le [Guide de compatibilité VMware](#).

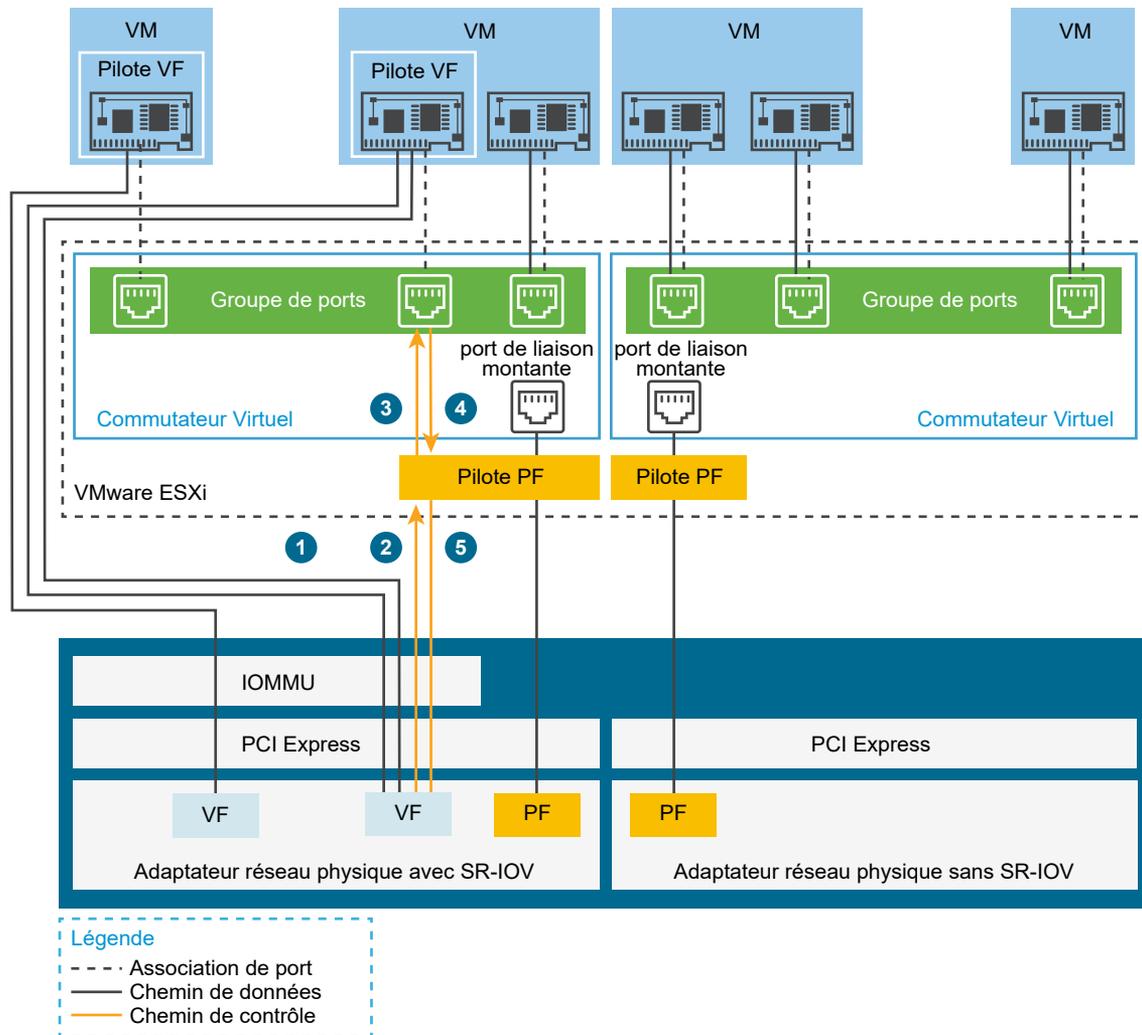
Architecture et interaction des composants SR-IOV

La prise en charge de vSphere SR-IOV repose sur l'interaction entre les fonctions virtuelles et la fonction physique du port de carte réseau pour l'amélioration des performances et sur l'interaction entre le pilote de la fonction physique et le commutateur de l'hôte pour le contrôle du trafic.

Dans un hôte qui exécute le trafic des machines virtuelles au-dessus des adaptateurs physiques SR-IOV, les adaptateurs de machine virtuelle contactent directement les fonctions virtuelles pour communiquer les données. Toutefois, la possibilité de configurer les réseaux dépend des stratégies actives sur le port auquel les machines virtuelles sont associées.

Sur un hôte ESXi sans SR-IOV, le commutateur virtuel envoie le trafic réseau externe via ses ports sur l'hôte à partir de ou vers l'adaptateur physique du groupe de ports approprié. Le commutateur virtuel applique également les stratégies de mise en réseau sur les paquets gérés.

Figure 10-1. Chemins de données et de configuration de la prise en charge SR-IOV de vSphere



Le chemin de données relie directement la machine virtuelle à la fonction virtuelle sur la carte réseau. Le chemin de contrôle inclut le commutateur virtuel et les stratégies actives sur la machine virtuelle.

Chemin de données dans SR-IOV

Une fois l'adaptateur réseau de machine virtuelle attribué à une fonction virtuelle, le pilote de la fonction virtuelle du système d'exploitation invité fait appel à la technologie d'unité de gestion de mémoire E/S (IOMMU, I/O memory management unit) pour accéder à la fonction virtuelle qui doit recevoir ou envoyer les données sur le réseau. Le noyau VMkernel, en l'occurrence le commutateur virtuel, ne traite pas le flux de données, ce qui réduit la latence globale des charges de travail compatibles SR-IOV.

Chemin de configuration dans SR-IOV

Si le système d'exploitation invité tente de modifier la configuration d'un adaptateur de machine virtuelle mappé à une fonction virtuelle, la modification a lieu si elle est autorisée par la stratégie du port associé à l'adaptateur de machine virtuelle.

Le workflow de configuration se déroule de la façon suivante :

- 1 Le système d'exploitation invité demande une modification de configuration à la fonction virtuelle.
- 2 La fonction virtuelle transmet la demande à la fonction physique via un mécanisme de messagerie.
- 3 Le pilote de la fonction physique vérifie la demande de configuration auprès du commutateur virtuel (commutateur standard ou commutateur de proxy hôte d'un commutateur distribué).
- 4 Le commutateur virtuel vérifie la demande de configuration par rapport à la stratégie du port auquel l'adaptateur de machine virtuelle compatible avec la fonction virtuelle est associé.
- 5 Le pilote de la fonction physique configure la fonction virtuelle si les nouveaux paramètres sont conformes à la stratégie du port de l'adaptateur de machine virtuelle.

Par exemple, si le pilote de la fonction virtuelle tente de modifier l'adresse MAC, l'adresse initiale est conservée si la stratégie de sécurité du port ou du groupe de ports n'autorise pas la modification des adresses MAC. Même si le système d'exploitation invité indique que la modification a été effectuée, un message du journal signale que l'opération a échoué. Par conséquent, le système d'exploitation invité et le périphérique virtuel enregistrent différentes adresses MAC. Il est possible que l'interface réseau du système d'exploitation invité ne parvienne ni à obtenir une adresse IP ni à communiquer. Dans ce cas, vous devez réinitialiser l'interface du système d'exploitation invité afin d'obtenir l'adresse MAC la plus récente du périphérique virtuel, ainsi qu'une adresse IP.

Interaction entre vSphere et fonction virtuelle

Les fonctions virtuelles (VF) sont des fonctions PCIe légères qui contiennent toutes les ressources nécessaires à l'échange des données, mais elles disposent d'un ensemble de ressources de configuration réduit. L'interaction entre vSphere et les VF est limitée.

- La carte réseau physique doit utiliser des interruptions MSI-X.
- Les VF ne mettent pas en œuvre un contrôle de débit dans vSphere. Chaque VF peut potentiellement utiliser toute la bande passante d'un lien physique.
- Lorsqu'un périphérique VF est configuré comme un périphérique de relais sur une machine virtuelle, les fonctions en attente et veille pour la machine virtuelle ne sont pas prises en charge.

- Le nombre maximal de VF que vous pouvez créer et le nombre maximal de VF que vous pouvez utiliser pour le relais sont différents. Le nombre maximal de fonctions virtuelles que vous pouvez instancier dépend de la capacité de la carte réseau et de la configuration matérielle de l'hôte. Cependant, en raison du nombre limité de vecteurs d'interruption disponibles pour les périphériques de relais, seul un nombre limité de toutes les VF instanciées peut être employé sur un hôte ESXi.

Le nombre total de vecteurs d'interruption sur chaque hôte ESXi peut atteindre 4 096 en présence de 32 CPU. Lorsque l'hôte démarre, les périphériques sur l'hôte (contrôleurs de stockage, adaptateurs réseau physiques et contrôleurs USB) consomment un sous-ensemble des 4 096 vecteurs. Si ces périphériques nécessitent plus que 1 024 vecteurs, le nombre maximal de fonctions virtuelles potentiellement prises en charge est réduit.

- Le nombre de fonctions virtuelles prises en charge sur une carte réseau Intel peut être différent du nombre pris en charge sur une carte réseau Emulex. Reportez-vous à la documentation technique du fournisseur de la carte réseau.
- Si vous disposez de cartes réseau Intel et Emulex sur lesquelles SR-IOV est activé, le nombre de fonctions virtuelles disponibles pour les cartes réseau Intel dépend du nombre de fonctions virtuelles configurées pour la carte réseau Emulex, et réciproquement. Vous pouvez utiliser la formule suivante pour estimer le nombre maximal de fonctions virtuelles disponibles pour l'utilisation si les 3072 vecteurs d'interruption sont tous disponibles à des fins de relais :

$$3x + 2y < 3072$$

où x est le nombre de VF Intel et y est le nombre de VF Emulex.

Ce nombre peut être inférieur si d'autres types de périphériques sur l'hôte utilisent plus que 1 024 vecteurs d'interruption parmi les 4 096 vecteurs sur l'hôte.

- vSphere SR-IOV prend en charge jusqu'à 1 024 fonctions virtuelles sur les cartes réseau Intel et Emulex prises en charge.
- vSphere SR-IOV prend en charge jusqu'à 64 fonctions virtuelles sur une carte réseau Intel ou Emulex prise en charge.
- Si une carte réseau Intel prise en charge perd sa connexion, toutes les fonctions virtuelles provenant de la carte réseau physique arrêtent la communication, notamment entre les fonctions virtuelles.
- Si une carte réseau Emulex prise en charge perd sa connexion, toutes les fonctions virtuelles cessent de communiquer avec l'environnement externe, mais la communication entre les fonctions virtuelles est maintenue.
- Les pilotes VF offrent de nombreuses fonctions, par exemple la prise en charge d'IPv6, TSO et le total de contrôle LRO. Pour obtenir plus d'informations, consultez la documentation technique proposée par le fournisseur de la carte réseau.

DirectPath I/O vs SR-IOV

SR-IOV offre des avantages en termes de performances et des compromis similaires à ceux de DirectPath I/O. DirectPath I/O et SR-IOV ont une fonction similaire mais vous les utilisez pour accomplir des tâches différentes.

SR-IOV est avantageux pour les charges de travail avec des taux de paquets très élevés ou des exigences de latence très faible. Comme DirectPath I/O, SR-IOV n'est pas compatible avec certaines fonctions de virtualisation principale, comme vMotion. Toutefois, SR-IOV permet à un périphérique physique unique d'être partagé entre plusieurs invités.

Avec DirectPath I/O vous ne pouvez mapper qu'une seule fonction physique vers une machine virtuelle. SR-IOV vous permet de partager un périphérique physique unique, permettant à plusieurs machines virtuelles de se connecter directement à la fonction physique.

Configurer une machine virtuelle pour utiliser SR-IOV

Pour utiliser les capacités de SR-IOV, vous devez activer les fonctions virtuelles de SR-IOV sur l'hôte et connecter une machine virtuelle aux fonctions.

Conditions préalables

Vérifiez que la configuration de votre environnement prend SR-IOV en charge. Consultez [Prise en charge SR-IOV](#).

Procédure

1 Activer SR-IOV sur un adaptateur physique d'hôte

Avant de pouvoir connecter des machines virtuelles aux fonctions virtuelles, utilisez vSphere Client pour activer SR-IOV et définissez le nombre de fonctions virtuelles sur votre hôte.

2 Attribuer une fonction virtuelle en tant qu'adaptateur relais SR-IOV à une machine virtuelle

Afin de vous assurer qu'une machine virtuelle et une carte réseau physique puissent échanger des données, vous devez associer la machine virtuelle à une ou plusieurs fonctions virtuelles, telles que des adaptateurs réseau relais SR-IOV.

Résultats

Le trafic transite de l'adaptateur de relais SR-IOV à l'adaptateur physique conformément à la stratégie active du port associé dans le commutateur standard ou distribué.

Pour déterminer la fonction virtuelle qui est attribuée à un adaptateur réseau de relais SR-IOV, accédez à l'onglet **Résumé** de la machine virtuelle, développez le panneau **Matériel VM** et vérifiez les propriétés de l'adaptateur.

Le diagramme de la topologie du commutateur marque avec l'icône  les adaptateurs de machines virtuelles qui utilisent des fonctions virtuelles.

Étape suivante

Configurez le trafic qui transite par les fonctions virtuelles attachées à la machine virtuelle à l'aide des stratégies de mise en réseau définies sur le commutateur, le groupe de ports et le port. Reportez-vous à la section [Options de mise en réseau pour le trafic associé à une machine virtuelle sur laquelle SR-IOV est activé](#).

Activer SR-IOV sur un adaptateur physique d'hôte

Avant de pouvoir connecter des machines virtuelles aux fonctions virtuelles, utilisez vSphere Client pour activer SR-IOV et définissez le nombre de fonctions virtuelles sur votre hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Adaptateurs physiques**.

Vous pouvez vérifier la propriété SR-IOV pour déterminer si un adaptateur physique prend en charge SR-IOV.
- 3 Sélectionnez l'adaptateur physique et cliquez sur **Modifier les paramètres de l'adaptateur**.
- 4 Sous SR-IOV, sélectionnez **Activé** dans le menu déroulant **Statut**.
- 5 Dans la zone de texte **Nombre de fonctions virtuelles**, tapez le nombre des fonctions virtuelles que vous souhaitez configurer pour l'adaptateur.

Une valeur de 0 signifie que SR-IOV n'est pas activé pour cette fonction physique.
- 6 Cliquez sur **OK**.
- 7 Redémarrez l'hôte.

Résultats

Les fonctions virtuelles deviennent actives sur le port de la carte réseau représenté par l'entrée de l'adaptateur physique. Elles sont affichées dans la liste des périphériques PCI de l'onglet **Paramètres** de l'hôte.

Vous pouvez utiliser les commandes vCLI `esxcli network sriovnic` pour vérifier la configuration des fonctions virtuelles sur l'hôte.

Étape suivante

Associez une machine virtuelle à une fonction virtuelle via un adaptateur réseau de relais SR-IOV.

Attribuer une fonction virtuelle en tant qu'adaptateur relais SR-IOV à une machine virtuelle

Afin de vous assurer qu'une machine virtuelle et une carte réseau physique puissent échanger des données, vous devez associer la machine virtuelle à une ou plusieurs fonctions virtuelles, telles que des adaptateurs réseau relais SR-IOV.

Conditions préalables

- Vérifiez que les fonctions virtuelles existent sur l'hôte.
- Vérifiez que les périphériques relais de mise en réseau pour les fonctions virtuelles sont actifs dans la liste Périphériques PCI de l'onglet **Paramètres** correspondant à l'hôte.
- Vérifiez que la machine virtuelle est compatible avec ESXi 5.5 et versions ultérieures.
- Vérifiez que Red Hat Enterprise Linux 6 et versions ultérieures ou Windows a été sélectionné comme système d'exploitation invité lors de la création de la machine virtuelle.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 4 Sélectionnez l'onglet **Matériel virtuel** dans la boîte de dialogue affichant les paramètres.
- 5 Dans le menu déroulant **Ajouter un nouveau périphérique**, sélectionnez **Adaptateur réseau**.
La section Nouveau réseau est ajoutée à la liste dans l'onglet **Matériel virtuel**.
- 6 Développez la section Nouveau réseau et connectez la machine virtuelle à un groupe de ports.
La carte réseau virtuelle n'utilise pas ce groupe de ports pour le trafic de données. Le groupe de ports est utilisé pour extraire les propriétés de mise en réseau, par exemple le balisage VLAN, à appliquer au trafic de données.
- 7 Dans le menu déroulant **Type d'adaptateur**, sélectionnez **Relais SR-IOV**.
- 8 Dans le menu déroulant **Fonction physique**, sélectionnez l'adaptateur physique devant épauler l'adaptateur relais de la machine virtuelle.
- 9 Pour autoriser les modifications dans le MTU des paquets provenant du système d'exploitation invité, utilisez le menu déroulant **Changement de MTU du SE client**.
- 10 Développez la section Mémoire, sélectionnez **Réserver toute la mémoire client (entièrement verrouillée)** et cliquez sur **OK**.
L'unité de gestion de mémoire d'E/S (IOMMU) doit atteindre toute la mémoire de la machine virtuelle afin que le périphérique relais puisse accéder à la mémoire à l'aide de l'accès mémoire direct (DMA).
- 11 Mettez la machine virtuelle sous tension.

Résultats

Lorsque vous mettez sous tension la machine virtuelle, l'hôte ESXi sélectionne une fonction virtuelle libre de l'adaptateur physique et la met en correspondance avec l'adaptateur relais SR-IOV. L'hôte valide toutes les propriétés de l'adaptateur de la machine virtuelle et de la fonction virtuelle sous-jacente par rapport aux paramètres du groupe de ports auquel la machine virtuelle appartient.

Options de mise en réseau pour le trafic associé à une machine virtuelle sur laquelle SR-IOV est activé

Dans vSphere, vous pouvez configurer certaines fonctionnalités de mise en réseau sur un adaptateur de machine virtuelle qui est associé à une fonction virtuelle (FV). Utilisez les paramètres du commutateur, du groupe de ports ou d'un port selon le type du commutateur virtuel (standard ou distribué) qui gère le trafic.

Tableau 10-2. Options de mise en réseau pour un adaptateur de machine virtuelle qui utilise une fonction virtuelle

Option de mise en réseau	Description
Taille de MTU	Changez la taille du MTU, par exemple pour activer les trames Jumbo.
Stratégie de sécurité pour le trafic de fonctions virtuelles	<ul style="list-style-type: none"> ■ Si le système d'exploitation invité change l'adresse MAC initialement définie d'un adaptateur réseau de machine virtuelle qui utilise une fonction virtuelle, acceptez ou refusez les trames entrantes de la nouvelle adresse en définissant l'option Modifications d'adresse MAC. ■ Activez le mode promiscuité des adaptateurs réseau de machine virtuelle, notamment les adaptateurs qui utilisent des fonctions virtuelles.
Mode de balisage VLAN	Configurez le balisage VLAN dans le commutateur standard ou distribué, c'est-à-dire activez le balisage de commutateur VLAN (VST), ou laissez le trafic balisé atteindre les machines virtuelles qui sont associées à des fonctions virtuelles, c'est-à-dire activez le balisage d'invité virtuel (VGT).

Utilisation d'un adaptateur physique SR-IOV pour gérer le trafic des machines virtuelles

Dans vSphere, la fonction physique (PF) et les fonctions virtuelles (VF) d'un adaptateur physique compatible SR-IOV peuvent être configurées pour gérer le trafic des machines virtuelles.

La fonction physique d'un adaptateur physique SR-IOV contrôle les fonctions virtuelles utilisées par les machines virtuelles et peut transporter le trafic qui passe par le commutateur standard ou distribué gérant la mise en réseau de ces machines virtuelles compatibles SR-IOV.

L'adaptateur physique SR-IOV fonctionne dans différents modes selon qu'il prend ou non en charge le trafic du commutateur.

Mode mixte

L'adaptateur physique fournit des fonctions virtuelles aux machines virtuelles connectées au commutateur et gère directement le trafic provenant des machines virtuelles non compatibles SR-IOV sur le commutateur.

Vous pouvez vérifier si l'adaptateur physique SR-IOV est en mode mixte dans le diagramme de topologie du commutateur. Un adaptateur physique SR-IOV en mode mixte s'affiche avec l'icône  dans la liste des adaptateurs physiques pour un commutateur standard ou dans la liste des adaptateurs de groupe de liaison montante pour un commutateur distribué.

Mode SR-IOV uniquement

L'adaptateur physique fournit des fonctions virtuelles aux machines virtuelles connectées au commutateur virtuel, mais ne prend pas en charge le trafic provenant des machines virtuelles non compatibles SR-IOV sur le commutateur.

Vous pouvez vérifier si l'adaptateur physique est en mode SR-IOV uniquement dans le diagramme de topologie du commutateur. Dans ce mode, l'adaptateur physique figure dans une liste séparée nommée Adaptateurs SR-IOV externes et s'affiche avec l'icône .

Mode non SR-IOV

L'adaptateur physique n'est pas utilisé pour le trafic concernant des machines virtuelles qui font appel aux fonctions virtuelles. Il gère le trafic des machines virtuelles non SR-IOV uniquement.

Activer SR-IOV à l'aide de profils d'hôte ou d'une commande ESXCLI

Vous pouvez configurer les fonctions virtuelles sur un hôte ESXi en utilisant une commande ESXCLI ou un profil d'hôte pour configurer plusieurs hôtes simultanément ou des hôtes sans état.

Activer SR-IOV dans un profil d'hôte

Pour plusieurs hôtes ou un hôte sans état, vous pouvez configurer les fonctions virtuelles de la carte réseau physique à l'aide d'un profil d'hôte et appliquer ce profil à un hôte à l'aide d'Auto Deploy.

Pour plus d'informations sur l'exécution d'ESXi à l'aide d'Auto Deploy avec des profils d'hôte, consultez la documentation *Installation et configuration de vCenter Server*.

Vous pouvez également activer les fonctions virtuelles SR-IOV sur l'hôte en utilisant la commande `vCLI esxcli system module parameters set` sur le paramètre du pilote de carte réseau pour des fonctions virtuelles, tel que présenté dans la documentation du pilote. Pour plus d'informations sur l'utilisation des commandes ESXCLI, reportez-vous à la documentation *Concepts et exemples d'ESXCLI*.

Conditions préalables

- Vérifiez que la configuration de votre environnement prend SR-IOV en charge. Consultez [Prise en charge SR-IOV](#).

- Créez un profil d'hôte en fonction de l'hôte compatible SR-IOV. Consultez la documentation *Profils d'hôte vSphere*.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Profils d'hôte**.
- 2 Sélectionnez un profil d'hôte dans la liste et cliquez sur l'onglet **Configurer**.
- 3 Cliquez sur **Modifier le profil d'hôte** et développez le nœud **Paramètres système généraux**.
- 4 Développez **Paramètre du module noyau**, puis sélectionnez le paramètre du pilote de la fonction physique pour créer des fonctions virtuelles.

Par exemple, le paramètre du pilote de la fonction physique d'une carte réseau physique Intel est `max_vfs`.

- 5 Dans la zone de texte **Valeur**, tapez une liste séparée par des virgules de nombres de fonctions virtuelles valides.

Chaque entrée de la liste indique le nombre de fonctions virtuelles que vous souhaitez configurer pour chaque fonction physique. Une valeur de 0 assure que SR-IOV n'est pas activé pour cette fonction physique.

Par exemple, si vous avez un double port, définissez la valeur sur `x, y`, où `x` ou `y` correspond au nombre de fonctions virtuelles que vous souhaitez activer sur un port unique.

Si le nombre cible de fonctions virtuelles sur un hôte unique est 30, vous pouvez avoir deux cartes à double port définies sur `0, 10, 10, 10`.

Note Le nombre de fonctions virtuelles prises en charge et disponibles pour configuration dépend de la configuration de votre système.

- 6 Cliquez sur **Terminer**.
- 7 Restaurez le profil d'hôte sur l'hôte de manière appropriée.

Résultats

Les fonctions virtuelles s'affichent dans la liste des périphériques PCI dans l'onglet **Paramètres** de l'hôte.

Étape suivante

Associez une fonction virtuelle à un adaptateur de machine virtuelle à l'aide de l'adaptateur réseau de relais de type SR-IOV. Reportez-vous à la section [Attribuer une fonction virtuelle en tant qu'adaptateur relais SR-IOV à une machine virtuelle](#).

Activer SR-IOV sur l'adaptateur physique d'un hôte à l'aide d'une commande ESXCLI

Pour résoudre un problème ou pour configurer des hôtes directement, vous pouvez exécuter une commande de console sur ESXi pour créer des fonctions virtuelles SR-IOV sur un adaptateur physique.

Vous pouvez créer des fonctions virtuelles SR-IOV sur l'hôte en modifiant le paramètre du pilote de la carte réseau pour que les fonctions virtuelles correspondent à la documentation du pilote.

Conditions préalables

Installez le package vCLI, déployez la machine virtuelle vMA (vSphere Management Assistant) ou utilisez ESXi Shell. Reportez-vous à *Démarrage avec ESXCLI*.

Procédure

- 1 Pour créer des fonctions virtuelles en définissant le paramètre des fonctions virtuelles du pilote de la carte réseau, exécutez la commande `esxcli system module parameters set` à l'invite de commande.

```
esxcli system module parameters set -m driver -p vf_param=w,x,y,z
```

driver représentant le nom du pilote de la carte réseau et *vf_param* le paramètre spécifique au pilote pour créer la fonction virtuelle.

Vous pouvez créer une liste séparée par des virgules pour définir les valeurs du paramètre *vf_param* dans laquelle chaque entrée indique le nombre de fonctions virtuelles d'un port. Une valeur de 0 assure que SR-IOV n'est pas activé pour cette fonction physique.

Si vous disposez de deux cartes réseau à double port, vous pouvez définir la valeur sur *w, x, y, z, w,x,y* et *z* représentant le nombre de fonctions virtuelles à activer pour un port unique. Par exemple, pour créer 30 fonctions virtuelles distribuées sur deux cartes Intel à double port à l'aide du pilote *ixgbe*, exécutez la commande suivante pour le pilote *ixgbe* et le paramètre `max_vfs` :

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

- 2 Redémarrez l'hôte pour créer les fonctions virtuelles.

Étape suivante

Associez une fonction virtuelle à un adaptateur de machine virtuelle à l'aide de l'adaptateur réseau de relais de type SR-IOV. Reportez-vous à la section [Attribuer une fonction virtuelle en tant qu'adaptateur relais SR-IOV à une machine virtuelle](#).

La mise sous tension d'une machine virtuelle qui utilise une fonction virtuelle SR-IOV échoue, car l'hôte n'a plus de vecteurs d'interruption

Sur un hôte ESXi, une ou plusieurs machines virtuelles qui utilisent des fonctions virtuelles SR-IOV pour la mise en réseau sont mises hors tension.

Problème

Sur un hôte ESXi, la mise sous tension d'une ou de plusieurs machines virtuelles qui utilisent des fonctions virtuelles SR-IOV pour la mise en réseau échoue lorsque le nombre total de fonctions virtuelles attribuées s'approche du nombre maximal de fonctions virtuelles spécifié dans le guide *Configurations maximales pour vSphere*.

Le fichier journal de la machine virtuelle `vmware.log` contient le message suivant sur la fonction virtuelle :

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

Le fichier journal VMkernel `vmkernel.log` contient les messages suivants sur la fonction virtuelle attribuée à la machine virtuelle :

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

Cause

Le nombre de vecteurs d'interruption pouvant être alloués augmente en fonction du nombre de CPU physiques dont dispose un hôte ESXi. Un hôte ESXi qui dispose de 32 CPU peut fournir un total de 4 096 vecteurs d'interruption. Lorsque l'hôte démarre, les périphériques sur l'hôte (contrôleurs de stockage, adaptateurs réseau physiques et contrôleurs USB) consomment un sous-ensemble des 4096 vecteurs. Si ces périphériques nécessitent plus de 1024 vecteurs, le nombre maximal de fonctions virtuelles potentiellement prises en charge est réduit.

Lorsqu'une machine virtuelle est mise sous tension et que le pilote de la fonction virtuelle du système d'exploitation invité démarre, des vecteurs d'interruption sont consommés. Si le nombre de vecteurs d'interruption n'est pas disponible, le système d'exploitation invité s'arrête de façon inattendue sans message d'erreur.

Il n'existe actuellement aucune règle permettant de déterminer le nombre de vecteurs d'interruption consommés ou disponibles sur un hôte. Ce nombre dépend de la configuration matérielle de l'hôte.

Solution

- ◆ Pour pouvoir mettre sous tension les machines virtuelles, réduisez le nombre de fonctions virtuelles attribuées aux machines virtuelles sur l'hôte.

Par exemple, remplacez l'adaptateur réseau SR-IOV d'une machine virtuelle par un adaptateur connecté à un commutateur standard vSphere ou un commutateur vSphere Distributed Switch.

Technologie RDMA (Remote Direct Memory Access) pour machines virtuelles

vSphere 6.5 et les versions ultérieures prennent en charge la communication RDMA (remote direct memory access) entre des machines virtuelles qui disposent d'adaptateurs réseau RDMA paravirtualisés (PVRDMA).

Présentation de RDMA

RDMA offre un accès direct à la mémoire depuis la mémoire d'un ordinateur vers la mémoire d'un autre ordinateur sans impliquer le système d'exploitation ni le CPU. Le transfert de la mémoire est déplacé vers les adaptateurs HCA compatibles avec la technologie RDMA. Un adaptateur réseau PVRDMA fournit un accès direct à la mémoire distante dans un environnement virtuel.

Utilisation de RDMA dans vSphere

Dans vSphere, une machine virtuelle peut utiliser un adaptateur réseau PVRDMA pour communiquer avec d'autres machines virtuelles équipées de périphériques PVRDMA. Les machines virtuelles doivent être connectées au même vSphere Distributed Switch.

Le périphérique PVRDMA sélectionne automatiquement la méthode de communication entre les machines virtuelles. Pour les machines virtuelles qui s'exécutent sur le même hôte ESXi avec ou sans périphérique RDMA physique, le transfert de données est un memcpy entre les deux machines virtuelles. Le matériel RDMA physique n'est pas utilisé dans ce cas.

Pour les machines virtuelles qui résident sur des hôtes ESXi différents et qui disposent d'une connexion RDMA physique, les périphériques RDMA physiques doivent être des liaisons montantes sur le commutateur distribué. Dans ce cas, la communication entre les machines virtuelles au moyen de PVRDMA utilise les périphériques RDMA physiques sous-jacents.

Pour deux machines virtuelles qui s'exécutent sur des hôtes ESXi différents, lorsque l'un des hôtes au moins ne dispose pas de périphérique RDMA physique, la communication se fait alors par le biais d'un canal TCP et les performances sont réduites.

Prise en charge de PVRDMA

vSphere 6.5 et les versions ultérieures prennent en charge PVRDMA uniquement dans les environnements ayant une configuration spécifique.

Configurations prises en charge

Pour utiliser PVRDMA dans vSphere 6.5 ou version ultérieure, votre environnement doit répondre à un certain nombre d'exigences de configuration.

Tableau 10-3. Configurations prises en charge pour l'utilisation de PVRDMA

Composant	Configuration requise
vSphere	<ul style="list-style-type: none"> ■ Hôte ESXi version 6.5 ou ultérieure. ■ vCenter Server 6.5 ou une version ultérieure. ■ vSphere Distributed Switch
Hôte physique	<ul style="list-style-type: none"> ■ Doit être compatible avec la version d'ESXi.
Host Channel Adapter (HCA)	<ul style="list-style-type: none"> ■ Doit être compatible avec la version d'ESXi. <p>Note Les machines virtuelles qui résident sur des hôtes ESXi différents nécessitent HCA pour pouvoir utiliser RDMA . Vous devez attribuer HCA en tant que liaison montante pour vSphere Distributed Switch. PVRDMA ne prend pas en charge l'association de cartes réseau. HCA doit être la seule liaison montante sur vSphere Distributed Switch.</p> <p>Pour les machines virtuelles qui résident sur les mêmes hôtes ESXi ou les machines virtuelles qui utilisent l'option de secours basée sur TCP, HCA n'est pas requis.</p>
Machine virtuelle	<ul style="list-style-type: none"> ■ Matériel virtuel version 13 ou ultérieure.
SE client	<ul style="list-style-type: none"> ■ Linux (64 bits)

Pour vérifier la compatibilité de vos hôtes physiques et HCA avec les versions d'ESXi, reportez-vous au *Guide de compatibilité VMware*.

Note Les tentatives d'activation ou de configuration des fonctionnalités non prises en charge par PVRDMA risquent d'entraîner des comportements inattendus dans votre environnement.

Prise en charge des espaces de noms PVRDMA

Dans les versions antérieures à vSphere 7.0, les identifiants de ressource publique virtualisée PVRDMA dans le matériel sous-jacent garantissaient qu'une ressource physique pouvait être allouée avec le même identifiant public lorsque l'exécution d'une machine virtuelle reprenait après l'utilisation de vMotion pour la déplacer d'un serveur hôte physique vers un autre. Pour ce faire, PVRDMA distribuait les conversions d'identifiant de ressources virtuelle en physique aux homologues lors de la création d'une ressource. Cela entraînait une charge supplémentaire qui pouvait être importante lors de la création d'un grand nombre de ressources.

Les espaces de noms PVRDMA permettent d'éviter cette charge supplémentaire en laissant plusieurs machines virtuelles coexister sans coordonner l'attribution des identifiants. Un espace de noms d'identifiant isolé est attribué à chaque machine virtuelle sur le matériel RDMA, de telle sorte qu'une machine virtuelle puisse sélectionner ses identifiants dans la même plage sans conflit avec les autres machines virtuelles. L'identifiant de ressource physique ne change plus même après une opération vMotion et les conversions de l'identifiant de ressource virtuelle en physique ne sont plus nécessaires.

Les espaces de noms PVRDMA sont activés automatiquement sur vSphere 7.0 et les versions ultérieures avec la version de matériel de machine virtuelle 17 ou ultérieure. Le matériel sous-jacent doit également prendre en charge les espaces de noms PVRDMA. Pour en savoir plus sur l'activation des espaces de noms PVRDMA sur le matériel de votre environnement, reportez-vous à la documentation du fournisseur RDMA.

Prise en charge des points de terminaison natifs PVRDMA

Les points de terminaison natifs PVRDMA sont pris en charge dans la version de matériel 18 et versions ultérieures de la machine virtuelle à partir de vSphere 7.0 Update 1 et versions ultérieures. Les points de terminaison natifs PVRDMA permettent à PVRDMA de communiquer avec des point de terminaison non-PVRDMA. Pour utiliser des points de terminaison natifs PVRDMA, vous devez activer les espaces de noms PVRDMA. Pour en savoir plus sur l'activation des espaces de noms PVRDMA sur le matériel spécifique de votre environnement, reportez-vous à la documentation du fournisseur RDMA.

Vous devez configurer la machine virtuelle pour qu'elle utilise des points de terminaison natifs PVRDMA. Reportez-vous à la section [Configurer une machine virtuelle pour utiliser les points de terminaison natifs PVRDMA](#).

Configurer un hôte ESXi pour PVRDMA

Configurez l'adaptateur VMkernel et la règle de pare-feu d'un hôte ESXi pour la communication PVRDMA.

Conditions préalables

Vérifiez que votre hôte ESXi réunit les critères requis pour PVRDMA. Reportez-vous à [Prise en charge de PVRDMA](#).

- [Baliser un adaptateur VMkernel pour PVRDMA](#)
Sélectionnez un adaptateur VMkernel et activez-le pour la communication avec PVRDMA.
- [Activer la règle de pare-feu pour PVRDMA](#)
Activez la règle de pare-feu pour PVRDMA dans le profil de sécurité de l'hôte ESXi.

Baliser un adaptateur VMkernel pour PVRDMA

Sélectionnez un adaptateur VMkernel et activez-le pour la communication avec PVRDMA.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Cliquez sur le bouton **Modifier**.
- 5 Localisez `Net.PVRDMAVmknics` à l'aide du champ de texte filtre .

- 6 Cliquez sur le champ de valeur et entrez la valeur de l'adaptateur VMkernel que vous souhaitez utiliser, par exemple vmk0 .
- 7 Cliquez sur **OK**.

Activer la règle de pare-feu pour PVRDMA

Activez la règle de pare-feu pour PVRDMA dans le profil de sécurité de l'hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Pare-feu**.
- 4 Cliquez sur le bouton **Modifier**.
- 5 Localisez la règle pvrDMA à l'aide du champ de texte du filtre.
- 6 Cochez la case en regard de la règle pvrDMA et cliquez sur **OK**.

Attribuer un adaptateur PVRDMA à une machine virtuelle

Pour activer une machine virtuelle afin d'échanger des données à l'aide de RDMA, vous devez associer la machine virtuelle à un adaptateur réseau PVRDMA.

Vous pouvez ajouter jusqu'à dix adaptateurs réseau PVRDMA à une machine virtuelle lorsque vous utilisez vSphere 7.0.2 et versions ultérieures.

Conditions préalables

- Vérifiez que l'hôte sur lequel la machine virtuelle s'exécute est configuré pour RDMA. Reportez-vous à la section [Configurer un hôte ESXi pour PVRDMA](#).
- Vérifiez que l'hôte est connecté à un vSphere Distributed Switch.
- Vérifiez que la machine virtuelle utilise la version 13 du matériel virtuel et les versions ultérieures.
- Vérifiez que le système d'exploitation invité est une distribution Linux 64 bits.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 4 Sélectionnez l'onglet **Matériel virtuel** dans la boîte de dialogue affichant les paramètres.

- 5 Dans le menu déroulant **Ajouter un nouveau périphérique**, sélectionnez **Adaptateur réseau**.
La section Nouveau réseau est ajoutée à la liste dans l'onglet **Matériel virtuel**.
- 6 Développez la section Nouveau réseau et connectez la machine virtuelle à un groupe de ports distribués.
- 7 Dans le menu déroulant **Type d'adaptateur**, sélectionnez PVRDMA.
- 8 Développez la section **Mémoire**, sélectionnez **Réserver toute la mémoire d'invité (entièrement verrouillée)** et cliquez sur **OK**
- 9 Mettez la machine virtuelle sous tension.

Configurer une machine virtuelle pour utiliser les points de terminaison natifs PVRDMA

Les points de terminaison natifs PVRDMA sont disponibles pour une configuration avancée de la machine virtuelle.

Les points de terminaison natifs PVRDMA sont pris en charge dans la version de matériel 18 et versions ultérieures de la machine virtuelle à partir de vSphere 7.0 Update 1 et versions ultérieures. Pour utiliser des points de terminaison natifs PVRDMA, vous devez activer les espaces de noms PVRDMA. Pour en savoir plus sur l'activation des espaces de noms PVRDMA sur le matériel spécifique de votre environnement, reportez-vous à la documentation du fournisseur.

Vous pouvez utiliser vSphere Client pour configurer des points de terminaison natifs ou modifier le fichier VMX de la machine virtuelle. Si vous modifiez le fichier VMX directement, ajoutez le paramètre `vrddmax.nativeEndpointSupport = "TRUE"`, où `x` correspond à l'index de l'adaptateur PVRDMA. La procédure suivante utilise vSphere Client pour configurer des points de terminaison natifs.

Conditions préalables

Vérifiez que votre environnement prend en charge PVRDMA. Reportez-vous à la section [Prise en charge de PVRDMA](#).

Procédure

- 1 Accédez à la machine virtuelle dans vSphere Client.
 - a Pour trouver une machine virtuelle, sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **VM**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 3 Cliquez sur **Options VM**.
- 4 Développez **Avancé**.
- 5 Sous Paramètres de configuration, cliquez sur le bouton **Modifier la configuration**.

- 6 Dans la boîte de dialogue qui apparaît, cliquez **Ajouter ligne** pour saisir un nouveau paramètre et sa valeur.
- 7 Entrez le paramètre `vrddm.max.nativeEndpointSupport`, où *x* correspond à l'index de l'adaptateur PVRDMA et définissez la valeur sur **TRUE**.

L'index *x* est le nombre de l'adaptateur PVRDMA moins 1. Par exemple, si l'adaptateur PVRDMA avec lequel vous souhaitez activer les points de terminaison natifs est nommé « Adaptateur réseau 2 », l'index est 1.

Configurer une machine virtuelle pour utiliser le mode VRDMA asynchrone

Apprenez à configurer une machine virtuelle pour utiliser le mode PVRDMA asynchrone. Il est disponible en tant que configuration de machine virtuelle avancée.

Le mode PVRDMA asynchrone est disponible sur les machines virtuelles s'exécutant sur vSphere 8.0 et versions ultérieures. Le mode asynchrone peut améliorer le débit et la latence des charges de travail RDMA s'exécutant sur la machine virtuelle. Lorsque le mode asynchrone est activé, une augmentation de l'utilisation du CPU peut être observée sur l'hôte. Lorsque le mode asynchrone est utilisé, il est recommandé que la machine virtuelle soit configurée pour une sensibilité de latence élevée.

Conditions préalables

Vérifiez que votre environnement prend en charge PVRDMA. Reportez-vous à la section [Prise en charge de PVRDMA](#).

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 3 Cliquez sur **Options VM**.
- 4 Développez **Avancé**.
- 5 Sous Paramètres de configuration, cliquez sur le bouton **Modifier la configuration**.
- 6 Dans la boîte de dialogue qui apparaît, cliquez **Ajouter ligne** pour saisir un nouveau paramètre et sa valeur.
- 7 Entrez le paramètre `vrddm.asyncMode` et définissez la valeur sur **TRUE**.

Configuration de réseau requise RoCE (RDMA over Converged Ethernet)

Le protocole RoCE (RDMA over Converged Ethernet) garantit une communication RDMA à faible latence, légère et à haut débit sur un réseau Ethernet. Le protocole RoCE nécessite un réseau configuré à des fins de trafic sans perte d'informations sur la couche 2 seule ou sur les couches 2 et 3.

Le protocole RoCE (RDMA over Converged Ethernet) est un protocole réseau qui utilise RDMA pour fournir un transfert de données plus rapide aux applications utilisant le réseau de manière intensive. Le protocole RoCE permet le transfert de mémoire direct entre les hôtes sans solliciter les CPU des hôtes.

Il existe deux versions du protocole RoCE. Le protocole RoCE v1 fonctionne au niveau de la couche du réseau de liaison (couche 2). Le protocole RoCE v2 fonctionne au niveau de la couche du réseau Internet (couche 3). Les protocoles RoCE v1 et RoCE v2 nécessitent une configuration réseau sans perte. Le protocole RoCE v1 nécessite un réseau de couche 2 sans perte et le protocole RoCE v2 nécessite que les couches 2 et 3 soient configurées pour un fonctionnement sans perte.

Réseau de couche 2 sans perte

Pour garantir un environnement de couche 2 sans perte, vous devez pouvoir contrôler les flux du trafic. Le contrôle de flux s'obtient en activant une interruption globale sur le réseau or ou à l'aide du protocole PFC (Priority Flow Control) défini par le groupe DCB (Data Center Bridging). Le protocole PFC est un protocole de couche 2 qui utilise la classe du champ de services de la balise VLAN 802.1Q afin de définir des priorités de trafic individuelles. Il interrompt le transfert de paquets vers un récepteur conformément à la classe individuelle de priorités de service. Ainsi, une simple liaison transporte le trafic RoCE sans perte et un autre trafic Meilleur effort avec perte. En cas d'encombrement du flux du trafic, un trafic avec perte important peut être affecté. Pour isoler différents flux les uns des autres, utilisez le protocole RoCE dans un VLAN sur lequel la priorité PFC est activée.

Réseau de couche 3 sans perte

Le protocole RoCE v2 nécessite que le transfert de données sans perte soit maintenu au niveau des périphériques de routage de la couche 3. Pour activer le transfert de priorités sans perte PFC de couche 2 entre des routeurs de couche 3, configurez le routeur pour mapper le paramètre de priorité reçu d'un paquet au paramètre QoS DSCP (Differentiated Serviced Code Point) correspondant fonctionnant au niveau de la couche 3. Les paquets RDMA transférés sont marqués d'un DSCP de couche 3, de PCP (Priority Code Points) de couche 2 ou des deux. Pour extraire des informations de priorité des routeurs de paquets, utilisez DSCP ou PCP. Si vous utilisez des PCP, le paquet doit porter une balise VLAN et le routeur doit copier les bits PCP de la balise et les transférer au réseau suivant. Si le paquet est marqué d'un DSCP, le routeur doit laisser les bits DSCP inchangés.

Comme le protocole RoCE v1, le protocole RoCE v2 doit s'exécuter sur un VLAN sur lequel la priorité PFC est activée.

Note N'associez pas de cartes réseau au protocole RoCE, si vous souhaitez utiliser RDMA sur celles-ci.

Pour obtenir des informations de configuration spécifiques du fournisseur, reportez-vous à la documentation officielle du fournisseur du périphérique ou du commutateur respectif.

Configurer des adaptateurs réseau RDMA

Vous pouvez installer un adaptateur réseau RDMA (Remote Direct Memory Access) sur vos hôtes ESXi. Une fois installé, vous pouvez utiliser vSphere Client pour afficher l'adaptateur RDMA et son adaptateur réseau correspondant, puis configurer sa liaison VMkernel.

RDMA fournit un accès direct à la mémoire depuis la mémoire d'un hôte vers la mémoire d'un autre hôte sans impliquer le système d'exploitation distant ni un CPU. Cela améliore les performances du réseau et de l'hôte avec une latence inférieure, une charge de CPU inférieure et une bande passante plus rapide.

Conditions préalables

Installez un adaptateur compatible RDMA sur votre hôte ESXi. Par exemple, Mellanox Technologies MT27700 Family ConnectX-4.

Afficher l'adaptateur réseau compatible RDMA

ESXi prend en charge les adaptateurs réseau compatibles RDMA. Une fois que vous avez installé un tel adaptateur sur votre hôte ESXi, vSphere Client affiche ses deux composants, l'adaptateur RDMA et un adaptateur réseau physique.

Vous pouvez utiliser vSphere Client pour afficher l'adaptateur RDMA et son adaptateur réseau correspondant.

Conditions préalables

Installez un adaptateur compatible RDMA qui prend en charge RDMA (RoCE v2) sur votre hôte ESXi. Par exemple, Mellanox Technologies MT27700 Family ConnectX-4.

Procédure

- 1 Sur votre hôte ESXi, installez un adaptateur compatible RDMA qui prend en charge RDMA (RoCE v2).

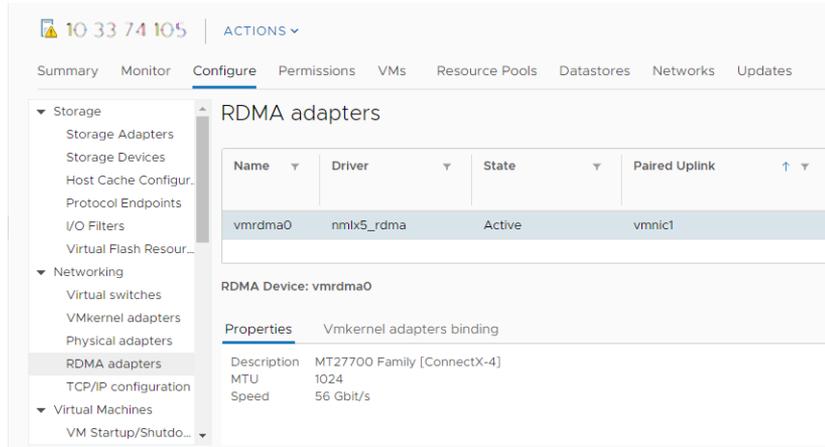
L'hôte découvre l'adaptateur et vSphere Client affiche ses deux composants, un adaptateur RDMA et un adaptateur réseau physique.

- 2 Accédez à l'hôte.

3 Sous **Mise en réseau**, cliquez sur **Adaptateurs RDMA**.

Dans cet exemple, l'adaptateur RDMA figure dans la liste en tant que `vmrdma0`. La colonne **Liaison montante couplée** affiche le composant réseau comme adaptateur réseau physique `vmnic1`.

Figure 10-2. Adaptateurs RDMA installés sur un hôte ESXi dans un environnement vSphere.



4 Pour vérifier la description de l'adaptateur, sélectionnez l'adaptateur RDMA dans la liste, puis cliquez sur l'onglet **Propriétés**.

Configurer des adaptateurs réseau RDMA

Vous pouvez installer un adaptateur réseau RDMA (Remote Direct Memory Access) et configurer sa liaison VMkernel.

Procédure

1 Installez un adaptateur compatible RDMA qui prend en charge RDMA (RoCE v2) sur votre hôte ESXi.

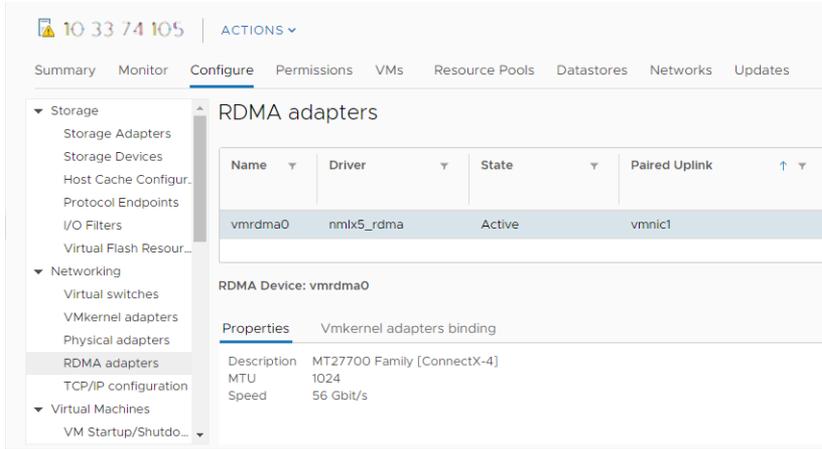
L'hôte découvre l'adaptateur et vSphere Client affiche ses deux composants, un adaptateur RDMA et un adaptateur réseau physique.

2 Dans vSphere Client, vérifiez que l'adaptateur RDMA est détecté par votre hôte.

- a Accédez à l'hôte.
- b Cliquez sur l'onglet **Configurer**.

- c Sous **Mise en réseau**, cliquez sur **Adaptateurs RDMA**.

Dans cet exemple, l'adaptateur RDMA figure dans la liste en tant que `vmrdma0`. La colonne **Liaison montante couplée** affiche le composant réseau comme adaptateur réseau physique `vmnic1`.



- d Pour vérifier la description de l'adaptateur, sélectionnez l'adaptateur RDMA dans la liste, puis cliquez sur l'onglet **Propriétés**.

- 3 Configurez la liaison VMkernel pour l'adaptateur RDMA.

Dans la configuration, vous pouvez utiliser un commutateur vSphere Standard ou un vSphere Distributed Switch. Les étapes suivantes utilisent le commutateur standard comme exemple.

- a Créez un commutateur vSphere Standard et ajoutez le composant réseau au commutateur.

Note Assurez-vous de sélectionner l'adaptateur réseau physique qui correspond à l'adaptateur RDMA. Dans cet exemple, il s'agit de l'adaptateur `vmnic1`.

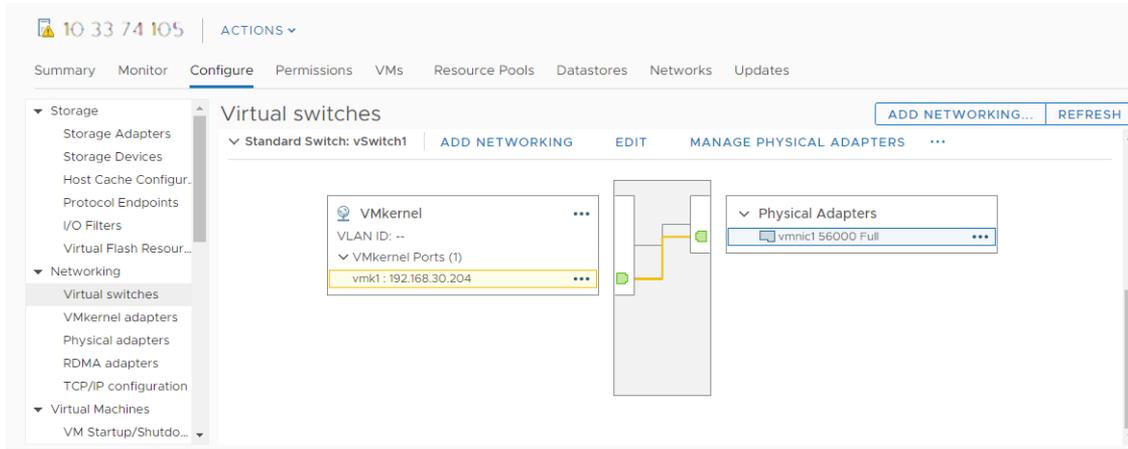
Pour plus d'informations sur la création du commutateur, reportez-vous à la section [Créer un commutateur vSphere standard](#) ou [Créer un vSphere Distributed Switch](#).

- b Ajoutez un adaptateur VMkernel au commutateur vSphere Standard que vous avez créé.

Attribuez une adresse IPv4 ou IPv6 statique appropriée à l'adaptateur VMkernel, afin que votre adaptateur RDMA puisse découvrir la cible NVMe over RDMA.

Pour plus d'informations sur l'ajout de l'adaptateur VMkernel, reportez-vous à la section [Chapitre 4 Comment configurer la mise en réseau d'adaptateurs VMkernel ?](#)

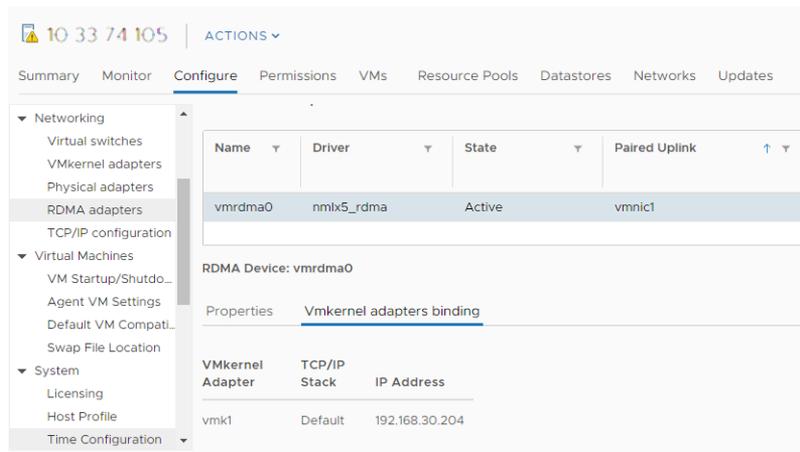
L'illustration montre que l'adaptateur réseau physique et l'adaptateur VMkernel sont connectés au commutateur vSphere Standard. Grâce à cette connexion, l'adaptateur RDMA est lié à l'adaptateur VMkernel.



4 Vérifiez la configuration de la liaison VMkernel pour l'adaptateur RDMA.

- a Accédez à l'adaptateur RDMA.
- b Cliquez sur l'onglet **Liaison des adaptateurs VMkernel** et vérifiez que l'adaptateur VMkernel associé s'affiche sur la page.

Dans cet exemple, l'adaptateur RDMA `vmrdma0` est couplé à l'adaptateur réseau `vmnic1` et est connecté à l'adaptateur VMkernel `vmk1`.



Étape suivante

Vous pouvez utiliser le composant réseau RDMA de l'adaptateur pour des configurations de stockage comme iSER ou NVMe over RDMA. Pour en savoir plus, reportez-vous à la documentation *Stockage vSphere*.

Trames jumbo

Avec les trames Jumbo, les hôtes ESXi peuvent envoyer des trames plus grandes sur le réseau physique. Le réseau doit prendre en charge des trames Jumbo de bout en bout, incluant adaptateurs réseau physiques, commutateurs physiques et périphériques de stockage.

Avant d'activer des trames Jumbo, consultez votre fournisseur de matériel afin de garantir que votre carte réseau physique prenne en charge les trames Jumbo.

Activez les trames Jumbo sur un vSphere Distributed Switch ou un commutateur standard vSphere en changeant l'unité de transmission maximale (MTU) pour une valeur supérieure à 1 500 octets. La taille de trame maximale est de 9 000 octets.

Activer les trames Jumbo sur un vSphere Distributed Switch

Activez les trames jumbo pour l'ensemble du trafic passant par un vSphere Distributed Switch.

Important Lorsque vous modifiez la taille MTU d'un vSphere Distributed Switch, les cartes réseau physiques qui sont attribuées en tant que liaisons montantes sont remises vers le bas et le haut. Cela provoque une brève panne de réseau pendant 5 à 10 millisecondes pour les machines virtuelles ou les services qui utilisent les liaisons montantes.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **Propriétés**.
- 3 Cliquez sur **Modifier**.
- 4 Sélectionnez **Avancé** et définissez une valeur supérieure à 1 500 octets pour le paramètre **MTU**.

La valeur de l'unité de transmission maximale (MTU) ne peut pas être supérieure à 9 000 octets.

- 5 Cliquez sur **OK**.

Activer les trames jumbo sur un commutateur standard vSphere

Activer les trames jumbo pour l'ensemble du trafic via un commutateur vSphere standard sur un hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la table des commutateurs virtuels et cliquez sur **Modifier les paramètres**.
- 4 Dans la section **Propriétés**, définissez la propriété **MTU** à une valeur supérieure à 1 500 octets.
La valeur de l'unité de transmission maximale (MTU) peut aller jusqu'à 9 000 octets.
- 5 Cliquez sur **OK**.

Activer les trames jumbo pour un adaptateur VMkernel

Les trames Jumbo réduisent la charge du processeur générée par le transfert de données. Activez des trames Jumbo sur un adaptateur VMkernel en modifiant l'unité de transmission maximale (MTU) de l'adaptateur.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- 3 Sélectionnez un adaptateur VMkernel dans la table des adaptateurs.
Les propriétés de l'adaptateur s'affichent.
- 4 Cliquez sur **Modifier**.
- 5 Sur la page Propriétés du port, définissez la propriété **MTU** sur une valeur supérieure à 1 500.
La valeur de l'unité de transmission maximale (MTU) peut aller jusqu'à 9 000 octets.
- 6 Cliquez sur **OK**.

Activer la prise en charge de Trames jumbo sur une machine virtuelle

L'activation de la prise en charge de trames Jumbo sur une machine virtuelle nécessite un adaptateur VMXNET amélioré pour cette machine virtuelle.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 3 Sélectionnez l'onglet **Matériel virtuel** dans la boîte de dialogue affichant les paramètres.
- 4 Développez la section **Adaptateur réseau**. Enregistrez les paramètres réseau et l'adresse MAC utilisés par la carte réseau.
- 5 Cliquez sur le bouton X en cercle pour supprimer la carte réseau de la machine virtuelle.
- 6 Dans le menu déroulant **Ajouter un nouveau périphérique**, sélectionnez **Adaptateur réseau**.
La section Nouveau réseau est ajoutée à la liste dans l'onglet Matériel virtuel.
- 7 Développez la section Nouveau réseau.
- 8 Dans le menu déroulant **Type d'adaptateur**, sélectionnez **VMXNET 2 (amélioré)** ou **VMXNET 3**.
- 9 Définissez les paramètres du réseau sur ceux enregistrés pour l'ancienne carte réseau.

- 10 Définissez l'**Adresse MAC** sur **Manuel**, puis saisissez l'adresse MAC utilisée par l'ancien adaptateur réseau.
- 11 Cliquez sur **OK**.

Étape suivante

- Vérifiez que l'adaptateur VMXNET amélioré est connecté à un commutateur standard ou à un vSphere Distributed Switch dont les trames Jumbo sont activées.
- Dans le système d'exploitation invité, configurez la carte réseau de manière à autoriser les trames Jumbo. Consultez la documentation de votre système d'exploitation client.
- Configurez tous les commutateurs physiques et les machines virtuelles ou physiques auxquelles cette machine virtuelle se connecte pour prendre en charge les trames Jumbo.

délestage de segmentation TCP

Utilisez le délestage de segmentation TCP (TSO) dans les adaptateurs réseau VMkernel et les machines virtuelles pour améliorer les performances du réseau dans les charges de travail ayant des exigences de latence importantes.

Le TSO sur le chemin de transmission des adaptateurs réseau physiques, et des adaptateurs réseau VMkernel et de machine virtuelle, améliorent les performances des hôtes ESXi en réduisant la charge sur la CPU liée aux opérations réseau TCP/IP. Lorsque le TSO est activé, l'adaptateur réseau divise les blocs de données volumineux en segments TCP au lieu de confier cette tâche à la CPU. Le VMkernel et le système d'exploitation invité disposent d'un plus grand nombre de cycles de CPU pour exécuter les applications.

Pour profiter de l'amélioration des performances que fournit le TSO, activez ce dernier sur le chemin de données d'un hôte ESXi incluant des adaptateurs réseau physiques, VMkernel et un système d'exploitation invité. Par défaut, le TSO est activé sur le VMkernel de l'hôte ESXi, ainsi que dans les adaptateurs de machine virtuelle VMXNET 2 et VMXNET 3.

Pour obtenir des informations sur l'emplacement de la segmentation de paquets TCP dans le chemin de données, reportez-vous à l'article [Comprendre le délestage de segmentation TCP \(TSO\) et le LRO \(Large Receive Offload\) dans un environnement VMware](#) de la base de connaissances VMware.

Gérer le TSO logiciel dans VMkernel

Si un adaptateur de réseau physique rencontre des problèmes avec TSO, vous pouvez activer temporairement la simulation logicielle de TSO dans VMkernel jusqu'à ce que ces problèmes soient résolus.

Procédure

- ◆ Exécutez ces commandes de console `esxcli network nic software set` pour activer ou désactiver la simulation logicielle de TSO dans VMkernel.

- Activez la simulation logicielle de TSO dans VMkernel.

```
esxcli network nic software set --ipv4tso=1 -n vmnicX
esxcli network nic software set --ipv6tso=1 -n vmnicX
```

- Désactivez la simulation logicielle de TSO dans VMkernel.

```
esxcli network nic software set --ipv4tso=0 -n vmnicX
esxcli network nic software set --ipv6tso=0 -n vmnicX
```

où *X* dans `vmnicX` représente le numéro des ports de la carte réseau sur l'hôte.

La modification de la configuration persiste lors des redémarrages de l'hôte.

Comment déterminer si TSO est pris en charge sur les adaptateurs réseau physiques sur un hôte ESXi

Déterminez si un adaptateur réseau physique décharge la segmentation des paquets TCP/IP lorsque vous évaluez les performances de mise en réseau sur un hôte qui exécute des charges de travail sensibles à la latence. Si un adaptateur réseau physique prend en charge TSO, TSO est activé par défaut.

Procédure

- ◆ Exécutez la commande de console suivante pour déterminer si TSO est activé sur les adaptateurs réseau physiques sur un hôte.

```
esxcli network nic tso get
```

Gérer TSO sur un hôte ESXi

Activez TSO (TCP Segmentation Offload) sur le chemin de transmission pour que la carte réseau divise les blocs de données volumineux en segments TCP. Désactivez TSO pour que le CPU assure la segmentation TCP.

Par défaut, un hôte utilise le TSO matériel si ses adaptateurs physiques le prennent en charge.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.

- 4 Modifiez la valeur du paramètre `Net.UseHwTSO` pour IPv4 et du paramètre `Net.UseHwTSO6` pour IPv6.
 - Pour activer TSO, définissez `Net.UseHwTSO` et `Net.UseHwTSO6` sur **1**.
 - Pour désactiver TSO, définissez `Net.UseHwTSO` et `Net.UseHwTSO6` sur **0**.
- 5 Cliquez sur **OK** pour appliquer les modifications.
- 6 Pour recharger le module du pilote de l'adaptateur physique, exécutez la commande de console `esxcli system module set` dans ESXi Shell sur l'hôte.
 - a Pour désactiver le pilote, exécutez la commande `esxcli system module set` avec l'option `--enabled false`.

```
esxcli system module set --enabled false --module nic_driver_module
```

- b Pour activer le pilote, exécutez la commande `esxcli system module set` avec l'option `--enabled true`.

```
esxcli system module set --enabled true --module nic_driver_module
```

Résultats

Si un adaptateur physique ne prend pas en charge le TSO matériel, VMkernel segmente les paquets TCP volumineux provenant du système d'exploitation invité et les envoie à l'adaptateur.

Comment savoir si le TSO est activé sur un hôte ESXi ?

Déterminez si le TSO matériel est activé dans le VMkernel lorsque vous évaluez les performances de mise en réseau sur un hôte qui exécute des charges de travail sensibles à la latence. Par défaut, le TSO matériel est activé sur un hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Examinez les valeurs des paramètres `Net.UseHwTSO` et `Net.UseHwTSO6`.

`Net.UseHwTSO` indique l'état du TSO pour IPv4, `Net.UseHwTSO6` pour IPv6. Le TSO est activé si la valeur de la propriété est définie sur 1.

Gérer TSO sur une machine virtuelle Linux

Activez la prise en charge de TSO sur l'adaptateur réseau d'une machine virtuelle Linux afin que le système d'exploitation invité redirige les paquets TCP nécessitant une segmentation vers le VMkernel.

Conditions préalables

- Vérifiez que ESXi prend en charge le système d'exploitation invité Linux.
Consultez la documentation de *Guide de compatibilité VMware*.
- Vérifiez que l'adaptateur réseau sur la machine virtuelle Linux est VMXNET2 ou VMXNET3.

Procédure

- ◆ Dans une fenêtre de terminal sur le système d'exploitation invité Linux, pour activer ou désactiver TSO, exécutez la commande `ethtool` avec les options `-K` et `tso`.

- Pour activer TSO, exécutez la commande suivante :

```
ethtool -K ethY tso on
```

- Pour désactiver TSO, exécutez la commande suivante :

```
ethtool -K ethY tso off
```

où *Y* (dans `eth Y`) est le numéro de séquence de la carte réseau dans la machine virtuelle.

Gérer TSO sur une machine virtuelle Windows

Par défaut, TSO est activé sur une machine virtuelle Windows sur les adaptateurs réseau VMXNET2 et VMXNET3. Pour des raisons de performances, vous pouvez désactiver TSO.

Conditions préalables

- Vérifiez que ESXi prend en charge le système d'exploitation invité Windows. Consultez la documentation de *Guide de compatibilité VMware*.
- Vérifiez que l'adaptateur réseau sur la machine virtuelle Windows est VMXNET2 ou VMXNET3.

Procédure

- 1 Dans le Centre Réseau et partage du Panneau de configuration de Windows, cliquez sur le nom de l'adaptateur réseau.
- 2 Cliquez sur son nom.
Une boîte de dialogue affiche l'état de l'adaptateur.
- 3 Cliquez sur **Propriétés** et, sous le type d'adaptateur réseau, cliquez sur **Configurer**.
- 4 Dans l'onglet **Avancé**, définissez les propriétés **Décharge d'envoi important V2 (IPv4)** et **Décharge d'envoi important V2 (IPv6)** sur **Activé** ou **Désactivé**.
- 5 Cliquez sur **OK**.
- 6 Redémarrez la machine virtuelle.

LRO (Large Receive Offload)

Utilisez LRO (Large Receive Offload) pour réduire la surcharge CPU lors du traitement des paquets qui arrivent du réseau selon un débit très élevé.

LRO rassemble les paquets réseau entrants dans de grands tampons et transfère les paquets ainsi obtenus, plus grands mais moins nombreux, à la pile réseau de l'hôte ou de la machine virtuelle. Le CPU doit traiter moins de paquets que lorsque LRO est désactivé, ce qui réduit son utilisation pour la mise en réseau, notamment dans le cas de connexions à bande passante élevée.

Pour bénéficier des améliorations de performances de LRO, activez LRO sur tout le chemin de données de l'hôte ESXi, y compris le VMkernel et le système d'exploitation invité. Par défaut, LRO est activé dans VMkernel et dans les adaptateurs de machine virtuelle VMXNET3.

Pour en savoir plus sur l'emplacement de l'agrégation de paquets TCP dans le chemin de données, reportez-vous à l'article de la base de connaissances VMware [Understanding TCP Segmentation Offload \(TSO\) and Large Receive Offload \(LRO\) in a VMware environment](#) (Comprendre TSO [TCP Segmentation Offload] et LRO [Large Receive Offload] dans un environnement VMware).

Gérer LRO matériel pour tous les adaptateurs VMXNET3 sur un hôte ESXi

Activez les possibilités matérielles des adaptateurs physiques hôtes pour agréger les paquets TCP entrants pour les adaptateurs de machine virtuelle VMXNET3 en utilisant la technologie LRO plutôt que de consommer des ressources pour l'assemblage dans le système d'exploitation invité.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Modifiez la valeur du paramètre `Net.Vmxnet3HwLRO`.
 - Pour activer LRO matériel, définissez `Net.Vmxnet3HwLRO` sur **1**.
 - Pour désactiver LRO matériel, définissez `Net.Vmxnet3HwLRO` sur **0**.
- 5 Cliquez sur **OK** pour appliquer les modifications.

Gérer LRO logiciel pour tous les adaptateurs VMXNET3 sur un hôte ESXi

Utilisez LRO logiciel dans le serveur principal VMkernel des adaptateurs VMXNET3 pour améliorer les performances réseau de machines virtuelles si les adaptateurs physiques hôtes ne prennent pas en charge LRO matériel.

vSphere prend en charge LRO logiciel pour les paquets IPv4 et IPv6.

Conditions préalables

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Modifiez la valeur du paramètre `Net.Vmxnet3SwLRO` des adaptateurs VMXNET3.
 - Pour activer LRO logiciel, définissez `Net.Vmxnet3SwLRO` sur 1.
 - Pour désactiver LRO logiciel, définissez `Net.Vmxnet3SwLRO` sur 0.
- 5 Cliquez sur **OK** pour appliquer les modifications.

Déterminer si LRO est activé pour les adaptateurs VMXNET3 sur un hôte ESXi

Examinez le statut de LRO sur un système ESXi lorsque vous évaluez les performances de mise en réseau sur un hôte qui exécute des charges de travail sensibles à la latence.

Conditions préalables

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Examinez la valeur des paramètres LRO pour VMXNET2 et VMXNET3.
 - Pour LRO matériel, examinez le paramètre `Net.Vmxnet3HwLRO`. S'il est égal à 1, LRO matériel est activé.
 - Pour LRO logiciel, examinez le paramètre `Net.Vmxnet3SwLRO`. S'il est égal à 1, LRO matériel est activé.

Modifier la taille du tampon LRO pour les adaptateurs VMXNET 3

Vous pouvez modifier la taille du tampon pour l'agrégation de paquets pour les connexions de machine virtuelle via les adaptateurs réseau VMXNET 3. Augmentez la taille du tampon pour réduire le nombre d'accusés de réception TCP et améliorer l'efficacité des charges de travail.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.

- 4 Définissez le paramètre `Net.VmxnetLROMaxLength` sur une valeur comprise entre 1 et 65 535 pour spécifier la taille du tampon LRO (en octets).

La taille par défaut du tampon LRO est de 32 000 octets.

Activer ou désactiver LRO pour tous les adaptateurs VMkernel sur un hôte ESXi

Utilisez LRO dans les adaptateurs réseau VMkernel sur un hôte ESXi pour améliorer les performances de mise en réseau pour le trafic d'infrastructure entrant.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Modifiez la valeur du paramètre `Net.TcpipDefLROEnabled`.
 - Pour activer LRO pour les adaptateurs réseau VMkernel sur l'hôte, définissez `Net.TcpipDefLROEnabled` sur **1**.
 - Pour désactiver SW LRO pour les adaptateurs réseau VMkernel sur l'hôte, définissez `Net.TcpipDefLROEnabled` sur **0**.
- 5 Cliquez sur **OK** pour appliquer les modifications.

Modifier la taille de la mémoire tampon LRO pour tous les adaptateurs VMkernel

Vous pouvez modifier la taille de la mémoire tampon pour l'agrégation de paquets des connexions VMkernel. Augmentez la taille de la mémoire tampon pour réduire le nombre d'accusés de réception TCP et améliorer l'efficacité du VMkernel.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système**.
- 3 Cliquez sur **Paramètres système avancés**.
- 4 Entrez une valeur comprise entre 1 et 65535 pour le paramètre `Net.TcpipDefLROMaxLength` afin de définir la taille de la mémoire tampon LRO en octets.

Par défaut, la taille de la mémoire tampon LRO est égale à 32 768 octets.

Gérer LRO sur un adaptateur VMXNET3 sur une machine virtuelle Linux

Si LRO est activé pour les adaptateurs VMXNET3 sur l'hôte, activez la prise en charge LRO sur un adaptateur réseau d'une machine virtuelle Linux afin de garantir que le système d'exploitation invité n'utilise aucune ressource pour agréger les paquets entrants dans de plus grands tampons.

Conditions préalables

Vérifiez que la version du noyau Linux est 2.6.24 ou une version ultérieure.

Procédure

- ◆ Dans une fenêtre de terminal sur le système d'exploitation invité Linux, exécutez la commande `ethtool` avec les options `-K` et `lro`.

- Pour activer LRO, exécutez la commande suivante :

```
ethtool -K ethY lro on
```

où Y (dans eth Y) est le numéro de séquence de la carte réseau dans la machine virtuelle.

- Pour désactiver LRO, exécutez la commande suivante :

```
ethtool -K ethY lro off
```

où Y (dans eth Y) est le numéro de séquence de la carte réseau dans la machine virtuelle.

Gérer LRO sur un adaptateur VMXNET3 sur une machine virtuelle Windows

Si LRO est activé pour les adaptateurs VMXNET3 sur l'hôte, activez la prise en charge LRO sur un adaptateur réseau d'une machine virtuelle Windows afin de garantir que le système d'exploitation invité n'utilise aucune ressource pour agréger les paquets entrants dans de plus grands tampons.

Sous Windows, la technologie LRO est également appelée coalescence côté réception (RSC, Receive Side Coalescing).

Conditions préalables

- Vérifiez que la machine virtuelle exécute Windows Server 2012 ou version ultérieure, ou Windows 8 ou version ultérieure.
- Vérifiez que la machine virtuelle est compatible avec ESXi 6.0 et versions ultérieures.
- Vérifiez que la version du pilote VMXNET3 installée sur le système d'exploitation invité est 1.6.6.0 ou une version ultérieure.
- Vérifiez que LRO est activé globalement sur une machine virtuelle qui exécute Windows Server 2012 ou version ultérieure, ou Windows 8 ou version ultérieure. Reportez-vous à la section [Gérer LRO globalement sur une machine virtuelle Windows](#).

Procédure

- 1 Dans le **Centre Réseau et partage** du Panneau de configuration du système d'exploitation invité, cliquez sur le nom de l'adaptateur réseau.
Une boîte de dialogue affiche l'état de l'adaptateur.
- 2 Cliquez sur **Propriétés** et, sous le type d'adaptateur réseau VMXNET3, cliquez sur **Configurer**.
- 3 Dans l'onglet **Avancé**, définissez **Coalescence du segment de réception (IPv4)** et **Coalescence du segment de réception (IPv6)** sur **Activé** ou **Désactivé**.
- 4 Cliquez sur **OK**.

Gérer LRO globalement sur une machine virtuelle Windows

Pour utiliser la fonctionnalité LRO (Large Receive offload) sur un adaptateur VMXNET3 sur une machine virtuelle qui fonctionne sous Windows 8 et versions ultérieures, ou Windows Server 2012 et versions ultérieures, vous devez l'activer globalement sur le système d'exploitation invité. Sous Windows, la technologie LRO est également appelée coalescence côté réception (RSC, Receive Side Coalescing).

Procédure

- 1 Pour vérifier si la fonctionnalité LRO est désactivée globalement sur un système d'exploitation invité Windows 8 et versions ultérieures ou Windows Server 2012, exécutez la commande `netsh int tcp show global` dans l'invite de commande.

```
netsh int tcp show global
```

La commande affiche l'état des paramètres TCP (Transmission Control Protocol) globaux définis sur le système d'exploitation Windows 8.x.

```
Paramètres globaux TCP ----- État de la mise
à l'échelle côté réception : activé État du déchargement Chimney : désactivé État
NetDMA : désactivé Accès direct au cache (DCA, Direct Cache Access) : désactivé Niveau
d'auto-réglage de la fenêtre Recevoir : désactivé Fournisseur de contrôle de surcharge
complémentaire : aucun Fonctionnalité ECN : désactivé Horodatage RFC 1323 : désactivé RTO
initial : 3 000 État de coalescence du segment de réception : désactivé
```

Si LRO est globalement désactivé sur la machine Windows 8 et versions ultérieures, ou Windows 2012, la propriété État de coalescence du segment de réception s'affiche comme étant désactivée.

- 2 Pour activer LRO globalement sur le système d'exploitation Windows, exécutez la commande `netsh int tcp set global` à l'invite de commande :

```
netsh int tcp set global rsc=enabled
```

Étape suivante

Activez LRO pour l'adaptateur VMXNET3 sur la machine virtuelle Windows 8 et versions ultérieures, ou Windows Server 2012. Reportez-vous à la section [Gérer LRO sur un adaptateur VMXNET3 sur une machine virtuelle Windows](#).

NetQueue et performances réseau

NetQueue tire parti de la possibilité de certains adaptateurs réseau de distribuer le trafic réseau vers le système dans plusieurs files d'attente de réception pouvant être traitées séparément, ce qui permet de dimensionner le traitement au niveau de plusieurs processeurs et d'améliorer les performances réseau à la réception.

Pour utiliser efficacement les files d'attente Rx dans les cartes réseau physiques en gérant la vNIC et les filtres d'adaptateur VMkernel, l'équilibrage NetQueue dans ESXi utilise des algorithmes d'équilibrage de charge.

Vous pouvez activer ou désactiver les différents types de files d'attente Rx. Pour plus d'informations, reportez-vous à la commande `esxcli network nic queue loadbalancer set` dans la documentation *Référence d'ESXCLI*.

Activer NetQueue sur un hôte

NetQueue est activé par défaut. Pour pouvoir utiliser NetQueue après qu'il ait été désactivé, vous devez le réactiver.

Conditions préalables

Procédure

- 1 Dans ESXi Shell, sur l'hôte, utilisez la commande suivante :

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

- 2 Pour configurer le pilote de carte réseau afin qu'il utilise NetQueue, utilisez la commande `esxcli module parameters set`.

Pour configurer le pilote avec huit files d'attente de réception sur une carte réseau Emulex à deux ports, exécutez cette commande ESXCLI.

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```

- 3 Redémarrez l'hôte.

Désactiver NetQueue sur un hôte

NetQueue est activé par défaut.

Conditions préalables

Prenez connaissance des informations sur la configuration des pilotes NIC dans *Démarrage avec ESXCLI*.

Procédure

- 1 Dans l'ESXCLI, utilisez la commande suivante, en fonction de la version de l'hôte :

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```

- 2 Pour désactiver NetQueue sur le pilote de carte réseau, utilisez la commande `esxcli module parameters set`.

Pour configurer le pilote avec une file d'attente de réception, exécutez les commandes ESXCLI sur une carte réseau Emulex à deux ports.

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```

- 3 Redémarrez l'hôte.

vSphere Network I/O Control

11

Utilisez vSphere Network I/O Control pour allouer de la bande passante réseau aux applications stratégiques et pour résoudre les problèmes issus de l'utilisation de ressources communes par différents types de trafic.

- **Qu'est-ce que vSphere Network I/O Control ?**

vSphere Network I/O Control version 3 présente une méthode de réservation de la bande passante pour le trafic système qui se fonde sur la capacité des adaptateurs physiques d'un hôte. Elle permet de contrôler de manière plus précise les ressources au niveau de l'adaptateur réseau de machine virtuelle, en suivant le modèle d'allocation des ressources de mémoire et de CPU.

- **Activer Network I/O Control sur un vSphere Distributed Switch**

Activez la gestion des ressources réseau sur un vSphere Distributed Switch afin de garantir la quantité de bande passante minimale au trafic système (pour les fonctionnalités de vSphere) et au trafic de machine virtuelle.

- **Allouer de la bande passante au trafic système**

Vous pouvez configurer Network I/O Control de manière à allouer une certaine quantité de bande passante au trafic généré par vSphere Fault Tolerance, vSphere vMotion et autres.

- **Allouer de la bande passante au trafic de la machine virtuelle**

La version 3 de Network I/O Control vous permet de configurer la bande passante requise des machines virtuelles individuelles. Vous pouvez également utiliser des pools de ressources réseau, dans lesquels vous attribuez un quota de bande passante à partir de la réservation agrégée pour le trafic de machines virtuelles, avant d'allouer de la bande passante aux machines virtuelles individuelles depuis le pool.

- **Retirer un adaptateur physique de l'étendue de Network I/O Control**

Si certaines conditions sont réunies, vous pouvez être amené à exclure des adaptateurs physiques à faible capacité du modèle d'allocation de bande passante de Network I/O Control version 3.

Qu'est-ce que vSphere Network I/O Control ?

vSphere Network I/O Control version 3 présente une méthode de réservation de la bande passante pour le trafic système qui se fonde sur la capacité des adaptateurs physiques d'un hôte.

Elle permet de contrôler de manière plus précise les ressources au niveau de l'adaptateur réseau de machine virtuelle, en suivant le modèle d'allocation des ressources de mémoire et de CPU.

Avec la version 3 de la fonctionnalité Network I/O Control, l'allocation et la réservation des ressources réseau sont améliorées sur l'ensemble du commutateur.

Modèles de réservation des ressources de bande passante

Network I/O Control version 3 prend en charge différents modèles de gestion des ressources des machines virtuelles et du trafic système relatif aux services d'infrastructure (comme vSphere Fault Tolerance).

Ces deux catégories de trafic sont différentes par nature. Le trafic système est exclusivement associé à un hôte ESXi. Le trafic réseau ne suit plus le même itinéraire lorsque vous migrez une machine virtuelle au sein de l'environnement. Dans Network I/O Control, pour fournir des ressources réseau à une machine virtuelle quel que soit l'hôte, vous pouvez configurer une allocation des ressources pour les machines virtuelles qui est valide dans l'étendue du Distributed Switch.

Garantie de bande passante pour les machines virtuelles

Network I/O Control version 3 provisionne les adaptateurs réseau des machines virtuelles en bande passante en utilisant les parts et les valeurs de réservation et de limite définis. Grâce à ces données, les charges de travail virtualisées peuvent compter sur le contrôle d'admission de vSphere Distributed Switch, vSphere DRS et vSphere HA pour s'assurer de recevoir une quantité suffisante de bande passante. Reportez-vous à la section [Contrôle d'admission pour la bande passante des machines virtuelles](#).

Disponibilité des fonctionnalités

SR-IOV n'est pas disponible pour les machines virtuelles configurées pour utiliser la version 3 de Network I/O Control.

Activer Network I/O Control sur un vSphere Distributed Switch

Activez la gestion des ressources réseau sur un vSphere Distributed Switch afin de garantir la quantité de bande passante minimale au trafic système (pour les fonctionnalités de vSphere) et au trafic de machine virtuelle.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Paramètres > Modifier les paramètres**.

- 3 Dans le menu déroulant **Network I/O Control**, sélectionnez **Activer**.

Note Lorsque la compatibilité des déchargements réseau est activée, **Network I/O Control** est désactivé. Lorsque **Déchargements réseau** est défini sur **Aucun**, **Network I/O Control** est pris en charge.

- 4 Cliquez sur **OK**.

Résultats

Lorsque Network I/O Control est activé, le modèle qu'il utilise pour gérer l'allocation de bande passante pour le trafic système et le trafic de machine virtuelle provient de la version de Network I/O Control qui est active sur le Distributed Switch. Reportez-vous à la section [Qu'est-ce que vSphere Network I/O Control ?](#) .

Allouer de la bande passante au trafic système

Vous pouvez configurer Network I/O Control de manière à allouer une certaine quantité de bande passante au trafic généré par vSphere Fault Tolerance, vSphere vMotion et autres.

Si vous utilisez Network I/O Control sur un Distributed Switch, vous pouvez configurer le mode d'allocation de bande passante pour le trafic relatif aux principales fonctionnalités de vSphere :

- Gestion
- Fault Tolerance
- NFS
- vSAN
- vMotion
- vSphere Replication
- Sauvegarde de vSphere Data Protection
- Machine virtuelle
- NVMe over TCP

vCenter Server propage l'allocation à partir du Distributed Switch vers chaque adaptateur physique des hôtes qui y sont connectés.

- [Paramètres d'allocation de bande passante pour le trafic système](#)

Network I/O Control alloue la bande passante au trafic provenant des fonctionnalités du système vSphere de base à l'aide de plusieurs paramètres de configuration.

- [Exemple de réservation de bande passante pour le trafic système](#)

La capacité des adaptateurs physiques détermine la bande passante garantie. En fonction de cette capacité, vous pouvez garantir une quantité de bande passante minimale à une fonctionnalité système afin qu'elle fonctionne de manière optimale.

■ **Allocation de bande passante pour le trafic système**

Attribuez de la bande passante pour la gestion des hôtes, les machines virtuelles, le stockage NFS, vSphere vMotion, vSphere Fault Tolerance, vSAN et vSphere Replication sur les adaptateurs physiques connectés à un vSphere Distributed Switch.

Paramètres d'allocation de bande passante pour le trafic système

Network I/O Control alloue la bande passante au trafic provenant des fonctionnalités du système vSphere de base à l'aide de plusieurs paramètres de configuration.

Tableau 11-1. Paramètres d'allocation pour le trafic système

Paramètre d'allocation de bande passante	Description
Parts	<p>Les parts (valeur de 1 à 100) désignent la priorité relative d'un type de trafic système par rapport aux autres types actifs sur le même adaptateur physique.</p> <p>La quantité de bande passante disponible pour un type de trafic système est déterminée par les parts définies et par la quantité de données transmises par les autres fonctionnalités du système.</p>
Réservation	<p>Quantité minimale de bande passante (en Mo/s) garantie sur chaque adaptateur physique. La quantité totale de bande passante réservée sur tous les types de trafic système ne peut pas dépasser 75 % de la bande passante que peut fournir l'adaptateur réseau physique de plus faible capacité.</p> <p>La bande passante non utilisée est mise à disposition des autres types de trafic système. Toutefois, Network I/O Control ne redistribue pas la capacité non utilisée par le trafic système au placement des machines virtuelles.</p>
Limite	<p>Quantité maximale de bande passante (en Mo/s) qu'un type de trafic système peut consommer sur chaque adaptateur physique.</p>

Exemple de réservation de bande passante pour le trafic système

La capacité des adaptateurs physiques détermine la bande passante garantie. En fonction de cette capacité, vous pouvez garantir une quantité de bande passante minimale à une fonctionnalité système afin qu'elle fonctionne de manière optimale.

Par exemple, sur un Distributed Switch connecté à des hôtes ESXi dotés d'adaptateurs réseau 10 GbE, vous pouvez configurer la réservation de manière à garantir 1 Go/s pour la gestion à travers vCenter Server, 1 Go/s pour vSphere Fault Tolerance, 1 Go/s pour le trafic vSphere vMotion et 0,5 Go/s pour le trafic de machine virtuelle. Network I/O Control alloue la bande passante requise à chaque adaptateur réseau physique. Vous ne pouvez pas réserver plus de 75 % de la bande passante d'un adaptateur réseau physique, c'est-à-dire 7,5 Go/s.

Vous pouvez ne pas réserver toute la capacité. Cela permet de laisser l'hôte allouer de la bande passante de forme dynamique en fonction des parts, des limites et de l'usage et de réserver uniquement la quantité de bande passante qui suffit au bon fonctionnement d'une fonctionnalité du système.

Allocation de bande passante pour le trafic système

Attribuez de la bande passante pour la gestion des hôtes, les machines virtuelles, le stockage NFS, vSphere vMotion, vSphere Fault Tolerance, vSAN et vSphere Replication sur les adaptateurs physiques connectés à un vSphere Distributed Switch.

Pour activer l'allocation de bande passante des machines virtuelles avec Network I/O Control, configurez le trafic système des machines virtuelles. La réservation de bande passante du trafic de machine virtuelle s'utilise également dans le contrôle d'admission. Lorsque vous mettez une machine virtuelle sous tension, le contrôle d'admission vérifie que la quantité suffisante de bande passante est disponible.

Conditions préalables

- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.
- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.
- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Allocation des ressources**.
- 3 Cliquez sur **Trafic système**.

L'allocation de bande passante pour les types de trafic système s'affiche.

- 4 Sélectionnez le type de trafic selon la fonctionnalité de vSphere à provisionner, puis cliquez sur **Modifier**.

Les paramètres de ressources réseau du type de trafic en question s'affichent.

- 5 Dans le menu déroulant **Parts**, modifiez la part du trafic dans le flux global à travers un adaptateur physique.

Network I/O Control applique les parts configurées lorsqu'un adaptateur physique est saturé.

Vous pouvez sélectionner une option pour définir une valeur prédéfinie, ou sélectionner **Personnalisé** et taper un nombre compris entre 1 et 100 pour définir une autre part.

- 6 Dans la zone de texte **Réservation**, entrez une valeur correspondant à la quantité minimale de bande passante qui doit être disponible pour le type de trafic.

La réservation totale du trafic système ne doit pas dépasser 75 % de la bande passante prise en charge par l'adaptateur physique, en considérant la capacité la plus faible de tous les adaptateurs connectés au Distributed Switch.

- 7 Dans une zone de texte **Limite**, définissez la bande passante maximale pouvant être utilisée par le trafic système du type sélectionné.
- 8 Cliquez sur **OK** pour appliquer les paramètres d'allocation.

Résultats

vCenter Server propage l'allocation à partir du Distributed Switch vers chaque adaptateur physique des hôtes qui y sont connectés.

Allouer de la bande passante au trafic de la machine virtuelle

La version 3 de Network I/O Control vous permet de configurer la bande passante requise des machines virtuelles individuelles. Vous pouvez également utiliser des pools de ressources réseau, dans lesquels vous attribuez un quota de bande passante à partir de la réservation agrégée pour le trafic de machines virtuelles, avant d'allouer de la bande passante aux machines virtuelles individuelles depuis le pool.

Allouer de la bande passante à des machines virtuelles

Network I/O Control utilise deux modèles pour allouer de la bande passante aux machines virtuelles : l'allocation sur l'ensemble du vSphere Distributed Switch en fonction des pools de ressources réseau et l'allocation sur l'adaptateur physique qui transporte le trafic d'une machine virtuelle.

Pools de ressources réseau

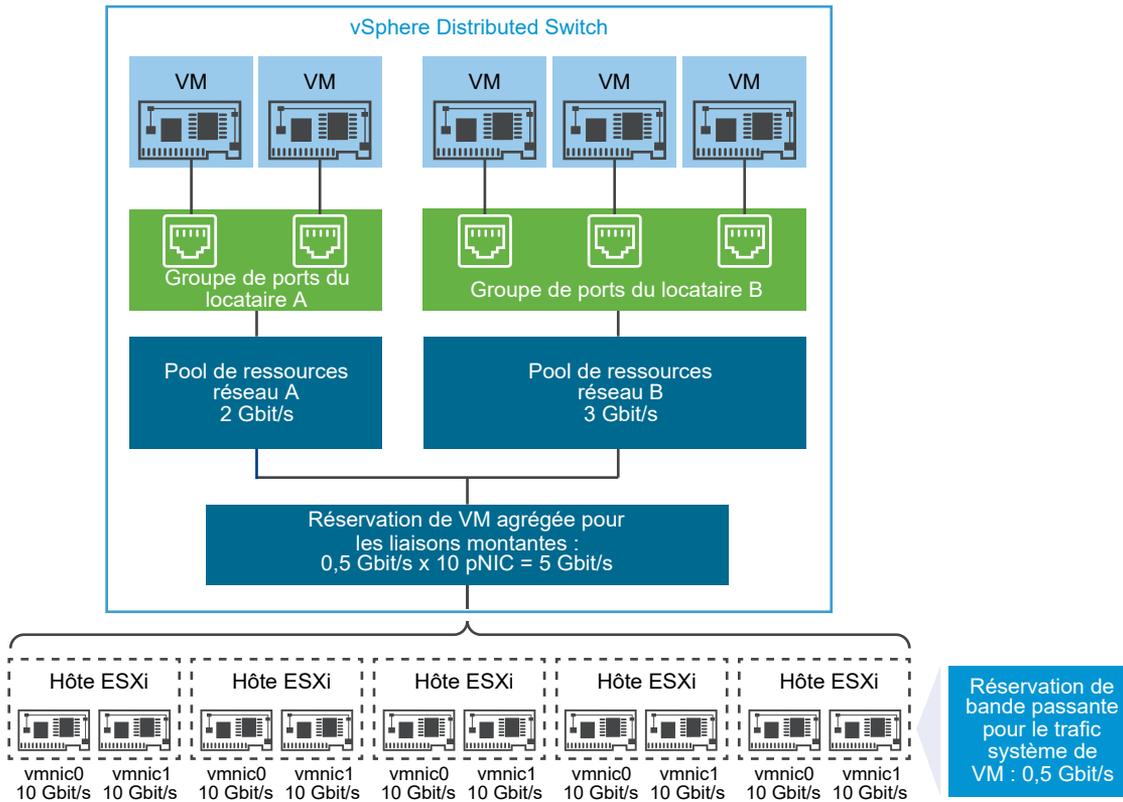
Un pool de ressources réseau représente une partie de la bande passante agrégée qui est réservée pour le trafic système des machines virtuelles sur tous les adaptateurs physiques connectés au Distributed Switch.

Par exemple, si une bande passante de 0,5 Go/s est réservée sur chaque liaison montante 10 GbE d'un Distributed Switch qui en possède 10, la bande passante agrégée totale pour la réservation de machine virtuelle est de 5 Go/s. Chaque pool de ressources réseau peut réserver un quota d'une capacité de 5 Go/s.

Le quota de bande passante dédié à un pool de ressources réseau est réparti entre les différents groupes de ports distribués associés au pool. Le pool envoie une quantité de bande passante à la machine virtuelle à travers le groupe de ports distribués à laquelle elle est connectée.

Par défaut, les groupes de ports distribués du commutateur sont attribués à un pool de ressources réseau appelé « default » et dont le quota n'est pas configuré.

Figure 11-1. Agrégation de bande passante pour les pools de ressources réseau dans les liaisons montantes d'un vSphere Distributed Switch



Définition de la bande passante requise pour une machine virtuelle

Vous allouez de la bande passante à une machine virtuelle individuelle de la même façon que vous allouez des ressources de mémoire et de CPU. Network I/O Control version 3 provisionne une machine virtuelle en bande passante en fonction des parts et des valeurs de réservation et de limite définies dans les paramètres matériels de machine virtuelle pour un adaptateur réseau. La réservation permet de garantir une quantité minimale de bande passante : le trafic de la machine virtuelle sera en droit de consommer cette quantité au moins. Si un adaptateur physique dispose de davantage de capacité, la machine virtuelle pourra alors éventuellement utiliser de la bande passante supplémentaire, selon les parts et la valeur de limite spécifiées.

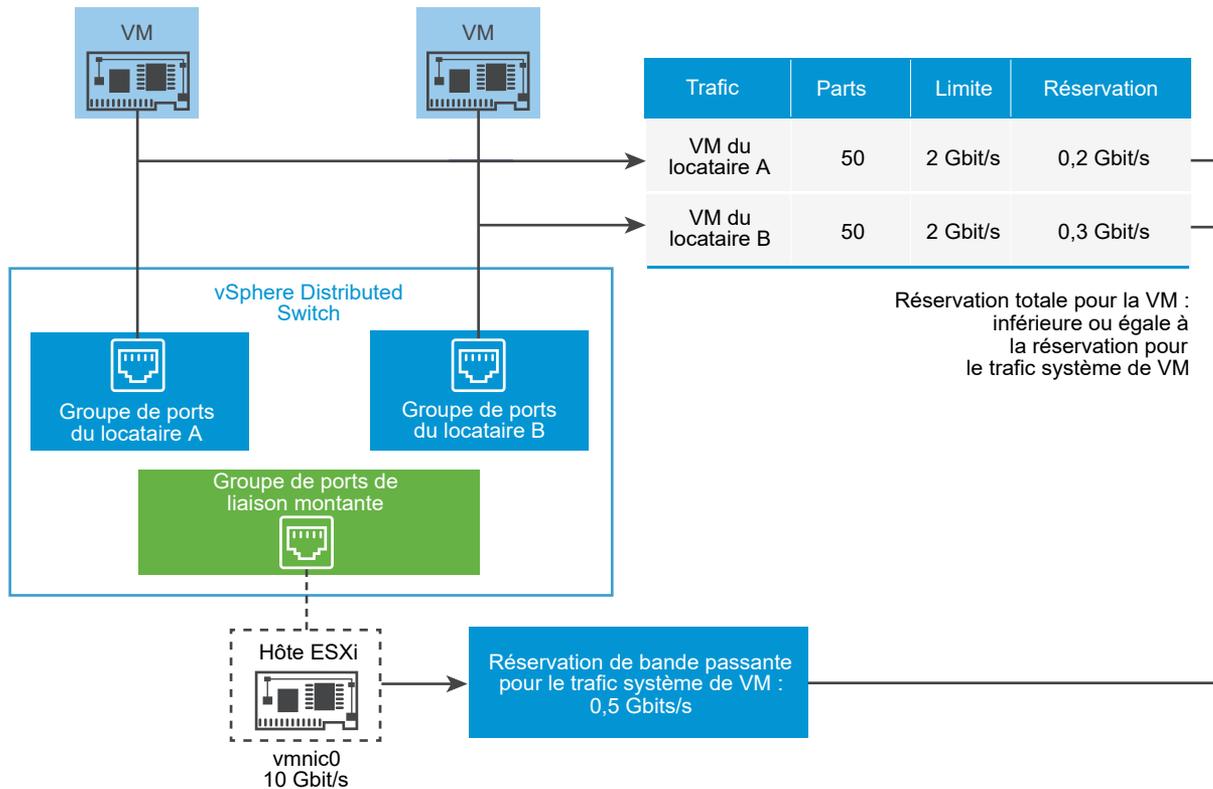
Provisionnement en bande passante d'une machine virtuelle sur l'hôte

Pour garantir une certaine quantité de bande passante, Network I/O Control utilise un moteur de placement du trafic qui s'active lorsqu'une réservation de bande passante est configurée pour une machine virtuelle. Le Distributed Switch tente de placer le trafic provenant d'un adaptateur réseau de machine virtuelle sur un adaptateur physique qui peut fournir la bande passante requise dans l'étendue de la stratégie d'association active.

La réservation de bande passante totale pour les machines virtuelles d'un hôte ne doit pas dépasser la bande passante réservée configurée pour le trafic système des machines virtuelles.

La limite et la réservation réelles dépendent également de la stratégie de formation du trafic appliquée au groupe de ports distribués auquel l'adaptateur est connecté. Par exemple, si une limite de 200 Mo/s est requise pour un adaptateur réseau de machine virtuelle et que la bande passante moyenne configurée de la stratégie de formation du trafic est de 100 Mo/s, la limite réelle sera de 100 Mo/s.

Figure 11-2. Configuration relative à l'allocation de bande passante pour les machines virtuelles individuelles



Dans Network I/O Control, la réservation de bande passante pour une machine virtuelle est garantie en fonction de la réservation du trafic système des machines virtuelles définie sur l'adaptateur physique qui envoie de trafic à partir de la machine virtuelle.

Paramètres d'allocation de bande passante pour le trafic de machine virtuelle

Network I/O Control version 3 alloue de la bande passante aux machines virtuelles individuelles en fonction des parts et des valeurs de réservation et de limite définies dans les paramètres matériels de machine virtuelle pour les adaptateurs réseau.

Tableau 11-2. Paramètres d'allocation de bande passante pour un adaptateur réseau de machine virtuelle

Paramètre d'allocation de bande passante	Description
Parts	Priorité relative (valeur entre 1 et 100) du trafic qui passe par cet adaptateur réseau de machine virtuelle par rapport à la capacité de l'adaptateur physique qui transporte le trafic de machine virtuelle sur le réseau.
Réservation	Quantité minimale de bande passante (en Mo/s) que l'adaptateur réseau de machine virtuelle reçoit sur l'adaptateur physique.
Limite	Quantité maximale de bande passante sur l'adaptateur réseau de machine virtuelle pour le trafic des autres machines virtuelles sur le même hôte ou sur un autre.

Contrôle d'admission pour la bande passante des machines virtuelles

Pour garantir qu'une machine virtuelle dispose de suffisamment de bande passante, vSphere effectue un contrôle d'admission au niveau de l'hôte et au niveau du cluster basé sur la stratégie d'association et la réservation de la bande passante.

Contrôle d'admission de la bande passante dans vSphere Distributed Switch

Lorsque vous mettez une machine virtuelle sous tension, la fonctionnalité Network I/O Control d'un Distributed Switch vérifie que l'hôte remplit les conditions suivantes.

- Un adaptateur physique de l'hôte doit fournir la bande passante minimale aux adaptateurs réseau des machines virtuelles, conformément à la stratégie d'association et à la réservation.
- La réservation pour un adaptateur réseau de machine virtuelle est inférieur au quota libre du pool de ressources réseau.

Si vous modifiez la réservation de l'adaptateur réseau d'une machine virtuelle en cours d'exécution, Network I/O Control vérifie de nouveau si le pool de ressources réseau associé peut prendre en charge la nouvelle réservation. Si le quota non réclamé du pool est insuffisant, la modification ne s'applique pas.

Pour utiliser le contrôle d'admission dans vSphere Distributed Switch, effectuez les tâches suivantes :

- Configurez l'allocation de bande passante du trafic système des machines virtuelles sur le Distributed Switch.
- Configurez un pool de ressources réseau avec quota de réservation à partir de la bande passante configurée pour le trafic système des machines virtuelles.
- Associez le pool de ressources réseau au groupe de ports distribués qui connecte les machines virtuelles au commutateur.
- Configurez la bande passante requise pour une machine virtuelle connectée au groupe de ports.

Contrôle d'admission de la bande passante dans vSphere DRS

Si vous mettez sous tension une machine virtuelle se trouvant dans un cluster, vSphere DRS place la machine virtuelle sur un hôte disposant de la capacité requise pour garantir la bande passante réservée pour la machine virtuelle selon la stratégie d'association active.

vSphere DRS répond aux besoins de la réservation de bande passante de la machine virtuelle en migrant cette dernière vers un autre hôte dans les cas de figure suivants :

- La valeur de la réservation est modifiée et l'hôte initial n'est plus en mesure de fournir cette valeur.
- Un adaptateur physique qui transporte le trafic depuis la machine virtuelle est hors ligne.

Pour utiliser le contrôle d'admission dans vSphere DRS, effectuez les tâches suivantes :

- Configurez l'allocation de bande passante du trafic système des machines virtuelles sur le Distributed Switch.
- Configurez la bande passante requise pour une machine virtuelle connectée au Distributed Switch.

Pour plus d'informations sur la gestion des ressources selon les besoins en bande passante des machines virtuelles, reportez-vous à la documentation *Gestion des ressources vSphere*.

Contrôle d'admission de la bande passante dans vSphere HA

Lorsqu'un hôte échoue ou est isolé, vSphere HA met sous tension une machine virtuelle sur un autre hôte du cluster, en fonction de la réservation de bande passante et de la stratégie d'association.

Pour utiliser le contrôle d'admission dans vSphere HA, effectuez les tâches suivantes :

- Allouez de la bande passante au trafic système des machines virtuelles.
- Configurez la bande passante requise pour une machine virtuelle connectée au Distributed Switch.

Pour plus d'informations sur la mise en place d'un basculement par vSphere HA selon les besoins en bande passante des machines virtuelles, reportez-vous à la documentation *Disponibilité vSphere*.

Créer un pool de ressources réseau

Réservez de la bande passante pour un ensemble de machines virtuelles en créant des pools de ressources réseau sur un vSphere Distributed Switch.

Un pool de ressources réseau permet de disposer d'un quota de réservation pour les machines virtuelles. Ce quota représente une partie de la bande passante qui est réservée au trafic système des machines virtuelles sur les adaptateurs physiques connectés au Distributed Switch. Vous pouvez mettre de côté pour les machines virtuelles associées au pool une quantité de bande passante de ce quota. La réservation des adaptateurs réseau des machines virtuelles sous tension associées au pool ne doit pas dépasser la valeur du quota du pool. Reportez-vous à [Allouer de la bande passante à des machines virtuelles](#).

Conditions préalables

- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.
- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.
- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).
- Vérifiez qu'une réservation de bande passante a été configurée pour le trafic système des machines virtuelles. Reportez-vous à la section [Allocation de bande passante pour le trafic système](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Allocation des ressources**.
- 3 Cliquez sur **Pools de ressources réseau**.
- 4 Cliquez sur l'icône **Ajouter**.
- 5 (Facultatif) Tapez un nom et une description pour le pool de ressources réseau.
- 6 Entrez une valeur dans **Quota de réservation** (en Mo/s) à partir de la bande passante disponible qui est réservée pour le trafic système des machines virtuelles.

Le quota maximal pouvant être attribué au pool est calculé selon la formule suivante :

```
max reservation quota = aggregated reservation for vm system traffic - quotas of the other resource pools
```

où

- `aggregated reservation for vm system traffic` = réservation de bande passante configurée pour le trafic système des machines virtuelles sur chaque carte réseau physique * nombre de cartes réseau physiques connectées au Distributed Switch
- `quotas of the other pools` = somme des quotas de réservation des autres pools de ressources réseau

- 7 Cliquez sur **OK**.

Étape suivante

Ajoutez au moins un groupe de ports distribués au pool de ressources réseau de manière à allouer de la bande passante aux machines virtuelles individuelles à partir du quota du pool. Reportez-vous à [Ajouter un groupe de ports distribués à un pool de ressources réseau](#).

Ajouter un groupe de ports distribués à un pool de ressources réseau

Si vous ajoutez un groupe de ports distribués à un pool de ressources réseau, vous pouvez allouer de la bande passante aux machines virtuelles qui sont connectées au groupe de ports.

Pour attribuer un pool de ressources réseau à plusieurs groupes de ports distribués à la fois, vous pouvez utiliser la stratégie d'allocation des ressources dans l'assistant **Gérer des groupes de ports distribués**. Reportez-vous à la section [Gérer les règles pour plusieurs groupes de ports sur vSphere Distributed Switch](#).

Network I/O Control se base sur la version de Network I/O Control qui est active sur le Distributed Switch pour allouer de la bande passante aux machines virtuelles associées au groupe de ports distribués. Reportez-vous à la section [Qu'est-ce que vSphere Network I/O Control ?](#).

Conditions préalables

- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués et sélectionnez **Modifier les paramètres**.
- 3 Dans la boîte de dialogue Modifier les paramètres, cliquez sur **Général**.
- 4 Dans le menu déroulant **Pool de ressources réseau**, sélectionnez le pool de ressources réseau et cliquez sur **OK**.

Si le Distributed Switch ne contient aucun pool de ressources réseau, seule l'option (**par défaut**) apparaît dans le menu déroulant.

Configurer l'allocation de bande passante d'une machine virtuelle

Vous pouvez configurer l'allocation de bande passante des machines virtuelles individuelles qui sont connectées à un groupe de ports distribués. Vous pouvez utiliser les paramètres de parts, de réservation et de limite pour la bande passante.

Conditions préalables

- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.

- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.
- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).
- Vérifiez qu'une réservation de bande passante a été configurée pour le trafic système des machines virtuelles. Reportez-vous à la section [Allocation de bande passante pour le trafic système](#).

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 3 Développez la section Adaptateur réseau de l'adaptateur réseau de machine virtuelle.
- 4 Si vous souhaitez configurer l'allocation de bande passante pour un nouvel adaptateur réseau de machine virtuelle, dans le menu déroulant **Ajouter un nouveau périphérique**, sélectionnez **Adaptateur réseau**.

Une section Nouveau réseau apparaît, contenant des options d'allocation de bande passante et d'autres paramètres d'adaptateur réseau.

- 5 Si l'adaptateur réseau de machine virtuelle n'est pas connecté au groupe de ports distribués, sélectionnez le groupe de ports dans le menu déroulant situé en regard de la section Adaptateur réseau ou Nouvelle étiquette de réseau.
- 6 Dans le menu déroulant **Parts**, définissez la priorité relative du trafic à partir de cette machine virtuelle en tant que parts de la capacité de l'adaptateur physique connecté.

Network I/O Control applique les parts configurées lorsqu'un adaptateur physique est saturé.

Vous pouvez sélectionner une option pour définir une valeur prédéfinie, ou sélectionner **Personnalisé** et taper un nombre compris entre 1 et 100 pour définir une autre part.

- 7 Dans la zone de texte **Réservation**, réservez une bande passante minimale dont l'adaptateur réseau de la machine virtuelle doit disposer à la mise sous tension de la machine virtuelle.

Si vous provisionnez de la bande passante en utilisant un pool de ressources réseau, la réservation à partir des adaptateurs réseau des machines virtuelles sous tension qui sont associés au pool ne doit pas dépasser le quota du pool.

Si vSphere DRS est activé, pour mettre sous tension la machine virtuelle, assurez-vous que la réservation de tous les adaptateurs réseau de machine virtuelle sur l'hôte ne dépasse pas la bande passante réservée au trafic système des machines virtuelles sur les adaptateurs physiques de l'hôte.

- 8 Dans la zone de texte **Limite**, définissez une limite de bande passante que l'adaptateur réseau de machine virtuelle peut consommer.
- 9 Cliquez sur **OK**.

Résultats

Réseau

I/O Control alloue la bande passante qui était réservée pour l'adaptateur réseau de la machine virtuelle, sans tenir compte du quota de réservation défini pour le pool de ressources réseau.

Configurer l'allocation de bande passante sur plusieurs machines virtuelles

Configurer l'allocation de bande passante sur plusieurs machines virtuelles connectées à un pool de ressources réseau spécifique en une seule fois, par exemple après la mise à niveau vers Network I/O Control version 3.

Conditions préalables

- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.
- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.
- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).
- Vérifiez qu'une réservation de bande passante a été configurée pour le trafic système des machines virtuelles. Reportez-vous à la section [Allocation de bande passante pour le trafic système](#).
- Vérifiez que les machines virtuelles sont associées à un pool de ressources réseau spécifique à travers les groupes de ports distribués connectés. Reportez-vous à [Ajouter un groupe de ports distribués à un pool de ressources réseau](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Allocation des ressources**.
- 3 Cliquez sur **Pools de ressources réseau**.
- 4 Sélectionnez un pool de ressources réseau.
- 5 Cliquez sur **Machines virtuelles**.

La liste des adaptateurs réseau de machine virtuelle connectés au pool de ressources réseau sélectionné s'affiche.

- 6 Sélectionnez les adaptateurs réseau de machine virtuelle dont vous souhaitez configurer les paramètres, puis cliquez sur **Modifier**.

- 7 Dans le menu déroulant **Parts**, définissez la priorité relative du trafic provenant de ces machines virtuelles dans l'étendue des adaptateurs physiques qui transportent le trafic.
Network I/O Control applique les parts configurées lorsqu'un adaptateur physique est saturé.
- 8 Dans la zone de texte **Réservation**, réservez la bande passante minimale qui doit être disponible pour chaque adaptateur réseau de machine virtuelle lorsque les machines virtuelles sont sous tension.
Si vous provisionnez de la bande passante en utilisant un pool de ressources réseau, la réservation à partir des adaptateurs réseau des machines virtuelles sous tension qui sont associés au pool ne doit pas dépasser le quota du pool.
- 9 Dans la zone de texte **Limite**, définissez la quantité limite de bande passante que chaque adaptateur réseau de machine virtuelle peut consommer.
- 10 Cliquez sur **OK**.

Modifier le quota d'un pool de ressources réseau

Vous pouvez modifier le quota de bande passante à réserver pour les machines virtuelles connectées à un ensemble de groupes de ports distribués.

Conditions préalables

- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.
- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.
- Vérifiez que Network I/O Control est activé. Reportez-vous à la section [Activer Network I/O Control sur un vSphere Distributed Switch](#).
- Vérifiez qu'une réservation de bande passante a été configurée pour le trafic système des machines virtuelles. Reportez-vous à la section [Allocation de bande passante pour le trafic système](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Allocation des ressources**.
- 3 Cliquez sur **Pools de ressources réseau**.
- 4 Sélectionnez un pool de ressources réseau de la liste et cliquez sur **Modifier**.
- 5 Dans la zone de texte **Quota de réservation**, entrez le quota de bande passante pour les machines virtuelles, issu de l'agrégation de bande passante disponible réservée pour le trafic système des machines virtuelles sur tous les adaptateurs physiques du commutateur.
- 6 Cliquez sur **OK**.

Supprimer un groupe de ports distribués d'un pool de ressources réseau

Pour interrompre l'allocation de bande passante aux machines virtuelles du quota de réservation d'un pool de ressources réseau, supprimez l'association entre le groupe de ports auquel les machines virtuelles sont connectées et le pool.

Procédure

- 1 Recherchez un groupe de ports distribués dans vSphere Client.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Groupes de ports distribués**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués et sélectionnez **Modifier les paramètres**.
- 3 Dans la boîte de dialogue Modifier les paramètres du groupe de ports, cliquez sur **Général**.
- 4 Dans le menu déroulant **Pool de ressources réseau**, sélectionnez (**par défaut**) et cliquez sur **OK**.

Résultats

Le groupe de ports distribués est alors associé au pool de ressources réseau des machines virtuelles par défaut.

Supprimer un pool de ressources réseau

Vous pouvez supprimer un pool de ressources réseau qui n'est plus utilisé.

Conditions préalables

Dissociez le pool de ressources réseau de tous les groupes de ports distribués qui y sont associés. Reportez-vous à la section [Supprimer un groupe de ports distribués d'un pool de ressources réseau](#).

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Allocation des ressources**.
- 3 Cliquez sur **Pools de ressources réseau**.
- 4 Sélectionnez un pool de ressources et cliquez sur **Supprimer**.
- 5 Cliquez sur **OK** pour supprimer le pool de ressources.

Retirer un adaptateur physique de l'étendue de Network I/O Control

Si certaines conditions sont réunies, vous pouvez être amené à exclure des adaptateurs physiques à faible capacité du modèle d'allocation de bande passante de Network I/O Control version 3.

Par exemple, si l'allocation de bande passante d'un vSphere Distributed Switch est personnalisée avec des cartes réseau 10 GbE, vous ne pourrez peut-être pas ajouter de carte réseau 1 GbE au commutateur, car ce type de carte ne répond pas aux exigences en matière d'allocation configurées sur les cartes réseau 10 GbE.

Conditions préalables

- Vérifiez que l'hôte exécute ESXi 6.5 ou version ultérieure.
- Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.
- Vérifiez que la version 3 de Network I/O Control est bien utilisée sur le commutateur.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système** et sélectionnez **Paramètres système avancés**.
- 3 Dans le paramètre `Net.IOControlPnicOptOut`, indiquez sous forme de liste séparée par des virgules les adaptateurs physiques qui doivent fonctionner hors de l'étendue de Network I/O Control.

Par exemple : `vmnic0,vmnic3`
- 4 Cliquez sur **OK** pour appliquer les modifications.

Gestion des adresses MAC

12

Les adresses MAC sont utilisées dans la couche 2 (la couche de liaison de données) de la pile de protocole réseau pour transmettre des trames à un destinataire. Dans vSphere, vCenter Server génère des adresses MAC pour les adaptateurs de machine virtuelle et les adaptateurs VMkernel, ou vous pouvez attribuer des adresses manuellement.

Chaque fabricant de carte réseau se voit attribuer un préfixe unique à trois octets nommé OUI (Organizationally Unique Identifier) qu'il peut utiliser pour générer des adresses MAC uniques.

VMware prend en charge plusieurs mécanismes d'allocation d'adresses, dont le OUI est différent pour chacun d'eux :

- Adresses MAC générées
 - Attribué par vCenter Server
 - Attribuées par l'hôte ESXi
- Adresses MAC configurées manuellement
- Générées pour les machines virtuelles héritées, mais plus utilisées avec ESXi

Si vous reconfigurez l'adaptateur réseau d'une machine virtuelle hors tension, par exemple en modifiant le type d'allocation d'adresses MAC automatique ou en définissant une adresse MAC statique, vCenter Server résout tous les conflits d'adresses MAC avant que la reconfiguration de l'adaptateur prenne effet.

Ce chapitre contient les rubriques suivantes :

- [Attribution d'adresses MAC depuis vCenter Server](#)
- [Génération d'adresse MAC sur des hôtes ESXi](#)
- [Définition d'une adresse MAC statique sur une machine virtuelle](#)

Attribution d'adresses MAC depuis vCenter Server

vSphere offre plusieurs schémas d'allocation automatique d'adresses MAC dans vCenter Server. Vous pouvez sélectionner le schéma qui convient le mieux à vos exigences de duplication d'adresses MAC, vos exigences OUI pour les adresses administrées localement ou universellement, etc.

Les schémas suivants de génération d'adresses MAC sont disponibles dans vCenter Server :

- Allocation de VMware OUI, allocation par défaut
- allocation basée sur préfixe
- allocation basée sur plage

Une fois que l'adresse MAC a été générée, elle ne change pas sauf si l'adresse MAC de la machine virtuelle entre en conflit avec celle d'une autre machine virtuelle enregistrée. L'adresse MAC dans le fichier de configuration de la machine virtuelle est enregistrée.

Note Si vous utilisez des valeurs d'allocation basées sur préfixe ou sur plage non valides, une erreur est consignée dans le fichier `vpzd.log`. vCenter Server n'alloue pas d'adresses MAC lors du provisionnement d'une machine virtuelle.

Prévention des conflits d'adresses MAC

L'adresse MAC d'une machine virtuelle hors tension n'est pas comparée aux adresses de machines virtuelles en exécution ou suspendues.

Lors de la remise sous tension d'une machine virtuelle, elle peut acquérir une adresse MAC différente. Le changement peut être causé par un conflit d'adresses avec une autre machine virtuelle. Pendant que cette machine virtuelle était hors tension, son adresse MAC a été attribuée à une autre machine virtuelle qui a été mise sous tension.

Si vous reconfigurez l'adaptateur réseau d'une machine virtuelle hors tension, par exemple en modifiant le type d'allocation d'adresses MAC ou en spécifiant une adresse MAC statique, vCenter Server résout tout conflit d'adresses MAC avant que la reconfiguration de l'adaptateur ne prenne effet.

Pour plus d'informations sur la résolution de conflits d'adresses MAC, reportez-vous à la documentation *Dépannage vSphere*.

Allocation de VMware OUI

L'allocation de VMware OUI (VMware Organizationally Unique Identifier) attribue des adresses MAC sur la base du préfixe VMware OUI par défaut `00:50:56` et de l'ID de vCenter Server.

L'allocation OUI VMware est le modèle d'attribution d'adresse MAC par défaut pour les machines virtuelles. Cette allocation fonctionne avec plus de 64 instances vCenter Server, et chaque vCenter Server peut attribuer jusqu'à 64 000 adresses MAC uniques. Le modèle d'allocation de VMware OUI convient aux déploiements à échelle réduite.

Format d'adresse MAC

Selon le schéma d'allocation de VMware OUI, une adresse MAC est au format `00:50:56:XX:YY:ZZ` où `00:50:56` représente VMware OUI, `XX` est calculé comme étant $(128 + \text{ID vCenter Server})$ et `YY` et `ZZ` sont des nombres hexadécimaux à deux chiffres aléatoires.

Les adresses créées via l'allocation de VMware OUI se trouvent dans la plage 00:50:56:80:YY:ZZ - 00:50:56:BF:YY:ZZ.

Allocation d'adresse MAC par préfixe

Vous pouvez utiliser l'allocation par préfixe pour spécifier un identificateur OUI autre que celui 00:50:56 utilisé par défaut par VMware ou pour introduire des adresses LAA (Locally Administered MAC Addresses) pour un espace d'adressage plus étendu.

L'allocation d'adresses MAC par préfixe permet de s'affranchir des limites de l'allocation VMware par défaut pour fournir des adresses uniques dans des déploiements à plus grande échelle. L'introduction d'un préfixe LAA permet d'obtenir un espace d'adressage MAC très étendu (2 à la puissance 46) au lieu d'un OUI universel unique qui donne uniquement 16 millions d'adresses MAC.

Vérifiez que les préfixes que vous fournissez pour différentes instances de vCenter Server dans le même réseau sont uniques. vCenter Server utilise les préfixes pour éviter les problèmes de duplication d'adresse MAC. Consultez la section [Dépannage de l'allocation d'adresses MAC](#).

Note Les paramètres d'allocation d'adresse MAC par préfixe sont perdus lorsque vous effectuez une mise à niveau vers une nouvelle version de vCenter Server. Vous devez recréer manuellement les paramètres d'allocation MAC par préfixe après la mise à niveau.

Allocation d'adresse MAC basée sur plage

Vous pouvez utiliser l'allocation basée sur plage pour inclure ou exclure des plages d'adresses administrées localement (LAA).

Vous pouvez spécifier une ou plusieurs plages en utilisant des adresses MAC de début et de fin, par exemple, (02:50:68:00:00:02, 02:50:68:00:00:FF). Les adresses MAC sont générées uniquement à partir de la plage spécifiée.

Vous pouvez spécifier plusieurs plages de LAA et vCenter Server suit le nombre d'adresses utilisées pour chaque plage. vCenter Server alloue des adresses MAC de la première plage qui disposent toujours d'adresses disponibles. vCenter Server vérifie les conflits d'adresse MAC dans ses plages.

Lorsque vous utilisez l'allocation basée sur des plages, vous devez fournir différentes instances de vCenter Server avec des plages qui ne se chevauchent pas. vCenter Server ne détecte pas les plages qui peuvent être en conflit avec d'autres instances de vCenter Server. Pour plus d'informations sur la résolution des problèmes d'adresses MAC dupliquées, consultez la section [Dépanner l'allocation d'adresses MAC](#).

Note Les paramètres d'allocation d'adresse MAC basés sur des plages sont perdus lorsque vous effectuez une mise à niveau vers une nouvelle version de vCenter Server. Vous devez recréer manuellement les paramètres d'allocation MAC basés sur la plage après la mise à niveau.

Attribution d'une adresse MAC

Utilisez vSphere Client pour activer l'allocation d'adresses MAC basée sur préfixe ou sur plage, et pour régler les paramètres d'allocation.

Si vous passez d'un type d'allocation à un autre, par exemple de l'allocation OUI VMware à une allocation basée sur plage, utilisez vSphere Client. Cependant, quand un schéma est basé sur préfixe ou sur plage et que vous voulez le changer en un schéma d'allocation différent, vous devez modifier le fichier `vpxd.cfg` manuellement et redémarrer vCenter Server.

Basculer vers ou ajuster les allocations basées sur préfixe ou sur plage

En basculant des OUI VMware par défaut vers l'allocation d'adresse MAC basée sur préfixe ou sur plage via vSphere Client, vous pouvez éviter et résoudre les conflits de duplication d'adresses MAC dans les déploiements vSphere.

Basculez le modèle d'allocation des OUI VMware par défaut vers l'allocation basée sur préfixes ou sur plages à l'aide des **Paramètres avancés** disponibles pour l'instance vCenter Server dans vSphere Client.

Pour retourner de l'allocation basée sur plages ou sur préfixes vers l'allocation OUI VMware, ou pour commuter entre les allocations sur plages et sur préfixes, modifiez le fichier `vpxd.cfg` manuellement. Reportez-vous à la section [Définir ou modifier le type d'allocation](#).

Procédure

- 1 Dans vSphere Client, accédez à une instance de vCenter Server.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et sélectionnez **Paramètres avancés**.
- 3 Cliquez sur **Modifier les paramètres**.
- 4 Ajoutez ou modifiez les paramètres du type d'allocation cible.

Utilisez un seul type d'allocation.

- Passer à l'allocation par préfixe.

Touche	Valeur d'exemple
<code>config.vpxd.macAllocScheme.prefixScheme.prefix</code>	005026
<code>config.vpxd.macAllocScheme.prefixScheme.prefixLength</code>	23

`prefix` et `prefixLength` déterminent la plage de préfixes d'adresse MAC dont disposent les vNIC nouvellement ajoutés. `prefix` est le préfixe OUI en tête des adresses MAC liées à l'instance vCenter Server, et `prefixLength` détermine la longueur en bits du préfixe.

Par exemple, les paramètres du tableau produisent des adresses MAC de carte réseau de machine virtuelle commençant par 00:50:26 ou 00:50:27.

- Passer à l'allocation par plage.

Touche	Valeur d'exemple
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].begin</code>	005067000000
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].end</code>	005067ffffff

X dans `range[X]` représente le numéro séquentiel de la plage. Par exemple, 0 dans `range[0]` représente les paramètres d'allocation de la première plage d'allocation d'adresses MAC.

- 5 Cliquez sur **Enregistrer**.

Définir ou modifier le type d'allocation

Si vous changez une allocation basée sur plage ou sur préfixe par une Allocation de VMware OUI, vous devez définir le type d'allocation dans le fichier `vpxd.cfg` et redémarrez vCenter Server.

Conditions préalables

Choisissez un type d'allocation avant de modifier le fichier `vpxd.cfg`. Pour plus d'information sur les types d'allocation, consultez [Attribution d'adresses MAC depuis vCenter Server](#)

Procédure

- 1 Sur la machine hôte de vCenter Server, accédez au répertoire `/etc/vmware-vpxd`.
- 2 Ouvrez le fichier `vpxd.cfg`
- 3 Décider sur un type d'allocation à utiliser et entrez le code XML correspondant dans le fichier pour configurer le type d'allocation.

Ce qui suit sont des exemples de code XML à utiliser.

Note Utilisez un seul type d'allocation.

- ◆ Allocation de VMware OUI

```
<vpxd>
  <macAllocScheme>
    <VMwareOUI>true</VMwareOUI>
  </macAllocScheme>
</vpxd>
```

- ◆ allocation basée sur préfixe

```
<vpxd>
  <macAllocScheme>
    <prefixScheme>
      <prefix>005026</prefix>
    </prefixScheme>
  </macAllocScheme>
</vpxd>
```

```
<prefixLength>23</prefixLength>
</prefixScheme>
</macAllocScheme>
</vpxd>
```

◆ allocation basée sur plage

```
<vpxd>
  <macAllocScheme>
    <rangeScheme>
      <range id="0">
        <begin>005067000001</begin>
        <end>005067000001</end>
      </range>
    </rangeScheme>
  </macAllocScheme>
</vpxd>
```

- 4 Enregistrez le `vpxd.cfg`
- 5 Redémarrer l'hôte vCenter Server.

Génération d'adresse MAC sur des hôtes ESXi

Un hôte ESXi génère l'adresse MAC d'un adaptateur de machine virtuelle lorsque l'hôte n'est pas connecté à vCenter Server. Les adresses MAC ont un préfixe VMware OUI distinct pour éviter les conflits.

L'hôte ESXi génère l'adresse MAC d'un adaptateur de machine virtuelle dans l'un des cas suivants :

- L'hôte n'est pas connecté à vCenter Server.
- Le fichier de configuration de la machine virtuelle ne contient ni l'adresse MAC ni les informations sur le type d'allocation d'adresse MAC.

Format d'adresse MAC

L'adresse MAC générée par l'hôte est constituée du préfixe VMware OUI `00:0c:29` et des trois derniers octets au format hexadécimal de l'UUID de la machine virtuelle. L'UUID de la machine virtuelle est créé par un hachage calculé à l'aide de l'UUID de la machine physique ESXi et du chemin du fichier de configuration (`.vmx`) de la machine virtuelle.

Prévention des conflits d'adresses MAC

Toutes les adresses MAC attribuées aux adaptateurs réseau de machines virtuelles suspendues et en cours d'exécution sur une machine physique donnée sont suivies pour détecter les conflits.

Si vous importez une machine virtuelle possédant une adresse MAC générée par l'hôte d'un système vCenter Server à un autre, sélectionnez l'option **Je l'ai copié** lors de la mise sous tension de la machine virtuelle pour régénérer l'adresse et éviter d'éventuels conflits dans le système vCenter Server cible ou entre les systèmes vCenter Server.

Définition d'une adresse MAC statique sur une machine virtuelle

Dans la plupart des déploiements réseau, les adresses MAC générées constituent une bonne approche. Cependant, vous devrez éventuellement attribuer à un adaptateur de machine virtuelle une adresse MAC statique d'une valeur spécifique.

Les cas suivants montrent à quel moment vous devrez éventuellement définir une adresse MAC statique :

- Les adaptateurs de machine virtuelle sur différents hôtes physiques partagent le même sous-réseau et se voient attribuer la même adresse MAC, ce qui provoque un conflit.
- Assurez-vous qu'un adaptateur de machine virtuelle ait toujours la même adresse MAC.

VMware utilise par défaut l'identificateur OUI (Organizationally Unique Identifier) 00:50:56 pour les adresses générées manuellement, mais toutes les adresses uniques générées manuellement sont prises en charge.

Note Assurez-vous qu'aucun autre terminal non-VMware n'est attribué aux composants VMware. Par exemple, vous pouvez avoir des serveurs physiques dans le même sous-réseau, qui utilisent 11:11:11:11:11:11, 22:22:22:22:22:22 comme adresses MAC statiques. Les serveurs physiques n'appartiennent pas à l'inventaire de vCenter Server, et vCenter Server ne peut pas vérifier l'absence de conflit d'adresses.

VMware OUI dans les adresses MAC statiques

Par défaut, les adresses MAC statiques ont comme préfixe l'identificateur VMware OUI (Organizationally Unique Identifier). Toutefois, la plage d'adresses libres fournie par VMware OUI est restreinte.

Si vous décidez d'utiliser l'identificateur VMware OUI, une partie de la plage est déjà réservée pour vCenter Server, les cartes réseau physiques de l'hôte, les cartes réseau virtuelles et une utilisation ultérieure.

Vous pouvez définir une adresse MAC statique qui contient le préfixe VMware OUI conformément au format suivant :

```
00:50:56:XX:YY:ZZ
```

où *XX* est un nombre hexadécimal valide compris entre 00 et 3F, et *YY* et *ZZ* sont des nombres hexadécimaux valides compris entre 00 et FF. Afin d'éviter tout conflit avec des adresses MAC générées par vCenter Server ou affectées aux adaptateurs VMkernel pour le trafic de l'infrastructure, la valeur de *XX* ne doit pas être supérieure à 3F.

La valeur maximale pour une adresse MAC générée manuellement est la suivante :

```
00:50:56:3F:FF:FF
```

Afin d'éviter tout conflit entre les adresses MAC générées et celles affectées manuellement, sélectionnez une valeur unique pour *XX:YY:ZZ* parmi vos adresses codées de manière irréversible.

Attribuer une adresse MAC statique

Vous pouvez attribuer des adresses MAC statiques à la carte réseau virtuelle d'une machine virtuelle hors tension à l'aide de vSphere Client.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans le menu Actions, sélectionnez Modifier les paramètres.
- 4 Sélectionnez l'onglet **Matériel virtuel** dans la boîte de dialogue affichant les paramètres.
- 5 Développez la section des adaptateurs réseau.
- 6 Sous Adresse MAC, sélectionnez **Manuel** dans le menu déroulant.
- 7 Tapez l'adresse MAC statique, puis cliquez sur **OK**.
- 8 Mettez la machine virtuelle sous tension.

Attribuer une adresse MAC statique dans le fichier de configuration de la machine virtuelle

Pour définir une adresse MAC statique pour une machine virtuelle, vous pouvez modifier le fichier de configuration de la machine virtuelle à l'aide de vSphere Client.

Procédure

- 1 Localisez la machine virtuelle dans vSphere Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **VM**
 - b Cliquez sur **Machines virtuelles**, puis cliquez sur la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans le menu déroulant **Actions**, sélectionnez **Modifier les paramètres**.
- 4 Sélectionnez l'onglet **Options VM** et développez **Avancé**.
- 5 Cliquez sur **Modifier la configuration**.

- 6 Pour attribuer une adresse MAC statique, ajoutez ou modifiez les paramètres requis.

Paramètre	Valeur
<code>ethernetX.addressType</code>	statique
<code>ethernetX.address</code>	<i>MAC_address_of_the_virtual_NIC</i>

Le signe *X* à côté d'`ethernet` représente le numéro séquentiel de la carte réseau virtuelle de la machine.

Par exemple, 0 dans `ethernet0` représente les paramètres de la première carte réseau virtuelle ajoutée à la machine virtuelle.

- 7 Cliquez sur **OK**.
- 8 Mettez la machine virtuelle sous tension.

Configurer vSphere pour IPv6

13

Configurez les hôtes ESXi et vCenter Server pour un fonctionnement dans un environnement purement IPv6 pour un espace d'adressage plus étendu et une attribution d'adresse améliorée.

IPv6 est désigné par le groupe de travail IETF comme le successeur de IPv4, avec les avantages suivants :

- Augmentation de la longueur de l'adresse. L'espace d'adressage étendu résout le problème d'épuisement d'adresses et élimine la conversion d'adresse réseau. IPv6 utilise des adresses 128 bits et non des adresses 32 bits comme IPv4.
- Possibilité de configuration automatique améliorée des nœuds.

Ce chapitre contient les rubriques suivantes :

- [Connectivité IPv6 vSphere](#)
- [Déployer vSphere sur IPv6](#)
- [Activer ou désactiver la prise en charge d'IPv6 sur un hôte](#)
- [Configurer IPv6 sur un hôte ESXi](#)
- [Configurer IPv6 sur vCenter Server](#)

Connectivité IPv6 vSphere

Dans un environnement basé sur vSphere 6.0 et version ultérieure, les nœuds et les fonctionnalités peuvent communiquer sur IPv6 en prenant en charge de façon transparente la configuration d'adresse statique et automatique.

IPv6 dans la communication entre des nœuds vSphere

Les nœuds d'un déploiement vSphere peuvent communiquer en utilisant IPv6 et accepter les adresses attribuées conformément à la configuration du réseau.

Tableau 13-1. Prise en charge d'IPv6 par les nœuds dans un environnement vSphere

Type de connexion	Support IPv6	Configuration d'adresse des nœuds vSphere
ESXi vers ESXi	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
Machine vCenter Server vers ESXi	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
Machine vCenter Server vers machine	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
ESXi vers machine vSphere Client	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
Machine virtuelle vers machine virtuelle	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
ESXi vers stockage iSCSI	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
ESXi vers stockage NFS	Oui	<ul style="list-style-type: none"> ■ Statique ■ Automatique : AUTOCONF/DHCPv6
ESXi vers Active Directory	Non Utiliser LDAP via vCenter Server pour connecter ESXi à la base de données Active Directory	-
vCenter Server vers Active Directory	Non Utiliser LDAP pour connecter vCenter Server à la base de données Active Directory	-

Connectivité IPv6 des fonctions de vSphere

Certaines fonctions de vSphere ne prennent pas en charge IPv6 :

- vSphere DPM sur l'interface IPMI (Intelligent Platform Management Interface) et iLO (Integrated Lights-Out) de Hewlett-Packard. vSphere 6.5 et version ultérieure prend uniquement en charge Wake-On-LAN (WOL) pour sortir un hôte du mode veille.
- Proxy d'authentification
- vSphere Management Assistant et ESXCLI connectés à Active Directory.

Utilisez LDAP pour connecter vSphere Management Assistant ou l'ESXCLI à la base de données Active Directory.

Connectivité IPv6 des machines virtuelles

Les machines virtuelles peuvent échanger des données sur le réseau sur IPv6. vSphere prend en charge l'attribution statique et automatique des adresses IPv6 pour les machines virtuelles.

La configuration d'une ou plusieurs adresses IPv6 est également possible lorsque vous personnalisez le système d'exploitation invité d'une machine virtuelle.

Connectivité vSAN

vSAN prend en charge IPv6. Utilisez NFS 4.1 avec AUTH_SYS.

Noms de domaine complets et adresses IPv6

Dans vSphere, vous devez utiliser des noms de domaine complets mappés sur des adresses IPv6 sur le serveur DNS. Vous pouvez utiliser des adresses IPv6 si elles possèdent un nom de domaine complet valide sur le serveur DNS pour la recherche inversée.

Pour déployer vCenter Server dans un environnement purement IPv6, vous devez utiliser uniquement des noms de domaine complets.

Déployer vSphere sur IPv6

Exécutez vSphere dans un environnement véritablement IPv6 pour utiliser un espace d'adressage étendu et une attribution d'adresses flexible.

Si vous envisagez de déployer des hôtes vCenter Server et ESXi dans un réseau IPv6, des étapes supplémentaires sont nécessaires.

- [Activer IPv6 sur une installation vSphere](#)

Si vous disposez d'un déploiement dans un environnement vierge de vSphere 6.5 dans un réseau IPv6, configurez ESXi et vCenter Server pour la connexion de gestion purement IPv6 en configurant IPv6 sur les nœuds déployés et en les connectant.

- [Activer IPv6 sur un environnement vSphere mis à niveau](#)

Sur un déploiement IPv4 de vSphere 6.5 qui comprend un vCenter Server installé ou mis à niveau et un ESXi mis à niveau, configurez ESXi et vCenter Server pour la connexion de gestion purement IPv6 en activant IPv6 sur les nœuds déployés et en les reconnectant.

Activer IPv6 sur une installation vSphere

Si vous disposez d'un déploiement dans un environnement vierge de vSphere 6.5 dans un réseau IPv6, configurez ESXi et vCenter Server pour la connexion de gestion purement IPv6 en configurant IPv6 sur les nœuds déployés et en les connectant.

Conditions préalables

- Vérifiez que les adresses IPv6 de vCenter Server, des hôtes ESXi et d'une base de données externe, le cas échéant, sont mappées sur des noms de domaine complets sur le serveur DNS.

- Vérifiez que l'infrastructure réseau fournit la connectivité IPv6 pour les hôtes ESXi, vCenter Server et une base de données externe, le cas échéant.
- Vérifiez que la version 6.5 de vCenter Server est installée avec un nom de domaine complet mappé sur une adresse IPv6. Consultez la documentation de *Installation et configuration de vCenter Server*.
- Vérifiez que ESXi 6.5 est installé sur les hôtes. Consultez la documentation de *Installation et configuration de vCenter Server*.

Procédure

- 1 Dans l'interface utilisateur de la console directe (DCUI), configurez chaque hôte ESXi comme un nœud purement IPv6.
 - a Dans l'interface DCUI, appuyez sur F2 et connectez-vous à l'hôte.
 - b Dans le menu **Configurer le réseau de gestion**, sélectionnez **Configuration IPv6** et appuyez sur Entrée.
 - c Attribuez une adresse IPv6 à l'hôte.

Option d'attribution d'adresse	Description
Attribution d'adresse automatique en utilisant DHCPv6	1 Sélectionnez l'option Utiliser l'adresse IPv6 dynamique et la configuration réseau , puis sélectionnez Utiliser DHCPv6 .
	2 Appuyez sur Entrée pour enregistrer les modifications.
Attribution d'adresse statique	1 Sélectionnez l'option Sélectionner l'adresse IPv6 statique et la configuration réseau , puis saisissez l'adresse IPv6 de l'hôte et la passerelle par défaut.
	2 Appuyez sur Entrée pour enregistrer les modifications.

- d Dans le menu **Configurer le réseau de gestion**, sélectionnez **Configuration IPv4** et appuyez sur Entrée.
 - e Sélectionnez **Désactiver la configuration IPv4 pour le réseau de gestion** et appuyez sur Entrée.
- 2 Dans vSphere Client, ajoutez l'hôte à l'inventaire.

Activer IPv6 sur un environnement vSphere mis à niveau

Sur un déploiement IPv4 de vSphere 6.5 qui comprend un vCenter Server installé ou mis à niveau et un ESXi mis à niveau, configurez ESXi et vCenter Server pour la connexion de gestion purement IPv6 en activant IPv6 sur les nœuds déployés et en les reconnectant.

Conditions préalables

- Vérifiez que l'infrastructure réseau fournit la connectivité IPv6 pour les hôtes ESXi, vCenter Server et une base de données externe, le cas échéant.
- Vérifiez que les adresses IPv6 de vCenter Server, des hôtes ESXi et d'une base de données externe, le cas échéant, sont mappées sur des noms de domaine complets sur le serveur DNS.

- Vérifiez que la version 6.x de vCenter Server est installée ou mise à niveau. Reportez-vous à la documentation *Installation et configuration de vCenter Server* et *Mise à niveau de vCenter Server*.
- Vérifiez que tous les hôtes ESXi sont mis à niveau vers la version 6.x. Consultez la documentation de *Mise à niveau de VMware ESXi*.

Procédure

- 1 Dans vSphere Client, déconnectez les hôtes de vCenter Server.

2 Configurez chaque hôte ESXi en tant que nœud purement IPv6.

a Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi.

b Exécutez la commande suivante :

```
esxcli network ip interface ipv6 set -i vmk0 -e true
```

c Attribuez une adresse IPv6 au réseau de gestion.

Option d'attribution d'adresse	Description
Attribution d'adresse statique	<p>1 Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi.</p> <p>2 Définissez une adresse IPv6 statique pour le réseau de gestion vmk0 en exécutant la commande suivante :</p> <pre>esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0</pre> <p>3 Définissez la passerelle par défaut pour le réseau de gestion vmk0 en exécutant la commande suivante :</p> <pre>esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address</pre> <p>4 Ajoutez un serveur DNS en exécutant la commande suivante :</p> <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre>
Attribution d'adresse automatique en utilisant DHCPv6	<p>1 Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi.</p> <p>2 Activer DHCPv6 pour le réseau de gestion vmk0 en exécutant la commande suivante :</p> <pre>esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true</pre> <p>3 Activez les annonces de routage IPv6 pour le réseau de gestion vmk0 en exécutant la commande suivante :</p> <pre>esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true</pre> <p>4 Ajoutez un serveur DNS ou utilisez la configuration DNS publiée par DHCPv6 en exécutant l'une des commandes suivantes :</p> <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre> <pre>esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true</pre>

- 3 Désactivez la configuration IPv4 pour le réseau de gestion.
 - a Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi.
 - b Exécutez la commande suivante :

```
esxcli network ip interface ipv4 set -i vmk0 --type=none
```

- 4 Si vCenter Server utilise une base de données externe, configurez celle-ci en tant que nœud IPv6.
- 5 Configurez vCenter Server en tant que nœud purement IPv6 et redémarrez-le.
- 6 Désactivez IPv4 sur le serveur de base de données.
- 7 Dans vSphere Client, ajoutez l'hôte à l'inventaire.
- 8 Désactivez IPv4 dans l'infrastructure réseau.

Activer ou désactiver la prise en charge d'IPv6 sur un hôte

La prise en charge d'IPv6 dans vSphere permet aux hôtes de fonctionner dans un réseau IPv6 disposant d'un grand espace d'adresses, d'une multidiffusion améliorée, d'un routage simplifié, etc.

Dans ESXi 6.0 et versions ultérieures, IPv6 est activé par défaut.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Mise en réseau** et sélectionnez **Configuration TCP/IP**.
- 3 Cliquez sur **Modifier**.
- 4 Utilisez le bouton bascule pour activer ou désactiver la prise en charge d'IPv6.
- 5 Cliquez sur **OK**.
- 6 Redémarrez l'hôte pour appliquer les modifications dans la prise en charge d'IPv6.

Étape suivante

Configurez les paramètres IPv6 des adaptateurs VMkernel sur l'hôte, par exemple, du réseau de gestion. Reportez-vous à la section [Configurer IPv6 sur un hôte ESXi](#).

Configurer IPv6 sur un hôte ESXi

Pour connecter un hôte ESXi sur IPv6 vers le réseau de gestion, vSphere vMotion, le stockage partagé, vSphere Fault Tolerance, etc., modifiez les paramètres IPv6 des adaptateurs VMkernel sur l'hôte.

Conditions préalables

Vérifiez que IPv6 est activé sur l'hôte ESXi. Reportez-vous à la section [Activer ou désactiver la prise en charge d'IPv6 sur un hôte](#).

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**, puis sélectionnez **Adaptateurs VMkernel**.
- 3 Sélectionnez l'adaptateur VMkernel sur le commutateur standard ou distribué cible, puis cliquez sur **Modifier**.
- 4 Dans la boîte de dialogue Modifier les paramètres, cliquez sur **Paramètres IPv6**.
- 5 Configurez l'attribution d'adresse de l'adaptateur VMkernel.

Option d'adresse IPv6	Description
Obtenir une adresse IPv6 automatiquement via DHCP	Recevez une adresse IPv6 pour l'adaptateur VMkernel à partir d'un serveur DHCPv6.
Obtenir une adresse IPv6 automatiquement via annonce du routeur	Recevez une adresse IPv6 pour l'adaptateur VMkernel à partir d'un routeur via une annonce du routeur.
Adresses IPv6 statiques	Définissez une ou plusieurs adresses. Pour chaque entrée d'adresse, saisissez l'adresse IPv6 de l'adaptateur, la longueur du préfixe de sous-réseau et l'adresse IPv6 de la passerelle par défaut.

Vous pouvez sélectionner plusieurs options d'attribution selon la configuration de votre réseau.

- 6 Cliquez sur **OK** pour appliquer les modifications sur l'adaptateur VMkernel.

Configurer IPv6 sur vCenter Server

Utilisez vSphere Client pour configurer vCenter Server pour les communications avec les hôtes ESXi sur un réseau IPv6.

Procédure

- 1 Sur la page principale de vSphere Client, cliquez sur **Accueil** et sélectionnez **Configuration système**.
- 2 Sous Configuration système, cliquez sur **Nœuds**.
- 3 Sous Nœuds, sélectionnez un nœud et cliquez sur l'onglet **Gérer**.
- 4 Sous Communs, sélectionnez **Mise en réseau** et cliquez sur **Modifier**.
- 5 Développez le nom de l'interface réseau pour modifier les paramètres de l'adresse IP.

6 Modifiez les paramètres de l'adresse IPv6.

Option	Description
Activer ou désactiver les paramètres IPv6	Active ou désactive l'adresse IPv6 en fonction de l'option choisie sur le commutateur.
Obtenir les paramètres IPv6 automatiquement via DHCP	Attribue automatiquement des adresses IPv6 à partir du réseau à l'aide de DHCP.
Obtenir les paramètres IPv6 automatiquement via l'annonce du routeur	Attribue automatiquement des adresses IPv6 au dispositif à partir du réseau en utilisant une annonce de routage.
Utiliser des adresses IPv6 statiques	<p>Utilise les adresses IPv6 que vous configurez manuellement.</p> <ol style="list-style-type: none"> 1 Cochez la case. 2 Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau. 3 Cliquez sur Ajouter pour entrer d'autres adresses IPv6. 4 Cliquez sur Enregistrer. <p>Note Pour les adresses IPv4 ou IPv6 statiques, le serveur DNS doit être défini manuellement.</p>

Vous pouvez configurer le dispositif pour obtenir automatiquement les paramètres IPv6 via DHCP et l'annonce de routage. Vous pouvez attribuer une adresse IPv6 statique en même temps.

Note Les solutions secondaires et tierces doivent être réenregistrées en cas de modification des adresses IP IPv4 et IPv6.

- 7 (Facultatif) Pour supprimer des adresses IPv6 attribuées automatiquement par annonce du routeur, cliquez sur **Supprimer les adresses** et supprimez les adresses.

Vous pouvez supprimer certaines adresses IPv6 que vCenter Server a obtenues via l'annonce du routeur pour arrêter la communication sur ces adresses et appliquer les adresses statiques configurées.

Étape suivante

Connectez les hôtes ESXi à vCenter Server sur IPv6 à l'aide de leur nom de domaine complet.

Surveiller la connexion réseau et le trafic

14

Surveillez la connexion et les paquets réseau qui transitent par les ports d'un commutateur standard vSphere ou d'un vSphere Distributed Switch pour analyser le trafic entre les machines virtuelles et les hôtes.

Ce chapitre contient les rubriques suivantes :

- Capturer des paquets réseau
- Capture et suivi des paquets réseau à l'aide de l'utilitaire `pktcap-uw`
- Configurer les paramètres NetFlow d'un vSphere Distributed Switch
- Présentation de la mise en miroir de ports
- Contrôle de santé de vSphere Distributed Switch
- Switch Discovery Protocol
- Afficher le diagramme de la topologie d'un commutateur virtuel distribué NSX

Capturer des paquets réseau

Découvrez comment utiliser l'utilitaire PacketCapture pour diagnostiquer les problèmes de mise en réseau (connexion lente, perte de paquets ou problèmes de connectivité, par exemple).

PacketCapture est un utilitaire `tcpdump` léger qui capture et stocke uniquement la quantité minimale de données nécessaire pour diagnostiquer les problèmes réseau. PacketCapture est intégré au service `rhttpproxy` d'ESXi et vCenter Server. Vous démarrez et arrêtez PacketCapture en modifiant le fichier de configuration XML du service `rhttpproxy`.

Procédure

- 1 Démarrez la capture des paquets.
 - a Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi ou vCenter Server.
 - b Ouvrez le fichier `config.xml` pour le modifier.

Composant de vSphere	Emplacement du fichier
ESXi	<code>/etc/vmware/rhttpproxy/config.xml</code>
vCenter Server	<code>/etc/vmware-rhttpproxy/config.xml</code>

- c Effectuez les modifications suivantes :

```
<config>
  <packetCapture>
    <enabled>>true</enabled>
```

- d (Facultatif) Configurez les options de PacketCapture.

Option et valeur par défaut	Description
<code><validity>72</validity></code>	Au démarrage, supprimez tous les fichiers <code>pcap</code> et <code>pcap.gz</code> qui ont été modifiés avant la période spécifiée et ne font pas partie du processus actuel.
<code><directory>/directory_path</directory></code>	Répertoire dans lequel les fichiers <code>pcap</code> et <code>pcap.gz</code> sont stockés. Le répertoire doit exister et être accessible.
<code><maxDataInPcapFile>52428800</maxDataInPcapFile></code>	Quantité de données capturées en octets que peut stocker chaque fichier <code>pcap</code> et <code>pcap.gz</code> avant de passer au fichier suivant. La taille minimale est de 5 Mo sur vCenter Server et de 2,5 Mo sur ESXi. Note Le stockage de 50 Mo de données capturées dans un fichier <code>pcap</code> requiert un fichier <code>pcap</code> d'environ 67,5 Mo.
<code><maxPcapFilesCount>5</maxPcapFilesCount></code>	Nombre de fichiers <code>pcap</code> ou <code>pcap.gz</code> pour la rotation. Le nombre minimal est 2.

- e Enregistrez et fermez le fichier `config.xml`.
- f Rechargez le fichier `config.xml` en exécutant la commande suivante :

```
kill -SIGHUP `pidof rhttpproxy`
```

2 Arrêtez la capture de paquets.

- a Ouvrez une connexion SSH et connectez-vous à l'hôte ESXi ou vCenter Server.
- b Ouvrez le fichier `config.xml` pour le modifier.
- c Effectuez les modifications suivantes :

```
<config>
  <packetCapture>
    <enabled>>false</enabled>
```

- d Enregistrez et fermez le fichier `config.xml`.
- e Rechargez le fichier `config.xml` en exécutant la commande suivante :

```
kill -SIGHUP `pidof rhttpproxy`
```

3 Collectez les données capturées.

Les fichiers `pcap` ou `pcap.gz` sont stockés dans les répertoires par défaut suivants.

Composant de vSphere	Emplacement du fichier
ESXi	<code>/var/run/log</code>
vCenter Server	<code>/var/log/vmware/rhttpproxy</code>

Étape suivante

Copiez les fichiers `pcap` et `pcap.gz` vers un système qui exécute un outil d'analyse réseau, tel que Wireshark, et examinez les détails des paquets.

Avant d'analyser les fichiers `pcap` et `pcap.gz` capturés à partir d'un hôte ESXi, utilisez l'utilitaire TraceWrangler pour corriger les métadonnées de la taille de la trame. Pour plus d'informations, consultez l'article <https://kb.vmware.com/kb/52843>.

Capture et suivi des paquets réseau à l'aide de l'utilitaire `pktcap-uw`

Découvrez comment surveiller le trafic qui s'écoule à travers les adaptateurs réseau physiques, les adaptateurs VMkernel et les adaptateurs de machines virtuelles, et analysez les informations sur les paquets à l'aide de l'interface utilisateur graphique des outils d'analyse réseau tels que Wireshark.

Dans vSphere, vous pouvez surveiller les paquets sur un hôte à l'aide de l'utilitaire de console `pktcap-uw`. Vous pouvez utiliser l'utilitaire sans installation supplémentaire sur un hôte ESXi. `pktcap-uw` fournit de nombreux points dans la pile réseau d'hôte auxquels vous pouvez surveiller le trafic.

Pour une analyse détaillée des paquets capturés, vous pouvez enregistrer le contenu des paquets à partir de l'utilitaire `pktcap-uw` dans des fichiers au format PCAP ou PCAPNG et les ouvrir dans Wireshark. Vous pouvez également résoudre les problèmes liés aux paquets abandonnés et suivre le chemin d'un paquet dans la pile réseau.

Note L'utilitaire `pktcap-uw` n'est pas intégralement pris en charge pour la compatibilité descendante avec les versions de vSphere. Les options de l'utilitaire peuvent faire l'objet de modifications ultérieures.

Syntaxe de la commande `pktcap-uw` pour la capture de paquets

Utilisez l'utilitaire `pktcap-uw` pour inspecter le contenu des paquets pendant qu'ils traversent la pile réseau sur un hôte ESXi.

Syntaxe pktcap-uw pour la capture des paquets

La syntaxe de la commande `pktcap-uw` pour la capture des paquets à un emplacement spécifique de la pile réseau est la suivante :

```
pktcap-uw
  switch_port_arguments
  capture_point_options
  filter_options
  output_control_options
```

Note Certaines options de l'utilitaire `pktcap-uw` sont prévues pour une utilisation interne de VMware uniquement et vous ne pouvez les utiliser que sous la supervision du support technique de VMware. Ces options ne sont pas décrites dans le guide *Mise en réseau vSphere*.

Tableau 14-1. Arguments `pktcap-uw` pour la capture de paquets

Groupe d'arguments	Argument	Description
<code>switch_port_arguments</code>	<code>--uplink vmnicX</code>	Capture de paquets associés à un adaptateur physique. Vous pouvez combiner les options <code>--uplink</code> et <code>--capture</code> afin de surveiller les paquets à un emplacement spécifique du chemin entre l'adaptateur physique et le commutateur virtuel. Reportez-vous à la section Capturer les paquets reçus sur un adaptateur physique .
	<code>--vmk vmkX</code>	Capture de paquets associés à un adaptateur VMKernel. Vous pouvez combiner les options <code>vmk</code> et <code>--capture</code> afin de surveiller les paquets à un emplacement spécifique du chemin entre l'adaptateur VMkernel et le commutateur virtuel. Reportez-vous à la section Capturer des paquets pour un adaptateur VMkernel .

Tableau 14-1. Arguments pktcap-uw pour la capture de paquets (suite)

Groupe d'arguments	Argument	Description
	<code>--switchport {vmxnet3_port_ID vmkernel_adapter_port_ID}</code>	<p>Capture de paquets associés à un adaptateur de machine virtuelle VMXNET3 ou à un adaptateur VMkernel connecté à un port du commutateur virtuel spécifique. Vous pouvez afficher l'ID du port sur le panneau Mise en réseau de l'utilitaire <code>esxtop</code>.</p> <p>Vous pouvez combiner les options <code>switchport</code> et <code>capture</code> afin de surveiller les paquets à un emplacement spécifique du chemin entre l'adaptateur VMXNET3 ou VMkernel et le commutateur virtuel.</p> <p>Reportez-vous à la section Capturer des paquets pour un adaptateur de machine virtuelle VMXNET3.</p>
	<code>--lifID lif_ID</code>	<p>Capture de paquets associés à l'interface logique d'un routeur distribué. Voir la documentation <i>VMware NSX</i>.</p>
<i>capture_point_options</i>	<code>--capture capture_point</code>	<p>Capture de paquets à un emplacement spécifique de la pile réseau. Par exemple, vous pouvez surveiller des paquets à leur arrivée en provenance d'un adaptateur physique.</p>
	<code>--dir {0 1 2}</code>	<p>Capture de paquets selon la direction du flux applicable au commutateur virtuel.</p> <p>0 représente le trafic entrant, 1 le trafic sortant et 2, le trafic bidirectionnel.</p> <p>Par défaut, l'utilitaire <code>pktcap-uw</code> capture le trafic d'entrée.</p> <p>Utilisez l'option <code>--dir</code> en même temps que l'option <code>--uplink</code>, <code>--vmk</code> ou <code>--switchport</code>.</p>

Tableau 14-1. Arguments `pktcap-uw` pour la capture de paquets (suite)

Groupe d'arguments	Argument	Description
	<code>--stage {0 1}</code>	Capture du paquet le plus proche de sa source ou de sa destination. Utilisez cette option pour vérifier le changement d'un module à mesure qu'il traverse les points de la pile. 0 représente le trafic le plus proche de la source et 1 le trafic le plus proche de la destination. Utilisez l'option <code>--stage</code> en même temps que l'option <code>--uplink</code> , <code>--vmk</code> , <code>--switchport</code> OU <code>--dvfilter</code> .
	<code>--dvfilter filter_name --capture PreDVFilter PostDVFilter</code>	Capture de paquets avant ou après leur interception par un vSphere Network Appliance (DVFilter). Reportez-vous à la section Capturer des paquets au niveau de DVFilter .
	<code>-A --availpoints</code>	Afficher tous les points de capture pris en charge par l'utilitaire <code>pktcap-uw</code> .
		Pour plus d'informations sur les points de capture de l'utilitaire <code>pktcap-uw</code> , voir Points de capture de l'utilitaire pktcap-uw .
<i>filter_options</i>		Filtrer les paquets capturés en fonction de l'adresse source ou de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP. Reportez-vous à la section Options de pktcap-uw pour le filtrage de paquets .
<i>output_control_options</i>		Enregistrement du contenu d'un paquet dans un fichier, capture uniquement un certain nombre de paquets, capture d'un certain nombre d'octets au début du paquet, etc. Reportez-vous à la section Options de pktcap-uw pour le contrôle de sortie .

Les barres verticales | représentent des valeurs alternatives et les accolades {} utilisées avec les barres verticales permettent de spécifier une liste de choix pour un argument ou une option.

Syntaxe de la commande `pktcap-uw` pour le suivi de paquets

Utilisez l'utilitaire `pktcap-uw` pour afficher le chemin d'accès d'un paquet dans la pile réseau d'un hôte ESXi à des fins d'analyse de latence.

Syntaxe de `pktcap-uw` pour le suivi des paquets

La commande de l'utilitaire `pktcap-uw` présente la syntaxe suivante pour le suivi des paquets dans la pile réseau :

```
pktcap-uw --trace filter_optionsoutput_control_options
```

Options de l'utilitaire `pktcap-uw` pour le suivi des paquets

L'utilitaire `pktcap-uw` prend en charge les options suivantes lorsque vous l'utilisez pour suivre des paquets :

Tableau 14-2. Options de `pktcap-uw` pour le suivi des paquets

Argument	Description
<code>filter_options</code>	Filtrez les paquets suivis en fonction de l'adresse source ou de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP. Reportez-vous à Options de <code>pktcap-uw</code> pour le filtrage de paquets .
<code>output_control_options</code>	Enregistrez le contenu d'un paquet dans un fichier et suivez uniquement un nombre de paquets. Reportez-vous à Options de <code>pktcap-uw</code> pour le contrôle de sortie .

Options de `pktcap-uw` pour le contrôle de sortie

Utilisez les options de contrôle de sortie de l'utilitaire `pktcap-uw` pour enregistrer le contenu des paquets dans un fichier, capturer un certain nombre d'octets dans chaque paquet et limiter le nombre de paquets capturés.

Options de `pktcap-uw` pour le contrôle de sortie

Les options de l'utilitaire `pktcap-uw` pour le contrôle de sortie sont valides lorsque vous capturez ou suivez des paquets. Pour plus d'informations sur la syntaxe de commande de l'utilitaire `pktcap-uw`, consultez [Syntaxe de la commande `pktcap-uw` pour la capture de paquets](#) et [Syntaxe de la commande `pktcap-uw` pour le suivi de paquets](#).

Tableau 14-3. Options de contrôle de sortie prises en charge par l'utilitaire `pktcap-uw`

Option	Description
<code>{-o --outfile} pcap_file</code>	Enregistrez les paquets capturés ou suivis dans un fichier au format de capture de paquets (PCAP). Utilisez cette option pour examiner les paquets dans un outil d'analyse visuelle tel que Wireshark.
<code>-P --ng</code>	Enregistrez le contenu des paquets au format de fichier PCAPNG. Utilisez cette option avec l'option <code>-o</code> ou <code>--outfile</code> .
<code>--console</code>	Imprimez les détails et le contenu des paquets dans la sortie de la console. Par défaut, l'utilitaire <code>pktcap-uw</code> affiche les informations relatives aux paquets dans la sortie de la console.
<code>{-c --count} number_of_packets</code>	Capturez les <code>number_of_packets</code> premiers paquets.

Tableau 14-3. Options de contrôle de sortie prises en charge par l'utilitaire `pktcap-uw` (suite)

Option	Description
<code>{-s --snaplen} snapshot_length</code>	<p>Capturez uniquement les <i>snapshot_length</i> premiers octets de chaque paquet. Si la densité du trafic sur l'hôte est forte, utilisez cette option pour réduire la charge sur la CPU et le stockage.</p> <p>Pour limiter la taille du contenu capturé, définissez une valeur supérieure à 24.</p> <p>Pour capturer le paquet complet, définissez cette option sur 0.</p>
<code>-h</code>	Affichez l'aide relative à l'utilitaire <code>pktcap-uw</code> .

Les barres verticales | représentent des valeurs alternatives et les accolades {} utilisées avec les barres verticales permettent de spécifier une liste de choix pour un argument ou une option.

Options de `pktcap-uw` pour le filtrage de paquets

Réduisez l'éventail de paquets que vous surveillez à l'aide de l'utilitaire `pktcap-uw` afin d'appliquer des options de filtrage en fonction des adresses source et de destination, du VLAN, du VXLAN et du protocole de niveau suivant qui consomme la charge utile de paquets.

Options de filtre

Les options de filtre pour `pktcap-uw` sont valides lorsque vous capturez et suivez des paquets. Pour plus d'informations sur la syntaxe de commande de l'utilitaire `pktcap-uw`, consultez [Syntaxe de la commande `pktcap-uw` pour la capture de paquets](#) et [Syntaxe de la commande `pktcap-uw` pour le suivi de paquets](#).

Tableau 14-4. Options de filtre de l'utilitaire `pktcap-uw`

Option	Description
<code>--srcmac mac_address</code>	Capturez ou suivez les paquets qui ont une adresse MAC source spécifique. Séparez les octets en utilisant deux points « : ».
<code>--dstmac mac_address</code>	Capturez ou suivez les paquets qui ont une adresse MAC de destination spécifique. Séparez les octets en utilisant deux points « : ».
<code>--mac mac_address</code>	Capturez ou suivez les paquets qui ont une adresse MAC source ou de destination spécifique. Séparez les octets en utilisant deux points « : ».

Tableau 14-4. Options de filtre de l'utilitaire pktcap-uw (suite)

Option	Description
<code>--ethertype 0xEtherType</code>	Capturez ou suivez les paquets de couche 2 en fonction du protocole de niveau suivant qui consomme la charge utile des paquets. <i>EtherType</i> correspond au champ EtherType des trames Ethernet. Il désigne le type de protocole de niveau suivant qui consomme la charge utile de la trame. Par exemple, pour surveiller le trafic du protocole LLDP (Link Layer Discovery Protocol), tapez --ethertype 0x88CC .
<code>--vlan VLAN_ID</code>	Capturez ou suivez les paquets appartenant à un VLAN.
<code>--srcip IP_address IP_address/subnet_range</code>	Capturez ou suivez les paquets qui ont un sous-réseau ou une adresse IPv4 source spécifique.
<code>--dstip IP_address IP_address/subnet_range</code>	Capturez ou suivez les paquets qui ont un sous-réseau ou une adresse IPv4 de destination spécifique.
<code>--ip IP_address</code>	Capturez ou suivez les paquets qui ont une adresse IPv4 source ou de destination spécifique.
<code>--proto 0xIP_protocol_number</code>	Capturez ou suivez les paquets de couche 3 en fonction du protocole de niveau suivant qui consomme la charge utile. Par exemple, pour surveiller le trafic pour le protocole UDP, tapez --proto 0x11 .
<code>--srcport source_port</code>	Capturez ou suivez les paquets en fonction de leur port TCP source.
<code>--dstport destination_port</code>	Capturez ou suivez les paquets en fonction de leur port TCP de destination.
<code>--tcpport TCP_port</code>	Capturez ou suivez les paquets en fonction de leur port TCP source ou de destination.
<code>--vxlan VXLAN_ID</code>	Capturez ou suivez les paquets appartenant à un VXLAN.

Tableau 14-4. Options de filtre de l'utilitaire `pktcap-uw` (suite)

Option	Description
<code>--rcf pcap_filter_expression</code>	<p>Capturez ou suivez les paquets à l'aide de l'expression de filtre commune enrichie.</p> <p>Par exemple, pour capturer tous les paquets d'entrée et de sortie dont la longueur du contenu de l'adresse IP est supérieure à 1 000 octets, utilisez l'expression de filtre <code>--rcf "ip[2:2]>1000"</code>.</p> <p>Pour sélectionner une adresse d'hôte source et un numéro de port spécifiques, utilisez l'expression de filtre <code>--rcf "src host 12.0.0.1 and port 5000"</code>. Cet exemple filtre le trafic pour l'adresse de l'hôte 12.0.0.1 à l'aide du port 5000.</p> <p>Pour en savoir plus sur le filtrage du trafic réseau avec l'option <code>--rcf</code>, reportez-vous à la documentation sur les expressions de filtre PCAP à l'aide d'analyseurs de paquets de ligne de commande, tels que <code>tcpdump</code>. Reportez-vous à la section pcap-filter - Syntaxe de filtre de paquets.</p> <hr/> <p>Note Lorsque vous utilisez l'option <code>--rcf</code>, respectez les limitations suivantes.</p> <ul style="list-style-type: none"> ■ Ne filtrez pas les paquets VLAN à l'aide de l'option <code>--rcf</code>. Pour suivre l'utilisation du VLAN ou du VXLAN, utilisez les options <code>pktcap-uw --vlan</code> ou <code>--vxlan</code>. ■ Ne filtrez pas une adresse de diffusion IP. ■ N'utilisez pas <code>--rcf</code> sur les ports ENS.
<code>--rcf-tcp-data tcp_packet_data_filter</code>	<p>Capturez ou suivez les paquets de données TCP à l'aide de l'expression de filtre commune enrichie.</p> <p>Par exemple, pour capturer tous les paquets de réponse HTTP/1.0 avec 200 OK, utilisez l'expression de filtre <code>--rcf-tcp-data "HTTP/1.0 200 OK"</code>.</p> <p>Pour filtrer des demandes HTTP GET renvoyant un fichier <code>index.html</code>, utilisez l'expression de filtre <code>--rcf-tcp-data "GET /index.html"</code>.</p>

Les barres verticales | représentent les valeurs alternatives.

Capture de paquets à l'aide de l'utilitaire `pktcap-uw`

Capturez des paquets à l'aide de l'utilitaire `pktcap-uw` sur le chemin d'accès entre un commutateur virtuel et des adaptateurs physiques, VMkernel et de machine virtuelle pour résoudre les problèmes de transfert de données dans la pile réseau sur un hôte ESXi.

Capturer les paquets reçus sur un adaptateur physique

Surveillez le trafic hôte associé au réseau externe en capturant des paquets à certains points du chemin entre un commutateur vSphere standard ou un vSphere Distributed Switch et un adaptateur physique.

Vous pouvez spécifier un certain point de capture sur le chemin de données entre un commutateur virtuel et un adaptateur physique, ou déterminer un point de capture par direction du trafic en fonction du commutateur et de la proximité de la source ou de la destination du paquet. Pour plus d'informations sur les points de capture pris en charge, consultez [Points de capture de l'utilitaire pktcap-uw](#).

Procédure

- 1 (Facultatif) Recherchez le nom de l'adaptateur physique à surveiller dans la liste des adaptateurs de l'hôte.
 - Dans vSphere Client, dans l'onglet **Configurer** de l'hôte, développez la section **Mise en réseau** et sélectionnez **Adaptateurs physiques**.
 - Dans ESXi Shell sur l'hôte, pour afficher la liste des adaptateurs physiques et examiner leur état, exécutez la commande ESXCLI suivante :

```
esxcli network nic list
```

Chaque adaptateur physique est représenté par `vmnicX`. `X` est le numéro attribué par ESXi au port de l'adaptateur physique.

- 2 Dans ESXi Shell, sur l'hôte, exécutez la commande `pktcap-uw` avec l'argument `--uplink vmnicX` avec des options permettant de surveiller les paquets à un point spécifique, de filtrer les paquets capturés et d'enregistrer les résultats dans un fichier.

```
pktcap-uw --uplink vmnicX [--capture capture_point|--dir 0|1] [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

où les options de la commande se trouvent entre crochets [] `pktcap-uw --uplink vmnicX` et où les barres verticales | représentent les autres valeurs possibles.

Si vous exécutez la commande `pktcap-uw --uplink vmnicX` sans options, vous obtenez le contenu des paquets entrants sur le commutateur standard ou distribué à la sortie de la console, au point où ils sont commutés.

- a Utilisez l'option `--capture` pour vérifier les paquets sur un autre point de capture ou l'option `--dir` pour une autre direction du trafic.

Option de commande <code>pktcap-uw</code>	Objectif
<code>--capture UplinkSnd</code>	Surveiller les paquets immédiatement avant leur entrée dans l'adaptateur physique.
<code>--capture UplinkRcv</code>	Surveiller les paquets immédiatement après leur réception dans la pile réseau à partir de l'adaptateur physique.
<code>--dir 1</code>	Surveiller les paquets qui quittent le commutateur virtuel.
<code>--dir 0</code>	Surveiller les paquets qui entrent dans le commutateur virtuel.

- b Utilisez `filter_options` pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- c Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.

- Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
- Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

- d Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.

- 3 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur Ctrl+C pour arrêter la capture ou le suivi de paquets.

Exemple : Capturer les paquets reçus sur vmnic0 à partir de l'adresse IP 192.168.25.113

Pour capturer les 60 premiers paquets d'un système source auquel l'adresse IP 192.168.25.113 est attribuée sur vmnic0 et les sauvegarder dans un fichier nommé `vmnic0_rcv_srcip.pcap`, exécutez la commande `pktcap-uw` suivante :

```
pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Capter des paquets pour un adaptateur de machine virtuelle VMXNET3

Surveillez le trafic transmis entre un commutateur virtuel et un adaptateur de machine virtuelle VMXNET3 à l'aide de l'utilitaire `pktcap-uw`.

Vous pouvez spécifier un point de capture spécifique dans le chemin d'accès de données entre un commutateur virtuel et un adaptateur de machine virtuelle. Vous pouvez également déterminer un point de capture par direction du trafic en fonction du commutateur et de la proximité de la source ou de la destination du paquet. Pour plus d'informations sur les points de capture pris en charge, consultez [Points de capture de l'utilitaire pktcap-uw](#).

Conditions préalables

Vérifiez que l'adaptateur de machine virtuelle est de type VMXNET3.

Procédure

- 1 Sur l'hôte, découvrez l'ID de port de l'adaptateur de machine virtuelle à l'aide de l'utilitaire `esxtop`.

- a Dans ESXi Shell sur l'hôte, pour démarrer l'utilitaire, exécutez `esxtop`.
- b Pour passer au panneau réseau de l'utilitaire, appuyez sur `n`.
- c Dans la colonne USED-BY, recherchez l'adaptateur de la machine virtuelle et notez la valeur PORT-ID correspondante.

Le champ USED-BY contient le nom de la machine virtuelle et le port auquel l'adaptateur de machine virtuelle est connecté.

- d Appuyez sur `Q` pour quitter `esxtop`.

- 2 Dans ESXi Shell, exécutez `pktcap-uw --switchport port_ID`.

`port_ID` est l'ID que l'utilitaire `esxtop` affiche pour l'adaptateur de machine virtuelle dans la colonne PORT-ID.

- 3 Dans ESXi Shell, exécutez la commande `pktcap-uw` avec l'argument `--switchport port_ID` et avec des options permettant de surveiller les paquets à un point spécifique, de filtrer les paquets capturés et d'enregistrer les résultats dans un fichier.

```
pktcap-uw --switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]
[filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

où les options de la commande `pktcap-uw --switchport port_ID` se trouvent entre crochets `[]` et où les barres verticales `|` représentent les autres valeurs possibles.

Si vous exécutez la commande `pktcap-uw --switchport port_ID` sans options, vous obtenez le contenu des paquets entrants sur le commutateur standard ou distribué à la sortie de la console, au point où ils sont commutés.

- a Pour vérifier les paquets à un autre point de capture ou dans une autre direction sur le chemin d'accès entre le système d'exploitation invité et le commutateur virtuel, utilisez l'option `--capture` ou combinez les valeurs des options `--dir` et `--stage`.

Options de commande <code>pktcap-uw</code>	Objectif
<code>--capture VnicTx</code>	Surveillez les paquets lorsqu'ils passent de la machine virtuelle au commutateur.
<code>--capture VnicRx</code>	Surveillez les paquets lorsqu'ils arrivent à la machine virtuelle.
<code>--dir 1 --stage 0</code>	Surveiller les paquets immédiatement après leur sortie du commutateur virtuel.
<code>--dir 1</code>	Surveillez les paquets immédiatement avant leur entrée dans la machine virtuelle.
<code>--dir 0 --stage 1</code>	Surveillez les paquets immédiatement après leur entrée dans le commutateur virtuel.

- b Utilisez *filter_options* pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- c Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.

- Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
- Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

- d Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.

- 4 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur `Ctrl+C` pour arrêter la capture ou le suivi de paquets.

Exemple : Capturer les paquets reçus par une machine virtuelle en provenance d'une adresse IP 192.168.25.113

Pour capturer les 60 premiers paquets d'une source à laquelle l'adresse IP 192.168.25.113 est attribuée lorsqu'ils arrivent à l'adaptateur de machine virtuelle avec l'ID de port 33554481 et les enregistrer dans un fichier appelé `vmxnet3_rcv_srcip.pcap`, exécutez la commande `pktcap-uw` suivante :

```
pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Capturer des paquets pour un adaptateur VMkernel

Surveillez les paquets échangés entre un adaptateur VMkernel et un commutateur virtuel à l'aide de l'utilitaire `pktcap-uw`.

Vous pouvez capturer des paquets à un certain point de capture sur le flux entre un commutateur virtuel et un adaptateur VMkernel. Vous pouvez également déterminer un point de capture par direction du trafic en fonction du commutateur et de la proximité de la source ou de la destination du paquet. Pour plus d'informations sur les points de capture pris en charge, consultez [Points de capture de l'utilitaire pktcap-uw](#).

Procédure

- (Facultatif) Recherchez le nom de l'adaptateur VMkernel à surveiller dans la liste des adaptateurs VMkernel.
 - Dans vSphere Web Client, développez la section **Mise en réseau** de l'onglet **Configurer** pour l'hôte et sélectionnez **Adaptateurs VMkernel**.
 - Dans ESXi Shell sur l'hôte, pour afficher la liste des adaptateurs physiques, exécutez la commande de console suivante :

```
esxcli network ip interface list
```

Chaque adaptateur VMkernel est représenté par `vmkX`, où `X` est le numéro de séquence attribué par ESXi à l'adaptateur.

- Dans ESXi Shell, sur l'hôte, exécutez la commande `pktcap-uw` avec l'argument `--vmk vmkX` et avec des options permettant de surveiller les paquets à un point spécifique, de filtrer les paquets capturés et d'enregistrer les résultats dans un fichier.

```
pktcap-uw --vmk vmkX [--capture capture_point|--dir 0|1 --stage 0|1] [filter_options]
[--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

où les options de la commande se trouvent entre crochets [] `pktcap-uw --vmk vmkX` et où les barres verticales | représentent les autres valeurs possibles.

Vous pouvez remplacer l'option `--vmk vmkX` par `--switchport vmkernel_adapter_port_ID`, où `vmkernel_adapter_port_ID` est la valeur PORT-ID que le panneau Mise en réseau de l'utilitaire `esxtop` affiche pour l'adaptateur.

Si vous exécutez la commande `pktcap-uw --vmk vmkX` sans options, vous obtenez le contenu des paquets qui quittent l'adaptateur VMkernel.

- a Pour vérifier les paquets transmis ou reçus à un emplacement et dans une direction spécifiques, utilisez l'option `--capture`, ou combinez les valeurs des options `--dir` et `--stage`.

Options de commande <code>pktcap-uw</code>	Objectif
<code>--dir 1 --stage 0</code>	Surveiller les paquets immédiatement après leur sortie du commutateur virtuel.
<code>--dir 1</code>	Surveiller les paquets immédiatement avant leur entrée dans l'adaptateur VMkernel.
<code>--dir 0 --stage 1</code>	Surveiller les paquets immédiatement avant leur entrée dans le commutateur virtuel.

- b Utilisez `filter_options` pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- c Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.

- Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
- Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

- d Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.

- 3 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur Ctrl+C pour arrêter la capture ou le suivi de paquets.

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Capturer de paquets abandonnés

Résolvez les problèmes de perte de connectivité en capturant les paquets abandonnés à l'aide de l'utilitaire `pktcap-uw`.

Un paquet peut être abandonné à un point dans le flux du réseau pour différentes raisons, par exemple, une règle de pare-feu, le filtrage d'une IOChain et du DVfilter, une incompatibilité VLAN, le dysfonctionnement d'un adaptateur physique, une erreur de total de contrôle, etc. Vous pouvez utiliser l'utilitaire `pktcap-uw` pour déterminer l'emplacement dans lequel les paquets sont abandonnés et la raison de l'abandon.

Procédure

- 1 Dans ESXi Shell sur l'hôte, exécutez la commande `pktcap-uw --capture Drop` avec des options permettant de surveiller les paquets à un point spécifique, de filtrer les paquets capturés et d'enregistrer les résultats dans un fichier.

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

où les options de la commande `pktcap-uw--capture Drop` se trouvent entre crochets `[]` et où les barres verticales `|` représentent des valeurs alternatives.

- a Utilisez *filter_options* pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- b Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.
 - Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
 - Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

Note Vous ne pouvez afficher l'emplacement dans lequel un paquet est abandonné et la raison de l'abandon que si vous capturez des paquets à la sortie de la console. L'utilitaire `pktcap-uw` enregistre uniquement le contenu des paquets dans un fichier `.pcap` ou `.pcapng`.

- c Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.
- 2 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur `Ctrl+C` pour arrêter la capture ou le suivi de paquets.

Résultats

Outre le contenu des paquets abandonnés, la sortie de l'utilitaire `pktcap-uw` affiche la raison de l'abandon et la dernière fonction de la pile réseau qui a géré le paquet.

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Capter des paquets au niveau de DVFilter

Vérifiez les changements des paquets lorsque ceux-ci traversent vSphere Network Appliance (DVFilter).

Les DVFilters sont des agents qui résident dans le flux entre un adaptateur de machine virtuelle et un commutateur virtuel. Ils interceptent des paquets afin de protéger les machines virtuelles contre les attaques de sécurité et le trafic indésirable.

Procédure

- 1 (Facultatif) Pour rechercher le nom du DVFilter à surveiller, exécutez la commande `summarize-dvfilter` dans ESXi Shell.

Le résultat de la commande contient les agents à chemin rapide et à chemin lent des DVFilters qui sont déployés sur l'hôte.

- 2 Exécutez l'utilitaire `pktcap-uw` avec l'argument `--dvfilterdvfilter_name` et avec des options permettant de surveiller les paquets à un point spécifique, de filtrer les paquets capturés et d'enregistrer les résultats dans un fichier.

```
pktcap-uw
--dvFilter
dvfilter_name
--capture PreDVFilter|PostDVFilter [filter_options] [--outfilepcap_file_path
[--ng]] [--countnumber_of_packets]
```

où les options de la commande `pktcap-uw--dvFilter vmnicX` se trouvent entre crochets `[]` et où les barres verticales `|` représentent des valeurs alternatives.

- a Utilisez l'option `--capture` pour surveiller les paquets avant ou après leur interception par le DVFilter.

Option de commande <code>pktcap-uw</code>	Objectif
<code>--capture PreDVFilter</code>	Capture de paquets avant leur entrée dans le DVFilter.
<code>--capture PostDVFilter</code>	Capture de paquets avant leur sortie du DVFilter.

- b Utilisez `filter_options` pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- c Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.

- Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
- Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

- d Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.

- 3 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur Ctrl+C pour arrêter la capture ou le suivi de paquets.

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Utilisation des points de capture de l'utilitaire `pktcap-uw`

Utilisez les points de capture de l'utilitaire `pktcap-uw` pour surveiller les paquets lorsqu'une fonction les gère à un emplacement spécifique dans la pile réseau sur un hôte.

Présentation des points de capture

Un point de capture dans l'utilitaire `pktcap-uw` désigne un emplacement dans le chemin entre un commutateur virtuel d'un côté et un adaptateur physique, VMkernel ou de machine virtuelle de l'autre.

Vous pouvez utiliser certains points de capture en combinaison avec une option d'adaptateur. Par exemple, vous utilisez le point UplinkRcv pour capturer le trafic d'une liaison montante. Vous pouvez utiliser d'autres points autonomes, comme le point Drop pour inspecter tous les paquets abandonnés.

Note Certains points de capture de l'utilitaire `pktcap-uw` sont prévus pour une utilisation interne de VMware uniquement et vous ne pouvez les utiliser que sous la supervision du support technique de VMware. Ces points de capture ne sont pas décrits dans le guide *Mise en réseau vSphere*.

Option d'utilisation des points de capture dans l'utilitaire `pktcap-uw`

Pour examiner l'état ou le contenu d'un paquet à un point de capture, ajoutez l'option `--capture capture_point` à l'utilitaire `pktcap-uw`.

Sélection automatique d'un point de capture

Pour le trafic associé à un adaptateur physique, VMkernel ou VMXNET3, en combinant les options `--dir` et `--stage`, vous pouvez sélectionner automatiquement des points de capture et passer de l'un à l'autre pour examiner la façon dont un paquet change avant et après un point.

Points de capture de l'utilitaire `pktcap-uw`

L'utilitaire `pktcap-uw` prend en charge des points de capture qui peuvent être utilisés uniquement lorsque vous surveillez le trafic de la liaison montante, VMkernel ou de la machine virtuelle et que vous capturez des points qui représentent des emplacements spéciaux sur la pile qui ne sont pas liés au type d'adaptateur.

Points de capture pertinents pour le trafic de l'adaptateur physique

La commande `pktcap-uw --uplink vmnix` prend en charge les points de capture pour les fonctions qui gèrent le trafic à un emplacement et dans une direction spécifiques sur le chemin entre l'adaptateur physique et le commutateur virtuel.

Point de capture	Description
UplinkRcv	Fonction qui reçoit les paquets de l'adaptateur physique.
UplinkSnd	Fonction qui envoie les paquets à l'adaptateur physique.
PortInput	Fonction qui transmet une liste de paquets de UplinkRcv à un port du commutateur virtuel.
PortOutput	Fonction qui transmet une liste de paquets d'un port du commutateur virtuel au point UplinkSnd.

Points de capture pertinents pour le trafic de la machine virtuelle

La commande `pktcap-uw --switchport vmxnet3_port_ID` prend en charge les points de capture pour les fonctions qui gèrent les paquets de trafic à un emplacement et dans une direction spécifiques sur le chemin entre un adaptateur VMXNET3 et un commutateur virtuel.

Point de capture	Description
VnicRx	Fonction du serveur principal de carte réseau de machine virtuelle qui reçoit des paquets du commutateur virtuel.
VnicTx	Fonction du serveur principal de carte réseau de machine virtuelle qui envoie des paquets de la machine virtuelle au commutateur virtuel.
PortOutput	Fonction qui transmet une liste de paquets d'un port du commutateur virtuel à Vmxnet3Rx.
PortInput	Fonction qui transmet une liste de paquets de Vmxnet3Tx à un port du commutateur virtuel. Point de capture par défaut du trafic associé à l'adaptateur VMXNET3.

Points de capture pertinents pour le trafic de l'adaptateur VMkernel

Les commandes `pktcap-uw --vmk vmkX` et `pktcap-uw --switchport vmkernel_adapter_port_ID` prennent en charge des points de capture qui représentent des fonctions à un emplacement et dans une direction spécifiques sur le chemin entre un adaptateur VMkernel et un commutateur virtuel.

Point de capture	Description
PortOutput	Fonction qui transmet une liste de paquets d'un port du commutateur virtuel à l'adaptateur VMkernel.
PortInput	Fonction qui transmet une liste de paquets de l'adaptateur VMkernel à un port du commutateur virtuel. Point de capture par défaut du trafic associé à l'adaptateur VMkernel.

Points de capture pertinents pour les filtres virtuels distribués

La commande `pktcap-uw --dvfilter divfilter_name` nécessite un point de capture indiquant si la capture des paquets doit s'effectuer lorsque ceux-ci entrent dans DVFilter ou lorsqu'ils en sortent.

Point de capture	Description
PreDVFilter	Point avant l'interception d'un paquet par DVFilter.
PostDVFilter	Point après l'interception d'un paquet par DVFilter.

Points de capture autonomes

Certains points de capture sont mappés directement à la pile réseau plutôt qu'à un adaptateur physique, VMkernel ou VMXNET3.

Point de capture	Description
Annuler	Capture les paquets abandonnés et affiche l'emplacement de l'abandon.
TcpipDispatch	Capture les paquets à la fonction qui répartit le trafic sur la pile TCP/IP du VMkernel à partir du commutateur virtuel, et inversement.
PktFree	Capture les paquets juste avant qu'ils ne soient libérés.
VdrRxLeaf	Capture les paquets sur la chaîne d'E/S de la feuille de réception d'un routeur dynamique dans VMware NSX. Utilisez ce point de capture en même temps que l'option <code>--lifID</code> .
VdrRxTerminal	Capture les paquets sur la chaîne d'E/S du terminal de réception d'un routeur dynamique dans VMware NSX. Utilisez ce point de capture en même temps que l'option <code>--lifID</code> .

Point de capture	Description
VdrTxLeaf	Capture les paquets sur la chaîne d'E/S de la feuille de transmission d'un routeur dynamique dans VMware NSX. Utilisez ce point de capture en même temps que l'option <code>--lifID</code> .
VdrTxTerminal	Capture les paquets sur la chaîne d'E/S du terminal de transmission d'un routeur dynamique dans VMware NSX. Utilisez ce point de capture en même temps que l'option <code>--lifID</code> .

Pour plus d'informations sur les routeurs dynamiques, consultez la documentation *VMware NSX*.

Liste des points de capture de l'utilitaire `pktcap-uw`

Affichez tous les points de capture de l'utilitaire `pktcap-uw` pour trouver le nom du point de capture qui permet de surveiller le trafic à un emplacement spécifique de la pile réseau sur l'hôte ESXi.

Pour plus d'informations sur les points de capture de l'utilitaire `pktcap-uw`, consultez [Points de capture de l'utilitaire `pktcap-uw`](#).

Procédure

- ◆ Dans ESXi Shell sur l'hôte, exécutez la commande `pktcap-uw -A` pour afficher tous les points de capture pris en charge par l'utilitaire `pktcap-uw`.

Suivi de paquets à l'aide de l'utilitaire `pktcap-uw`

Utilisez l'utilitaire `pktcap-uw` pour suivre le chemin traversé par les paquets dans la pile réseau afin d'analyser la latence et de localiser le point sur lequel un paquet est corrompu ou abandonné.

L'utilitaire `pktcap-uw` affiche le chemin des paquets ainsi que les horodatages qui notent l'heure à laquelle un paquet est géré par une fonction de mise en réseau sur ESXi. L'utilitaire signale le chemin d'un paquet immédiatement après avoir été libéré de la pile.

Pour afficher les informations concernant le chemin complet d'un paquet, vous devez imprimer le résultat à partir de l'utilitaire `pktcap-uw` dans la sortie de la console ou l'enregistrer dans un fichier PCAPNG.

Procédure

- 1 Dans ESXi Shell sur l'hôte, exécutez la commande `pktcap-uw --trace` avec des options permettant de filtrer les paquets suivis, d'enregistrer le résultat dans un fichier et de limiter le nombre de paquets suivis.

```
pktcap-uw --trace [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

où les options de la commande `pktcap-uw --trace` se trouvent entre crochets [] et où les barres verticales | représentent des valeurs alternatives.

- a Utilisez *filter_options* pour filtrer les paquets en fonction de l'adresse source et de destination, de l'ID VLAN, de l'ID VXLAN, du protocole de couche 3 et du port TCP.

Par exemple, pour surveiller les paquets en provenance d'un système source portant l'adresse IP 192.168.25.113, utilisez l'option de filtrage `--srcip 192.168.25.113`.

- b Utilisez des options permettant d'enregistrer le contenu de chaque paquet ou le contenu d'un nombre limité de paquets dans un fichier `.pcap` ou `.pcapng`.

- Pour enregistrer les paquets dans un fichier `.pcap`, utilisez l'option `--outfile`.
- Pour enregistrer les paquets dans un fichier `.pcapng`, utilisez les options `--ng` et `--outfile`.

Vous pouvez ouvrir le fichier dans un outil d'analyse de paquets réseau tel que Wireshark.

Par défaut, l'utilitaire `pktcap-uw` enregistre les fichiers de paquets dans le dossier racine du système de fichiers ESXi.

Note Un fichier `.pcap` comprend uniquement le contenu des paquets suivis. Pour collecter les chemins des paquets en plus de leur contenu, enregistrez la sortie dans un fichier `.pcapng`.

- c Utilisez l'option `--count` pour surveiller uniquement un certain nombre de paquets.

- 2 Si vous n'avez pas limité le nombre de paquets à l'aide de l'option `--count`, appuyez sur Ctrl+C pour arrêter la capture ou le suivi de paquets.

Étape suivante

Si le contenu du paquet est enregistré dans un fichier, copiez le fichier à partir de l'hôte ESXi dans le système qui exécute l'outil d'analyse graphique, tel que Wireshark, et ouvrez-le dans l'outil pour examiner les détails des paquets.

Configurer les paramètres NetFlow d'un vSphere Distributed Switch

Pour analyser le trafic IP des machines virtuelles qui passe par un vSphere Distributed Switch donné, vous pouvez envoyer des rapports à un collecteur NetFlow.

IPFIX est pris en charge par vSphere Distributed Switch (NetFlow version 10).

Note Pour configurer IPFIX sur un vSphere Distributed Switch sauvegardé par ESXi sur DPU, vous devez créer une vmknic sur une pile TCP/IP d'opérateur. Dans le cas contraire, les informations de flux ne sont pas exportées vers le collecteur.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Paramètres > Modifier NetFlow**.
- 3 Entrez l'**adresse IP** et le **port** du collecteur NetFlow.
Vous pouvez contacter le collecteur NetFlow par le biais d'une adresse IPv4 ou IPv6.
- 4 Définissez un **ID domaine d'observation** qui identifie les informations relatives au commutateur.
- 5 Pour afficher les informations du Distributed Switch dans le collecteur NetFlow en tant que périphérique réseau unique (et non comme s'il existait différents périphériques, un pour chaque hôte du commutateur), tapez une adresse IPv4 dans la zone de texte **Adresse IP du commutateur**.
- 6 (Facultatif) Dans les zones de texte **Délai d'attente pour l'exportation du flux actif** et **Délai d'attente pour l'exportation du flux inactif**, définissez le temps d'attente (en secondes) préalable à l'envoi des informations une fois le flux en marche.
- 7 (Facultatif) Pour que le commutateur collecte une autre partie des données, configurez le **taux d'échantillonnage**.

Le taux d'échantillonnage représente le nombre de paquets annulés par NetFlow après chaque collecte de paquet. Un taux d'échantillonnage x indique à NetFlow d'annuler les paquets selon un rapport *collected packets:dropped packets* de 1: x . Si le taux est 0, NetFlow traite chaque paquet (c'est-à-dire 1 paquet collecté et 0 paquet annulé). Si le taux est 1, NetFlow traite un paquet et annule le suivant, et ainsi de suite.

- 8 (Facultatif) Pour collecter les données relatives à l'activité réseau entre machines virtuelles du même hôte, activez l'option **Traiter les flux internes uniquement**.

Ne collectez les flux internes que si NetFlow est activé sur le périphérique réseau physique afin d'éviter la duplication d'informations (qui seraient envoyées du Distributed Switch et du périphérique réseau physique à la fois).

- 9 Cliquez sur **OK**.

Étape suivante

Activez les rapports NetFlow pour le trafic provenant des machines virtuelles connectées à un groupe de ports distribués ou à un port. Reportez-vous à la section [Gérer la surveillance NetFlow sur un port distribué ou un groupe de ports distribués](#).

Présentation de la mise en miroir de ports

La mise en miroir de ports permet de mettre en miroir le trafic d'un port distribué sur d'autres ports distribués ou des ports de commutateur physiques spécifiques.

La mise en miroir de ports est utilisée sur un commutateur pour envoyer une copie des paquets vus sur un port de commutateur (ou l'intégralité de VLAN) à une connexion de surveillance sur un autre port de commutateur. La mise en miroir de port est utilisée pour analyser et déboguer des données ou diagnostiquer des erreurs sur un réseau.

Interopérabilité de la mise en miroir de ports

Certains problèmes d'interopérabilité sont à prendre en compte lors de l'utilisation de la mise en miroir du port vSphere avec d'autres fonctionnalités de vSphere.

vMotion

vMotion fonctionne différemment en fonction du type de session de mise en miroir du port vSphere que vous sélectionnez. Pendant vMotion, un chemin de mise en miroir peut être temporairement non valide, mais il est restauré lorsque vMotion s'achève.

Tableau 14-5. Interopérabilité vMotion avec la mise en miroir de port

Type de session de mise en miroir de port	Source et destination	Interopérable avec vMotion	Fonctionnalité
Mise en miroir de ports distribué	Source et destination de port distribué de liaison non montante	Oui	La mise en miroir de port entre des ports distribués peut seulement être locale. Si la source et la destination sont sur différents hôtes à cause de vMotion, la mise en miroir entre eux ne fonctionne pas. Toutefois, si la source et la destination sont déplacées sur le même hôte, la mise en miroir de port fonctionne.
Source de mise en miroir distante	Source de port distribué de liaison non montante	Oui	Lorsqu'un port distribué source est déplacé d'un hôte A à un hôte B, le chemin de mise en miroir initial du port source vers la liaison montante de A est supprimé et un nouveau chemin de mise en miroir du port source vers la liaison montante de B est créé sur B. Cette liaison montante utilisée est déterminée par le nom de liaison montante indiqué dans la session.
	Destinations de port de liaison montante	Non	Les liaisons montantes ne peuvent pas être déplacées par vMotion.
Destination de mise en miroir distante	Source VLAN	Non	

Tableau 14-5. Interopérabilité vMotion avec la mise en miroir de port (suite)

Type de session de mise en miroir de port	Source et destination	Interopérable avec vMotion	Fonctionnalité
	Destination de port distribué de liaison non montante	Oui	Lorsqu'un port distribué de destination est déplacé d'un hôte A à un hôte B, tous les chemins de mise en miroir initiaux à partir des VLAN sources vers le port de destination sont déplacés de A à B.
Source de mise en miroir distante (L3) encapsulée	Source de port distribué de liaison non montante	Oui	Lorsqu'un port distribué source est déplacé d'un hôte A à un hôte B, tous les chemins de mise en miroir initiaux à partir du port source vers les IP de destination sont déplacés de A à B.
	Destination IP	Non	
Mise en miroir de port distribué (héritage)	Source IP	Non	
	Destination de port distribué de liaison non montante	Non	Lorsqu'un port distribué de destination est déplacé d'un hôte A à un hôte B, tous les chemins de mise en miroir initiaux à partir des IP sources vers le port de destination sont invalides car la source de session de mise en miroir de port affiche toujours la destination A.

TSO et LRO

TSO (TCP Segmentation Offload) et LRO (large receive offload) peuvent rendre le nombre de paquets de mise en miroir différent du nombre de paquets mis en miroir.

Lorsque TSO est activé sur une carte vNIC, la carte vNIC peut envoyer un paquet important au commutateur distribué. Lorsque LRO est activé sur une carte vNIC, les petits paquets envoyés à cette carte peuvent être fusionnés en un paquet important.

Source	Destination	Description
TSO	LRO	Les paquets provenant de la vNIC source peuvent être des paquets importants et ils seront divisés selon que leur taille soit supérieure ou non à la limitation LRO de la vNIC de destination.
TSO	Toute destination	Les paquets provenant de la vNIC source peuvent être des paquets importants et ils sont divisés en paquets standard à la vNIC de destination.
Toute source	LRO	Les paquets provenant de la vNIC source sont des paquets standard et ils sont fusionnés en paquets plus importants à la vNIC de destination.

Créer une session de mise en miroir de ports

Créer une session de mise en miroir de ports à l'aide de vSphere Client pour mettre en miroir le trafic vSphere Distributed Switch sur des ports, des liaisons montantes et des adresses IP distantes.

Conditions préalables

Vérifiez que vSphere Distributed Switch a bien la version 5.0.0 et versions ultérieures.

Procédure

1 Sélectionner un type de session de mise en miroir de ports

Pour commencer une session de mise en miroir des ports, vous devez spécifier le type de session de mise en miroir des ports.

2 Spécifier le nom et les informations de session de mise en miroir de ports

Pour continuer à créer une session de mise en miroir de port, spécifiez un nom, description et détails de session pour la nouvelle session de mise en miroir de ports.

3 Sélectionner les sources de mise en miroir de ports

Pour continuer à créer une session de mise en miroir de port, sélectionnez les sources et les sens de trafic pour la nouvelle session de mise en miroir de ports.

4 Sélectionner les destinations de mise en miroir de ports et vérifier les paramètres

Pour compléter la création d'une session de mise en miroir des ports, sélectionner les ports ou liaisons montantes en tant que destinations pour la session de mise en miroir de ports.

Sélectionner un type de session de mise en miroir de ports

Pour commencer une session de mise en miroir des ports, vous devez spécifier le type de session de mise en miroir des ports.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de vSphere Client.
- 2 Cliquez sur l'onglet **Configurer**, puis développez **Paramètres**.
- 3 Sélectionnez l'option **Mise en miroir de ports** et cliquez sur **Nouveau**.

4 Sélectionnez le type de session pour la session de mise en miroir des ports.

Option	Description
Mise en miroir de ports distribué	Paquets miroir d'un certain nombre de ports distribués à d'autres ports distribués sur le même hôte. Si la source et la destination sont sur des hôtes différents, ce type de session ne fonctionne pas.
Source de mise en miroir distante	Paquets miroir d'un certain nombre de ports distribués à des ports de liaison montante sur l'hôte qui correspond.
Destination de mise en miroir distante	Paquets miroir à partir d'un certain nombre de VLAN aux ports distribués.
Source de mise en miroir distante (L3) encapsulée	Paquets en miroir d'un certain nombre de ports distribués vers les adresses IP d'un agent distant. Le trafic de la machine virtuelle est mis en miroir sur une destination physique ou virtuelle à travers un tunnel IP.

5 Cliquez sur **Suivant**.

Spécifier le nom et les informations de session de mise en miroir de ports

Pour continuer à créer une session de mise en miroir de port, spécifiez un nom, description et détails de session pour la nouvelle session de mise en miroir de ports.

Procédure

- 1 Définissez les propriétés de la session. Différentes options sont disponibles pour la configuration en fonction du type de session que vous avez sélectionné.

Option	Description
Nom	Vous pouvez entrer un nom unique pour la session de mise en miroir des ports, ou accepter le nom de session généré automatiquement.
État	Utilisez le menu déroulant pour activer ou désactiver la session.
Type de session	Affiche le type de session que vous avez sélectionné.
Type d'encapsulation	Sélectionnez GRE , ERSPAN TWO , ou ERSPAN THREE . Note Cette option est activée lorsque le type de session est défini sur Source de mise en miroir distante (L3) encapsulée .
ID de session	Spécifiez un ID ERSPAN si le type d'encapsulation est défini sur ERSPAN TWO ou ERSPAN THREE . Note Cette option est activée lorsque le type de session est défini sur Source de mise en miroir distante (L3) encapsulée .
ID VLAN d'encapsulation	ID de VLAN qui encapsule toutes les trames sur les ports de destination. Note Si les trames d'origine disposent d'un VLAN et que l'option Préserver le VLAN d'origine n'est pas sélectionnée, le VLAN d'encapsulation remplace le VLAN d'origine. Cette option est activée lorsque le type de session est défini sur Source de mise en miroir distante .

Option	Description
Conserver le VLAN d'origine	<p>Sélectionnez Conserver le VLAN d'origine pour conserver le réseau VLAN d'origine dans une balise interne afin que les trames mises en miroir fassent l'objet d'une double encapsulation.</p> <p>Cette option est activée lorsque le type de session est défini sur Source de mise en miroir distante.</p>
E/S normal sur les ports de destination	<p>Utilisez le menu déroulant pour activer ou désactiver l'E/S normal sur les ports de destination. Cette propriété n'est disponible que pour les destinations de port de liaison montante et de port distribué.</p> <p>Si vous désactivez cette option, le trafic en miroir sera autorisé sur les ports de destination sortants, mais le trafic entrant ne sera pas autorisé.</p>
Pile TCP/IP	<p>Utilisez le menu déroulant pour sélectionner le type de pile TCP/IP.</p> <ul style="list-style-type: none"> ■ Par défaut : la pile TCP/IP par défaut. ■ Mise en miroir : l'utilisation de la pile de mise en miroir au lieu de la pile réseau TCP/IP par défaut permet de séparer le trafic de mise en miroir du trafic de gestion. Sans pile de mise en miroir, le trafic de mise en miroir est lié à la pile TCP/IP par défaut. Le trafic de gestion utilise également la pile TCP/IP par défaut. Si le trafic de mise en miroir est volumineux, il affecte le trafic de gestion. Si vous souhaitez séparer le trafic de mise en miroir de la pile TCP/IP par défaut, vous pouvez disposer d'une pile réseau de mise en miroir dédiée sur l'hôte ESXi. Vous pouvez activer cette pile réseau dédiée lors de la configuration des sessions de mise en miroir distante encapsulée. <p>Note Si vous souhaitez configurer ERSPAN sur un vSphere Distributed Switch sauvegardé par ESXi sur DPU, créez un vmknic sur la pile TCP/IP miroir.</p> <p>Note Cette option est activée lorsque le type de session est défini sur Source de mise en miroir distante (L3) encapsulée.</p>
Longueur du paquet en miroir (Octets)	<p>Utilisez la case à cocher pour activer la longueur du paquet en miroir en octets. Cela impose limite sur la taille des trames en miroir. Si vous sélectionnez cette option, toutes les trames en miroir sont tronquées en fonction de la longueur définie.</p>
Taux d'échantillonnage	<p>Sélectionnez la vitesse à laquelle les paquets sont échantillonnés. Cette option est activée par défaut pour toutes les sessions de mise en miroir des ports à l'exception des sessions héritées.</p> <p>Note Le taux d'échantillonnage n'est pas activé si le nœud de transport NSX et la pile réseau améliorée (ENS) sont activés.</p>
Description	<p>Vous avez la possibilité d'entrer une description de la configuration de session de mise en miroir de ports.</p>

2 Cliquez sur **Suivant**.

Sélectionner les sources de mise en miroir de ports

Pour continuer à créer une session de mise en miroir de port, sélectionnez les sources et les sens de trafic pour la nouvelle session de mise en miroir de ports.

Vous pouvez créer une session de mise en miroir de ports sans définir la source et les destinations. Lorsqu'une source et une destination ne sont pas définies, une session de mise en miroir de port est créée sans le chemin de mise en miroir. Cela vous permet de créer une session de mise en miroir des ports avec l'ensemble des propriétés correct. Une fois que les propriétés sont définies, vous pouvez éditer la session de mise en miroir des ports pour ajouter les informations de source et de destination.

Note Tenez compte des limitations suivantes lors de la sélection des sources de mise en miroir de ports.

- Un port de miroir source ne peut pas être utilisé dans plusieurs sessions de miroir.
- Un port ne peut pas être utilisé comme source de mise en miroir et destination de mise en miroir dans la même session de mise en miroir ou dans des sessions de mise en miroir différentes en même temps.

Procédure

- 1 Sélectionnez la source du trafic à être mise en miroir et le sens du trafic.

Selon le type de session de mise en miroir des ports sélectionnés, différentes options sont disponibles pour la configuration.

Option	Description
Ajouter des ports existants à partir d'une liste	Cliquez sur Sélectionner les ports distribués . Une boîte de dialogue affiche la liste des ports existants. Cochez la case à côté du port distribuée et cliquez sur OK . Vous pouvez choisir plus d'un port distribuée.
Ajouter des ports existants par numéro de port	Cliquez sur Ajouter des ports distribués , entrez le numéro du port et cliquez sur OK .
Sélectionnez le sens du trafic	Après l'ajout de ports, sélectionnez le port dans la liste et cliquez sur le bouton entrée, sortie, ou à entrée/sortie. Votre choix s'affiche dans la colonne de Sens du trafic.
Spécifiez le VLAN source	Si vous avez sélectionné le type de session Destination de mise en miroir distante, vous devez spécifier un VLAN source. Cliquez sur Ajouter pour ajouter un ID de VLAN. Modifiez l'ID au moyen des flèches haut et bas ou en cliquant sur le champ et en entrant l'ID de VLAN manuellement.

- 2 Cliquez sur **Suivant**.

Sélectionner les destinations de mise en miroir de ports et vérifier les paramètres

Pour compléter la création d'une session de mise en miroir des ports, sélectionner les ports ou liaisons montantes en tant que destinations pour la session de mise en miroir de ports.

Vous pouvez créer une session de mise en miroir des ports, sans réglage de la source et de destination. Quand la source et la destination ne sont pas définies, une session de mise en miroir de port est créée sans le chemin de mise en miroir. Cela vous permet de créer une session de mise en miroir des ports avec l'ensemble des propriétés correct. Une fois que les propriétés sont définies, vous pouvez éditer la session de mise en miroir des ports pour ajouter les informations de source et de destination.

La mise en miroir de ports est vérifiée par rapport à la règle de transfert de VLAN. Si le VLAN des trames d'origine n'est pas égal ou tronqué par le port de destination, les trames ne sont pas mise en miroir.

Procédure

- 1 Choisissez la destination pour la session de mise en miroir de ports.

Selon le type de session que vous avez choisi, différentes options sont disponibles.

Option	Description
Sélectionnez un port distribué de destination	Cliquez sur Sélectionner les ports distribués pour sélectionner les ports à partir d'une liste, ou cliquez sur Ajouter des ports distribués pour ajouter des ports par leur numéro de port. Vous pouvez ajouter plus d'un port distribué.
Sélectionnez une liaison montante	Sélectionnez une liaison montante disponible à partir de la liste et cliquez sur Ajouter pour ajouter la liaison montante à la session de mise en miroir de ports. Vous pouvez sélectionner plus d'une liaison montante.
Sélectionnez les ports ou les liaisons montantes	Cliquez sur Sélectionner les ports distribués pour sélectionner les ports à partir d'une liste, ou cliquez sur Ajouter des ports distribués pour ajouter des ports par leur numéro de port. Vous pouvez ajouter plus d'un port distribué. Cliquez sur Ajouter des liaisons montantes pour ajouter des liaisons montantes comme destination. Sélectionnez des liaisons montantes de la listes et cliquez sur OK .
Indiquez l'adresse IP	Cliquez sur Ajouter . Une nouvelle entrée de liste est créée. Sélectionnez l'entrée et cliquez soit sur le bouton Modifier pour entrer l'adresse IP, soit directement dans le champ Adresse IP et entrez l'adresse IP. Une avertissement s'ouvre si l'adresse IP n'est pas valide.

- 2 Cliquez sur **Suivant**.
- 3 Vérifiez les informations que vous avez entrées pour la session de mise en miroir de port sur la page **Prêt à terminer**.
- 4 (Facultatif) Utilisez le bouton **Précédent** pour modifier les paramètres.
- 5 Cliquez sur **Terminer**.

Résultats

La nouvelle session de mise en miroir de ports apparaît dans la section Mise en miroir de ports de l'onglet **Paramètres**

Afficher les détails de la session de mise en miroir de ports

Affichez les détails de la session de mise en miroir de ports, notamment son état, ses sources et ses destinations.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et cliquez sur **Mise en miroir de ports**.
- 3 Sélectionnez une session de mise en miroir des ports de la liste pour afficher des informations plus détaillées au bas de l'écran. Utilisez les onglets pour examiner les détails de configuration.
- 4 (Facultatif) Cliquez sur **Nouveau** pour ajouter une nouvelle session de mise en miroir de ports.
- 5 (Facultatif) Cliquez sur **Modifier** pour modifier les informations de la session sélectionnée de mise en miroir de ports.
- 6 (Facultatif) Cliquez sur **Supprimer** pour supprimer la session sélectionnée de mise en miroir de ports.

Modifier les détails, les sources et les destinations de session de mise en miroir de port

Modifiez les détails d'une session de mise en miroir de ports, nom inclus, sa description, son statut, sources et destinations.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans l'onglet **Configurer**, développez la section **Paramètres** et cliquez sur **Mise en miroir de ports**.
- 3 Sélectionnez une session de mise en miroir de ports dans la liste et cliquez sur **Modifier**.
- 4 Sur la page **Propriétés**, modifiez les propriétés de la session.

Selon le type de session de mise en miroir de ports en cours d'édition, différentes options sont disponibles pour la configuration.

Option	Description
Nom	Vous pouvez entrer un nom unique pour la session de mise en miroir des ports, ou accepter le nom de session généré automatiquement.
État	Utilisez le menu déroulant pour activer ou désactiver la session.

Option	Description
E/S normal sur les ports de destination	Utilisez le menu déroulant pour activer ou désactiver l'E/S normal sur les ports de destination. Cette propriété n'est disponible que pour les destinations de port de liaison montante et de port distribué. Si vous ne sélectionnez pas cette option, le trafic en miroir est autorisé en sortie sur les ports de destination, mais pas le trafic entrant.
Taux d'échantillonnage	Sélectionnez la vitesse à laquelle les paquets sont échantillonnés. Cette option est activée par défaut pour toutes les sessions de mise en miroir des ports à l'exception des sessions héritées. Note Le taux d'échantillonnage n'est pas activé si le nœud de transport NSX et la pile réseau améliorée sont activés.
Longueur du paquet en miroir (Octets)	Utilisez la case à cocher pour activer la longueur du paquet en miroir en octets. Cela impose limite sur la taille des trames en miroir. Si vous sélectionnez cette option, toutes les trames en miroir sont tronquées en fonction de la longueur définie.
Description	Vous avez la possibilité d'entrer une description de la configuration de session de mise en miroir de ports.

- 5 Sur la page **Sources**, modifier les sources pour la session de mise en miroir de ports.

Selon le type de session de mise en miroir de ports en cours d'édition, différentes options sont disponibles pour la configuration.

Option	Description
Ajouter des ports existants à partir d'une liste	Cliquez sur le bouton Sélectionnez les ports distribués à ajouter à cette session de mise en miroir de port . Une boîte de dialogue s'ouvre avec une liste de ports existants. Cochez la case à côté du port distribuée et cliquez sur OK . Vous pouvez choisir plus d'un port distribuée.
Sélectionnez le sens du trafic	Après l'ajout de ports, sélectionnez le port dans la liste et cliquez sur le bouton entrée, sortie, ou à entrée/sortie. Votre choix s'affiche dans la colonne de Sens du trafic.

- 6 Dans la section **Destinations**, modifier les destinations pour la session de mise en miroir des ports.

Selon le type de session de mise en miroir de ports en cours d'édition, différentes options sont disponibles pour la configuration.

Option	Description
Sélectionnez un port distribué de destination	Cliquez sur le bouton Sélectionnez les ports distribués à ajouter à cette session de mise en miroir de port pour sélectionner des ports dans une liste. Vous pouvez ajouter plus d'un port distribué.

- 7 Cliquez sur **OK**.

Contrôle de santé de vSphere Distributed Switch

La prise en charge du contrôle de santé vous aide à identifier et à résoudre les erreurs de configuration dans un vSphere Distributed Switch.

Utilisez le contrôle de santé de vSphere Distributed Switch pour examiner certains paramètres sur les commutateurs distribués et physiques afin d'identifier les erreurs courantes de la configuration réseau de votre environnement. L'intervalle par défaut entre deux contrôles de santé est de 1 minute.

Important Utilisez le contrôle de santé pour dépanner les problèmes réseau, puis désactivez-le après les avoir identifiés et résolus. Après avoir désactivé le contrôle de santé de vSphere Distributed Switch, les adresses MAC générées sont exclues de votre environnement réseau physique selon la stratégie réseau. Pour plus d'informations, consultez l'article [KB 2034795](#) de la base de connaissances.

Erreur de configuration	Contrôle de santé	Configuration requise sur le commutateur distribué
Les plages de jonction VLAN configurées sur le commutateur distribué ne correspondent pas aux plages de jonction sur le commutateur physique.	Vérifie si les paramètres VLAN du commutateur distribué correspondent à la configuration du port de jonction sur les ports de commutateur physiques connectés.	Au moins deux cartes réseau physiques actives
Les paramètres MTU ne correspondent pas entre les adaptateurs réseau physiques, le commutateur distribué et les ports de commutateur physiques.	Vérifie si le paramètre de trames jumbo du port de commutateur MTU d'accès physique basé sur VLAN correspond au paramètre MTU de vSphere Distributed Switch.	Au moins deux cartes réseau physiques actives
La stratégie d'association configurée sur les groupes de ports ne correspond pas à la stratégie configurée sur le canal de port du commutateur physique.	Vérifie si les ports d'accès connectés du commutateur physique qui participent à un EtherChannel sont couplés aux ports distribués dont la stratégie d'association est définie sur Hachage IP.	Au moins deux cartes réseau physiques actives et deux hôtes

Le contrôle de santé est limité au port de commutateur d'accès auquel la liaison montante du commutateur distribué est connectée.

Gérer le contrôle de santé vSphere Distributed Switch

Le contrôle de santé surveille les modifications apportées aux configurations de vSphere Distributed Switch. Vous devez activer le contrôle de santé du vSphere Distributed Switch pour effectuer la vérification des configurations du Distributed Switch.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Sélectionnez l'onglet **Configurer** et développez Paramètre.
- 3 Sélectionnez **Contrôle de santé** et cliquez sur le bouton **Modifier**.

- Utilisez les menus déroulants pour activer ou désactiver les options de contrôle d'intégrité.

Option	Description
VLAN et MTU	Signale l'état des ports de liaison montante distribués et des plages VLAN.
Association et basculement	Vérifie l'existence d'une incompatibilité de configuration entre l'hôte ESXi et le commutateur physique utilisé dans la stratégie d'association.

- Cliquez sur **OK**.

Étape suivante

Lorsque vous modifiez la configuration d'un vSphere Distributed Switch, vous pouvez visualiser les informations sur la modification dans l'onglet **Surveiller** dans vSphere Client. Reportez-vous à la section [Afficher l'état de santé de vSphere Distributed Switch](#).

Afficher l'état de santé de vSphere Distributed Switch

Une fois que vous avez activé le contrôle de santé sur un vSphere Distributed Switch, vous pouvez afficher l'état de santé réseau des hôtes connectés dans vSphere Client .

Conditions préalables

Vérifiez que le contrôle de santé est activé sur le vSphere Distributed Switch pour VLAN, MTU et la stratégie d'association. Reportez-vous à la section [Gérer le contrôle de santé vSphere Distributed Switch](#).

Procédure

- Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- Dans l'onglet **Surveiller**, cliquez sur **Santé**.
- Dans la section État d'intégrité du membre hôte, examinez la santé globale, VLAN, MTU et d'association des hôtes connectés au commutateur.

Switch Discovery Protocol

Les protocoles SDP (Switch Discovery Protocols) aident les administrateurs vSphere à identifier le port du commutateur physique connecté à un commutateur standard vSphere ou à un vSphere Distributed Switch.

vSphere 5.0 et versions ultérieures prend en charge le protocole CDP (Cisco Discovery Protocol) et le protocole LLDP (Link Layer Discovery Protocol). CDP est disponible pour les commutateurs standard vSphere et vSphere Distributed Switches connectés aux commutateurs physiques Cisco. LLDP est disponible pour les vSphere Distributed Switches 5.0.0 et les versions suivantes.

Lorsque le protocole CDP ou LLDP est activé pour un vSphere Distributed Switch ou un commutateur standard vSphere, vous pouvez afficher les propriétés du commutateur physique homologue, tel que l'ID de périphérique, la version logicielle et le délai d'expiration à partir de vSphere Client.

Activer le protocole découverte Cisco (CDP) sur un vSphere Distributed Switch

Le protocole CDP (Cisco Discovery Protocol) permet aux administrateurs vSphere de déterminer quel port d'un commutateur physique Cisco est connecté à un commutateur vSphere standard ou à un vSphere Distributed Switch. Lorsque CDP est activé pour un vSphere Distributed Switch, vous pouvez afficher les propriétés du commutateur Cisco, telles que l'ID de périphérique, la version du logiciel et le délai d'expiration.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Paramètres > Modifier les paramètres**.
- 3 Dans la boîte de dialogue Modifier les paramètres, cliquez sur **Avancé**.
- 4 Dans la section Protocole de découverte, sélectionnez **Protocole découverte Cisco** dans le menu déroulant **Type**.
- 5 Dans le menu déroulant **Opération**, sélectionnez le mode de fonctionnement des hôtes ESXi connectés au commutateur.

Option	Description
Écouter	ESXi détecte et affiche les informations sur le port de commutateur Cisco associé, mais les informations sur le vSphere Distributed Switch ne sont pas mises à disposition de l'administrateur du commutateur Cisco.
Annoncer	ESXi met les informations sur le vSphere Distributed Switch à disposition de l'administrateur du commutateur Cisco, mais ne détecte ni n'affiche aucune information sur le commutateur Cisco.
Les deux	ESXi détecte et affiche les informations sur le commutateur Cisco associé et met les informations sur le vSphere Distributed Switch à disposition de l'administrateur du commutateur Cisco.

- 6 Cliquez sur **OK**.

Activer le protocole LLDP (Link Layer Discovery Protocol) sur un vSphere Distributed Switch

Le protocole LLDP (Link Layer Discovery Protocol) permet aux administrateurs vSphere de déterminer quel port de commutateur physique est connecté à un vSphere Distributed Switch donné. Lorsque le protocole LLDP est activé pour un commutateur distribué particulier, vous

pouvez afficher les propriétés du commutateur physique (telles que l'ID du châssis, le nom et la description du système, ainsi que les capacités du périphérique) à partir de .

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Paramètres > Modifier les paramètres**.
- 3 Dans la boîte de dialogue Modifier les paramètres, cliquez sur **Avancé**.
- 4 Dans la section Protocole de découverte, sélectionnez **Protocole de découverte de couche de lien** dans le menu déroulant **Type**.
- 5 Dans le menu déroulant **Opération**, sélectionnez le mode de fonctionnement des hôtes ESXi connectés au commutateur.

Opération	Description
Écouter	ESXi détecte et affiche les informations sur le port physique associé, mais les informations sur le vSphere Distributed Switch ne sont pas mises à disposition de l'administrateur du commutateur.
Annoncer	ESXi met les informations sur le vSphere Distributed Switch à disposition de l'administrateur du commutateur, mais ne détecte ni n'affiche aucune information sur le commutateur physique.
Les deux	ESXi détecte et affiche les informations sur le commutateur physique associé et met les informations sur le vSphere Distributed Switch à disposition de l'administrateur du commutateur.

- 6 Cliquez sur **OK**.

Afficher les informations de commutateur

Lorsque les protocoles CDP (Cisco Discovery Protocol) ou LLDP (Link Layer Discovery Protocol) sont activés sur le Distributed Switch et que le mode de fonctionnement des hôtes connectés au commutateur est Écouter ou Les deux, vous pouvez afficher les informations concernant le commutateur physique dans vSphere Client.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez **Mise en réseau** et cliquez sur **Adaptateurs physiques**.
- 3 Sélectionnez un adaptateur physique de la liste pour afficher ses informations détaillées.

Résultats

Selon le protocole SDP (Switch Discovery Protocol) qui est activé, les propriétés du commutateur s'affichent sous l'onglet **CDP** ou **LLDP**. Si les informations sont disponibles dans le réseau, vous pouvez alors examiner les capacités système du commutateur sous Fonction de périphérique homologue.

Afficher le diagramme de la topologie d'un commutateur virtuel distribué NSX

Vous pouvez examiner la structure et les composants d'un commutateur virtuel distribué NSX (N-VDS) en affichant son diagramme de topologie.

À partir du diagramme, vous pouvez afficher les paramètres d'un groupe de ports sélectionné et d'un adaptateur sélectionné.

Conditions préalables

Le diagramme de la topologie d'un commutateur N-VDS fournit une représentation visuelle des adaptateurs et des groupes de ports connectés au commutateur.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez l'option **Mise en réseau** et sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur N-VDS dans la liste.

Résultats

Le diagramme apparaît sous la liste de commutateurs virtuels sur l'hôte.

Étape suivante

Le diagramme de la topologie permet notamment de déterminer si une machine virtuelle ou un adaptateur VMkernel est connecté au réseau externe et d'identifier l'adaptateur physique qui transmet les données.

Configurer des profils de protocole pour la mise en réseau de machines virtuelles

15

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6 que vCenter Server affecte aux vApp ou aux machines virtuelles disposant de la fonctionnalité vApp qui sont connectées aux groupes de ports associés au profil.

Les profils de protocole réseau contiennent également les paramètres du sous-réseau IP, du DNS et du serveur proxy HTTP.

Pour configurer les paramètres de mise en réseau des machines virtuelles à l'aide des profils de protocole réseau, effectuez les opérations suivantes :

- Créez des profils réseau au niveau d'un centre de données ou d'un vSphere Distributed Switch.
- Associez un profil de protocole au groupe de ports d'une machine virtuelle vApp.
- Activez la stratégie d'allocation d'adresses IP temporaire ou statique dans les paramètres du vApp ou dans les options vApp d'une machine virtuelle.

Note Si vous déplacez vers un autre centre de données un vApp ou une machine virtuelle qui récupère ses paramètres réseau d'un profil de protocole, vous devez attribuer un profil de protocole au groupe de ports connectés sur le centre de données de destination pour mettre le vApp ou la machine virtuelle sous tension.

- **Ajouter un profil de protocole réseau**

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6. vCenter Server attribue ces ressources aux vApp ou aux machines virtuelles disposant de la fonctionnalité vApp qui sont connectés aux groupes de ports associés au profil.

- **Associer un groupe de ports à un profil de protocole réseau**

Pour appliquer la plage d'adresses IP d'un profil de protocole réseau à une machine virtuelle qui fait partie d'un vApp ou sur laquelle la fonctionnalité vApp est activée, associez le profil à un groupe de ports qui contrôle la mise en réseau de la machine virtuelle.

- **Utiliser un profil de protocole réseau pour allouer des adresses IP à une machine virtuelle ou à un vApp**

Après avoir associé un profil de protocole réseau à un groupe de ports d'un commutateur standard ou d'un commutateur distribué, vous pouvez utiliser le profil pour allouer dynamiquement des adresses IP à une machine virtuelle qui se trouve dans un vApp.

Ajouter un profil de protocole réseau

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6. vCenter Server attribue ces ressources aux vApp ou aux machines virtuelles disposant de la fonctionnalité vApp qui sont connectés aux groupes de ports associés au profil.

Vous pouvez configurer des plages de profil de protocole réseau pour IPv4, IPv6 ou les deux. vCenter Server utilise ces plages pour allouer dynamiquement des adresses IP aux machines virtuelles dans un vApp, lorsque le vApp utilise la stratégie d'allocation IP temporaire.

Les profils de protocole réseau contiennent également les paramètres du sous-réseau IP, du DNS et des serveurs proxy HTTP.

Note Si vous déplacez vers un autre centre de données un vApp ou une machine virtuelle qui récupère ses paramètres réseau d'un profil de protocole, pour mettre sous tension le vApp ou la machine virtuelle, vous devez attribuer un profil de protocole au groupe de ports connectés dans le centre de données de destination.

Procédure

- 1 Accédez à un centre de données associé à un vApp.
- 2 Dans l'onglet **Configurer**, sélectionnez **Plus > Profils de protocole réseau**.
Les profils de protocole réseau existants sont répertoriés.
- 3 Cliquez sur le bouton **Ajouter**.
L'assistant **Ajouter un profil de protocole réseau** s'ouvre.
- 4 Sur la page **Nom et réseau**, entrez le nom du profil de protocole réseau et sélectionnez les réseaux qui utilisent ce profil. Cliquez sur **Suivant**.
Un réseau peut être associé à un seul profil de protocole réseau à la fois.
- 5 Sur la page **IPv4**, configurez les paramètres IPv4 pertinents.
 - a Dans les zones de texte **Sous-réseau** et **Passerelle**, entrez le sous-réseau et la passerelle IP.
 - b Pour indiquer que le serveur DHCP est disponible sur le réseau, sélectionnez la case d'option **DHCP présent**.
 - c Dans la zone de texte **Adresses de serveur DNS**, entrez les informations sur le serveur DNS.
 - d Pour spécifier une plage de pools IP, activez l'option **pool d'adresses IP**.

- e Si vous activez les pools IP, saisissez une liste de plages d'adresses d'hôtes séparées par une virgule dans la zone de texte **Plage de pool IP**.

Une plage est constituée d'une adresse IP, du caractère # et d'un nombre indiquant la longueur de la plage.

Par exemple, **10.20.60.4#10**, **10.20.61.0#2** indique que les adresses IPv4 peuvent s'échelonner de 10.20.60.4 à 10.20.60.13 et de 10.20.61.0 à 10.20.61.1.

La passerelle et les plages doivent se situer à l'intérieur du sous-réseau. Les plages que vous entrez dans la zone de texte **Plage de pool IP** ne peuvent pas inclure l'adresse de la passerelle.

- f Cliquez sur **Suivant**.

6 Sur la page **IPv6**, configurez les paramètres IPv6 pertinents.

- a Dans les zones de texte **Sous-réseau** et **Passerelle**, entrez le sous-réseau et la passerelle IP.
- b Cochez la case d'option **DHCP présent** pour indiquer que le serveur DHCP est disponible sur ce réseau.
- c Dans le champ **Adresses de serveur DNS**, entrez les informations sur le serveur DNS.
- d Activez l'option de **Pool d'adresses IP** pour spécifier une plage de pools IP.
- e Si vous activez les pools IP, saisissez une liste de plages d'adresses d'hôtes séparées par une virgule dans la zone de texte **Plage de pool IP**.

Une plage est constituée d'une adresse IP, du caractère # et d'un nombre indiquant la longueur de la plage.

Supposons, par exemple, que vous spécifiez la plage de pool IP suivante :

fe80:0:0:0:2bff:fe59:5a:2b#10, **fe80:0:0:0:2bff:fe59:5f:b1#2**. Les adresses se situent alors dans la plage suivante :

fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

et

fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2.

La passerelle et les plages doivent se situer à l'intérieur du sous-réseau. Les plages que vous entrez dans la zone de texte **Plage de pool IP** ne peuvent pas inclure l'adresse de la passerelle.

- f Cliquez sur **Suivant**.

7 Sur la page **Autres configurations réseau**, spécifiez les configurations réseau supplémentaires.

- a Entrez le domaine DNS.
- b Entrez le préfixe d'hôte.

- c Entrez le chemin de recherche DNS.

Les chemins de recherche sont définis sous la forme d'une liste de domaines DNS séparés par des virgules, de points-virgules ou des espaces.

- d Saisissez le nom de serveur et le numéro de port du serveur proxy.

Le nom du serveur doit inclure un caractère deux points et un numéro de port. Par exemple, `web-proxy:3912` est un serveur proxy correct.

- e Cliquez sur **Suivant**.

- 8 Sur la page **Attribution de nom et de réseau**, passez en revue les paramètres et cliquez sur **Terminer**.

Sélectionner le nom et le réseau du profil de protocole réseau

Donnez un nom au profil de protocole réseau et sélectionnez le réseau qui doit l'utiliser.

Procédure

- 1 Saisissez le nom du profil de protocole réseau.
- 2 Sélectionnez les réseaux qui utilisent ce profil de protocole réseau.
Un réseau peut être associé à un seul profil de protocole réseau à la fois.
- 3 Cliquez sur **Suivant**.

Spécifier la configuration IPv4 du profil de protocole réseau

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6 utilisables par les vApp. Lorsque vous créez un profil de protocole réseau, vous définissez sa configuration IPv4.

Vous pouvez configurer des plages de profil de protocole réseau pour IPv4, IPv6, ou les deux. vCenter Server utilise ces plages pour allouer dynamiquement des adresses IP à des machines virtuelles lorsqu'un vApp est configuré afin d'utiliser l'allocation d'adresses IP temporaire.

Procédure

- 1 Entrez le **sous-réseau IP** et la **passerelle** dans les champs correspondants.
- 2 Sélectionnez **DHCP présent** pour indiquer que le serveur DHCP est disponible sur ce réseau.
- 3 Saisissez les informations concernant le serveur DNS.
Définissez les serveurs avec les adresses IP en les séparant avec une virgule, un point-virgule ou un espace.
- 4 Cochez la case **Activer pool IP** pour déterminer une plage de pool IP.
- 5 Si vous activez les pools IP, saisissez une liste de plages d'adresses d'hôtes séparées par une virgule dans le champ **Plage de pool IP**.
Une plage est constituée d'une adresse IP, du caractère # et d'un nombre indiquant la longueur de la plage.

La passerelle et les plages doivent se situer à l'intérieur du sous-réseau. Les plages que vous entrez dans le champ **Plage de pool IP** ne peuvent pas inclure l'adresse de la passerelle.

Par exemple, **10.20.60.4#10**, **10.20.61.0#2** indique que les adresses IPv4 peuvent s'échelonner de 10.20.60.4 à 10.20.60.13 et de 10.20.61.0 à 10.20.61.1.

6 Cliquez sur **Suivant**.

Spécifier la configuration IPv6 du profil de protocole réseau

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6 utilisables par les vApp. Lorsque vous créez un profil de protocole réseau, vous définissez sa configuration IPv6.

Vous pouvez configurer des plages de profil de protocole réseau pour IPv4, IPv6, ou les deux. vCenter Server utilise ces plages pour allouer dynamiquement des adresses IP à des machines virtuelles lorsqu'un vApp est configuré afin d'utiliser une allocation d'adresses IP temporaires.

Procédure

- 1 Entrez le **sous-réseau IP** et la **passerelle** dans les champs correspondants.
- 2 Sélectionnez **DHCP présent** pour indiquer que le serveur DHCP est disponible sur ce réseau.
- 3 Saisissez les informations concernant le serveur DNS.

Définissez les serveurs avec les adresses IP en les séparant avec une virgule, un point-virgule ou un espace.

- 4 Cochez la case **Activer pool IP** pour déterminer une plage de pool IP.
- 5 Si vous activez les pools IP, saisissez une liste de plages d'adresses d'hôtes séparées par une virgule dans le champ **Plage de pool IP**.

Une plage est constituée d'une adresse IP, du caractère # et d'un nombre indiquant la longueur de la plage. Par exemple, supposons que vous avez spécifié la plage de pool d'adresses IP suivante :

```
fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2
```

Les adresses se situent alors dans la plage suivante :

```
fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34
```

et

```
fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2
```

La passerelle et les plages doivent se situer à l'intérieur du sous-réseau. Les plages que vous entrez dans le champ **Plage de pool IP** ne peuvent pas inclure l'adresse de la passerelle.

6 Cliquez sur **Suivant**.

Spécifier une configuration DNS et d'autres configurations de profil de protocole réseau

Lorsque vous créez un profil de protocole réseau, vous pouvez spécifier le domaine DNS, le chemin de recherche DNS, un préfixe d'hôte et un proxy HTTP.

Procédure

1 Entrez le domaine DNS.

2 Entrez le préfixe d'hôte.

3 Entrez le chemin de recherche DNS.

Les chemins de recherche sont définis sous la forme d'une liste de domaines DNS séparés par des virgules, de points-virgules ou des espaces.

4 Saisissez le nom de serveur et le numéro de port du serveur proxy.

Le nom du serveur peut en option contenir un caractère deux points et un numéro de port.

Par exemple, `web-proxy:3912` est un serveur proxy correct.

5 Cliquez sur **Suivant**.

Terminer le profil de protocole réseau

Procédure

- ◆ Vérifiez les paramètres et cliquez sur **Terminer** afin de terminer l'ajout du profil de protocole réseau.

Associer un groupe de ports à un profil de protocole réseau

Pour appliquer la plage d'adresses IP d'un profil de protocole réseau à une machine virtuelle qui fait partie d'un vApp ou sur laquelle la fonctionnalité vApp est activée, associez le profil à un groupe de ports qui contrôle la mise en réseau de la machine virtuelle.

Vous pouvez associer un groupe de ports d'un commutateur standard ou un groupe de ports distribués d'un commutateur distribué à un profil de protocole réseau en utilisant les paramètres du groupe.

Procédure

1 Dans la vue Mise en réseau de vSphere Client, accédez à un groupe de ports distribués d'un vSphere Distributed Switch ou à un groupe de ports d'un commutateur standard vSphere.

Les groupes de ports des commutateurs standard sont situés sous le centre de données. vSphere Client affiche les groupes de ports distribués sous l'objet commutateur distribué parent.

2 Dans l'onglet **Configurer**, développez l'option **Plus** et cliquez sur **Profils de protocole réseau**.

- 3 Dans le coin supérieur droit, cliquez sur l'icône **Associer un profil de protocole réseau au réseau sélectionné**.

L'assistant **Associer un profil de protocole réseau** s'ouvre.

- 4 Sur la page Définir un type d'association, sélectionnez **Utiliser un profil de protocole réseau existant** et cliquez sur **Suivant**.

Si les profils de protocole réseau existants ne contiennent pas les paramètres adaptés aux machines virtuelles vApp du groupe de ports, vous devez créer un profil.

- 5 Sur la page Choisir un profil de protocole réseau existant, sélectionnez le profil de protocole réseau et cliquez sur **Suivant**.

- 6 Sur la page Prêt à terminer, passez en revue l'association et les paramètres du profil de protocole réseau et cliquez sur **Terminer**.

Utiliser un profil de protocole réseau pour allouer des adresses IP à une machine virtuelle ou à un vApp

Après avoir associé un profil de protocole réseau à un groupe de ports d'un commutateur standard ou d'un commutateur distribué, vous pouvez utiliser le profil pour allouer dynamiquement des adresses IP à une machine virtuelle qui se trouve dans un vApp.

Conditions préalables

Assurez-vous que la machine virtuelle est connectée à un groupe de ports associé au profil de protocole réseau.

Procédure

- ◆ Sélectionnez votre tâche.

Option	Description
Utiliser un profil de protocole réseau pour allouer des adresses IP à une machine virtuelle	<p>a Accédez à une machine virtuelle dans l'inventaire vCenter Server.</p> <p>b Dans l'onglet Configurer, développez la section Paramètres et sélectionnez Options vApp.</p> <p>c Cliquez sur le bouton Modifier.</p> <p>La boîte de dialogue Modifier les options vApp s'ouvre.</p> <p>d Si les options vApp ne sont pas activées, cochez la case Activer les options vApp.</p> <p>e Cliquez sur l'onglet Allocation IP.</p> <p>f Dans la section Création, sélectionnez Environnement OVF comme un schéma d'allocation d'adresses IP.</p> <p>g Dans la section Déploiement, définissez Allocation IP sur Temporaire - Pool IP ou Statique - Pool IP.</p> <p>h Cliquez sur OK.</p>
Utiliser un profil de protocole réseau pour allouer des adresses IP à un vApp	<p>a Accédez à vApp dans l'inventaire vCenter Server</p> <p>b Cliquez avec le bouton droit sur le vApp et sélectionnez Modifier les paramètres.</p> <p>La boîte de dialogue Modifier le vApp s'ouvre.</p> <p>c Cliquez sur l'onglet Allocation IP.</p> <p>d Dans la section Création, sélectionnez Environnement OVF comme un schéma d'allocation d'adresses IP.</p> <p>e Dans la section Déploiement, définissez Allocation IP sur Temporaire - Pool IP ou Statique - Pool IP.</p> <p>f Cliquez sur OK.</p>

Les options **Statique - Pool IP** et **Temporaire - Pool IP** allouent toutes les deux une adresse IP figurant dans la plage définie dans le profil de protocole réseau qui est associé au groupe de ports. Si vous sélectionnez **Statique - Pool IP**, l'adresse IP est attribuée à la première mise sous tension de la machine virtuelle ou du vApp. L'adresse IP attribuée persiste lors des redémarrages successifs. Si vous sélectionnez **Temporaire - Pool IP**, une adresse IP est attribuée à chaque mise sous tension de la machine virtuelle ou du vApp.

Résultats

Lors de la mise sous tension de la machine virtuelle, les adaptateurs connectés au groupe de ports reçoivent les adresses IP de la plage définie dans le profil de protocole. Lors de la mise hors tension de la machine virtuelle, les adresses IP sont libérées.

Qu'est-ce que le filtrage multidiffusion ?

16

Dans vSphere 6.0 et version ultérieure, vSphere Distributed Switch prend en charge les modèles de base et d'écoute pour le filtrage des paquets de multidiffusion associés à des groupes de multidiffusion individuels. Choisissez un modèle en fonction du nombre de groupes de multidiffusion auxquels les machines virtuelles sur le commutateur s'abonnent.

■ Modes de filtrage multidiffusion

Outre le trafic de multidiffusion de base par défaut pour le filtrage du trafic multidiffusion, vSphere Distributed Switch 6.0.0 et versions ultérieures prend en charge l'écoute multidiffusion qui transfère le trafic multidiffusion de façon plus précise en utilisant les messages définis par le protocole de gestion de groupes Internet (IGMP, Internet Group Management Protocol) et par le protocole MLD (Multicast Listener Discovery) provenant des machines virtuelles.

■ Activer l'écoute multidiffusion sur un vSphere Distributed Switch

Utilisez l'écoute multidiffusion sur un vSphere Distributed Switch pour transférer le trafic de façon précise conformément aux informations d'appartenance Internet Group Management Protocol (IGMP) ou Multicast Listener Discovery (MLD) que les machines virtuelles envoient pour s'abonner au trafic multidiffusion.

■ Modifier l'intervalle d'interrogation pour l'écoute multidiffusion

Lorsque l'écoute multidiffusion IGMP ou MLD est activée sur vSphere Distributed Switch, le commutateur envoie des requêtes générales concernant l'appartenance des machines virtuelles dans le cas où une requête d'écoute n'est pas configurée sur le commutateur physique. Sur les hôtes ESXi qui sont connectés au commutateur distribué, vous pouvez modifier l'intervalle qui sépare l'envoi par le commutateur des requêtes générales.

■ Modifier le nombre d'adresses IP sources pour IGMP et MLD

Lorsque vous activez une écoute multidiffusion IGMP ou MLD sur un vSphere Distributed Switch, vous pouvez modifier le nombre maximal de sources IP à partir desquelles les membres d'un groupe de multidiffusion reçoivent des paquets.

Modes de filtrage multidiffusion

Outre le trafic de multidiffusion de base par défaut pour le filtrage du trafic multidiffusion, vSphere Distributed Switch 6.0.0 et versions ultérieures prend en charge l'écoute multidiffusion qui transfère le trafic multidiffusion de façon plus précise en utilisant les messages définis par le

protocole de gestion de groupes Internet (IGMP, Internet Group Management Protocol) et par le protocole MLD (Multicast Listener Discovery) provenant des machines virtuelles.

Filtrage multidiffusion de base

En mode de filtrage multidiffusion de base, un commutateur vSphere standard ou un vSphere Distributed Switch transfère le trafic multidiffusion pour les machines virtuelles selon l'adresse MAC de destination du groupe de multidiffusion. Lors de la jonction à un groupe de multidiffusion, le système d'exploitation invité pousse l'adresse MAC multidiffusion du groupe vers le réseau par l'intermédiaire du commutateur. Le commutateur enregistre le mappage entre le port et l'adresse MAC multidiffusion de destination dans une table de transfert locale.

Le commutateur n'interprète pas les messages IGMP qu'une machine virtuelle envoie pour rejoindre ou quitter un groupe. Le commutateur les envoie directement au routeur multidiffusion local, qui les interprète ensuite pour joindre la machine virtuelle au groupe ou la retirer de celui-ci.

Le mode de base présente les restrictions suivantes :

- Une machine virtuelle peut recevoir des paquets des groupes pour lesquels elle n'est pas abonnée, car le commutateur transfère les paquets en fonction de l'adresse MAC de destination d'un groupe de multidiffusion, qui peut être potentiellement mappé vers 32 groupes de multidiffusion IP.
- Une machine virtuelle abonnée au trafic de plus de 32 adresses MAC multidiffusion reçoit des paquets pour lesquels elle n'est pas abonnée du fait d'une limitation du modèle de transfert.
- Le commutateur ne filtre pas les paquets en fonction de l'adresse source définie dans la version 3 d'IGMP.

Écoute multidiffusion

En mode d'écoute multidiffusion, une instance de vSphere Distributed Switch fournit l'écoute IGMP et MLD conformément à la norme RFC 4541. Le commutateur répartit le trafic multidiffusion plus précisément en utilisant des adresses IP. Ce mode prend en charge les adresses de groupe de multidiffusion IGMPv1, IGMPv2 et IGMPv3 pour IPv4 et les adresses de groupe de multidiffusion MLDv1 et MLDv2 pour IPv6.

Le commutateur détecte de façon dynamique l'appartenance d'une machine virtuelle. Lorsqu'une machine virtuelle envoie un paquet qui contient des informations d'appartenance IGMP ou MLD par l'intermédiaire d'un port de commutateur, le commutateur crée un enregistrement concernant l'adresse IP de destination du groupe et, dans le cas d'IGMPv3, concernant une adresse IP source à partir de laquelle une machine virtuelle préfère recevoir le trafic. Si une machine virtuelle ne renouvelle pas son appartenance à un groupe au cours d'une période donnée, le commutateur supprime l'entrée du groupe des enregistrements de recherche.

En mode d'écoute multidiffusion d'un commutateur distribué, une machine virtuelle peut recevoir le trafic multidiffusion sur un port de commutateur unique à partir de 512 groupes et 10 sources au maximum.

Activer l'écoute multidiffusion sur un vSphere Distributed Switch

Utilisez l'écoute multidiffusion sur un vSphere Distributed Switch pour transférer le trafic de façon précise conformément aux informations d'appartenance Internet Group Management Protocol (IGMP) ou Multicast Listener Discovery (MLD) que les machines virtuelles envoient pour s'abonner au trafic multidiffusion.

Utilisez l'écoute multidiffusion si des charges de travail virtualisées sur le commutateur s'abonnent à plus de 32 groupes de multidiffusion ou doivent recevoir le trafic de nœuds sources spécifiques. Pour plus d'informations sur les modes de filtrage multidiffusion de vSphere Distributed Switch, reportez-vous à [Modes de filtrage multidiffusion](#).

Conditions préalables

Vérifiez que la version de vSphere Distributed Switch est bien 6.5.0 ou version ultérieure.

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **Mise en réseau** et accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Paramètres > Modifier les paramètres**.
- 3 Dans la boîte de dialogue qui affiche les paramètres du commutateur, cliquez sur **Avancé**.
- 4 Dans le menu déroulant **Mode de filtrage multidiffusion**, sélectionnez **Écoute IGMP/MLD** et cliquez sur **OK**.

Résultats

L'écoute multidiffusion devient active sur les hôtes exécutant ESXi 6.0 et version ultérieure.

Modifier l'intervalle d'interrogation pour l'écoute multidiffusion

Lorsque l'écoute multidiffusion IGMP ou MLD est activée sur vSphere Distributed Switch, le commutateur envoie des requêtes générales concernant l'appartenance des machines virtuelles dans le cas où une requête d'écoute n'est pas configurée sur le commutateur physique. Sur les hôtes ESXi qui sont connectés au commutateur distribué, vous pouvez modifier l'intervalle qui sépare l'envoi par le commutateur des requêtes générales.

L'intervalle par défaut d'envoi des requêtes d'écoute est de 125 secondes.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système** et sélectionnez **Paramètres système avancés**.

- 3 Cliquez sur **Modifier**.
- 4 Localisez le paramètre système `Net.IGMPQueryInterval` et saisissez une nouvelle valeur du paramètre en secondes.
- 5 Cliquez sur **OK**

Modifier le nombre d'adresses IP sources pour IGMP et MLD

Lorsque vous activez une écoute multidiffusion IGMP ou MLD sur un vSphere Distributed Switch, vous pouvez modifier le nombre maximal de sources IP à partir desquelles les membres d'un groupe de multidiffusion reçoivent des paquets.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez la section **Système** et sélectionnez **Paramètres système avancés**.
- 3 Cliquez sur **Modifier**.
- 4 Localisez le paramètre système `Net.IGMPV3MaxSrcIPNum` ou `Net.MLDV2MaxSrcIPNum` et entrez une nouvelle valeur comprise entre 1 et 32 pour le paramètre.
- 5 Cliquez sur **OK**.

Présentation d'un déploiement de réseau sans état

17

Le mode sans état est un mode d'exécution pour les hôtes ESXi sans stockage qui aurait précédemment enregistré la configuration ou l'état. Les configurations sont extraites dans un profil d'hôte, qui est un modèle qui s'applique à une classe de machines. Le mode sans état permet le remplacement, le retrait et l'ajout faciles de matériel en panne et améliore la facilité de mise à l'échelle d'un déploiement matériel.

Tous les démarrages ESXi sans état ressemblent à un premier démarrage. Les démarrages d'hôtes ESXi avec une connexion réseau à vCenter Server par le biais du commutateur standard intégré. Si le profil d'hôte spécifie une appartenance à un commutateur distribué, vCenter Server joint l'hôte ESXi aux VMware Distributed Switches.

Lors de la planification de la configuration réseau pour les hôtes ESXi sans état, vous devez laisser la configuration aussi générique que possible et évitez les éléments spécifiques à l'hôte. Actuellement, la conception n'a pas d'attaches pour reconfigurer les commutateurs physiques lors du déploiement d'un nouvel hôte. De tels besoins requièrent une manipulation particulière.

Pour configurer le déploiement sans état, un hôte ESXi doit être installé de façon standard. Ensuite, trouvez et sauvegardez les informations relatives au réseau suivantes à enregistrer le profil d'hôte :

- Les instances et paramètres de commutateurs standard vSphere standard (groupes de ports, liaisons montantes, MTU, etc.)
- Instances de commutateur distribué
- Les règles de sélection pour les liaisons montantes et le port ou groupe de ports de liaisons montantes
- Informations vNIC :
 - Informations sur l'adresse (IPv4 ou IPv6, statique ou DHCP, passerelle)
 - Groupes de ports et groupes de ports distribués attribués à l'adaptateur réseau physique (`vmknic`)
 - S'il existe des commutateurs distribués, un enregistrement VLAN, des NIC physiques associées à `vmknic`, et si `Etherchannel` est configuré

Les informations enregistrées sont utilisées comme modèle pour le profil d'hôte. Une fois que les informations du commutateur virtuel de profil d'hôte ont été extraites et placées dans le profil d'hôte, vous avez la possibilité de modifier n'importe quelle information. Les modifications sont fournies pour les commutateurs standard et distribués dans ces sections : la stratégie de sélection de liaison montante, basée sur le nom de carte réseau virtuelle ou le numéro de périphérique, et la découverte automatique basée sur l'ID de VLAN. Les informations (éventuellement modifiées) sont stockées par l'infrastructure de démarrage sans état et appliquées à un hôte ESXi sans état lors de son prochain démarrage. Pendant l'initialisation du réseau, un plug-in réseau générique interprète le paramètre de profil d'hôte enregistré et effectue ce qui suit :

- Charge les pilotes de NIC physiques appropriés.
- Crée toutes les instances de commutateurs standard, ainsi que les groupes de ports. Il sélectionne les liaisons montantes selon la stratégie. Si la stratégie est basée sur l'ID VLAN, un processus de sondage est exécuté pour recueillir les informations pertinentes.
- Pour les adaptateurs réseau VMkernel connectés au commutateur standard, il crée des adaptateurs réseau et les connecte aux groupes de ports.
- Pour chaque adaptateur réseau VMkernel connecté à un commutateur distribué, il crée un commutateur standard temporaire (si besoin) avec des liaisons montantes associées à l'adaptateur réseau VMkernel. Il crée un groupe de ports temporaire avec des règles de VLAN et d'association basées sur les informations enregistrées. Le hachage IP est particulièrement utilisé si Etherchannel a été utilisé dans le commutateur distribué.
- Configure tous les paramètres d'adaptateur réseau VMkernel (attribue l'adresse, la passerelle, le MTU, etc.).

La connectivité de base fonctionne et la configuration de mise en réseau est terminée si aucun commutateur distribué n'est présent.

En cas de présence d'un commutateur distribué, le système reste en mode maintenance jusqu'à ce que la correction du commutateur distribué soit terminée. Aucune machine virtuelle n'est démarrée à cet instant. Étant donné que les commutateurs distribués ont besoin de vCenter Server, le processus de démarrage continue jusqu'à ce que la connectivité de vCenter Server soit établie et vCenter Server remarque que l'hôte doit faire partie d'un commutateur distribué. Il émet un hôte joint au commutateur distribué, en créant un commutateur standard proxy commutateur distribué sur l'hôte, sélectionne les liaisons montantes appropriées et migre le vmknic du commutateur standard au commutateur distribué. Lorsque cette opération est terminée, il supprime les groupes de ports et le commutateur standard temporaires.

À la fin du processus de correction, l'hôte ESXi est sorti du mode maintenance et HA ou DRS peut démarrer les machines virtuelles sur l'hôte.

En cas d'absence d'un profil d'hôte, un commutateur standard temporaire est créé avec la logique « réseau par défaut », qui crée un commutateur de réseau de gestion (sans balise VLAN) dont la liaison montante correspond à la vNIC de démarrage PXE. Un vmknic est créé sur le groupe de ports de réseau de gestion avec la même adresse MAC que la vNIC de démarrage PXE. Cette

logique a été précédemment utilisée pour le démarrage PXE. S'il existe un profil d'hôte, mais que le profil d'hôte de mise en réseau est désactivé ou gravement incomplet, vCenter Server revient à la mise en réseau par défaut afin que l'hôte ESXi puisse être géré à distance. Cela déclenche une défaillance de conformité, donc vCenter Server lance alors les actions de récupération.

Meilleures pratiques de mise en réseau vSphere

18

Prenez en compte ces meilleures pratiques lors de la configuration de votre réseau.

- Pour garantir une connexion stable entre vCenter Server, ESXi, et d'autres produits et services, ne définissez pas de limites et de délais d'attente de connexion entre les produits. La définition de limites et de délais d'attente peut affecter le flux des paquets et provoquer des interruptions de services.
- Isolez les uns des autres les réseaux de la gestion des hôtes, de vSphere vMotion, de vSphere FT, et ainsi de suite, pour améliorer les performances et la sécurité.
- Réservez une carte réseau NIC physique distincte à un groupe de machines virtuelles ou utilisez Network I/O Control et la formation du trafic pour garantir la bande passante aux machines virtuelles. Cette séparation permet également de distribuer une partie de la charge de travail totale du réseau sur plusieurs CPU. Les machines virtuelles isolées peuvent ensuite mieux gérer le trafic des applications, par exemple, à partir d'une instance de vSphere Client.
- Pour séparer physiquement des services réseau et dédier un ensemble particulier de cartes réseau à un service réseau spécifique, créez un commutateur standard vSphere ou un vSphere Distributed Switch pour chaque service. Si cela est impossible, séparez les services réseau sur un seul commutateur en les associant à des groupes de ports avec différents ID de VLAN. Dans les deux cas, vérifiez auprès de votre administrateur réseau que les réseaux ou VLAN que vous choisissez sont isolés du reste de votre environnement et qu'aucun routeur ne les connecte.
- Conservez la connexion vSphere vMotion sur un réseau distinct. Lorsqu'une migration avec vMotion survient, le contenu de la mémoire du système d'exploitation invité est transmis sur le réseau. Vous pouvez effectuer cette opération soit en utilisant les VLAN pour segmenter un réseau physique unique, soit en séparant des réseaux physiques (la dernière option est préférable).

Pour la migration vers des sous-réseaux IP et l'utilisation de pools de tampons et de sockets distincts, placez le trafic de vMotion sur la pile TCP/IP vMotion et le trafic pour la migration des machines virtuelles hors tension et le clonage sur la pile TCP/IP de provisionnement. Reportez-vous à la section [Couche de mise en réseau VMkernel](#).

- Vous pouvez ajouter et supprimer les adaptateurs réseau d'un commutateur standard ou distribué sans affecter les machines virtuelles ou le service réseau exécuté derrière ce commutateur. Si vous supprimez tout le matériel en cours d'exécution, les machines virtuelles peuvent toujours communiquer entre elles. Si vous laissez un adaptateur réseau intact, toutes les machines virtuelles peuvent toujours se connecter au réseau physique.
- Pour protéger vos machines virtuelles les plus sensibles, déployez des pare-feu dans les machines virtuelles qui acheminent du trafic entre les réseaux virtuels avec des liaisons montantes vers des réseaux physiques et les réseaux virtuels purs sans liaisons montantes.
- Pour optimiser les performances, utilisez des cartes réseau de machine virtuelle VMXNET 3.
- Les adaptateurs réseau physiques connectés à un même commutateur standard vSphere ou à un même vSphere Distributed Switch doivent également être connectés au même réseau physique.
- Configurez la même MTU sur tous les adaptateurs réseau VMkernel d'un vSphere Distributed Switch. Si plusieurs adaptateurs réseau VMkernel configurés avec différentes MTU sont connectés aux vSphere Distributed Switches, vous risquez de rencontrer des problèmes de connexion.

Dépanner la mise en réseau vSphere

19

Les rubriques de dépannage concernant la mise en réseau dans vSphere proposent des solutions aux problèmes potentiels qui peuvent apparaître avec la connectivité des hôtes ESXi, vCenter Server et des machines virtuelles.

Ce chapitre contient les rubriques suivantes :

- Directives pour le dépannage
- Dépanner l'allocation d'adresses MAC
- Impossible de supprimer un hôte d'un vSphere Distributed Switch
- Hôtes d'un commutateur vSphere Distributed Switch qui perdent la connectivité à vCenter Server
- Alarme indiquant une perte de redondance du réseau sur un hôte
- Les machines virtuelles perdent leur connectivité après la modification de l'ordre de basculement des liaisons montantes d'un groupe de ports distribués
- Impossible d'ajouter un adaptateur physique à un vSphere Distributed Switch sur lequel Network I/O Control est activé
- Dépanner les charges de travail activées pour SR-IOV
- Une machine virtuelle exécutant un client VPN provoque un déni de service pour les machines virtuelles sur l'hôte ou sur un cluster vSphere HA
- Faible débit pour les charges de travail UDP sur des machines virtuelles Windows
- Des machines virtuelles situées dans un même groupe de ports distribués mais sur des hôtes différents ne peuvent pas communiquer entre elles
- Les tentatives de mise sous tension d'un vApp migré échouent, car le profil de protocole associé est manquant
- Restauration d'une opération de configuration de mise en réseau et déconnexion d'un hôte de vCenter Server

Directives pour le dépannage

Pour dépanner votre implémentation de vSphere, identifiez les symptômes du problème, déterminez les composants affectés et testez les solutions possibles.

Identification des symptômes

Un certain nombre de causes possibles peuvent conduire à un sous-rendement ou à l'inexécution de votre implémentation. La première étape d'un dépannage efficace est d'identifier précisément le problème.

Définition de l'espace de problème

Après avoir isolé les symptômes du problème, vous devez définir l'espace de problème. Identifiez les composants logiciels ou matériels affectés pouvant être la cause du problème et les composants qui ne sont pas impliqués.

Test de solutions possibles

Après avoir identifié les symptômes du problème et les composants impliqués, testez les solutions de manière systématique jusqu'à ce que le problème soit résolu.



(Principes de base du dépannage)

Identification des symptômes

Avant d'essayer de résoudre un problème dans votre implémentation, vous devez identifier précisément la raison pour laquelle elle échoue.

La première étape du processus de dépannage consiste à collecter des informations qui définissent les symptômes spécifiques du problème. Vous pouvez être amené à vous poser les questions suivantes lors de la collecte de ces informations :

- Quelle tâche ou quel comportement devrait se produire ?
- La tâche affectée peut-elle être divisée en sous-tâches que vous pouvez évaluer séparément ?
- La tâche se termine-t-elle par une erreur ? Un message d'erreur y est-il associé ?
- La tâche se termine-t-elle dans un délai anormalement long ?
- L'échec est-il permanent ou sporadique ?
- Un changement récent dans le logiciel ou le matériel peut-il être lié à l'échec ?

Définition de l'espace de problème

Après avoir identifié les symptômes du problème, déterminez les composants affectés dans votre configuration, ceux qui peuvent être la source du problème et ceux qui ne sont pas impliqués.

Pour définir l'espace de problème dans une implémentation de vSphere, tenez compte des composants présents. En plus du logiciel VMware, prenez en compte le logiciel tiers utilisé et le matériel utilisé avec le matériel virtuel VMware.

La reconnaissance des caractéristiques des éléments logiciels et matériels et la manière dont ils peuvent affecter le problème vous permet d'explorer les problèmes généraux qui peuvent provoquer les symptômes.

- Configuration défectueuse des paramètres du logiciel
- Échec du matériel physique
- Incompatibilité des composants

Décomposez le processus et examinez chaque pièce ainsi que la probabilité de son implication séparément. Par exemple, un problème lié à un disque virtuel sur un stockage local n'est probablement pas lié à la configuration du routeur tiers. Cependant, l'un des paramètres du contrôleur de disque local peut contribuer au problème. Si un composant n'est pas lié aux symptômes spécifiques, vous pouvez probablement l'éliminer comme candidat au test de la solution.

Pensez aux derniers changements apportés à la configuration avant l'apparition des problèmes. Recherchez les éléments communs au problème. Si plusieurs problèmes sont apparus en même temps, vous pouvez probablement lier tous les problèmes à la même cause.

Test de solutions possibles

Après avoir pris connaissance des symptômes du problème et des composants logiciels ou matériels probablement impliqués, vous pouvez tester des solutions de manière systématique jusqu'à ce que le problème soit résolu.

Grâce aux informations obtenues sur les symptômes et les composants concernés, vous pouvez concevoir des tests visant à repérer le problème et à le résoudre. Ces conseils peuvent améliorer l'efficacité de ce processus.

- Tentez de générer autant d'idées que de solutions possibles.
- Vérifiez que chaque solution détermine explicitement si le problème a été corrigé. Testez chaque solution possible, mais ignorez rapidement les correctifs qui ne résolvent pas le problème.
- Développez et suivez une hiérarchie de solutions possibles en fonction de la probabilité de résolution. Éliminez systématiquement chaque problème potentiel du plus probable au moins probable jusqu'à ce que les symptômes disparaissent.
- Lors du test des solutions possibles, ne modifiez qu'un seul élément à la fois. Si votre installation fonctionne après avoir modifié de nombreux éléments à la fois, il se peut que vous ne soyez pas en mesure de discerner l'élément qui a fait la différence.
- Si les modifications que vous avez apportées à une solution ne permettent pas de résoudre le problème, annulez-les et revenez à l'état précédent. Si vous n'annulez pas la modification pour revenir à l'état précédent, de nouvelles erreurs peuvent apparaître.
- Trouvez une application similaire qui fonctionne et testez-la en parallèle avec la modification qui ne fonctionne pas correctement. Apportez des modifications aux deux systèmes en même temps jusqu'à ce qu'il n'existe presque aucune différence entre eux.

Dépannage avec les journaux vCenter Server

Les journaux fournis par les différents services et agents utilisés par votre implémentation offrent généralement de précieuses informations sur le dépannage.

La plupart des journaux sont situés dans `/var/log/vmware/<nom_du_service>` pour les déploiements de vCenter Server.

Journaux communs

Les journaux suivants sont communs à tous les déploiements de vCenter Server.

Tableau 19-1. Répertoires des journaux communs

Répertoire journal	Description
<code>./firstboot</code>	Stocke les journaux du premier démarrage
<code>applmgmt</code> et <code>applmgmt-audit</code>	Stockent les journaux liés à VMware Appliance Management Service
<code>cloudvm</code>	Stocke les journaux pour l'attribution et la distribution des ressources entre les services
<code>rhttpproxy</code>	Stocke les journaux pour le service VMware HTTP Reverse Proxy
<code>sca</code>	Stocke les journaux pour le service VMware Service Control Agent
<code>vapi</code>	Stocke les journaux pour le service VMware vAPI Endpoint
<code>vmafdd</code>	Stocke les journaux pour le service LDAP de VMware Authentication Framework
<code>vmdir</code>	Stocke les journaux pour le service LDAP de VMware Directory Service
<code>vmon</code>	Stocke les journaux pour le service VMware Service Lifecycle Manager

Journaux des nœuds de gestion

Les journaux suivants sont disponibles si un déploiement de nœud de gestion est sélectionné.

Tableau 19-2. Répertoires des journaux des nœuds de gestion

Répertoire journal	Service
<code>rbd</code>	VMware vSphere Auto Deploy
<code>content-library</code>	VMware Content Library Service
<code>eam</code>	VMware ESX Agent Manager
<code>netdumper</code>	VMware vSphere ESXi Dump Collector
<code>perfcharts</code>	VMware Performance Charts Service
<code>vmcam</code>	VMware vSphere Authentication Proxy
<code>vmdir</code>	VMware Directory Service - LDAP

Tableau 19-2. Répertoires des journaux des nœuds de gestion (suite)

Répertoire journal	Service
vmware-sps	VMware vSphere Profile-Driven Storage Service
vpxd	VMware vCenter Server
vpostgres	Service VMware Postgres
vcha	Service VMware vCenter High Availability

Dépanner l'allocation d'adresses MAC

Dans vSphere, certaines restrictions sur la plage d'adresses MAC pouvant être attribuées aux machines virtuelles peuvent provoquer une perte de connectivité ou l'incapacité d'activer les charges de travail.

Adresses MAC dupliquées de machines virtuelles appartenant à un même réseau

Vous rencontrez des problèmes de pertes de paquets et de connectivité, car vCenter Server génère des adresses MAC dupliquées pour les machines virtuelles.

Problème

Les adresses MAC des machines virtuelles d'un même domaine de diffusion ou sous-réseau IP sont en conflit ou vCenter Server génère une adresse MAC dupliquée pour une machine virtuelle récemment qui vient d'être créée.

Une machine virtuelle se met sous tension et fonctionne correctement, mais partage son adresse MAC avec une autre machine virtuelle. Ce cas de figure peut entraîner des pertes de paquets et d'autres problèmes.

Cause

La duplication des adresses MAC des machines virtuelles peut être causée par plusieurs raisons.

- Deux instances de vCenter Server dont les ID sont identiques provoquent un chevauchement des adresses MAC des adaptateurs réseau des machines virtuelles.

Chaque instance de vCenter Server dispose d'un ID compris entre 0 et 63 qui est généré de manière aléatoire lors de l'installation, mais qui peut être reconfiguré une fois celle-ci terminée. vCenter Server utilise l'ID de l'instance pour générer des adresses MAC pour les adaptateurs réseau de la machine.

- Une machine virtuelle hors tension a été transférée d'une instance de vCenter Server vers une autre au sein d'un même réseau (à l'aide du stockage partagé, par exemple), et un nouvel adaptateur réseau de machine virtuelle sur la première instance de vCenter Server reçoit l'adresse MAC libérée.

Solution

- ◆ Modifiez manuellement l'adresse MAC de l'adaptateur réseau de machine virtuelle.

Si une machine virtuelle existante comporte une adresse MAC qui est en conflit, vous devez fournir une adresse MAC unique dans les paramètres **Matériel virtuel**.

- Mettez la machine virtuelle hors tension, configurez l'adaptateur de sorte à utiliser une adresse MAC manuelle, puis entrez la nouvelle adresse.
- Si vous ne pouvez pas mettre la machine virtuelle hors tension pour la configurer, recréez l'adaptateur réseau qui est en conflit en activant l'attribution manuelle d'adresses MAC, puis entrez la nouvelle adresse. Dans le système d'exploitation invité, attribuez la même adresse IP statique qu'avant à l'adaptateur que vous venez de créer.

Pour plus d'informations sur la configuration des adaptateurs réseau des machines virtuelles, reportez-vous à la documentation *Mise en réseau vSphere* et *Administration d'une machine virtuelle vSphere*.

- ◆ Si l'instance de vCenter Server génère les adresses MAC des machines virtuelles en fonction de leur allocation par défaut, VMware OUI, modifiez l'ID de l'instance de vCenter Server ou utilisez une autre méthode d'allocation pour résoudre les conflits.

Note La modification de l'ID de l'instance de vCenter Server ou l'utilisation d'un autre modèle d'allocation ne résout pas les conflits d'adresses MAC sur les machines virtuelles existantes. Seules les machines virtuelles créées ou les adaptateurs réseau ajoutés après la modification reçoivent des adresses conformes au nouveau modèle.

Pour plus d'informations sur la configuration et les modèles d'allocation d'adresses MAC, reportez-vous à la documentation *Mise en réseau vSphere*.

Solution	Description
<p>Modifier l'ID de vCenter Server</p>	<p>Vous pouvez continuer à utiliser le modèle d'allocation VMware OUI si votre déploiement concerne un petit nombre d'instances de vCenter Server. Selon ce modèle, le format d'une adresse MAC est le suivant :</p> <pre data-bbox="625 430 1430 489">00:50:56:XX:YY:ZZ</pre> <p>où 00:50:56 représente le VMware OUI, <i>XX</i> est une valeur calculée selon la formule « 80 + ID de vCenter Server » et <i>YY:ZZ</i> est un nombre aléatoire.</p> <p>Pour modifier l'ID de vCenter Server, configurez l'option ID unique de vCenter Server, située dans la section Paramètres d'exécution des paramètres Général de l'instance de vCenter Server, puis redémarrez cette dernière.</p> <p>L'allocation VMware OUI fonctionne avec un maximum de 64 instances de vCenter Server et convient aux déploiements à petite échelle.</p>
<p>Passer à l'allocation par préfixe</p>	<p>Vous pouvez utiliser un Organizationally Unique Identifier (OUI) personnalisé. Par exemple, pour une plage d'adresses administrées localement 02:12:34, les adresses MAC sont au format 02:12:34:XX:YY:ZZ. Vous pouvez utiliser le quatrième octet <i>XX</i> pour répartir l'espace d'adresses OUI entre les différentes instances de vCenter Server. Cette structure engendre 255 clusters d'adresse, chacun d'eux étant géré par une instance de vCenter Server, et environ 65 000 adresses MAC par vCenter Server. Par exemple, 02:12:34:01:YY:ZZ pour vCenter Server A, 02:12:34:02:YY:ZZ pour vCenter Server B, et ainsi de suite.</p> <p>L'allocation par préfixe convient aux déploiements à plus grande échelle.</p> <p>Si vous souhaitez des adresses MAC qui soient uniques au niveau mondial, il faut enregistrer l'OUI auprès de l'association IEEE.</p>

- a Configurez l'allocation d'adresses MAC.
- b Appliquez le nouveau modèle d'allocation d'adresses MAC à une machine virtuelle existante dans les paramètres **Matériel virtuel**.
 - Mettez la machine virtuelle hors tension, configurez l'adaptateur de sorte à utiliser une adresse MAC manuelle, rétablissez l'allocation automatique d'adresses MAC, puis remettez la machine sous tension.
 - Si la machine virtuelle est en production et que vous ne pouvez pas la mettre hors tension pour la configurer, après avoir changé l'ID de vCenter Server ou le modèle d'allocation d'adresses, recréez l'adaptateur réseau qui est en conflit en activant l'attribution manuelle d'adresses MAC. Dans le système d'exploitation invité, attribuez la même adresse IP statique qu'avant à l'adaptateur que vous venez de créer.

- ◆ Appliquez la régénération des adresses MAC au cours du transfert d'une machine virtuelle entre des instances de vCenter Server en utilisant les fichiers de la machine virtuelle provenant d'une banque de données.

- a Mettez une machine virtuelle hors tension, supprimez-la de l'inventaire, puis définissez le paramètre `ethernetX.addressType` de son fichier de configuration (`.vmx`) sur **generated**.

Le signe `x` à côté d'`ethernet` représente le numéro séquentiel de la carte réseau virtuelle de la machine.

- b Importez la machine virtuelle d'un système vCenter Server à un autre en enregistrant la machine virtuelle provenant d'une banque de données dans le système vCenter Server cible.

Les fichiers de la machine virtuelle peuvent se trouver dans une banque de données partagée entre les deux instances de vCenter Server ou être téléchargés vers une banque de données accessible uniquement à partir du système vCenter Server cible.

Pour plus d'informations sur l'enregistrement d'une machine virtuelle depuis une banque de données, reportez-vous à *Administration d'une machine virtuelle vSphere*.

- c Mettez pour la première fois les machines virtuelles sous tension.

Au cours du démarrage, une icône d'information s'affiche sur la machine virtuelle dans vSphere Client.

- d Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **SE invité > Répondre à une question**.

- e Choisissez l'option **Je l'ai copié**.

Le système vCenter Server cible génère à nouveau l'adresse MAC de la machine virtuelle. La nouvelle adresse MAC commence par le préfixe VMware OUI `00:0c:29` et se base sur l'UUID BIOS de la machine virtuelle. L'UUID BIOS de la machine virtuelle est calculé à partir de celui de l'hôte.

- ◆ Si la version de vCenter Server et des hôtes est 6.0 et versions ultérieures et que les instances de vCenter Server sont connectées en mode Enhanced Linked Mode, migrez les machines virtuelles à l'aide de vMotion entre les systèmes vCenter Server.

Lorsqu'une machine virtuelle est migrée entre les systèmes vCenter Server, la source vCenter Server ajoute l'adresse MAC de la machine virtuelle à une liste d'exclusion et ne l'attribue pas à d'autres machines virtuelles.

Échec de la tentative de mise sous tension d'une machine virtuelle en raison d'un conflit d'adresses MAC

Après la définition d'une adresse MAC statique sur un adaptateur de machine virtuelle, vous ne pouvez pas mettre sous tension la machine virtuelle.

Problème

Dans vSphere Client, après l'attribution d'une adresse MAC dans la plage 00:50:56:40:YY:ZZ – 00:50:56:7F:YY:ZZ à une machine virtuelle, les tentatives de mise sous tension de la machine virtuelle échouent avec un message d'état indiquant que l'adresse MAC crée un conflit.

```
00:50:56:XX:YY:ZZ n'est pas une adresse Ethernet statique valide. Elle est en conflit avec des adresses MAC VMware réservées à un autre usage.
```

Cause

Vous tentez d'attribuer une adresse MAC qui commence par le préfixe VMware OUI 00:50:56 et qui se trouve dans la plage d'adresses allouée à des adaptateurs VMkernel hôtes sur le système vCenter Server.

Solution

Si vous souhaitez conserver le préfixe VMware OUI, définissez une adresse MAC statique dans la plage 00:50:56:00:00:00 – 00:50:56:3F:FF:FF. Sinon, définissez une adresse MAC arbitraire dont le préfixe est différent du préfixe VMware OUI. Pour obtenir des informations sur les plages disponibles pour les adresses MAC ayant le préfixe VMware OUI, reportez-vous à la documentation *Mise en réseau vSphere*.

Impossible de supprimer un hôte d'un vSphere Distributed Switch

Dans certains cas, il se peut que vous ne puissiez pas supprimer un hôte du vSphere Distributed Switch.

Problème

- Les tentatives de suppression d'un hôte d'un vSphere Distributed Switch échouent et vous recevez une notification indiquant que des ressources sont toujours en cours d'utilisation. La notification que vous recevez peut être similaire à la suivante :

```
La ressource « 16 » est en cours d'utilisation. Le port vDS DSwitch 16 est toujours sur l'hôte 10.23.112.2 connecté à MyVM nic=4000 type=vmVnic
```

- Les tentatives de suppression d'un commutateur proxy hôte qui existe encore sur l'hôte d'une configuration de mise en réseau précédente échouent. Par exemple, vous avez déplacé l'hôte vers un autre centre de données ou système vCenter Server, ou vous avez mis à niveau les logiciels ESXi et vCenter Server et créé une nouvelle configuration de la mise en réseau. Lors d'une tentative de suppression du commutateur proxy hôte, l'opération échoue car des ressources du commutateur proxy sont toujours en cours d'utilisation.

Cause

Vous ne pouvez supprimer ni l'hôte du commutateur distribué ni le commutateur proxy hôte pour les raisons suivantes.

- Des adaptateurs VMkernel sont en cours d'utilisation sur le commutateur.
- Des adaptateurs réseau de machines virtuelles sont connectés au commutateur.

Solution

Problème	Solution
Impossible de supprimer un hôte d'un commutateur distribué	<ol style="list-style-type: none"> 1 Dans vSphere Client, accédez au commutateur distribué. 2 Dans l'onglet Configurer, sélectionnez Plus > Ports. 3 Localisez tous les ports qui sont encore en cours d'utilisation et déterminez les adaptateurs réseau VMkernel ou de machines virtuelles qui sont encore rattachés aux ports sur l'hôte. 4 Migrez ou supprimez les adaptateurs VMkernel et les adaptateurs réseau des machines virtuelles qui sont encore connectés au commutateur. 5 Utilisez l'assistant Ajoutez et gérez les hôtes dans vSphere Client pour supprimer l'hôte du commutateur. <p>Une fois l'hôte supprimé, le commutateur proxy hôte est automatiquement supprimé.</p>
Impossible de supprimer un commutateur proxy hôte	<ol style="list-style-type: none"> 1 Dans vSphere Client, accédez à l'hôte. 2 Supprimez ou migrez tous les adaptateurs réseau VMkernel ou adaptateurs de machines virtuelles qui sont encore connectés au commutateur. 3 Supprimez le commutateur proxy hôte de la vue Mise en réseau sur l'hôte.

Hôtes d'un commutateur vSphere Distributed Switch qui perdent la connectivité à vCenter Server

Les hôtes d'un vSphere Distributed Switch ne peuvent pas se connecter à vCenter Server après la configuration d'un groupe de ports.

Problème

Suite à la modification de la configuration de mise en réseau d'un groupe de ports sur vSphere Distributed Switch contenant les adaptateurs VMkernel du réseau de gestion, les hôtes du commutateur perdent leur connectivité à vCenter Server. Dans vSphere Client, les hôtes ne répondent pas.

Cause

Si un commutateur vSphere Distributed Switch fonctionne dans vCenter Server et que sa fonction de restauration de mise en réseau est désactivée, le groupe de ports contenant les adaptateurs VMkernel du réseau de gestion est mal configuré dans vCenter Server et cette erreur se propage sur les hôtes du commutateur.

Note Dans vSphere, la restauration de mise en réseau est activée par défaut. Toutefois, vous pouvez activer ou désactiver les restaurations au niveau de vCenter Server. Pour plus d'informations, reportez-vous à la documentation *Mise en réseau vSphere*.

Solution

- 1 Dans l'interface utilisateur de la console directe (DCUI) d'un hôte affecté, utilisez l'option **Restaurer vDS** du menu **Options de restauration réseau** pour configurer les liaisons montantes et l'ID du VLAN du réseau de gestion.

L'interface DCUI crée un port local éphémère et lui applique la configuration des liaisons montantes et du réseau VLAN. L'interface DCUI modifie l'adaptateur VMkernel du réseau de gestion pour qu'il utilise le nouveau port local de l'hôte afin de restaurer la connectivité à vCenter Server.

Une fois l'hôte reconnecté à vCenter Server, vSphere Client affiche un avertissement indiquant que la configuration de mise en réseau de certains hôtes du commutateur est différente de celle stockée sur le vSphere Distributed Switch.

- 2 Dans vSphere Client, configurez le groupe de ports distribués du réseau de gestion avec les paramètres appropriés.

Situation	Solution
Vous avez modifié la configuration du groupe de ports une seule fois	Vous pouvez retourner en arrière et récupérer la configuration précédente du groupe de ports. Cliquez avec le bouton droit sur le groupe de ports, cliquez sur Restaurer la configuration , puis sélectionnez Restaurer vers une configuration antérieure .
Vous avez sauvegardé une configuration valide du groupe de ports	Vous pouvez restaurer la configuration du groupe de ports en utilisant le fichier de sauvegarde. Cliquez avec le bouton droit sur le groupe de ports, cliquez sur Restaurer la configuration , puis sélectionnez Restaurer une configuration depuis un fichier . Vous pouvez également restaurer la configuration de l'intégralité du commutateur, y compris du groupe de ports, à partir d'un fichier de sauvegarde du commutateur.
Vous avez effectué plusieurs étapes de la configuration et vous n'avez pas de fichier de sauvegarde	Vous devez indiquer manuellement les paramètres valides pour le groupe de ports.

Pour plus d'informations sur la restauration et la récupération de la mise en réseau, reportez-vous à la documentation *Mise en réseau vSphere*.

- 3 Migrez l'adaptateur VMkernel du réseau de gestion à partir du port local éphémère de l'hôte vers un port distribué du commutateur à l'aide de l'assistant **Ajouter et gérer les hôtes**.

À la différence des ports distribués, le port local éphémère du VMKernel dispose d'un ID non numérique.

Pour plus d'informations sur la gestion des adaptateurs VMkernel à l'aide de l'assistant **Ajouter et gérer les hôtes**, reportez-vous à la documentation *Mise en réseau vSphere*.

- 4 Appliquez la configuration du groupe de ports et de l'adaptateur VMkernel de vCenter Server à l'hôte.
 - Envoyez la configuration correcte du groupe de ports et de l'adaptateur VMkernel de vCenter Server à l'hôte.
 - a Dans vSphere Client, accédez à l'hôte.
 - b Dans l'onglet **Configurer**, cliquez sur **Mise en réseau**.
 - c Dans la liste **Commutateurs virtuels**, sélectionnez le commutateur distribué et cliquez sur **Rectifier l'état du commutateur distribué sélectionné sur l'hôte**.
 - Patientez pendant les prochaines vingt-quatre heures pour que vCenter Server applique les paramètres.

Alarme indiquant une perte de redondance du réseau sur un hôte

Une alarme signale une perte de redondance de la liaison montante sur un commutateur standard ou un vSphere Distributed Switch d'un hôte.

Problème

Aucune carte réseau physique redondante d'un hôte n'est connectée à un commutateur standard ou distribué particulier et l'alarme suivante s'affiche :

```
Host name or IP Perte de redondance de la liaison montante
```

Cause

Une seule carte réseau physique de l'hôte est connectée au commutateur standard ou distribué particulier. Les cartes réseau physiques redondantes sont hors service ou ne sont pas attribuées au commutateur.

Par exemple, supposons qu'un hôte de votre environnement dispose des cartes réseau physiques *vmnic0* et *vmnic1* connectées à *vSwitch0*; *vmnic1* se déconnecte, ce qui ne laisse que *vmnic0* connectée à *vSwitch0*. Cela entraîne la perte de la redondance de la liaison montante de *vSwitch0* sur l'hôte.

Solution

Déterminez le commutateur qui a perdu la redondance de la liaison montante sur l'hôte. Connectez au moins une carte réseau physique supplémentaire de l'hôte à ce commutateur, puis réinitialisez l'alarme sur la couleur verte. Vous pouvez utiliser vSphere Client ou ESXi Shell.

Si une carte réseau physique est hors service, tentez de la récupérer à l'aide d'ESXi Shell sur l'hôte.

Pour plus d'informations sur l'utilisation des commandes de mise en réseau dans ESXi Shell, reportez-vous à *Référence d'ESXCLI*. Pour plus d'informations sur la configuration de la mise en réseau sur un hôte dans vSphere Client, reportez-vous à *Mise en réseau vSphere*.

Les machines virtuelles perdent leur connectivité après la modification de l'ordre de basculement des liaisons montantes d'un groupe de ports distribués

Si l'ordre de basculement des cartes réseau sur un groupe de ports distribués est modifié, les machines virtuelles associées au groupe se déconnectent du réseau externe.

Problème

Après la réorganisation des liaisons montantes dans les groupes de basculement d'un groupe de ports distribués dans vCenter Server, à l'aide de vSphere Client par exemple, certaines machines virtuelles du groupe de ports ne peuvent plus accéder au réseau externe.

Cause

Après la modification de l'ordre de basculement, de nombreuses raisons peuvent provoquer la perte de connectivité des machines virtuelles au réseau externe.

- L'hôte qui exécute les machines virtuelles ne dispose pas de cartes réseau physiques associées aux liaisons montantes actives ou en veille. Toutes les liaisons montantes associées aux cartes réseau physiques de l'hôte pour le groupe de ports passent à l'état Inutilisé.
- Un groupe d'agrégation de liens (LAG) qui ne dispose pas de cartes réseau physiques de l'hôte est défini comme la seule liaison montante active selon les conditions d'utilisation de LACP dans vSphere.
- Si le trafic des machines virtuelles est séparé dans les réseaux VLAN, les adaptateurs physiques hôtes des liaisons montantes actives peuvent être connectés aux ports du tronc sur le commutateur physique qui ne gère pas le trafic de ces réseaux VLAN.
- Si le groupe de ports est configuré avec une stratégie d'équilibrage de charge basée sur le hachage IP, un adaptateur de liaison montante active est connecté à un port de commutateur physique qui n'est pas nécessairement dans une configuration EtherChannel.

Vous pouvez vérifier la connectivité des machines virtuelles du groupe de ports aux liaisons montantes hôtes et aux adaptateurs de liaison montante associés dans le diagramme de topologie central du commutateur distribué ou dans le diagramme du commutateur proxy de l'hôte.

Solution

- ◆ Restaurez à l'état actif l'ordre de basculement et la liaison montante associée à une carte réseau physique unique sur l'hôte.
- ◆ Créez un groupe de ports avec des paramètres identiques, faites-lui utiliser le nombre de liaisons montantes valide pour l'hôte et migrez la mise en réseau des machines virtuelles vers le groupe de ports.

- ◆ Déplacez la carte réseau vers une liaison montante qui participe au groupe de basculement actif.

Vous pouvez utiliser vSphere Client pour déplacer la carte réseau physique hôte vers une autre liaison montante.

- Utilisez l'assistant **Ajouter et gérer des hôtes** sur le commutateur distribué.
 - a Accédez au commutateur distribué dans vSphere Client.
 - b Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
 - c Sur la page **Sélectionner une tâche**, sélectionnez l'option **Gérer la mise en réseau de l'hôte** et sélectionnez l'hôte.
 - d Pour affecter la carte réseau de l'hôte à une liaison montante active, naviguez vers la page **Gérer les adaptateurs réseau physiques** et associez la carte réseau à la liaison montante du commutateur.
- Déplacez la carte réseau au niveau de l'hôte.
 - a Naviguez jusqu'à l'hôte dans vSphere Client et, dans l'onglet **Configurer**, développez le menu **Mise en réseau**.
 - b Sélectionnez **Commutateurs virtuels**, ainsi que le commutateur proxy distribué.
 - c Cliquez sur **Gérer les adaptateurs réseau physiques connectés au commutateur sélectionné** et déplacez la carte réseau vers la liaison montante active.

Impossible d'ajouter un adaptateur physique à un vSphere Distributed Switch sur lequel Network I/O Control est activé

Vous ne pourrez peut-être pas ajouter un adaptateur physique de faible vitesse (par exemple, 1 Gbits/s) à un vSphere Distributed Switch sur lequel vSphere Network I/O Control version 3 est configuré.

Problème

Vous tentez d'ajouter un adaptateur physique de faible vitesse (par exemple, 1 Gbits/s), à un vSphere Distributed Switch connecté à des adaptateurs physiques de haute vitesse (par exemple, 10 Gbits/s). Network I/O Control version 3 est activé sur le commutateur et des réservations de bande passante existent pour un ou plusieurs types de trafic système (par exemple, le trafic de gestion vSphere, le trafic vSphere vMotion, le trafic vSphere NFS, etc.). La tâche d'ajout de l'adaptateur physique échoue avec un message d'état indiquant qu'un paramètre est incorrect.

```
A specified parameter was not correct: spec.host[].backing.pnicSpec[]
```

Cause

Network I/O Control aligne la bande passante disponible pour réservation sur la vitesse de 10 Gbits/s des adaptateurs physiques individuels qui sont déjà connectés au Distributed Switch. Si, après avoir réservé une partie de cette bande passante, vous ajoutez un adaptateur physique d'une vitesse inférieure à 10 Gbits/s, cela risque de ne pas répondre aux besoins potentiels d'un type de trafic système.

Pour obtenir des informations sur Network I/O Control version 3, reportez-vous à la documentation *Mise en réseau vSphere*.

Solution

- 1 Dans vSphere Client, accédez à l'hôte.
- 2 Dans l'onglet **Configurer**, développez le groupe de paramètres **Système**.
- 3 Sélectionnez **Paramètres système avancés** puis cliquez sur **Modifier**.
- 4 Entrez les adaptateurs physiques que vous souhaitez utiliser hors de l'étendue de Network I/O Control sous la forme d'une liste séparée par des virgules avec le paramètre `Net.IOControlPnicOptOut`.

Par exemple : `vmnic2,vmnic3`
- 5 Cliquez sur **OK** pour appliquer les modifications.
- 6 Dans vSphere Client, ajoutez l'adaptateur physique au Distributed Switch.

Dépanner les charges de travail activées pour SR-IOV

Dans certains cas, vous pouvez rencontrer des problèmes de connectivité ou de mise sous tension avec les machines virtuelles qui utilisent SR-IOV pour envoyer des données à des adaptateurs réseau physiques.

Une charge de travail compatible SR-IOV ne peut pas communiquer après la modification de son adresse MAC

Lorsque vous modifiez l'adresse MAC spécifiée dans le système d'exploitation invité d'une machine virtuelle sur laquelle SR-IOV est activé, la machine virtuelle perd la connectivité.

Problème

Lorsque vous connectez l'adaptateur réseau d'une machine virtuelle à une fonction virtuelle (VF) SR-IOV, vous créez un adaptateur réseau relais pour la machine virtuelle. Lorsque le pilote (VF) du système d'exploitation invité modifie l'adresse MAC de l'adaptateur réseau relais, le système d'exploitation invité indique que la modification a bien été effectuée, mais l'adaptateur réseau de la machine virtuelle perd la connectivité. Le système d'exploitation invité indique que la nouvelle adresse MAC est activée, mais dans le fichier `/var/log/vmkernel.log`, un message de journal indique que l'opération a échoué.

```
L'adresse MAC demandée devient new MAC address sur le port VM NIC port number, ce qui est interdit par la stratégie vswitch.
```

où

- *new MAC address* est l'adresse MAC du système d'exploitation invité.
- *VM NIC port number* est le numéro de port de l'adaptateur réseau de la machine virtuelle au format hexadécimal.

Cause

La stratégie de sécurité appliquée par défaut au groupe de ports auquel l'adaptateur réseau relais est connecté interdit de modifier l'adresse MAC définie dans le système d'exploitation invité. Dans le système d'exploitation invité, l'interface de mise en réseau se voit donc incapable d'acquérir une adresse IP et perd la connectivité.

Solution

- ◆ Dans le système d'exploitation invité, réinitialisez l'interface afin que l'adaptateur réseau relais récupère son adresse MAC valide. Si l'interface est configurée afin d'utiliser DHCP pour l'attribution d'adresse, elle acquiert automatiquement une adresse IP.

Par exemple, sur une machine virtuelle Linux, exécutez la commande de console `ifconfig`.

```
ifconfig ethX down
ifconfig ethX up
```

où *X* dans `ethX` représente le numéro de séquence de l'adaptateur réseau de la machine virtuelle dans le système d'exploitation invité.

Une machine virtuelle exécutant un client VPN provoque un déni de service pour les machines virtuelles sur l'hôte ou sur un cluster vSphere HA

Si une machine virtuelle envoie des trames BPDU (Bridge Protocol Data Unit), par exemple, un client VPN, certaines machines connectées au même groupe de ports peuvent perdre la connectivité. La transmission de trames BPDU peut aussi provoquer une perte de connexion de l'hôte ou du cluster vSphere HA parent.

Problème

Une machine virtuelle qui est censée envoyer des trames BPDU entraîne le blocage du trafic vers le réseau externe des machines virtuelles du même groupe de ports.

Si cette machine virtuelle s'exécute sur un hôte qui fait partie d'un cluster vSphere HA et que cet hôte devient, dans certaines conditions, isolé du réseau, vous observez un déni de service (DoS) sur les hôtes du cluster.

Cause

Il est recommandé d'activer les fonctions PortFast et BPDU Guard sur un port de commutateur physique connecté à un hôte ESXi afin d'appliquer la limite du protocole STP (Spanning Tree Protocol). Un commutateur standard ou distribué ne prend pas en charge le protocole STP et n'envoie aucune trame BPDU au port de commutateur. Cependant, si une trame BPDU issue d'une machine virtuelle compromise atteint un port de commutateur physique accessible par un hôte ESXi, la fonction BPDU Guard désactive le port afin d'empêcher les trames d'affecter la topologie STP du réseau.

Dans certains cas, on attend d'une machine virtuelle qu'elle envoie des trames BPDU ; par exemple, lorsqu'elle déploie un client VPN connecté via un périphérique pont Windows ou une fonction de pont. Si la fonction BPDU Guard du port de commutateur physique couplé avec l'adaptateur physique qui gère le trafic à partir de cette machine virtuelle est activée, l'état du port est « error-disabled » et les machines virtuelles et adaptateurs VMkernel qui utilisent l'adaptateur physique de l'hôte ne peuvent plus communiquer avec le réseau externe.

Si la stratégie d'association et de basculement du groupe de ports contient d'autres liaisons montantes actives, le trafic BPDU est déplacé vers l'adaptateur de la liaison montante active suivante. Le nouveau port de commutateur physique est alors désactivé et la charge de travail supplémentaire ne parvient plus à échanger des paquets avec le réseau. En fin de compte, il est possible que presque toutes les entités de l'hôte ESXi deviennent inaccessibles.

Si cette machine virtuelle s'exécute sur un hôte qui fait partie d'un cluster vSphere HA et que cet hôte est isolé du réseau en raison de la désactivation de la plupart des ports de commutateur physique qui y sont connectés, l'hôte principal actif du cluster déplace la machine virtuelle dont est issu le trafic BPDU vers un autre hôte. La machine virtuelle commence alors à désactiver les ports de commutateur physique connectés au nouvel hôte. La migration à travers le cluster vSphere HA entraîne finalement un cumul de dénis de service (DoS) dans tout le cluster.

Solution

- ◆ Si le logiciel VPN doit continuer son travail sur la machine virtuelle, autorisez le trafic sortant de la machine virtuelle et configurez individuellement le port de commutateur physique afin de l'autoriser à transmettre les trames BPDU.

Périphérique réseau	Configuration
Commutateur standard ou distribué	<p>Choisissez l'option Accepter pour la propriété de sécurité Transmission forgée du groupe de ports afin de permettre aux trames BPDU de quitter l'hôte et d'atteindre le port de commutateur physique.</p> <p>Vous pouvez isoler les paramètres et l'adaptateur physique du trafic VPN en plaçant la machine virtuelle dans un groupe de ports séparé et en attribuant l'adaptateur physique au groupe.</p> <p>Attention La définition de la propriété de sécurité Transmission forgée sur Accepter pour permettre à un hôte d'envoyer des trames BPDU comporte un risque de sécurité, car une machine virtuelle compromise peut effectuer des attaques d'usurpation.</p>
Commutateur physique	<ul style="list-style-type: none"> ■ Ne désactivez pas la fonction PortFast. ■ Activez le filtre BPDU sur le port individuel. Lorsqu'une trame BPDU atteint le port, elle est éliminée par le filtre. <p>Note N'activez pas le filtre BPDU de manière globale. Si ce filtre est activé de manière globale, le mode PortFast se désactive et tous les ports de commutateur physique appliquent les fonctions STP au complet.</p>

- ◆ Pour déployer un périphérique pont entre deux cartes réseau de machine virtuelle connectées au même réseau de couche 2, autorisez le trafic BPDU sortant des machines virtuelles et désactivez les fonctions de prévention des boucles PortFast et BPDU.

Périphérique réseau	Configuration
Commutateur standard ou distribué	<p>Choisissez l'option Accepter pour la propriété Transmission forgée de la stratégie de sécurité des groupes de ports afin de permettre aux trames BPDU de quitter l'hôte et d'atteindre le port de commutateur physique.</p> <p>Vous pouvez isoler les paramètres, ainsi qu'un ou plusieurs adaptateurs physiques du trafic de pont, en plaçant la machine virtuelle dans un groupe de ports séparé et en attribuant les adaptateurs physiques au groupe.</p> <p>Attention La définition de la propriété de sécurité Transmission forgée sur Accepter pour permettre un déploiement de pont comporte un risque de sécurité, car une machine virtuelle compromise peut effectuer des attaques d'usurpation.</p>
Commutateur physique	<ul style="list-style-type: none"> ■ Désactivez la fonction PortFast des ports du périphérique pont virtuel afin de pouvoir exécuter le protocole STP sur ces ports. ■ Désactivez le filtre BPDU et la fonction BPDU Guard sur les ports accessibles au périphérique pont.

- ◆ Protégez l'environnement de toute attaque de déni de service (DoS) en activant le filtre BPDU sur l'hôte ESXi ou sur le commutateur physique.
- ◆ Sur un hôte auquel le filtre Invité BPDU n'est pas appliqué, activez le filtre BPDU sur le port de commutateur physique du périphérique pont virtuel.

Périphérique réseau	Configuration
Commutateur standard ou distribué	Choisissez l'option Rejeter pour la propriété Transmission forgée de la stratégie de sécurité du groupe de ports.
Commutateur physique	<ul style="list-style-type: none"> ■ Conservez la configuration PortFast. ■ Activez le filtre BPDU sur le port de commutateur physique. Lorsqu'une trame BPDU atteint le port physique, elle est éliminée par le filtre. <p>Note N'activez pas le filtre BPDU de manière globale. Si ce filtre est activé de manière globale, le mode PortFast est désactivé et tous les ports de commutateur physique appliquent les fonctions STP au complet.</p>

Faible débit pour les charges de travail UDP sur des machines virtuelles Windows

Lorsqu'une machine virtuelle Windows dans vSphere transmet de grands paquets UDP, le débit est inférieur à celui attendu ou oscille même en l'absence d'un trafic significatif.

Problème

Lorsqu'une machine virtuelle Windows transmet des paquets UDP d'une taille supérieure à 1 024 octets, vous obtenez un débit plus faible que prévu ou oscillant même en l'absence d'un trafic significatif. Dans le cas d'un serveur de flux vidéo, la lecture vidéo marque des pauses.

Cause

Pour chaque paquet UDP d'une taille supérieure à 1 024 octets, la pile réseau de Windows attend une interruption de fin de transmission avant d'envoyer le paquet suivant. vSphere ne fournit pas de solution transparente pour ce problème.

Solution

- ◆ Augmentez le seuil en octets auquel Windows change son comportement pour les paquets UDP en modifiant le Registre du système d'exploitation Windows invité.
 - a Localisez la clé de Registre
`HKLM\System\CurrentControlSet\Services\Afd\Parameters.`
 - b Ajoutez une valeur sous le nom `FastSendDatagramThreshold` de type `DWORD` égale à 1500.

Pour obtenir des informations sur la résolution de ce problème dans le Registre Windows, reportez-vous à l'article <http://support.microsoft.com/kb/235257>.

- ◆ Modifiez les paramètres de fusion de la carte réseau de machine virtuelle.

Si la machine virtuelle Windows dispose d'un adaptateur vNIC VMXNET3, configurez l'un des paramètres suivants du fichier `.vmx` de la machine virtuelle. Utilisez vSphere Client ou modifiez directement le fichier `.vmx`.

Action	Paramètre	Valeur
Augmentez le taux d'interruptions de la machine virtuelle à une valeur supérieure au taux de paquets attendu. Par exemple, si le taux de paquets attendu est de 15 000 interruptions par seconde, réglez le taux d'interruptions à 16 000 interruptions par seconde. Définissez le paramètre <code>ethernetX.coalescingScheme</code> sur rbc et le paramètre <code>ethernetX.coalescingParams</code> sur 16000 . Le taux d'interruptions par défaut est de 4 000 interruptions par seconde.	<code>ethernetX.coalescingScheme</code>	rbc
	<code>ethernetX.coalescingParams</code>	16000
Désactivez la fusion pour un faible débit ou pour les charges de travail sensibles à la latence. Pour plus d'informations sur la configuration des charges de travail à faible latence, reportez-vous à Meilleures pratiques pour l'ajustement des performances des charges de travail sensibles à la latence sur les machines virtuelles vSphere .	<code>ethernetX.coalescingScheme</code>	désactivé
Rétablissez l'algorithme de fusion des versions antérieures d'ESXi.	<code>ethernetX.coalescingScheme</code>	étalonner
<p>Note La possibilité de rétablir un algorithme antérieur ne sera pas disponible dans les versions ultérieures de vSphere.</p>		

`X` près d'`ethernet` représente le numéro de séquence de la vNIC dans la machine virtuelle.

Pour obtenir des informations sur la configuration des paramètres dans le fichier `.vmx`, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

- ◆ Modifiez les paramètres de fusion d'hôte d'ESXi.

Cette approche affecte toutes les machines virtuelles et toutes les cartes réseau de machine virtuelle sur l'hôte.

Vous pouvez modifier la liste des paramètres système avancés pour l'hôte dans vSphere Client ou en utilisant une commande de console vCLI sur l'hôte à partir d'ESXi Shell.

Action	Paramètre dans vSphere Client	Paramètre pour la commande <code>esxcli system settings advanced set</code>	Valeur
Définissez un taux d'interruptions supérieur au taux de paquets attendu. Par exemple, définissez-le sur 16 000 si vous attendez 15 000 interruptions par seconde.	Net.CoalesceScheme Net.CoalesceParams	/Net/CoalesceScheme /Net/CoalesceParams	rbc 16000
Désactivez la fusion pour un faible débit ou pour les charges de travail sensibles à la latence. Pour plus d'informations sur la configuration des charges de travail à faible latence, reportez-vous à Meilleures pratiques pour l'ajustement des performances des charges de travail sensibles à la latence sur les machines virtuelles vSphere .	Net.CoalesceDefaultOn	/Net/ CoalesceDefaultOn	0
Rétablissez le schéma de fusion de versions antérieures d'ESXi.	Net.CoalesceScheme	/Net/CoalesceScheme	étalonner

Note La possibilité de rétablir un algorithme antérieur ne sera pas disponible dans les versions ultérieures de vSphere.

Pour obtenir des informations sur la configuration d'un hôte dans vSphere Client, reportez-vous à la documentation *Gestion de vCenter Server et des hôtes*. Pour obtenir des informations sur la définition des propriétés d'hôte à l'aide d'une commande vCLI, reportez-vous à la documentation *Référence d'ESXCLI*.

Des machines virtuelles situées dans un même groupe de ports distribués mais sur des hôtes différents ne peuvent pas communiquer entre elles

Sous certaines conditions, les machines virtuelles résidant sur le même groupe de ports distribués mais sur des hôtes différents ne peuvent pas communiquer entre elles.

Problème

Des machines virtuelles se trouvant sur des hôtes différents, mais dans le même groupe de ports, ne parviennent pas à communiquer. Les commandes ping envoyées depuis une machine virtuelle vers une autre restent sans effet. Vous ne parvenez pas à migrer les machines virtuelles entre les hôtes avec vMotion.

Cause

- Sur certains hôtes, aucune carte réseau physique n'est attribuée à des liaisons montantes actives ou en veille dans l'ordre d'association et de basculement du groupe de ports distribués.

- Sur les hôtes, les cartes réseau physiques qui sont attribuées aux liaisons montantes actives ou en veille se trouvent sur différents réseaux VLAN sur le commutateur physique. Les cartes réseau physiques dans des VLAN différents ne peuvent pas se voir et ne peuvent donc pas communiquer entre elles.

Solution

- Dans la topologie du commutateur distribué, vérifiez quel est l'hôte sur lequel aucune carte réseau physique n'est attribuée à une liaison montante active ou en veille dans le groupe de ports distribués. Sur cet hôte, attribuez au moins une carte réseau physique à une liaison montante active dans le groupe de ports.
- Dans la topologie du commutateur distribué, vérifiez les ID VLAN des cartes réseau physiques attribuées aux liaisons montantes actives dans le groupe de ports distribués. Sur tous les hôtes, attribuez des cartes réseau physiques provenant du même réseau VLAN à une liaison montante active dans le groupe de ports distribués.
- Pour vérifier qu'il n'y a aucun problème au niveau de la couche physique, migrez les machines virtuelles vers le même hôte et contrôlez la communication entre elles. Vérifiez que le trafic ICMP entrant et sortant est activé sur le système d'exploitation invité. Par défaut, le trafic ICMP est désactivé dans Windows Server 2008 et Windows Server 2012.

Les tentatives de mise sous tension d'un vApp migré échouent, car le profil de protocole associé est manquant

Vous ne pouvez pas mettre sous tension un vApp ou une machine virtuelle que vous avez transféré vers un centre de données ou un système vCenter Server, car un profil de protocole réseau est manquant.

Problème

Après avoir migré à froid un vApp ou une machine virtuelle vers un autre centre de données ou système vCenter Server, sa mise sous tension échoue. Un message d'erreur indique qu'une propriété ne peut être ni initialisée ni allouée, car le réseau du vApp ou de la machine virtuelle n'est associé à aucun profil de protocole réseau.

```
Impossible d'initialiser la propriété « property ». Le réseau « port group » n'a pas de profil de protocole réseau associé.
```

```
Impossible d'allouer une adresse IP pour la propriété « property ». Le réseau « port group » n'a pas de profil de protocole réseau associé.
```

Cause

À l'aide de l'environnement OVF, le vApp ou la machine virtuelle récupère les paramètres réseau d'un profil de protocole réseau associé au groupe de ports du vApp ou de la machine virtuelle.

vCenter Server crée un profil de protocole réseau pour vous lorsque vous installez l'environnement OVF d'un vApp et associe le profil au groupe de ports que vous avez spécifié au cours de l'installation.

Le mappage entre le profil de protocole et le groupe de ports est valide uniquement dans l'étendue d'un centre de données. Lorsque vous déplacez le vApp, le profil de protocole n'est pas transféré vers le centre de données cible pour les raisons suivantes :

- Les paramètres réseau du profil de protocole peuvent ne pas être valides dans l'environnement réseau du centre de données cible.
- Un groupe de ports portant le même nom et associé à un autre profil de protocole peut déjà exister dans le centre de données cible, et les vApps ainsi que les machines virtuelles peuvent être connectés à ce groupe. Le remplacement des profils de protocole pour le groupe de ports peut affecter la connectivité de ces vApp et machines virtuelles.

Solution

- Créez un profil de protocole réseau sur le centre de données ou le système vCenter Server cible avec les paramètres réseau requis et associez le profil de protocole au groupe de ports auquel le vApp ou la machine virtuelle sont connectés. Par exemple, cette méthode est valable si le vApp ou la machine virtuelle est une extension de vCenter Server qui utilise vCenter Extension vService.

Pour plus d'informations sur la fourniture des paramètres réseau à un vApp ou à une machine virtuelle à partir d'un profil de protocole réseau, consultez la documentation *Mise en réseau vSphere*.

- Utilisez vSphere Client pour exporter le fichier OVF du vApp ou de la machine virtuelle à partir du centre de données ou du système vCenter Server source et le déployer sur le centre de données ou le système vCenter Server cible.

Lorsque vous utilisez vSphere Client pour déployer le fichier OVF, le système vCenter Server cible crée le profil de protocole réseau pour le vApp.

Pour plus d'informations sur la gestion des fichiers OVF dans vSphere Client, consultez la documentation *Administration d'une machine virtuelle vSphere*.

Restauration d'une opération de configuration de mise en réseau et déconnexion d'un hôte de vCenter Server

Lorsque vous tentez d'ajouter ou de configurer la mise en réseau sur un vSphere Distributed Switch sur un hôte, l'opération est restaurée et l'hôte est déconnecté de vCenter Server.

Problème

Une tentative de configuration de mise en réseau sur un vSphere Distributed Switch sur un hôte, comme la création d'un adaptateur de machine virtuelle ou d'un groupe de ports, entraîne la déconnexion de l'hôte de vCenter Server et l'affichage du message d'erreur `Transaction restaurée sur l'hôte`.

Cause

En cas de conditions de stress sur un hôte, par exemple, si de nombreuses opérations de mise en réseau simultanées entrent en concurrence pour des ressources limitées, la durée nécessaire pour effectuer certaines opérations peut dépasser le délai d'expiration par défaut défini pour la restauration des opérations de configuration de réseau sur le commutateur distribué. Par conséquent, ces opérations sont restaurées.

Par exemple, ce type de condition peut apparaître lorsque vous créez un adaptateur VMkernel sur un hôte disposant d'un nombre très élevé de ports commutés ou d'adaptateurs virtuels qui utilisent tous les ressources système sur l'hôte.

Le délai d'expiration par défaut pour restaurer une opération est de 30 secondes.

Solution

- ◆ Utilisez vSphere Client pour augmenter le délai d'expiration de la restauration sur vCenter Server.

Si vous rencontrez à nouveau le même problème, augmentez progressivement le délai de restauration de 60 secondes jusqu'à ce que l'opération dispose de suffisamment de temps pour s'achever correctement.

- Dans l'onglet **Configurer** d'une instance de vCenter Server, cliquez sur **Paramètres**.
 - Sélectionnez **Paramètres avancés** puis cliquez sur **Modifier**.
 - Si la propriété est absente, ajoutez le paramètre `config.vpxd.network.rollbackTimeout` aux paramètres.
 - Entrez une nouvelle valeur, en secondes, pour le paramètre `config.vpxd.network.rollbackTimeout`.
 - Cliquez sur **OK**.
 - Redémarrez le système vCenter Server pour appliquer les modifications.
- ◆ Augmentez le délai d'expiration de la restauration en modifiant le fichier de configuration `vpxd.cfg`.

Si vous rencontrez à nouveau le même problème, augmentez progressivement le délai de restauration de 60 secondes jusqu'à ce que l'opération dispose de suffisamment de temps pour s'achever correctement.

- Sur la machine hôte de vCenter Server, accédez au répertoire `/etc/vmware-vpx`.
- Ouvrez le fichier `vpxd.cfg` pour modification.

- c Dans la section <network>, augmentez le délai d'expiration dans l'élément <rollbackTimeout>.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

- d Enregistrez et fermez le fichier.
- e Redémarrez le système vCenter Server pour appliquer les modifications.