

Mise en réseau vSphere

Mise à jour 1
vSphere 5.5
ESXi 5.5
vCenter Server 5.5

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur :
<http://www.vmware.com/fr/support/pubs>.

FR-001359-00

vmware®

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

<http://www.vmware.com/fr/support/>

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

Copyright © 2009–2014 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos de la mise en réseau vSphere	9
1 Introduction à la mise en réseau	11
Présentation des concepts de mise en réseau	11
Services réseau dans ESXi	13
Configuration VLAN	13
Prise en charge de VMware ESXi Dump Collector	14
2 Configurer les communications réseau avec des commutateurs standard vSphere	15
commutateur standard vSphere	15
Configuration du groupes de ports pour des machines virtuelles	17
Ajout d'un groupe de ports de machine virtuelle avec Client Web vSphere	17
Modification d'un groupe de ports de commutateur standard dans Client Web vSphere	18
Supprimer un groupe de ports d'un commutateur standard vSphere dans Client Web vSphere	19
Propriétés des commutateurs standard vSphere	20
Modifier le nombre de ports d'un commutateur standard vSphere dans Client Web vSphere	20
Modifier la vitesse d'un adaptateur physique dans Client Web vSphere	20
Ajouter et associer les adaptateurs physiques d'un commutateur standard dans Client Web vSphere	21
Afficher le diagramme de la topologie d'un commutateur standard vSphere dans Client Web vSphere	21
3 Configuration des communications réseau avec des vSphere Distributed Switches	23
Architecture de vSphere Distributed Switch	24
Créer un vSphere Distributed Switch avec Client Web vSphere	25
Mettre à niveau un vSphere Distributed Switch vers une version ultérieure avec Client Web vSphere	27
Modifier les paramètres généraux et avancés dans vSphere Distributed Switch avec Client Web vSphere	28
Gestion de la mise en réseau sur plusieurs hôtes sur un vSphere Distributed Switch	29
Tâches de gestion de la mise en réseau d'hôte sur un vSphere Distributed Switch	30
Ajouter des hôtes à un vSphere Distributed Switch avec Client Web vSphere	31
Configurer des adaptateurs réseau physiques sur un vSphere Distributed Switch dans Client Web vSphere	33
Migrer des adaptateurs VMkernel vers un vSphere Distributed Switch dans Client Web vSphere	34
Créer un adaptateur VMkernel sur un vSphere Distributed Switch dans Client Web vSphere	34
Migrer la mise en réseau de machines virtuelles vers le vSphere Distributed Switch dans Client Web vSphere	36

Mettre à jour le nombre maximal de ports distribués autorisés sur les hôtes dans Client Web vSphere	37
Utiliser un hôte comme un modèle pour créer une configuration de la mise en réseau uniforme sur un vSphere Distributed Switch dans Client Web vSphere	37
Supprimer des hôtes d'un vSphere Distributed Switch avec Client Web vSphere	38
Gestion de la mise en réseau sur des commutateurs proxy hôtes	39
Migrer les adaptateurs réseau d'un hôte vers un vSphere Distributed Switch dans Client Web vSphere	39
Migrer l'adaptateur VMkernel d'un hôte vers un commutateur vSphere standard dans Client Web vSphere	40
Attribuer une carte réseau physique à un vSphere Distributed Switch dans Client Web vSphere	41
Supprimer une carte réseau physique de vSphere Distributed Switch dans Client Web vSphere	41
Définir le nombre de ports d'un commutateur de proxy hôte dans Client Web vSphere	41
Suppression des cartes réseau des machines virtuelles actives	42
Groupes de ports distribués	43
Ajouter un groupe de ports distribués dans Client Web vSphere	43
Modifier les paramètres généraux d'un groupe de ports distribués avec Client Web vSphere	46
Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere	47
Supprimer un groupe de ports distribués dans Client Web vSphere	48
Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere	48
Utilisation des ports distribués	50
Surveiller l'état d'un port distribué avec Client Web vSphere	50
Configurer les paramètres d'un port distribué avec Client Web vSphere	51
Configurer les communications réseau virtuelles sur un vSphere Distributed Switch	51
Migrer des machines virtuelles vers ou depuis un vSphere Distributed Switch avec Client Web vSphere	51
Connecter une machine virtuelle à un groupe de ports distribués avec Client Web vSphere	52
Diagrammes de la topologie d'un vSphere Distributed Switch dans Client Web vSphere	52
Afficher la topologie d'un vSphere Distributed Switch dans Client Web vSphere	53
Afficher la topologie d'un commutateur de proxy hôte dans Client Web vSphere	54
Contrôle de l'intégrité d'un vSphere Distributed Switch	55
Activer ou désactiver le contrôle de l'intégrité du vSphere Distributed Switch dans Client Web vSphere	55
Afficher les informations du contrôle de l'intégrité d'un vSphere Distributed Switch	56
Exporter, importer et restaurer des configurations de commutateurs distribués	56
Exporter les configurations de groupe de ports distribués avec Client Web vSphere	57
Importer un vSphere Distributed Switch à l'aide de Client Web vSphere	57
Restaurer la configuration de vSphere Distributed Switch à l'aide de Client Web vSphere	58
VLAN privés	59
Créer un VLAN privé avec Client Web vSphere	59
Supprimer un VLAN privé principal avec Client Web vSphere	60
Supprimer un VLAN privé secondaire avec Client Web vSphere	60
Prise en charge de LACP sur vSphere Distributed Switch	61
Convertir vers la prise en charge étendue du protocole LACP sur un vSphere Distributed Switch dans Client Web vSphere	63
Configuration de l'association et du basculement LACP pour des groupes de ports distribués	65
Configurer un LAG pour gérer le trafic des groupes de ports distribués dans Client Web vSphere	65
Modifier un LAG dans Client Web vSphere	69

Activer la prise en charge du protocole LACP 5.1 pour un groupe de ports de liaison montante dans Client Web vSphere	70
Limitations de la prise en charge LACP sur vSphere Distributed Switch	71
4 Configuration de la mise en réseau VMkernel	73
La couche réseau VMkernel	74
Afficher les informations sur les adaptateurs VMkernel d'un hôte dans Client Web vSphere	75
Créer un adaptateur VMkernel sur un vSphere Standard Switch dans Client Web vSphere	76
Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch dans vSphere Web Client	78
Modifier la configuration d'un adaptateur VMkernel dans Client Web vSphere	79
Afficher la configuration de la pile TCP/IP d'un hôte dans Client Web vSphere	80
Modifier la configuration d'une pile TCP/IP sur un hôte dans Client Web vSphere	81
Créer une pile TCP/IP personnalisée	81
Supprimer un adaptateur VMkernel dans Client Web vSphere	82
5 Règles de mise en réseau	83
Stratégie d'association et de basculement	84
Modifier la stratégie d'association et de basculement d'un commutateur standard vSphere dans Client Web vSphere	84
Modifier la stratégie d'association et de basculement d'un groupe de ports standard dans Client Web vSphere	86
Modifier la stratégie d'association et de basculement d'un groupe de ports distribués dans Client Web vSphere	88
Modifier les stratégies d'association et de basculement de port distribué avec Client Web vSphere	90
Règle VLAN	92
Modifier la règle VLAN d'un groupe de ports distribués dans Client Web vSphere	92
Modifier la règle VLAN d'un port distribué avec Client Web vSphere	93
Modifier la règle VLAN sur un groupe de ports de liaison montante dans Client Web vSphere	93
Modifier la règle VLAN d'un port liaison montante avec Client Web vSphere	94
Règle de sécurité	95
Modifier la règle de sécurité d'un commutateur standard vSphere dans Client Web vSphere	95
Modifier l'exception de règle de sécurité de la couche 2 pour un groupe de ports standard dans Client Web vSphere	96
Modifier la règle de sécurité d'un groupe de ports distribués dans Client Web vSphere	97
Modifier les règles de sécurité de port distribué avec Client Web vSphere	98
Règle de formation du trafic	99
Modifier la stratégie de formation du trafic d'un commutateur standard vSphere dans Client Web vSphere	100
Modifier la règle de formation du trafic d'un groupe de ports standard dans Client Web vSphere	101
Modifier la stratégie de formation du trafic d'un groupe de ports distribués dans Client Web vSphere	101
Modifier la stratégie de formation du trafic d'un port distribué dans Client Web vSphere	102
Règle d'allocation des ressources	103
Modifier la règle d'allocation des ressources d'un groupe de ports distribués dans Client Web vSphere	103

Modifier la règle d'allocation des ressources d'un port distribué dans vSphere Web Client	104
Règle de surveillance	104
Modifier la règle de surveillance d'un groupe de ports distribués dans Client Web vSphere	105
Modifier la règle de surveillance d'un port distribué dans Client Web vSphere	105
Règle de filtrage et de balisage du trafic	106
Filtrage et balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere	106
Filtrage et balisage du trafic sur un port distribué ou un port de liaison montante dans Client Web vSphere	114
Qualification du trafic pour le filtrage et le balisage	122
Règles de blocage des ports	124
Modifier la règle de blocage d'un groupe de ports distribués dans Client Web vSphere	124
Modifier les règles de blocage de port distribué ou de port de liaison montante avec Client Web vSphere	125
Gérer les stratégies de plusieurs groupes de ports sur un vSphere Distributed Switch dans Client Web vSphere	125

6 Gestion des ressources réseau 133

Contrôle d'E/S réseau vSphere	133
Activer Network I/O Control sur un vSphere Distributed Switch avec Client Web vSphere	134
Créer un pool de ressources réseau avec Client Web vSphere	134
Ajouter ou supprimer des groupes de ports distribués dans un pool de ressources réseau avec Client Web vSphere	135
Modifier les paramètres de pool de ressources réseau avec Client Web vSphere	136
Supprimer un pool de ressources réseau défini par l'utilisateur avec Client Web vSphere	136
Délestage de segmentation TCP et trames Jumbo	137
Activation du TSO (délestage de segmentation TCP)	137
Activation de trames Jumbo	138
NetQueue et performances réseau	140
Activer NetQueue sur un hôte	140
Désactiver NetQueue sur un hôte	141
DirectPath I/O	141
Activer un relais pour un périphérique réseau sur un hôte dans Client Web vSphere	142
Configurer un périphérique PCI sur une machine virtuelle avec Client Web vSphere	143
Activer DirectPath I/O avec vMotion sur une machine virtuelle avec Client Web vSphere	143
Virtualisation des E/S à racine unique (SR-IOV)	144
Prise en charge SR-IOV	145
Architecture et interaction des composants SR-IOV	147
Interaction entre vSphere et fonction virtuelle	149
DirectPath I/O vs SR-IOV	150
Configurer une machine virtuelle pour utiliser SR-IOV dans Client Web vSphere	150
Options de mise en réseau pour le trafic associé à une machine virtuelle sur laquelle SR-IOV est activé	152
Utilisation d'un adaptateur physique SR-IOV pour gérer le trafic des machines virtuelles	153
Activation de SR-IOV en utilisant des profils d'hôte dans Client Web vSphere ou via une commande ESXCLI	153
Une machine virtuelle qui utilise une fonction virtuelle SR-IOV est mise hors tension, car l'hôte n'a plus de vecteurs d'interruption	155

7	Gestion des adresses MAC	157
	Attribution d'adresses MAC depuis vCenter Server	157
	Allocation de VMware OUI	158
	Allocation d'adresse MAC par préfixe	158
	Allocation d'adresse MAC basée sur plage	159
	Attribution d'une adresse MAC	159
	Génération d'adresse MAC sur des hôtes ESXi	161
	Définition d'une adresse MAC statique pour une machine virtuelle	162
	VMware OUI dans les adresses MAC statiques	162
	Attribuer une adresse MAC statique à l'aide de Client Web vSphere	163
	Attribuer une adresse MAC statique dans le fichier de configuration de la machine virtuelle	163
8	Mise en réseau avancée	165
	Activer ou désactiver la prise en charge d'IPv6 sur un hôte à l'aide de Client Web vSphere	165
	Utilisation de la mise en miroir de ports	166
	Compatibilité de version de mise en miroir	166
	Interopérabilité de la mise en miroir de ports	167
	Créer une session de mise en miroir de ports avec Client Web vSphere	169
	Afficher les détails de la session de mise en miroir des ports dans Client Web vSphere	172
	Modifier les détails, les sources et les destinations de la session de mise en miroir de ports avec Client Web vSphere	172
	Configurer les paramètres NetFlow avec Client Web vSphere	174
	Switch Discovery Protocol	174
	Activer le protocole CDP (Cisco Discovery Protocol) sur un vSphere Distributed Switch avec Client Web vSphere	175
	Activer le protocole LLDP (Link Layer Discovery Protocol) sur un vSphere Distributed Switch dans Client Web vSphere	175
	Afficher les informations du commutateur sur Client Web vSphere	176
	Montage de volumes NFS	176
	Récupération et restauration de mise en réseau	176
	Restauration de mise en réseau vSphere	177
	Restaurer une configuration de la mise en réseau précédente avec Client Web vSphere	179
	Résoudre les erreurs dans la configuration du réseau de gestion sur un vSphere Distributed Switch	179
	Configurer les profils de protocole pour la mise en réseau des machines virtuelles	180
	Ajouter un profil de protocole réseau	181
	Associer un groupe de ports à un profil de protocole réseau dans Client Web vSphere	183
	Configurer une machine virtuelle ou un vApp pour utiliser un profil de protocole réseau dans Client Web vSphere	183
	Déploiement de réseau sans état	184
9	Surveillance des paquets réseau	187
	Capture et suivi des paquets réseau à l'aide de l'utilitaire pktcap-uw	187
	Syntaxe de la commande pktcap-uw pour la capture de paquets	187
	Syntaxe de la commande pktcap-uw pour le suivi de paquets	189
	Options de pktcap-uw pour le contrôle de sortie	190
	Options de pktcap-uw pour le filtrage de paquets	191

	Capture de paquets à l'aide de l'utilitaire pktcap-uw	192
	Suivi de paquets à l'aide de l'utilitaire pktcap-uw	201
10	Meilleures pratiques de mise en réseau	203
	Index	205

À propos de la mise en réseau vSphere

La documentation *Mise en réseau vSphere* donne des informations sur la configuration de la mise en réseau de VMware vSphere[®], notamment comment créer des vSphere Distributed Switches 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.

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

Cette rubrique porte sur les concepts de base des communications réseau ESXi et la manière d'installer et de configurer un réseau dans un environnement vSphere.

Ce chapitre aborde les rubriques suivantes :

- [« Présentation des concepts de mise en réseau », page 11](#)
- [« Services réseau dans ESXi », page 13](#)
- [« Configuration VLAN », page 13](#)
- [« Prise en charge de VMware ESXi Dump Collector », page 14](#)

Présentation des concepts de mise en réseau

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

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.
Commutateur Ethernet physique	Il 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.
Commutateur standard vSphere	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.
Groupe de ports standard	Il spécifie les options de configuration de ports, telles que les restrictions de bande passante et les stratégies de balisage VLAN pour chaque port membre. 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.
vSphere Distributed Switch	Il fait office de commutateur unique sur tous les hôtes associés dans un centre de données pour assurer le provisionnement, l'administration et la surveillance centralisée des réseaux virtuels. Lorsque vous configurez un vSphere Distributed Switch sur le système vCenter Server, la configuration est renseignée sur tous les hôtes associés au commutateur. Ceci permet aux machines virtuelles de conserver une configuration de mise en réseau cohérente pendant qu'elles migrent sur plusieurs hôtes.
Commutateur de proxy hôte	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.
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.
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 dans l'éventualité d'une défaillance matérielle ou d'une indisponibilité du réseau.
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 Virtual SAN.

Stockage IP

Toute forme de stockage basée sur la communication de réseau TCP/IP. iSCSI peut être utilisé comme banque de données de machine virtuelle et NFS comme banque de données de machine virtuelle. NFS peut également être utilisé pour le montage direct de fichiers .ISO, présentés comme 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 entêtes initiaux TCP/IP.

Services réseau dans ESXi

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.

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.

La configuration ESXi avec les VLAN est recommandée pour les raisons suivantes.

- Intégration de l'hôte dans un environnement préexistant.
- Isolation et sécurisation du trafic réseau.
- Réduction de la congestion du trafic réseau.

Vous pouvez configurer les VLAN dans ESXi en procédant de trois manières : Balisage de commutateur externe (EST), Balisage de commutateur virtuel (VST) et Balisage d'invité virtuel (VGT).

Avec EST, tous les balisages VLAN de paquets sont exécutés sur le commutateur physique. Les adaptateurs réseau hôtes sont connectés aux ports d'accès sur le commutateur physique. Les groupes de ports connectés au commutateur virtuel doivent avoir leur ID VLAN réglée sur 0.

Avec VST, tous les balisages VLAN de paquets sont exécutés par le commutateur virtuel avant de quitter l'hôte. Les adaptateurs réseau hôtes doivent être connectés aux ports trunk sur le commutateur physique. L'ID VLAN des groupes de ports connectés au commutateur virtuel doit être compris entre 1 et 4 094.

Avec VGT, tous les balisages VLAN sont exécutés par la machine virtuelle. Les balises VLAN sont conservées entre la pile de mise en réseau de la machine virtuelle et le commutateur externe quand les trames passent par les commutateurs virtuels. Les adaptateurs réseau hôtes doivent être connectés aux ports trunk sur le commutateur physique. Pour un commutateur standard, l'ID VLAN des groupes de ports avec VGT doit être défini sur 4095. Pour un commutateur distribué, la stratégie de jonction VLAN doit inclure la plage de VLAN auxquels les machines virtuelles sont connectées.

REMARQUE En utilisant VGT, vous devez avoir un pilote trunk 802.1Q VLAN installé sur la machine virtuelle.

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 5.1 et les versions ultérieures prend en charge les commutateurs standard vSphere et les vSphere Distributed Switches. 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 l'image 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. Vous devez autant que possible configurer ESXi Dump Collector sur un VLAN distinct pour isoler le vidage de la 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 vSphere*.

Configurer les communications réseau avec des commutateurs standard vSphere

2

Les commutateurs standard vSphere gèrent le trafic réseau au niveau de l'hôte dans un déploiement vSphere.

Ce chapitre aborde les rubriques suivantes :

- [« commutateur standard vSphere », page 15](#)
- [« Configuration du groupes de ports pour des machines virtuelles », page 17](#)
- [« Propriétés des commutateurs standard vSphere », page 20](#)

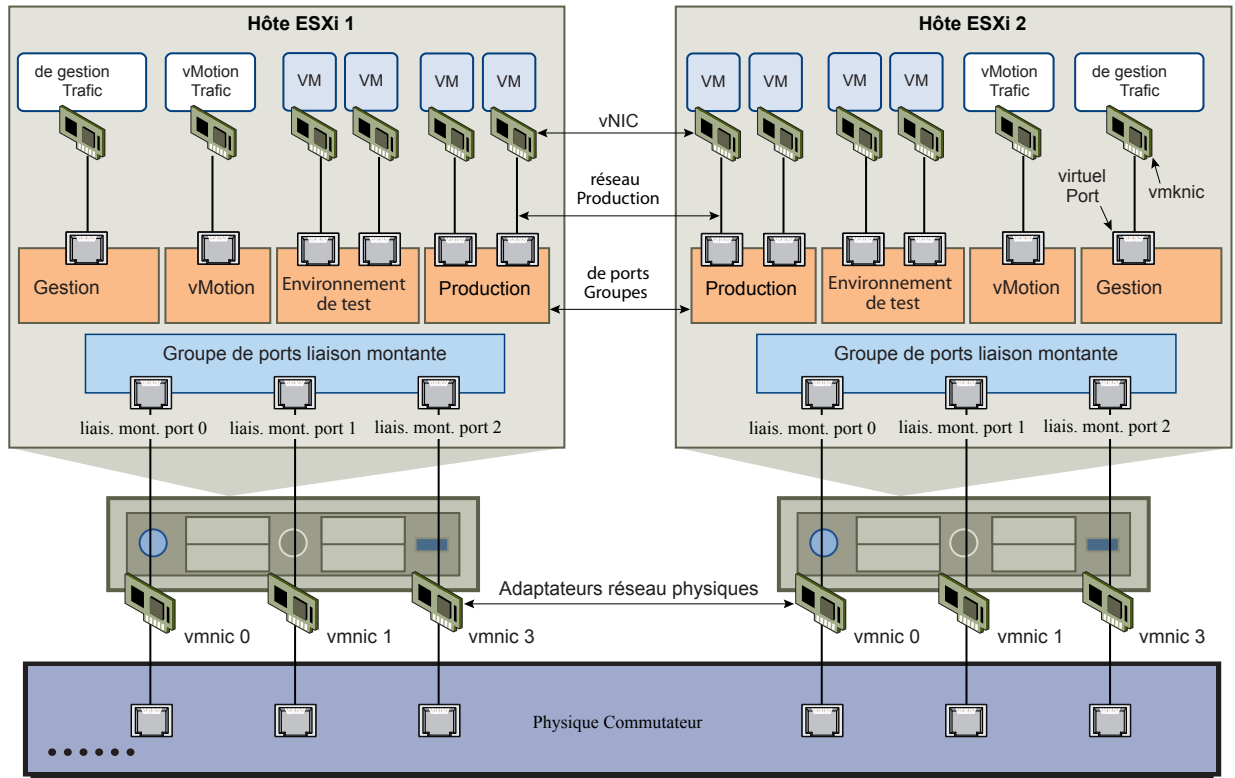
commutateur standard vSphere

Vous pouvez créer des périphériques réseau abstraits nommés commutateurs standard vSphere. Les commutateurs standard vous permettent d'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 est très similaire à un commutateur Ethernet physique. Le nombre par défaut de ports logiques d'un commutateur standard est 120. 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 utilise 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).

Configuration du 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 Client Web vSphere vous aide à créer un réseau virtuel auquel les machines virtuelles pourront se connecter, ainsi qu'un commutateur standard vSphere. Il vous aide également à définir les paramètres de configuration 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. Dans ce cas, veillez à ce que les deux hôtes se trouvent dans le même domaine de diffusion, à savoir 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 avec Client Web vSphere

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

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Cliquez avec le bouton droit de la souris sur l'hôte dans le navigateur puis sélectionnez **Toutes les actions vCenter > 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) Dans la page Créer un commutateur standard, attribuez des adaptateurs réseau physiques au commutateur standard.

Vous pouvez créer un commutateur standard avec ou sans adaptateurs.

Si vous créez un commutateur standard sans adaptateurs réseau physique, tout le 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**.
 - c Utilisez le menu déroulant **Groupe d'ordre de basculement** pour attribuer l'adaptateur au groupe Adaptateurs actifs, Adaptateurs en veille ou Adaptateurs inutilisés et cliquez sur **OK**.
 - d (Facultatif) Utilisez les flèches haut et bas dans la liste **Adaptateurs affectés** pour chanter la position de l'adaptateur si nécessaire.
 - e 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.
 - 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 de commutateur virtuel (VST)	De 1 à 4094	Le commutateur virtuel identifie le trafic avec la balise saisie.
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.

Modification d'un groupe de ports de commutateur standard dans Client Web vSphere

En utilisant Client Web vSphere, 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 Client Web vSphere, accédez à l'hôte.
 - 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis 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 Cliquez sur **Modifier** sous le titre du diagramme de la topologie.
 - 6 Dans la section **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 de commutateur virtuel (VST)	De 1 à 4094	Le commutateur virtuel identifie le trafic avec la balise saisie.
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 Dans la section **Sécurité**, remplacez les paramètres du commutateur pour assurer la protection contre l'emprunt d'identité MAC et pour exécuter les machines virtuelles en mode promiscuité.
- 9 Dans la section **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 section **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 dans Client Web vSphere

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

Prérequis

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

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis 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 le groupe de ports sélectionné**.

Propriétés des commutateurs standard vSphere

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

Modifier le nombre de ports d'un commutateur standard vSphere dans Client Web vSphere

Pour les hôtes qui exécutent ESXi 5.1 et versions antérieures, vous pouvez configurer le nombre de ports disponibles sur un commutateur standard en fonction de l'évolution de votre environnement.

Chaque commutateur virtuel sur les hôtes qui exécutent ESXi 5.1 et versions antérieures, fournit un nombre déterminé de ports via lesquels les machines virtuelles et les services réseau peuvent atteindre un ou plusieurs réseaux. Vous devez augmenter ou diminuer le nombre de ports manuellement en fonction de vos besoins en déploiement.

REMARQUE L'augmentation du nombre de ports d'un commutateur conduit à réserver et consommer plus de ressources sur l'hôte. Si certains ports ne sont pas occupés, les ressources hôtes qui pourraient être nécessaires pour d'autres opérations sont verrouillées et inutilisées.

Pour garantir une utilisation efficace des ressources hôtes sur les hôtes exécutant ESXi 5.5, les ports des commutateurs virtuels évoluent dynamiquement. 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.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la table et cliquez sur **Modifier les paramètres**.
- 4 Dans la section **Propriétés**, définissez le **Nombre de ports** du commutateur standard à l'aide du menu déroulant.
- 5 (Facultatif) Modifiez la valeur **MTU (octets)** du commutateur standard.

Vous pouvez activer les trames Jumbo en définissant la valeur **MTU (octets)** sur un nombre supérieur à 1 500. La taille de l'unité MTU ne doit pas être supérieure à 9 000 octets.
- 6 Cliquez sur **OK**.

Modifier la vitesse d'un adaptateur physique dans Client Web vSphere

Un adaptateur physique peut devenir un goulot d'étranglement pour le trafic réseau si la vitesse de l'adaptateur ne correspond pas aux exigences de l'application. Vous pouvez modifier la vitesse et le duplex de la connexion d'un adaptateur physique pour transférer des données selon le débit du trafic.

Procédure

- 1 Accédez à un hôte dans le navigateur Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Adaptateurs physiques** dans **Mise en réseau**.

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 **Modifier**.

- 4 Sélectionnez la vitesse et le mode duplex de l'adaptateur réseau physique dans le menu déroulant.
- 5 (Facultatif) Si l'adaptateur réseau physique prend en charge SR-IOV, activez-le et configurez le nombre de fonctions virtuelles à utiliser pour la mise en réseau des machines virtuelles.
- 6 Cliquez sur **OK**.

Ajouter et associer les adaptateurs physiques d'un commutateur standard dans Client Web 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 devez associer plusieurs adaptateurs physiques à un seul commutateur vSphere standard.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard auquel vous souhaitez ajouter un adaptateur physique.
- 4 Cliquez sur **Gérer les adaptateurs réseau physiques**.
- 5 Cliquez sur **Ajouter des adaptateurs**.
- 6 Sélectionnez un ou plusieurs adaptateurs physiques dans la liste et sélectionnez le **Groupe d'ordre de basculement** auquel vous souhaitez affecter les adaptateurs, puis cliquez sur **OK**.
Les adaptateurs sélectionnés s'affichent dans la liste du groupe de basculement située sous la liste Adaptateurs affectés.
- 7 (Facultatif) Utilisez les flèches haut et bas pour changer la position d'un adaptateur dans les groupes de basculement.
- 8 Cliquez sur **OK** pour appliquer la configuration des adaptateurs physiques.

Afficher le diagramme de la topologie d'un commutateur standard vSphere dans Client Web 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 Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur standard dans la liste.

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

Configuration des communications réseau avec des vSphere Distributed Switches

3

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

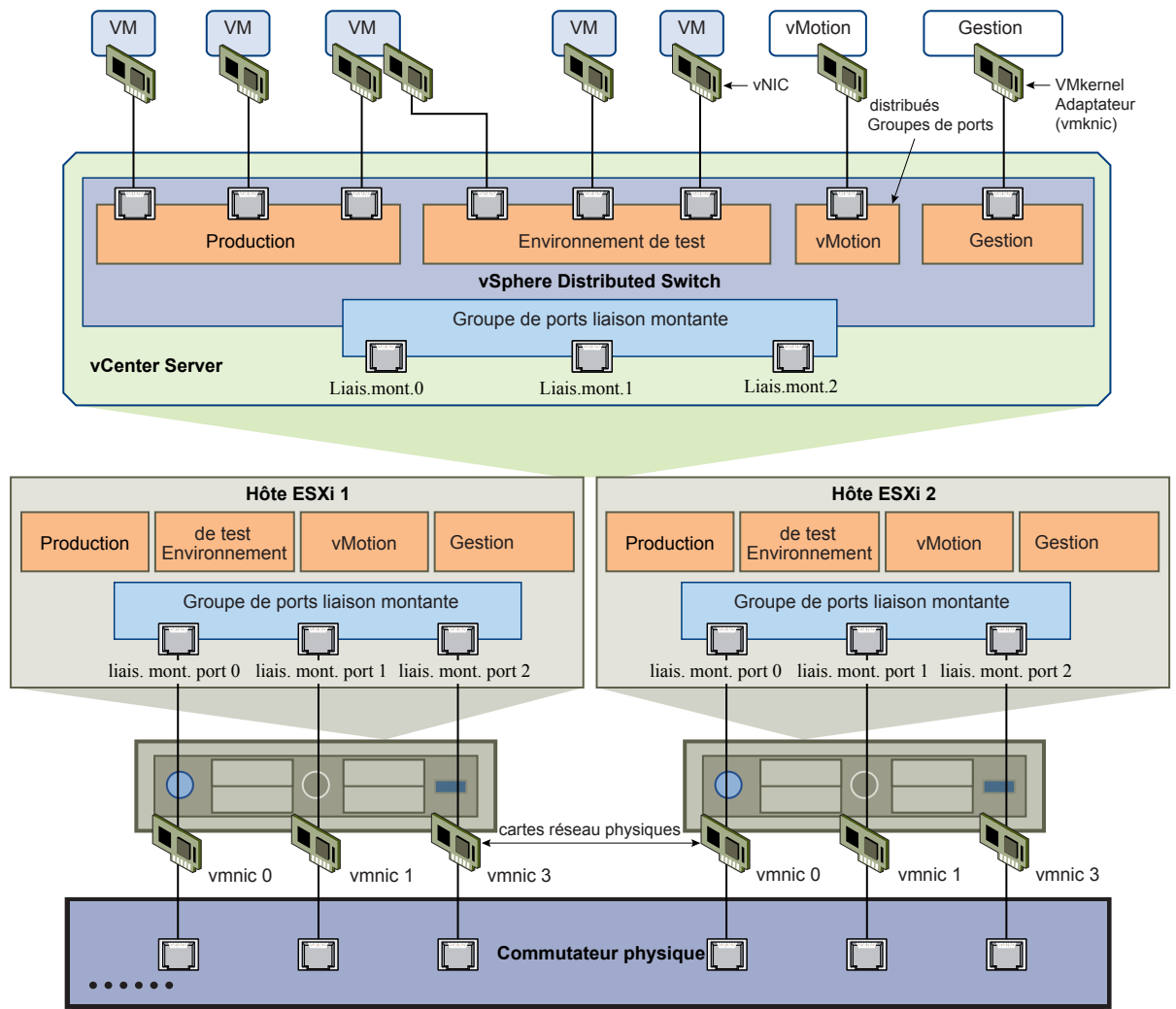
Ce chapitre aborde les rubriques suivantes :

- [« Architecture de vSphere Distributed Switch », page 24](#)
- [« Créer un vSphere Distributed Switch avec Client Web vSphere », page 25](#)
- [« Mettre à niveau un vSphere Distributed Switch vers une version ultérieure avec Client Web vSphere », page 27](#)
- [« Modifier les paramètres généraux et avancés dans vSphere Distributed Switch avec Client Web vSphere », page 28](#)
- [« Gestion de la mise en réseau sur plusieurs hôtes sur un vSphere Distributed Switch », page 29](#)
- [« Gestion de la mise en réseau sur des commutateurs proxy hôtes », page 39](#)
- [« Groupes de ports distribués », page 43](#)
- [« Utilisation des ports distribués », page 50](#)
- [« Configurer les communications réseau virtuelles sur un vSphere Distributed Switch », page 51](#)
- [« Diagrammes de la topologie d'un vSphere Distributed Switch dans Client Web vSphere », page 52](#)
- [« Contrôle de l'intégrité d'un vSphere Distributed Switch », page 55](#)
- [« Exporter, importer et restaurer des configurations de commutateurs distribués », page 56](#)
- [« VLAN privés », page 59](#)
- [« Prise en charge de LACP sur vSphere Distributed Switch », page 61](#)

Architecture de vSphere Distributed Switch

Un vSphere Distributed Switch fournit une gestion centralisée et une surveillance de la configuration de la mise en réseau de tous les hôtes associés au commutateur. Lorsque vous configurez un commutateur distribué sur le système vCenter Server, les paramètres que vous définissez sont propagés sur tous les hôtes associés au commutateur.

Figure 3-1. Architecture de vSphere Distributed Switch



L'association d'un vSphere Distributed Switch à un centre de données s'effectue dans un système vCenter Server. La configuration et la gestion de la mise en réseau de tous les hôtes associés au commutateur sont centralisées sur le système vCenter Server. Chaque hôte associé dispose d'un commutateur proxy hôte qui contient les paramètres de mise en réseau de l'hôte, configurés sur le commutateur distribué.

Par exemple, supposons que vous associez les hôtes ESXi A et ESXi B à un commutateur distribué et que vous connectez la carte réseau physique vmnic1 des deux hôtes à la liaison montante 1 sur le commutateur. En conséquence, la vmnic1 des hôtes ESXi A et ESXi B est connectée à la liaison montante 1 sur le commutateur distribué. Sur les commutateurs proxy hôtes des deux hôtes, la carte réseau physique vmnic1 est connectée au port de liaison montante 1.

Un commutateur distribué possède un ou plusieurs groupes de ports distribués. Ces groupes de ports distribués fournissent la connectivité de mise en réseau aux machines virtuelles et gèrent le trafic VMkernel. Chaque groupe de ports distribués est identifié à l'aide d'une étiquette de réseau qui doit être unique dans le centre de données actuel. Un exemplaire de chaque groupe de ports distribués créé est également disponible sur tous les commutateurs proxy hôtes et tous les hôtes associés au commutateur distribué. Les stratégies configurées sur un groupe de ports distribués sont homogènes sur l'ensemble des hôtes associés au commutateur distribué.

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.

Outre les vSphere Distributed Switches, vSphere 5 prend également en charge des commutateurs virtuels tiers. Pour plus d'informations sur la configuration du commutateur Cisco Nexus 1000v, consultez le site Web de Cisco Systems.

Créer un vSphere Distributed Switch avec Client Web vSphere

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 Client Web vSphere, accédez à un centre de données.
- 2 Dans le navigateur, cliquez avec le bouton droit sur le centre de données et sélectionnez **Nouveau commutateur distribué**.
- 3 Dans le champ **Nom et emplacement**, tapez un nom pour le nouveau commutateur distribué, ou acceptez le nom généré, puis cliquez sur **Suivant**.
- 4 Dans **Sélectionner une version**, sélectionnez une version de commutateur distribué et cliquez sur **Suivant**.

Option	Description
Distributed Switch : 5.5.0	Compatible avec ESXi 5.5 et versions ultérieures.
Distributed Switch : 5.1.0	Compatible avec VMware ESXi 5.1 et versions ultérieures. Les fonctions commercialisées dans les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 5.0.0	Compatible avec VMware ESXi 5.0 et versions ultérieures. Les fonctions commercialisées dans les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 4.1.0	Compatible avec ESX/ESXi version 4.1 et ultérieures. Les fonctions commercialisées dans les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.
Distributed Switch : 4.0.0	Compatible avec ESX/ESXi version 4.0 et ultérieures. Les fonctions commercialisées dans les versions ultérieures de vSphere Distributed Switch ne sont pas prises en charge.

- 5 Dans **Modifier les paramètres**, configurez les paramètres du commutateur distribué.
 - a 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.
 - b 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.
 - c 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.
 - d (Facultatif) Pour créer un groupe de ports distribués par défaut, tapez le nom du groupe de ports dans **Nom du 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.
 - e Cliquez sur **Suivant**.
- 6 Dans **Prêt à terminer**, vérifiez les paramètres que vous avez sélectionnés et cliquez sur **Terminer**.
 Utilisez le bouton **Précédent** pour modifier des paramètres.

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

Suivant

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

Mettre à niveau un vSphere Distributed Switch vers une version ultérieure avec Client Web vSphere

Vous pouvez mettre à niveau la version 4.0, 4.1, 5.0 ou 5.1 de vSphere Distributed Switch 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 est une opération qui n'entraîne pas d'interruption, c'est à dire que les hôtes et les machines virtuelles attachées au commutateur ne présenteront pas d'interruption.

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

Vous pouvez exporter la configuration du commutateur avant de mettre à niveau vCenter Server si vous effectuez une mise à niveau à partir de vCenter Server 5.1. Si vous mettez à niveau vCenter Server à partir d'une version antérieure à 5.1, sauvegardez la configuration du commutateur après la mise à niveau de vCenter Server vers la version 5.5.

Si la mise à niveau échoue, pour recréer le commutateur avec ses groupes de ports et les hôtes connectés, vous pouvez importer le fichier de configuration du commutateur en sélectionnant l'option **Conserver les identifiants d'origine du commutateur distribué et de tous les groupes de ports** dans l'assistant Importer un commutateur distribué.

Reportez-vous à la section « [Exporter les configurations de groupe de ports distribués avec Client Web vSphere](#) », page 57 et « [Importer un vSphere Distributed Switch à l'aide de Client Web vSphere](#) », page 57.

Prérequis

- Mettez à niveau vCenter Server vers la version 5.5.
- Mettez à niveau tous les hôtes connectés au commutateur distribué vers ESXi 5.5.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué et sélectionnez **Mettre à niveau un 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
Version 5.5.0	Compatible avec ESXi version 5.5 et versions ultérieures.
Version 5.1.0	Compatible avec ESXi version 5.1 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de commutateur distribué vSphere ne sont pas prises en charge.
Version 5.0.0	Compatible avec ESXi version 5.0 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de commutateur distribué vSphere ne sont pas prises en charge.
Version 4.1.0	Compatible avec ESX/ESXi version 4.1 et versions ultérieures. Les fonctions publiées avec les versions ultérieures de commutateur distribué vSphere ne sont pas prises en charge.

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

Certaines instances de VMware ESX en cours d'exécution sur le commutateur distribué peuvent être incompatibles avec la version de mise à niveau sélectionnée. Mettez à niveau ou supprimez les hôtes incompatibles, ou sélectionnez une autre version de mise à niveau pour le commutateur distribué.

- 5 Passez vos paramètres en revue et cliquez sur **Terminer**.

Une fois un vSphere Distributed Switch mis à niveau, vous ne pouvez pas le restaurer à une version antérieure. Vous ne pouvez pas ajouter des hôtes VMware ESX qui exécutent une version antérieure incompatible avec la nouvelle version du commutateur.

Modifier les paramètres généraux et avancés dans vSphere Distributed Switch avec Client Web vSphere

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 Client Web vSphere, accédez au commutateur distribué.
- 2 Cliquez sur l'onglet **Gérer**, cliquez sur **Paramètres**, puis sélectionnez **Propriétés**.
- 3 Cliquez sur **Éditer**.
- 4 Cliquez sur **Général** pour modifier les paramètres de vSphere Distributed Switch.

Option	Description
Nom	Entrez le nom du commutateur distribué.
Nombre de liaisons montantes	Sélectionnez le nombre de ports de liaison montante du commutateur distribué. Cliquez sur Modifier les noms de liaison montante pour changer les noms des liaisons montantes.
Nombre de ports	Le nombre de ports pour ce commutateur distribué. Ceci ne peut pas être édité.
Network I/O Control	Utilisez le menu déroulant pour activer ou désactiver Network I/O Control.
Description	Ajouter ou modifier 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.
Discovery Protocol	<ol style="list-style-type: none"> a Sélectionnez le protocole CDP (Cisco Discovery Protocol), Link Layer Discovery Protocol, désactivé à partir du menu déroulant Type b Assignez Opération les valeurs Écoute, Annoncer, ou les deux. Pour plus d'informations sur les Protocoles de Découverte, consultez « Switch Discovery Protocol » , page 174 .
Contacteur l'administrateur	Tapez le nom et autres détails de l'administrateur pour le commutateur distribué.

- 6 Cliquez sur **OK**.

Gestion de 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](#) page 30
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.
- [Ajouter des hôtes à un vSphere Distributed Switch avec Client Web vSphere](#) page 31
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 dans Client Web vSphere](#) page 33
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 dans Client Web vSphere](#) page 34
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 sur un vSphere Distributed Switch dans Client Web vSphere](#) page 34
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 Virtual SAN. Vous pouvez créer des adaptateurs VMkernel sur plusieurs hôtes simultanément en utilisant l'assistant Ajouter et gérer des hôtes.
- [Migrer la mise en réseau de machines virtuelles vers le vSphere Distributed Switch dans Client Web vSphere](#) page 36
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.
- [Mettre à jour le nombre maximal de ports distribués autorisés sur les hôtes dans Client Web vSphere](#) page 37
Si un hôte exécute ESXi 5.1 ou une version antérieure, vous pouvez modifier le nombre maximal de ports distribués autorisés sur le commutateur de proxy de l'hôte.
- [Utiliser un hôte comme un modèle pour créer une configuration de la mise en réseau uniforme sur un vSphere Distributed Switch dans Client Web vSphere](#) page 37
Si vous prévoyez d'avoir des hôtes dont la configuration de mise en réseau est uniforme, vous pouvez sélectionner un hôte comme modèle et appliquer sa configuration de cartes réseau physiques et d'adaptateurs VMkernel à tous les autres hôtes sur le commutateur distribué.

- [Supprimer des hôtes d'un vSphere Distributed Switch avec Client Web vSphere](#) page 38
Supprimez des hôtes d'un vSphere Distributed Switch si vous avez configuré un commutateur différent pour les 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 dans Client Web vSphere 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 commutateur distribué sont associés à d'autres commutateurs dans votre centre de données, vous pouvez migrer les adaptateurs réseau vers le commutateur distribué 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.

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 avec Client Web vSphere

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.

Prérequis

- 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 Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Ajouter des hôtes**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Nouveaux hôtes**, sélectionnez des hôtes dans votre centre de données, puis cliquez sur **OK**.
- 5 Sélectionnez les tâches de configuration des adaptateurs réseau dans le commutateur distribué et cliquez sur **Suivant**.

- 6 Configurez les cartes réseau physiques sur le commutateur distribué.
 - a Dans la liste Sur d'autres commutateurs/non réclamés, sélectionnez une carte réseau physique.
Si vous sélectionnez des cartes réseau physiques qui sont déjà connectés à d'autres commutateurs, elles migrent vers le commutateur distribué actuel.
 - b Cliquez sur **Attribuer une liaison montante**.
 - c Sélectionnez une liaison montante et cliquez sur **OK**.

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.
- 7 Cliquez sur **Suivant**.
- 8 Configurez les adaptateurs VMkernel.
 - a Sélectionnez un adaptateur VMkernel, puis cliquez sur **Assigner un groupe de ports**.
 - b Sélectionnez un groupe de ports distribués et cliquez sur **OK**.
- 9 Vérifiez les services affectés, ainsi que le niveau d'impact.

Option	Description
Aucun impact	Le service continue de fonctionner normalement une fois la nouvelle configuration de mise en réseau appliquée.
Impact important	Le fonctionnement du service peut être affecté si la nouvelle configuration de mise en réseau est appliquée.
Impact critique	Le fonctionnement du service est interrompu si la nouvelle configuration de la mise en réseau est appliquée.

- a Si l'impact sur le fonctionnement d'un service est important ou critique, cliquez sur le service et vérifiez les raisons affichées dans le volet Détails de l'analyse.
 - b Une fois que vous avez résolu les problèmes d'impact sur l'ensemble des services dépendants, appliquez votre configuration de la mise en réseau.
- 10 Cliquez sur **Suivant**.
- 11 Configurez la mise en réseau de la machine virtuelle.
 - a Pour connecter tous les adaptateurs réseau d'une machine virtuelle à un groupe de ports distribués, sélectionnez la machine virtuelle, ou sélectionnez un adaptateur réseau individuel pour connecter uniquement cet adaptateur.
 - b Cliquez sur **Assigner un groupe de ports**.
 - c Sélectionnez un groupe de ports distribués dans la liste et cliquez sur **OK**.
- 12 Cliquez sur **Suivant**, puis sur **Terminer**.

Suivant

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

Configurer des adaptateurs réseau physiques sur un vSphere Distributed Switch dans Client Web vSphere

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 Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Hôtes attachés**, puis sélectionnez un hôte dans la liste des hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sélectionnez **Gérer adaptateurs physiques** puis cliquez sur **Suivant**.
- 7 Dans la liste **Sur d'autres commutateurs/non réclamés**, sélectionnez une carte réseau physique.
Si vous sélectionnez des cartes réseau physiques déjà attribuées à d'autres commutateurs, celles-ci sont migrées vers le commutateur distribué actuel.
- 8 Cliquez sur **Attribuer une liaison montante**.
- 9 Sélectionnez une liaison montante ou sélectionnez **Assignation automatique**.
- 10 Cliquez sur **Suivant**.
- 11 Vérifiez les services affectés, ainsi que le niveau d'impact.

Option	Description
Aucun impact	Le service continue de fonctionner normalement une fois la nouvelle configuration de mise en réseau appliquée.
Impact important	Le fonctionnement du service peut être affecté si la nouvelle configuration de mise en réseau est appliquée.
Impact critique	Le fonctionnement du service est interrompu si la nouvelle configuration de la mise en réseau est appliquée.

- a Si l'impact sur le fonctionnement d'un service est important ou critique, cliquez sur le service et vérifiez les raisons affichées dans le volet **Détails** de l'analyse.
 - b Une fois que vous avez résolu les problèmes d'impact sur l'ensemble des services dépendants, appliquez votre configuration de la mise en réseau.
- 12 Cliquez sur **Suivant**, puis sur **Terminer**.

Migrer des adaptateurs VMkernel vers un vSphere Distributed Switch dans Client Web vSphere

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 Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Hôtes attachés**, puis sélectionnez un hôte dans la liste des hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sélectionnez **Gérer les adaptateurs VMkernel**, puis cliquez sur **Suivant**.
- 7 Sélectionnez l'adaptateur et cliquez sur **Affecter un groupe de ports**.
- 8 Sélectionnez un groupe de ports distribués et cliquez sur **OK**.
- 9 Cliquez sur **Suivant**.
- 10 Vérifiez les services affectés, ainsi que le niveau d'impact.

Option	Description
Aucun impact	Le service continue de fonctionner normalement une fois la nouvelle configuration de mise en réseau appliquée.
Impact important	Le fonctionnement du service peut être affecté si la nouvelle configuration de mise en réseau est appliquée.
Impact critique	Le fonctionnement du service est interrompu si la nouvelle configuration de la mise en réseau est appliquée.

- a Si l'impact sur le fonctionnement d'un service est important ou critique, cliquez sur le service et vérifiez les raisons affichées dans le volet Détails de l'analyse.
 - b Une fois que vous avez résolu les problèmes d'impact sur l'ensemble des services dépendants, appliquez votre configuration de la mise en réseau.
- 11 Cliquez sur **Suivant**, puis sur **Terminer**.

Créer un adaptateur VMkernel sur un vSphere Distributed Switch dans Client Web vSphere

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 Virtual SAN. Vous pouvez créer des adaptateurs VMkernel sur plusieurs hôtes simultanément en utilisant l'assistant Ajouter et gérer des hôtes.

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 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.

- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Hôtes attachés**, puis sélectionnez un hôte dans la liste des hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sélectionnez **Gérer les adaptateurs VMkernel**, puis cliquez sur **Suivant**.
- 7 Cliquez sur **Nouvel adaptateur**.
L'assistant Ajouter une mise en réseau s'ouvre.
- 8 Sur la page Sélectionner un périphérique cible de l'assistant Ajouter une mise en réseau, sélectionnez un groupe de ports distribués.
- 9 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. REMARQUE L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.
Pile TCP/IP	Si des piles personnalisées sont disponibles, sélectionnez-en une dans la liste.
Activer les services	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 : <ul style="list-style-type: none"> ■ Trafic vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Vous pouvez activer cette propriété pour un seul adaptateur VMkernel vMotion et de stockage IP par hôte. Si cette propriété n'est activée pour aucun adaptateur VMkernel, la migration avec vMotion vers l'hôte sélectionné n'est pas possible. ■ Trafic Fault Tolerance. Active la journalisation de Fault Tolerance sur l'hôte. ■ Trafic de 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. ■ Virtual SAN. Active le trafic de Virtual SAN sur l'hôte. Chaque hôte faisant partie d'un cluster de Virtual SAN doit disposer de ce type d'adaptateur VMkernel.

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

Option	Description
Obtenir automatiquement les paramètres IP	Utilisez DHCP pour obtenir les paramètres IP.
Utiliser des paramètres IP 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.

- 11 (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.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Adresses IPv6 statiques	<ol style="list-style-type: none"> a Cliquez sur Ajouter pour ajouter une nouvelle adresse IPv6. b Tapez 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 Modifier.

- 12 Vérifiez vos sélections dans la page Prêt à terminer et cliquez sur **Terminer**.
- 13 Suivre les commandes pour achever l'assistant intelligent.

Migrer la mise en réseau de machines virtuelles vers le vSphere Distributed Switch dans Client Web vSphere

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.

Prérequis

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 Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Hôtes attachés**, puis sélectionnez un hôte dans la liste des hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sélectionnez **Migrer la mise en réseau de machines virtuelles**, puis cliquez sur **Suivant**.
- 7 Configurez les adaptateurs réseau des machines virtuelles sur le commutateur distribué.
 - a Pour connecter tous les adaptateurs réseau d'une machine virtuelle à un groupe de ports distribués, sélectionnez la machine virtuelle, ou sélectionnez un adaptateur réseau individuel pour connecter uniquement cet adaptateur.
 - b Cliquez sur **Assigner un groupe de ports**.
 - c Sélectionnez un groupe de ports distribués dans la liste et cliquez sur **OK**.
- 8 Cliquez sur **Suivant**, puis sur **Terminer**.

Mettre à jour le nombre maximal de ports distribués autorisés sur les hôtes dans Client Web vSphere

Si un hôte exécute ESXi 5.1 ou une version antérieure, vous pouvez modifier le nombre maximal de ports distribués autorisés sur le commutateur de proxy de l'hôte.

Chaque commutateur proxy présent sur les hôtes ESXi 5.1 (et versions antérieures) fournit un nombre déterminé de ports au travers desquels les machines virtuelles et les services réseau peuvent atteindre un ou plusieurs réseaux. Vous devez diminuer ou augmenter manuellement le nombre de ports en fonction de vos besoins en déploiement.

REMARQUE L'augmentation du nombre de ports distribués sur les commutateurs proxy des hôtes entraîne la réservation et la consommation d'un plus grand nombre de ressources sur les hôtes. Si certains ports ne sont pas occupés, les ressources hôtes qui pourraient être nécessaires pour d'autres opérations sont verrouillées et inutilisées.

Pour optimiser l'utilisation des ressources de l'hôte, le nombre de ports distribués des commutateurs proxy évolue de manière dynamique pour les hôtes ESXi 5.5. 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.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Gérer la mise en réseau de l'hôte**, puis cliquez sur **Suivant**.
- 4 Cliquez sur **Hôtes attachés**, puis sélectionnez un hôte dans la liste des hôtes associés au commutateur distribué.
- 5 Cliquez sur **Suivant**.
- 6 Sélectionnez un hôte et cliquez sur **Modifier les paramètres**.
- 7 Modifiez le nombre maximal de ports distribués autorisés sur l'hôte et cliquez sur **OK**.
- 8 Cliquez sur **Suivant**, puis sur **Terminer**.

Utiliser un hôte comme un modèle pour créer une configuration de la mise en réseau uniforme sur un vSphere Distributed Switch dans Client Web vSphere

Si vous prévoyez d'avoir des hôtes dont la configuration de mise en réseau est uniforme, vous pouvez sélectionner un hôte comme modèle et appliquer sa configuration de cartes réseau physiques et d'adaptateurs VMkernel à tous les autres hôtes sur le commutateur distribué.

Procédure

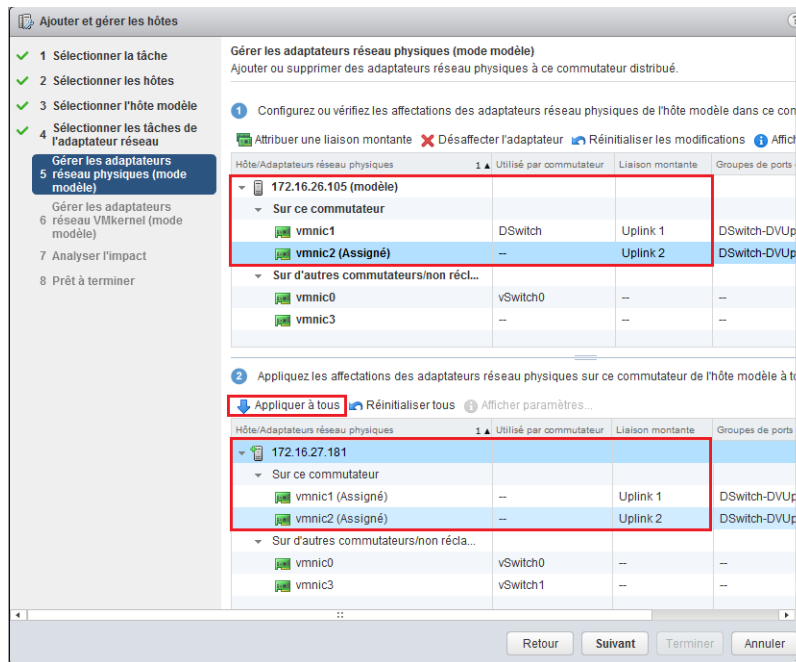
- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez une tâche pour gérer la mise en réseau d'hôtes et cliquez sur **Suivant**.
- 4 Sélectionnez les hôtes à ajouter ou à gérer sur le commutateur distribué.
- 5 En bas de la boîte de dialogue, sélectionnez **Configurer des paramètres réseau identiques sur plusieurs hôtes**, puis cliquez sur **Suivant**.
- 6 Sélectionnez un hôte à utiliser comme modèle, puis cliquez sur **Suivant**.
- 7 Sélectionnez les tâches de l'adaptateur réseau et cliquez sur **Suivant**.

- 8 Dans les pages Gérer les adaptateurs réseau physiques et Gérer les adaptateurs réseau VMkernel, effectuez les modifications de configuration souhaitées sur le modèle d'hôte, puis cliquez sur **Appliquer à tous** pour tous les autres hôtes.
- 9 Sur la page Prêt à terminer, cliquez sur **Terminer**.

Exemple : Configurer des cartes réseau physiques à l'aide d'un hôte modèle

Connectez simultanément les cartes réseau physiques de deux hôtes à un vSphere Distributed Switch en utilisant le mode hôte modèle dans l'assistant Ajouter et gérer des hôtes. Dans la page Gérer les adaptateurs réseau physiques de l'assistant, attribuez deux cartes réseau physiques aux liaisons montantes sur l'hôte modèle, puis cliquez sur **Appliquer à tous** pour créer la même configuration sur l'autre hôte.

Figure 3-2. Application de la configuration de cartes réseau physiques sur un vSphere Distributed Switch en utilisant un hôte modèle



Supprimer des hôtes d'un vSphere Distributed Switch avec Client Web vSphere

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

Prérequis

- 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 « [Tâches de gestion de la mise en réseau d'hôte sur un vSphere Distributed Switch](#) », page 30

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Ajouter et gérer les hôtes**.
- 3 Sélectionnez **Supprimer les hôtes** et cliquez sur **Suivant**.

- 4 Sélectionnez les hôtes que vous souhaitez supprimer et cliquez sur **Suivant**.
- 5 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 sur un vSphere Distributed Switch dans Client Web vSphere](#) », page 34.

Migrer les adaptateurs réseau d'un hôte vers un vSphere Distributed Switch dans Client Web vSphere

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.

Si vous souhaitez migrer des adaptateurs VMkernel ou des adaptateurs réseau de machines virtuelles, veillez à ce qu'au moins une liaison montante soit active pour les groupes de ports distribués de destination et que cette liaison montante soit connectée à une carte réseau physique sur l'hôte. Sinon, migrez à la fois les cartes réseau physiques, les adaptateurs réseau virtuels et les adaptateurs VMkernel.

Si vous souhaitez 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 VLAN sur le commutateur standard seront connectées entre elles mais pas au réseau externe.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur distribué de destination, puis cliquez sur **Migrer des adaptateurs réseau physiques ou virtuels**.
- 4 Sélectionnez les tâches de migration des adaptateurs réseau et cliquez sur **Suivant**.
- 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 Vérifiez les services affectés par la nouvelle configuration de mise en réseau.
 - a Si l'impact sur le fonctionnement d'un service est important ou alarmant, cliquez sur le service et vérifiez les détails de l'analyse.

Par exemple, une mauvaise configuration d'association et de basculement dans le groupe de ports distribués sur lequel vous migrez l'adaptateur VMkernel iSCSI peut avoir un impact important sur le protocole iSCSI. Vous devez laisser une liaison montante active dans l'ordre d'association et de basculement du groupe de ports distribués, laisser la liste des éléments en veille vide et déplacer les autres liaisons montantes vers les éléments inutilisés.
 - b Après avoir résolu les éventuels problèmes rencontrés dans les services affectés par la configuration, cliquez sur **Suivant**.
- 8 Configurez les adaptateurs réseau des machines virtuelles.
 - a 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.
 - b Sélectionnez un groupe de ports distribués dans la liste et cliquez sur **OK**.
 - c Cliquez sur **Suivant**.
- 9 Dans la page Prêt à terminer, vérifiez la nouvelle configuration de mise en réseau et cliquez sur **Terminer**.

Migrer l'adaptateur VMkernel d'un hôte vers un commutateur vSphere standard dans Client Web vSphere

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 sur un vSphere Distributed Switch dans Client Web vSphere](#) », page 34

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis 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 un adaptateur réseau VMkernel, sélectionnez l'adaptateur réseau virtuel à migrer vers le commutateur standard de la liste.
- 6 Dans la page Configurer les paramètres, modifiez les valeurs **Étiquette réseau** et **ID VLAN** pour l'adaptateur réseau.
- 7 Vérifiez les informations de migration dans la page Prêt à terminer, puis cliquez sur **Terminer**.
Cliquez sur **Précédent** pour changer des paramètres.

Attribuer une carte réseau physique à un vSphere Distributed Switch dans Client Web vSphere

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

Supprimer une carte réseau physique de vSphere Distributed Switch dans Client Web vSphere

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

Procédure

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

Suivant

Lorsque vous retirez des cartes réseau physiques d'une machine virtuelle active, il peut arriver que les cartes figurent toujours dans Client Web vSphere. Reportez-vous à la section « [Suppression des cartes réseau des machines virtuelles actives](#) », page 42.

Définir le nombre de ports d'un commutateur de proxy hôte dans Client Web vSphere

Vous pouvez augmenter ou diminuer le nombre maximal de ports distribués disponibles sur le commutateur de proxy des hôtes ESXi 5.1 et versions antérieures qui sont connectés à un vSphere Distributed Switch.

Chaque commutateur de proxy sur les hôtes qui exécutent ESXi 5.1 et versions antérieures fournit un nombre défini de ports à travers lesquels les machines virtuelles et les services réseau peuvent accéder à un ou plusieurs réseaux. Vous devez augmenter ou diminuer le nombre de ports manuellement en fonction de vos besoins en déploiement.

REMARQUE L'augmentation du nombre de ports distribués sur les commutateurs proxy des hôtes entraîne la réservation et la consommation d'un plus grand nombre de ressources sur les hôtes. Si certains ports ne sont pas occupés, les ressources hôtes qui pourraient être nécessaires pour d'autres opérations sont verrouillées et inutilisées.

Pour garantir une utilisation efficace des ressources hôtes, le nombre de ports distribués des commutateurs de proxy augmente et diminue dynamiquement sur les hôtes ESXi 5.5. 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.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur distribué dans la liste.
- 4 Cliquez sur **Mettre à jour le nombre maximum de ports distribués sur cet hôte**.
- 5 Utilisez les flèches haut et bas pour définir le nombre maximal de ports de l'hôte et cliquez sur **OK**.

Suivant

Si vous changez le nombre maximum de ports pour un hôte après avoir ajouté l'hôte au commutateur distribué, vous devez redémarrer l'hôte pour que le nouveau maximum soit appliqué.

Suppression des cartes réseau des machines virtuelles actives

Lorsque vous supprimez des cartes réseau d'une machine virtuelle active, il peut arriver qu'elles figurent toujours dans Client Web vSphere.

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.

Client Web vSphere 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 Client Web vSphere. 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 toujours 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 dans Client Web vSphere

Ajoutez un groupe de ports distribués à un vSphere Distributed Switch pour créer un réseau de commutation distribué pour les machines virtuelles et pour y associer des adaptateurs VMkernel.

Procédure

- 1 Accédez à un commutateur distribué dans le Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué dans le navigateur et sélectionnez **Nouveau groupe de ports distribués**.
- 3 Dans la section **Sélectionner un nom et un emplacement**, tapez le nom du nouveau groupe de ports distribués ou acceptez le nom généré puis cliquez sur **Suivant**.
- 4 Dans la section **Configuration des paramètres**, établissez les propriétés générales pour le nouveau groupe de ports distribués et cliquez sur **Suivant**.

Paramètre	Description
Liaison de port	<p>Choisissez quand les ports sont affectés aux machines virtuelles connectées au groupe de ports distribués.</p> <ul style="list-style-type: none"> ■ Liaison statique : Attribuez un port à une machine virtuelle quand celle-ci se connecte au groupe de ports distribués. ■ Liaison dynamique : Assignez un port à une machine virtuelle lorsque celle-ci se met sous tension pour la première fois ou après qu'elle soit connectée au groupe de ports distribués. La liaison dynamique est obsolète depuis ESXi 5.0. ■ Éphémère : Aucune liaison du 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 huit. Lorsque tous les ports sont affectés, une nouvelle série de huit ports est créé. il s'agit de la configuration par défaut. ■ Fixe : Le nombre de ports par défaut est huit. Aucun port supplémentaire n'est créé lorsque tous les ports sont affectés.
Nombre de ports	Entrez le nombre de ports dans le groupe de ports distribués.
pool de ressources réseau	Utilisez le menu déroulant pour affecter le nouveau groupe de ports distribués à un pool de ressources réseau défini par l'utilisateur. Si vous n'avez pas créé de pool de ressources réseau, ce menu reste vide.
VLAN	<p>Utilisez le menu déroulant Type pour sélectionner les options VLAN :</p> <ul style="list-style-type: none"> ■ 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. ■ VLAN Privé : Sélectionnez une entrée de VLAN privé. Si vous n'avez pas créé de réseaux VLAN privés, ce menu est vide.
Mise en réseau	Cochez cette case pour personnaliser les configurations des stratégies du nouveau groupe de ports distribués.

- 5 (Facultatif) Dans la section **Sécurité**, modifiez les exceptions de sécurité et cliquez sur **Suivant**.

Configuration	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	<ul style="list-style-type: none"> ■ Rejeter. Si vous définissez cette option 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>.vmx</code>, 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 tout trame sortante dont l'adresse MAC source est différente de celle indiquée dans le fichier de configuration <code>.vmx</code>. ■ Accepter. Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

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

Configuration	Description
Statut	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 stratégie, les services bénéficient d'une connexion libre et claire au réseau physique par défaut.
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 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 ainsi transférés à une vitesse plus élevée.

- 7 (Facultatif) Dans la section **Association et basculement**, modifiez les paramètres et cliquez sur **Suivant**.

Configuration	Description
Équilibrage de charge	<p>Spécifiez 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. <p>REMARQUE L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, désactivez etherchannel.</p>
Détection de basculement de 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 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 adaptateurs réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. <p>REMARQUE Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.</p>
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>REMARQUE 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>

Configuration	Description
Retour arrière	Sélectionnez Oui ou Non pour mettre hors tension ou activer le retour arrière. 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 emplacement 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.
Ordre de basculement	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 : <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 attente. Utilisez cette liaison montante si la connectivité de l'un des adaptateurs actif est indisponible. ■ Liaisons montantes inutilisées. N'utilisez pas cette liaison montante. REMARQUE En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.

- 8 (Facultatif) Dans la section de **Surveillance**, activez ou désactivez NetFlow et cliquez sur **Suivant**.

Configuration	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.

- 9 (Facultatif) Dans la section **Divers**, sélectionnez **Oui** ou **Non** et cliquez sur **Suivant**.
Sélectionner **Oui** arrête tous les ports dans le groupe de ports. Cette action risque de perturber les opérations normales du réseau des hôtes ou des VM qui utilisent les ports.
- 10 (Facultatif) Dans la section **Modifier des paramètres supplémentaires**, ajoutez une description du groupe de ports et définissez stratégies de remplacement par port et cliquez sur **Suivant**.
- 11 Vérifiez vos paramètres dans la section **Prêt à terminer** et cliquez sur **Terminer**.
Cliquez sur le bouton **Précédent** pour modifier des paramètres.

Modifier les paramètres généraux d'un groupe de ports distribués avec Client Web vSphere

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

- Recherchez un groupe de ports distribués dans Client Web vSphere.
 - Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - Cliquez sur **Groupe de ports distribués**.
- 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	<p>Choisissez quand les ports sont affectés aux machines virtuelles connectées au groupe de ports distribués.</p> <ul style="list-style-type: none"> ■ Liaison statique : Attribuez un port à une machine virtuelle quand celle-ci se connecte au groupe de ports distribués. ■ Liaison dynamique : Assignez un port à une machine virtuelle lorsque celle-ci se met sous tension pour la première fois ou après qu'elle soit connectée au groupe de ports distribués. La liaison dynamique est obsolète depuis ESXi 5.0. ■ Éphémère : Aucune liaison du port. Vous pouvez attribuer une machine virtuelle à un groupe de ports distribués avec 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 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 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**.

Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere

Vous pouvez modifier les paramètres avancés de groupe de ports distribués, tels que les paramètres de remplacement et la réinitialisation à la déconnexion.

Procédure

- Déterminez l'emplacement d'un groupe de ports distribués dans Client Web vSphere
 - Pour déterminer l'emplacement d'un groupe de ports distribués, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - Cliquez sur **Groupes de ports distribués** et sélectionnez un groupe de ports distribués de la liste.
- Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- Cliquez sur **Edit**.
- Sélectionnez la page **Avancé** pour modifier les paramètres de groupes de ports distribués.

Option	Description
Configurez la réinitialisation à la déconnexion	<p>Dans le menu déroulant, activez ou désactivez la réinitialisation à la déconnexion.</p> <p>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.</p>
Remplacer les règles de port	Sélectionnez les règles de groupes de ports distribués au niveau de chaque port à remplacer.

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

Supprimer un groupe de ports distribués dans Client Web vSphere

Supprimez un groupe de ports distribués lorsque vous n'avez plus besoin du réseau étiqueté correspondant pour fournir une connectivité aux machines virtuelles ou à la mise en réseau VMkernel.

Prérequis

- 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 Dans Client Web vSphere, accédez au groupe de ports distribués.
- 2 Dans le menu **Actions**, sélectionnez **Toutes les actions vCenter > Supprimer de l'inventaire**.

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 « [Exporter, importer et restaurer des configurations de commutateurs distribués](#) », page 56.

Exporter les configurations de groupe de ports distribués avec Client Web 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.

Cette fonctionnalité est disponible uniquement avec Client Web vSphere 5.1 ou ultérieure. Cependant, vous pouvez exporter les paramètres de n'importe quelle version d'un port distribué si vous utilisez Client Web vSphere 5.1 ou une version ultérieure.

Procédure

- 1 Déterminer l'emplacement d'un groupe de ports distribués dans Client Web vSphere
 - a Pour déterminer l'emplacement d'un groupe de ports distribués, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Cliquez sur **Groupes de ports distribués** et sélectionnez un groupe de ports distribués de la liste.
- 2 Cliquez avec le bouton droit de la souris dans le navigateur puis sélectionnez **Toutes les actions vCenter > Exporter une configuration**.
- 3 (Facultatif) Tapez des notes au sujet de cette configuration dans le champ **Descriptions**.
- 4 Cliquez sur **OK**.

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

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.

Suivant

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 avec Client Web vSphere](#) », page 49 .
- Pour remplacer les paramètres sur un groupe de ports distribués existant, consulter « [Restaurer une configuration de groupe de ports distribués vSphere avec Client Web vSphere](#) », page 49 .

Importer une configuration de groupe de ports distribués vSphere avec Client Web vSphere

Utilisez l'importation pour créer un groupe de ports distribués à partir d'un fichier de configuration. Tous les groupes de ports distribués sont convertis en conformité aux paramètres dans le fichier de configuration.

Cette fonctionnalité est disponible uniquement avec Client Web vSphere 5.1 ou version ultérieure. Cependant, vous pouvez exporter les paramètres de n'importe quelle version d'un port distribué si vous utilisez Client Web vSphere 5.1 ou une version ultérieure.

Procédure

- 1 Accédez à un commutateur distribué dans le Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris dans le navigateur puis sélectionnez **Toutes les actions vCenter > Importer un groupe de ports distribués**.
- 3 Accédez à l'emplacement de votre fichier de configuration sauvegardé et cliquez sur **Suivant**.

Vous pouvez utiliser un fichier de configuration d'un groupe de ports distribués, ou un fichier de configuration d'un commutateur distribué. Cependant, vous pouvez utiliser un fichier contenant à la fois les configurations du commutateur distribué et du groupe de ports distribués uniquement si ce fichier contient les paramètres d'un seul groupe de ports. Si plusieurs paramètres de groupe de ports sont sauvegardés dans le fichier de configuration du commutateur distribué, vous devez utiliser un autre fichier.

- 4 Vérifiez les paramètres d'importation avant de compléter l'importation.
- 5 Cliquez sur **Terminer**

Restaurer une configuration de groupe de ports distribués vSphere avec Client Web 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.

Cette fonctionnalité n'est disponible uniquement avec Client Web vSphere 5.1 ou ultérieure. Cependant, vous pouvez importer les paramètres de n'importe quelle version d'un commutateur distribué si vous utilisez Client Web vSphere 5.1 ou une version ultérieure.

Procédure

- 1 Déterminer l'emplacement d'un groupe de ports distribués dans Client Web vSphere
 - a Pour déterminer l'emplacement d'un groupe de ports distribués, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Cliquez sur **Groupes de ports distribués** et sélectionnez un groupe de ports distribués de la liste.

- 2 Cliquez avec le bouton droit sur le groupe de ports distribués dans le navigateur puis sélectionnez **Toutes les actions vCenter > Restaurer 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**.

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 d'un port distribué avec Client Web vSphere

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 Déterminer l'emplacement d'un groupe de ports distribués dans Client Web vSphere
 - a Pour déterminer l'emplacement d'un groupe de ports distribués, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Cliquez sur **Groupes de ports distribués** et sélectionnez un groupe de ports distribués de la liste.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Cliquez sur **Démarrer la surveillance de l'état du port**.

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.

Configurer les paramètres d'un port distribué avec Client Web vSphere

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

Procédure

- 1 Déterminez l'emplacement d'un groupe de ports distribués dans Client Web vSphere
 - a Pour déterminer l'emplacement d'un groupe de ports distribués, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Cliquez sur **Groupes de ports distribués** et sélectionnez un groupe de ports distribués de la liste.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port distribué du tableau.
Les informations sur le port distribué s'affichent au bas de l'écran.
- 4 Cliquez sur **Modifier les paramètres du port distribué**.
- 5 Sur la page **Propriétés** et les pages de règles, modifiez les informations du port distribué et cliquez sur **OK**.

Si les remplacements ne sont pas autorisés, les options de règles sont grisées.

Vous pouvez autoriser des remplacements au niveau du port en changeant les paramètres **Avancés** du groupe de ports distribués. Consultez « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Configurer les communications réseau 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 vSphere Distributed Switchs en connectant leurs adaptateurs réseau virtuelles à des 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 un vSphere Distributed Switch avec Client Web vSphere

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 Accédez à un centre de donnée dans le navigateur Client Web vSphere.
- 2 Cliquez avec le bouton droit sur le centre de données dans le navigateur et sélectionnez **Migrer la 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 Sélectionnez un réseau de destination. Cliquez sur **Parcourir** pour sélectionner un réseau de destination spécifique puis 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 à un groupe de ports distribués avec Client Web vSphere

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

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 3 Cliquez sur **Edit**.
- 4 Développez la section **Adaptateur réseau** et sélectionnez un groupe de ports distribués dans le menu déroulant.
- 5 Cliquez sur **OK**.

Diagrammes de la topologie d'un vSphere Distributed Switch dans Client Web vSphere

Les diagrammes de la topologie d'un vSphere Distributed Switch dans Client Web vSphere 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 virtuel et sur chaque hôte y participant.

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.

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 dans Client Web vSphere

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

Procédure

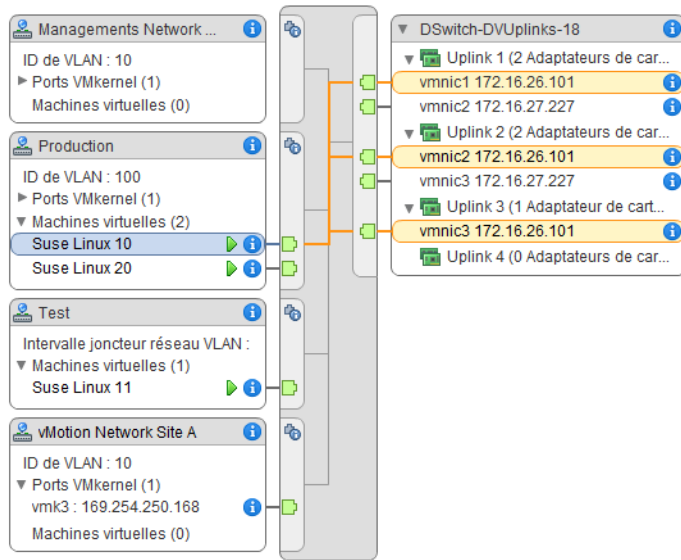
- 1 Accédez au vSphere Distributed Switch dans Client Web vSphere.
- 2 Dans l'onglet **Gérer**, cliquez sur **Paramètres** et sélectionnez **Topologie**.

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



Suivant

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](#) », page 13.

Afficher la topologie d'un commutateur de proxy hôte dans Client Web vSphere

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 Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez le commutateur distribué dans la liste.

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

Contrôle de l'intégrité d'un vSphere Distributed Switch

Le contrôle de l'intégrité de vSphere 5.1 Distributed Switch permet d'identifier et de corriger les erreurs de configuration de vSphere Distributed Switches.

Les erreurs suivantes sont des erreurs de configuration fréquentes que les contrôles d'intégrité aident à identifier.

- Jonctions VLAN non correspondantes entre un vSphere Distributed Switch et un commutateur physique.
- Paramètres MTU non correspondants entre des adaptateurs réseau physiques, des commutateurs distribués et des ports de commutateur physiques.
- Règles d'association de commutateur virtuel non correspondantes pour les paramètres du canal de port du commutateur physique.

Le contrôle d'intégrité effectue les vérifications suivantes :

- VLAN. Vérifie si les paramètres VLAN de vSphere Distributed Switch correspondent à la configuration du port trunk sur les ports de commutateur physiques adjacents.
- MTU. 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.
- Règles d'association. Vérifie si le paramètre EtherChannel des ports de commutateur d'accès physique correspond aux paramètres de la règle d'association IPHash du groupe de ports de commutateur distribué.

Le contrôle de l'intégrité est limité au port de commutateur d'accès auquel la liaison montante du commutateur distribué est connectée.

REMARQUE Pour ce qui est des vérifications VLAN et MTU, le commutateur distribué doit disposer d'au moins deux NIC montants physiques de liaison.

Pour effectuer le contrôle de l'intégrité d'association, vous devez disposer d'au moins deux NIC montants physiques de liaison et de deux hôtes lors de l'application de la règle.

Activer ou désactiver le contrôle de l'intégrité du vSphere Distributed Switch dans Client Web vSphere

Le contrôle d'intégrité effectue les vérifications pour les modifications des configurations de vSphere Distributed Switch. Vous devez activer le contrôle d'intégrité du vSphere Distributed Switch pour effectuer les vérifications des configurations du commutateur distribué.

Le contrôle d'intégrité est uniquement disponible pour les commutateurs distribués ESXi 5.1. Vous pouvez visualiser les informations sur le contrôle d'intégrité par le biais de Client Web vSphere 5.1 ou version ultérieure.

Procédure

- 1 Accédez à un vSphere Distributed Switch dans Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**.
- 3 Sélectionnez **Paramètres** et sélectionnez **Contrôle de l'intégrité**.
- 4 Pour activer ou désactiver le contrôle d'intégrité, cliquez sur **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 le commutateur ESXi et le commutateur physique utilisé dans la règle d'association.

- Cliquez sur **OK**.

Suivant

Lorsque vous modifiez la configuration d'un vSphere Distributed Switch, vous pouvez visualiser les informations sur la modification dans l'onglet **Surveiller** dans Client Web vSphere. Reportez-vous à [« Afficher les informations du contrôle de l'intégrité d'un vSphere Distributed Switch »](#), page 56.

Afficher les informations du contrôle de l'intégrité d'un vSphere Distributed Switch

Une fois que vous avez activé le contrôle de l'intégrité, vous pouvez afficher les informations sur le contrôle de l'intégrité du vSphere Distributed Switch dans Client Web vSphere.

Prérequis

Activez le contrôle de l'intégrité sur chaque vSphere Distributed Switch. Reportez-vous à [« Activer ou désactiver le contrôle de l'intégrité du vSphere Distributed Switch dans Client Web vSphere »](#), page 55.

Procédure

- Accédez à un vSphere Distributed Switch dans Client Web vSphere.
- Cliquez sur l'onglet **Surveiller** puis sur **Santé**.
- Dans la section Détails de l'état de santé, cliquez sur l'onglet pour afficher l'état de santé du contrôle sélectionné.

Les trois tableaux comprennent : **VLAN**, **MTU** et **Association et basculement**.

Exporter, importer et restaurer des configurations de commutateurs distribués

Vous pouvez exporter la configuration de vSphere Distributed Switch à partir de Client Web vSphere, y compris des configurations de groupes de ports distribués. La configuration exportée conserve les paramètres de mise en réseau valides, ce qui permet de distribuer ces configurations dans d'autres déploiements.

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 »](#), page 48.

REMARQUE 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 groupe de ports distribués avec Client Web vSphere

Vous pouvez exporter les configurations de groupes de ports distribués et de vSphere Distributed Switch dans un fichier. Le fichier conserve les configurations de réseau valides, permettant de répartir ces configurations vers d'autres déploiements.

Cette fonctionnalité est disponible uniquement avec Client Web vSphere 5.1 ou ultérieure. Cependant, vous pouvez exporter les paramètres de n'importe quelle version d'un port distribué si vous utilisez Client Web vSphere ou une version ultérieure.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris dans le navigateur puis sélectionnez **Toutes les actions vCenter > 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.

Vous avez maintenant un fichier de configuration qui contient tous les paramètres pour le commutateur distribué et 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 commutateur distribués et de groupes de ports distribués existants pour qu'ils se conforment aux paramètres sélectionnés.

Suivant

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

- Pour créer une copie du commutateur distribué exporté, consulter « [Importer un vSphere Distributed Switch à l'aide de Client Web vSphere](#) », page 57
- Pour remplacer les paramètres sur un commutateur distribué existant, consulter « [Restaurer la configuration de vSphere Distributed Switch à l'aide de Client Web vSphere](#) », page 58 .

Vous ne pouvez exporter, importer, et restaurer que les configurations de groupe de ports. Reportez-vous à « [Exporter, importer et restaurer des configurations de groupes de ports distribués vSphere](#) », page 48.

Importer un vSphere Distributed Switch à l'aide de Client Web vSphere

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

Dans vSphere 5.1 ou versions ultérieures, vous pouvez importer un commutateur distribué à l'aide de Client Web vSphere.

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.

REMARQUE 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 Client Web vSphere, accédez à un centre de données.
- 2 Cliquez avec le bouton droit sur le centre de données et sélectionnez **Toutes les actions vCenter > 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**.

Si vous cochez la case **Conserver les identifiants d'origine du commutateur distribué et de tous les groupes de ports** lorsque vous créez un commutateur en utilisant le fichier de configuration d'un commutateur supprimé, tous les hôtes qui ont été connectés au commutateur supprimé sont réajoutés.

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

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 la configuration de vSphere Distributed Switch à l'aide de Client Web vSphere

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.

Vous pouvez uniquement restaurer la configuration d'un commutateur distribué dans vCenter Server et Client Web vSphere version 5.1 ou ultérieure.

REMARQUE 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 Client Web vSphere, accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit sur le commutateur distribué dans le navigateur puis sélectionnez **Toutes les actions vCenter > 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.

VLAN privés

Les VLAN privés servent à résoudre les restrictions d'ID VLAN et le gaspillage d'adresses IP pour certaines configurations réseau.

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.

Pour configurer des ports distribués afin d'utiliser la fonctionnalité VLAN privé, vous devez créer les VLAN privés requis sur le vSphere Distributed Switch auquel les ports distribués sont connectés.

Créer un VLAN privé avec Client Web vSphere

Vous pouvez créer un VLAN privé pour l'utiliser sur un vSphere Distributed Switch et ses ports distribués associés.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres**.
- 3 Sélectionnez **VLAN privé** et cliquez sur **Modifier**.
- 4 Cliquez sur **Ajouter** pour ajouter un **ID primaire VLAN** à la liste.
- 5 Cliquez les flèches haut et bas pour sélectionner un ID VLAN privé primaire.
- 6 Cliquez sur le **signe plus (+)** à côté de l'ID VLAN primaire pour l'ajouter à la liste.
Ce VLAN privé primaire apparaît également sous l'ID du VLAN privé secondaire.
- 7 Pour ajouter un VLAN secondaire, cliquez sur **Ajouter** sous la liste **VLAN secondaire** et cliquez sur le flèches haut et bas pour entrer le numéro du VLAN secondaire.
- 8 Cliquez sur le **signe plus (+)** à côté de l'ID du VLAN secondaire pour l'ajouter à la liste.
- 9 Dans la colonne **Type de VLAN secondaire**, cliquez dans la colonne pour activer un menu déroulant. Sélectionnez soit **Isolé**, soit **Communauté** pour le type de VLAN.
- 10 Cliquez sur **OK**.

Suivant

Configurez un port distribué ou un groupe de ports distribués pour associer le trafic au réseau VLAN privé. Reportez-vous à la section « [Modifier la règle VLAN d'un groupe de ports distribués dans Client Web vSphere](#) », page 92 et « [Modifier la règle VLAN d'un port distribué avec Client Web vSphere](#) », page 93.

Supprimer un VLAN privé principal avec Client Web vSphere

Supprimez les VLAN privés primaires non utilisés de la vue de paramètres distribués de Client Web vSphere. Incompatibilité de chiffres Tâches communes pour MSCS (flex).xml.ttx (51) 0% Dans le menu déroulant <ut><uicontrol></ut>Nouveau périphérique<ut></uicontrol></ut> sélectionnez <ut><uicontrol></ut>Réseau<ut></uicontrol></ut> et cliquez sur <ut><uicontrol></ut>Ajouter<ut></uicontrol></ut>. Incompatibilité de chiffres Exécuter une recherche avancée dans le NextGen Client.xml.ttx (12) 0% Cliquez sur <ut><?xm-insertion_mark_start author="Administrator" time="20120203T152704-0800"?></ut>l'icône de triangle à côté de la zone de recherche rapide<ut><?xm-insertion_mark_start author="Administrator" time="20120203T152704-0800"?></ut> <ut><image id="IMAGE_5CE788FD6BB445949628FF3BDAC1DB16" href="GUID-CF8D1017-9337-4663-9EA1-76532FD119CB"></ut>

Prérequis

Avant de supprimer un VLAN privé, assurez-vous qu'aucun groupe de ports n'est configuré pour l'utiliser.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres**.
- 3 Sélectionnez **VLAN privé** et cliquez sur **Modifier**.
- 4 Sélectionnez un VLAN privé principal à supprimer.

Supprimer un VLAN privé primaire supprime également l'ensemble des VLANs privés secondaires associés.

- 5 Cliquez sur **Supprimer** dans la liste des ID de VLAN principal.
- 6 Cliquez sur **OK** pour confirmer que vous voulez supprimer le VLAN primaire.
- 7 Cliquez sur **OK**.

Supprimer un VLAN privé secondaire avec Client Web vSphere

Supprimez les VLAN privés secondaire non utilisés de la vue de paramètres distribués de Client Web vSphere.

Prérequis

Avant de supprimer un VLAN privé, assurez-vous qu'aucun groupe de ports ne soit configuré pour l'utiliser.

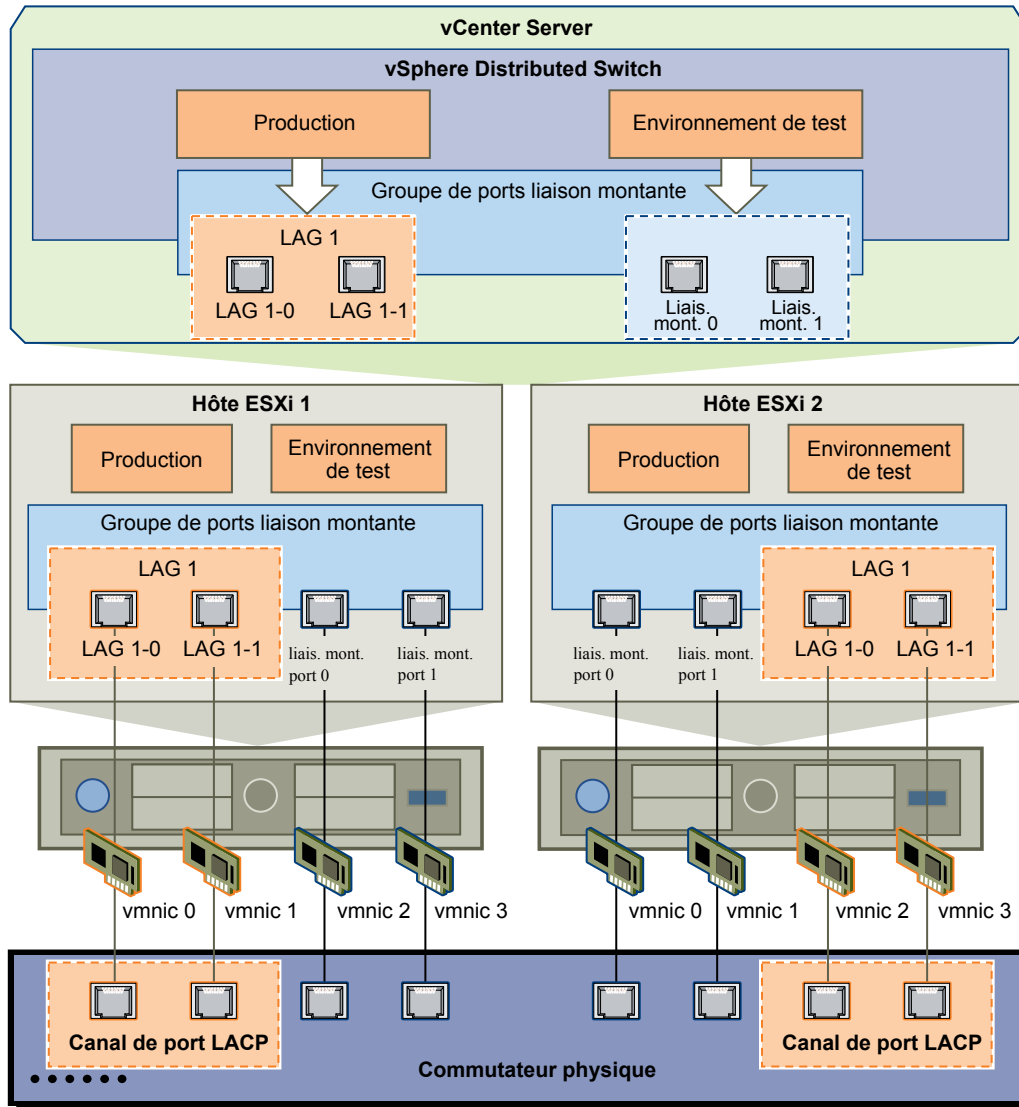
Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres**.
- 3 Sélectionnez **VLAN privé** et cliquez sur **Modifier**.
- 4 Sélectionnez un VLAN privé principal pour afficher l'ensemble de ses VLAN privés secondaires associés.
- 5 Sélectionnez un VLAN privé secondaire à supprimer.
- 6 Cliquez sur **Supprimer** dans la liste des ID de VLAN secondaire, puis cliquez sur **OK**.

Prise en charge de LACP sur vSphere Distributed Switch

La prise en charge du protocole LACP sur un vSphere Distributed Switch 5.5 vous permet de 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 3-4. 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 chacun des hôtes connectés 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. Toutefois, le nombre de LAG que vous pouvez réellement utiliser dépend de la capacité 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.

Configuration du canal de port sur le commutateur physique

Pour chacun des hôtes sur lesquels vous souhaitez utiliser LACP, vous devez créer un canal de port LACP séparé 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 utilisé 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.

Comparaison de prise en charge du protocole LACP entre vSphere Distributed Switch 5.5 et 5.1

La prise en charge du protocole LACP sur un vSphere Distributed Switch 5.5 améliore la capacité de gestion de l'agrégation de liens par rapport à la version 5.1.

Tableau 3-1. Différences de prise en charge du protocole LACP entre vSphere Distributed Switch 5.1 et 5.5

Fonctionnalité	vSphere Distributed Switch 5.1	vSphere Distributed Switch 5.5	Description
Prise en charge de plusieurs LAG	Non	Oui	Dans vSphere Distributed Switch 5.1, la prise en charge du protocole LACP est activée sur l'intégralité d'un groupe de ports de liaison montante et celui-ci joue le rôle de LAG unique pour le commutateur. vSphere Distributed Switch 5.5 prend en charge plusieurs LAG.
Configurer des groupes de ports distribués pour utiliser des LAG comme liaisons montantes actives	Non	Oui	Dans vSphere Distributed Switch 5.1, vous pouvez configurer un LAG pour gérer le trafic de tous les groupes de ports distribués sur le commutateur distribué. vSphere Distributed Switch 5.5 vous permet d'utiliser un LAG pour gérer le trafic de groupes de ports distribués individuels. Vous pouvez définir des LAG en tant que liaisons montantes actives dans l'ordre d'association et de basculement des groupes de ports.
Plusieurs algorithmes d'équilibrage de charge LACP	Non	Oui	La prise en charge du protocole LACP dans vSphere Distributed Switch 5.1 ne concerne que l'équilibrage de charge par hachage IP. Dans vSphere Distributed Switch 5.5, tous les algorithmes d'équilibrage de charge de LACP sont pris en charge.

Convertir vers la prise en charge étendue du protocole LACP sur un vSphere Distributed Switch dans Client Web vSphere

Après avoir mis à niveau un vSphere Distributed Switch vers la version 5.5, vous pouvez effectuer la conversion vers la prise en charge étendue du protocole LACP pour créer plusieurs LAG sur le commutateur distribué.

Si une configuration LACP existe sur le commutateur distribué, l'étendue de la prise en charge crée un nouveau LAG et migre toutes les cartes réseau physiques des liaisons montantes autonomes aux ports LAG. Pour créer une autre configuration LACP, vous devez désactiver la prise en charge de LACP sur le groupe de ports de liaison montante avant de commencer la conversion.

En cas d'échec de la conversion vers la prise en charge étendue du protocole LACP, consultez la section *Dépannage vSphere* pour obtenir plus d'informations sur la manière de procéder manuellement.

Prérequis

- Vérifiez que la version du vSphere Distributed Switch est 5.5.
- Vérifiez qu'aucun des groupes de ports distribués ne permet de remplacer sa stratégie d'association de liaison montante sur les ports individuels.
- Si vous effectuez une conversion à partir d'une configuration LACP existante, vérifiez qu'il n'existe qu'un seul groupe de ports de liaison montante sur le commutateur distribué.
- Vérifiez que les hôtes qui intègrent le commutateur distribué sont connectés et répondent.
- Vérifiez que vous disposez du privilège **Groupe dvPort.Modifier** sur les groupes de ports distribués du commutateur.
- Vérifiez que vous disposez du privilège **Hôte.Configuration.Modifier** sur les hôtes du commutateur distribué.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.

- 2 Sélectionnez **Résumé**.
- 3 Dans la section Fonctions, cliquez sur **Étendre** en regard de Protocole LACP (Link Aggregation Control Protocol).
- 4 (Facultatif) Sélectionnez **Exporter une configuration** pour sauvegarder la configuration du commutateur distribué, puis cliquez sur **Suivant**.

La sauvegarde stocke uniquement la configuration du commutateur distribué du côté vCenter Server. En cas d'échec de la conversion vers la prise en charge étendue du protocole LACP, vous pouvez soit utiliser la sauvegarde pour créer un nouveau commutateur distribué avec la même configuration, soit effectuer la conversion manuellement.

- 5 Vérifiez les conditions préalables de la validation.

Conditions préalables	Description
Accessibilité au groupe de ports	Vous disposez des privilèges suffisants pour accéder à la liaison montante et aux groupes de ports distribués du commutateur, et les modifier.
Configuration LACP	Vous ne disposez que d'un seul groupe de ports de liaison montante sur le commutateur distribué.
Remplacement de la stratégie d'association de liaison montante	Les groupes de ports distribués ne permettent pas de remplacer leur stratégie d'association de liaison montante sur les ports individuels.
Accessibilité de l'hôte	Vous disposez des privilèges suffisants pour modifier la configuration de mise en réseau des hôtes connectés au commutateur distribué.
Connectivité de l'hôte	Les hôtes qui intègrent le commutateur distribué sont connectés et répondent.

- 6 Cliquez sur **Suivant**.
- 7 Si vous effectuez une conversion à partir d'une configuration LACP existante, tapez le nom du nouveau LAG dans la zone de texte Nom.
- 8 Cliquez sur **Suivant** pour passer en revue les détails de la conversion, puis cliquez sur **Terminer**.

Vous avez effectué la conversion vers la prise en charge étendue du protocole LACP sur le vSphere Distributed Switch.

Suivant

Créez des LAG sur le commutateur distribué pour agréger la bande passante de plusieurs cartes réseau physiques sur les hôtes associés.

Configuration de l'association et du basculement LACP pour des 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 3-2. Configuration de l'association et du basculement LACP pour des groupes de ports distribués

Ordre de basculement	Liaisons montantes	Description
Actif	LAG unique	Vous ne pouvez utiliser qu'un LAG actif ou plusieurs liaisons montantes autonomes pour gérer le trafic de 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 LAG pour gérer le trafic des groupes de ports distribués dans Client Web vSphere

Pour agréger la bande passante de plusieurs cartes réseau physiques sur les hôtes, vous pouvez créer un LAG sur le commutateur distribué 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.

Prérequis

- 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 « [Prise en charge de LACP sur vSphere Distributed Switch](#) », page 61.
- Vérifiez que la version du vSphere Distributed Switch sur lequel vous configurez le LAG est la version 5.5.
- Vérifiez que le commutateur distribué intègre la prise en charge étendue du protocole LACP.

Procédure

- 1 [Créer un LAG dans Client Web vSphere](#) page 66

Pour migrer le trafic réseau de plusieurs groupes de ports distribués vers un LAG, vous devez créer un nouveau LAG.

- 2 [Définir un LAG en mode veille dans l'association et l'ordre de basculement des groupes de ports distribués dans Client Web vSphere](#) page 67

Le nouveau 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 [Affecter des cartes réseau physiques à des ports LAG dans Client Web vSphere](#) page 67

Vous avez défini le nouveau LAG en attente dans l'ordre d'association et 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 le LAG en mode actif dans l'association et l'ordre de basculement du groupe de ports distribués dans Client Web vSphere](#) page 69

Vous avez migré les cartes réseau physiques vers les ports 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 LAG dans Client Web vSphere

Pour migrer le trafic réseau de plusieurs groupes de ports distribués vers un LAG, vous devez créer un nouveau LAG.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Sélectionner **Gérer,,** puis sélectionnez **Paramètres**.
- 3 Sous **LACP**, cliquez sur **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
Actif	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. Ils 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.

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

8 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.

9 Cliquez sur **OK**.

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.

Suivant

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 LAG en mode veille dans l'association et l'ordre de basculement des groupes de ports distribués dans Client Web vSphere

Le nouveau 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 **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**.

Suivant

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

Affecter des cartes réseau physiques à des ports LAG dans Client Web vSphere

Vous avez défini le nouveau LAG en attente dans l'ordre d'association et 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.

Prérequis

- 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.

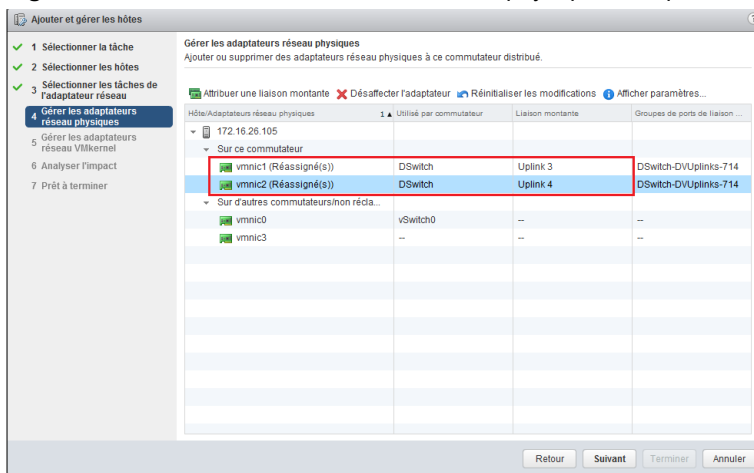
Procédure

- 1 Dans Client Web vSphere, 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 réseau 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.

Figure 3-5. Connexion de deux cartes réseau physiques aux ports LAG



Suivant

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 le LAG en mode actif dans l'association et l'ordre de basculement du groupe de ports distribués dans Client Web vSphere

Vous avez migré les cartes réseau physiques vers les ports 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

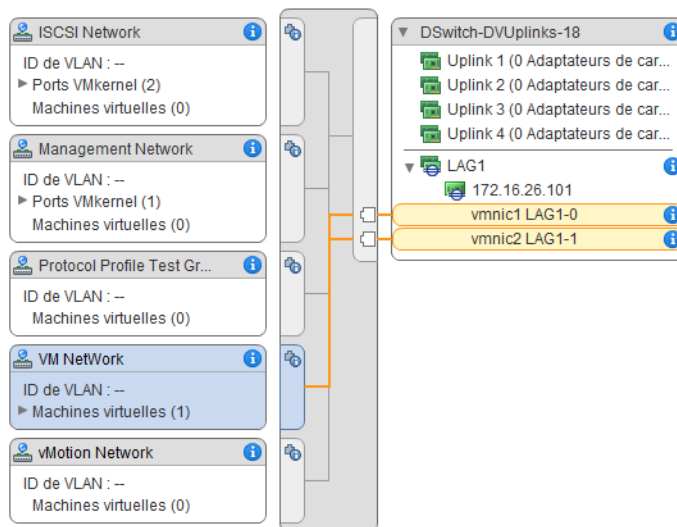
- 1 Accédez au commutateur distribué.
- 2 Dans le menu **Actions**, sélectionnez **Gérer des groupes de ports distribués**.
- 3 Sélectionnez **Association et basculement**, puis cliquez sur **Suivant**.
- 4 Sélectionnez les groupes de ports pour lesquels vous souhaitez mettre le LAG en attente, puis 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**.

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 3-6. Topologie d'un commutateur distribué avec un LAG



Modifier un LAG dans Client Web vSphere

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

Procédure

- 1 Dans Client Web vSphere, accédez au vSphere Distributed Switch.

- 2 Sélectionnez **Gérer**, puis **Paramètres**.
- 3 Sélectionnez **LACP**.
- 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 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.
- 9 Cliquez sur **OK**.

Activer la prise en charge du protocole LACP 5.1 pour un groupe de ports de liaison montante dans Client Web vSphere

Vous pouvez activer la prise en charge du protocole LACP sur un groupe de ports de liaison montante pour vSphere Distributed Switches 5.1 et pour les commutateurs mis à niveau vers la version 5.5 ne disposant pas d'une prise en charge étendue du protocole LACP.

Prérequis

- Pour chacun des hôtes sur lesquels vous souhaitez utiliser LACP, vérifiez qu'un canal de port LACP séparé existe sur le commutateur physique.
- Vérifiez que la règle d'équilibrage de charge des groupes de ports distribués est définie sur Hachage IP.
- Vérifiez que le canal de port LACP sur le commutateur physique est configuré avec l'équilibrage de charge par hachage IP.
- Vérifiez que la stratégie de détection de panne réseau des groupes de ports distribués est définie sur État de lien seulement.
- Vérifiez que l'association et l'ordre de basculement de toutes les liaisons montantes des groupes de ports distribués sont définis sur Actif.
- Vérifiez que toutes les cartes réseau physiques connectées aux liaisons montantes ont la même vitesse et sont configurées en mode duplex intégral.

Procédure

- 1 Dans Client Web vSphere, accédez à un groupe de ports de liaison montante.
 - a Sélectionnez un commutateur distribué et cliquez sur **Éléments associés**.
 - b Cliquez sur **Groupes de ports de liaison montante**, puis sélectionnez le groupe de ports de liaison montante.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Cliquez sur **Edit**.

- 4 Dans la section LACP, activez ou désactivez LACP à l'aide de la liste déroulante.
- 5 Définissez le mode de négociation LACP pour le groupe de ports de liaison montante.

Option	Description
Active	Tous les ports de liaison montante du groupe sont en mode de négociation active. Les ports de liaison montante lancent les négociations avec les ports LACP sur le commutateur physique en envoyant des paquets LACP.
Passif	Tous les ports de liaison montante sont en mode de négociation passive. Ils répondent aux paquets LACP reçus, 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 régler les ports de liaison montante en mode passif et inversement.

- 6 Cliquez sur **OK**.

Limitations de la prise en charge LACP sur 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.

- La prise en charge du protocole LACP n'est pas compatible avec la gestion multivoie iSCSI de logiciels.
- 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.
- La prise en charge du protocole LACP ne fonctionne pas avec la mise en miroir des ports.
- 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.
- La prise en charge du protocole LACP 5.1 fonctionne uniquement avec l'équilibrage de charge de hachage d'IP et la détection de basculement de réseau de l'état de lien.
- La prise en charge du protocole LACP 5.1 ne fournit qu'un seul LAG par commutateur distribué et par hôte.

Configuration de la mise en réseau VMkernel

4

La configuration d'adaptateurs VMkernel permet de fournir la connectivité réseau aux hôtes afin de gérer le trafic de vMotion, de stockage IP, de journalisation de Fault Tolerance et de Virtual SAN.

- [La couche réseau VMkernel](#) page 74

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 Virtual SAN. Vous pouvez configurer des adaptateurs VMkernel pour le trafic d'infrastructure standard sur des commutateurs vSphere standard et sur des vSphere Distributed Switches.

- [Afficher les informations sur les adaptateurs VMkernel d'un hôte dans Client Web vSphere](#) page 75

Pour chaque adaptateur VMkernel, vous pouvez consulter les services attribués, le commutateur associé, les paramètres de port, les paramètres IP, la pile TCP/IP, l'ID VLAN et les règles.

- [Créer un adaptateur VMkernel sur un vSphere Standard Switch dans Client Web vSphere](#) page 76

Créez un adaptateur réseau VMkernel sur un commutateur standard vSphere pour fournir la connectivité réseau aux hôtes et gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance ou de Virtual SAN. Il est recommandé de ne dédier un adaptateur VMkernel qu'à un seul type de trafic.

- [Créer un adaptateur VMkernel sur un hôte associé à un vSphere Distributed Switch dans vSphere Web Client](#) page 78

Créez un adaptateur VMkernel sur un hôte associé à un commutateur distribué 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 Virtual SAN. Vous devez dédier un groupe de ports distribués pour chaque adaptateur VMkernel. Un adaptateur VMkernel doit gérer un type de trafic.

- [Modifier la configuration d'un adaptateur VMkernel dans Client Web vSphere](#) page 79

Il peut s'avérer nécessaire de modifier le type de trafic pris en charge pour un adaptateur VMkernel ou le mode d'obtention des adresses IPv4 ou IPv6.

- [Afficher la configuration de la pile TCP/IP d'un hôte dans Client Web vSphere](#) page 80

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

- [Modifier la configuration d'une pile TCP/IP sur un hôte dans Client Web vSphere](#) page 81

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

- [Créer une pile TCP/IP personnalisée](#) page 81

Vous pouvez créer une pile TCP/IP personnalisée sur un hôte pour transférer le trafic VMkernel via une application personnalisée.

- [Supprimer un adaptateur VMkernel dans Client Web vSphere](#) page 82

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.

La couche réseau VMkernel

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 Virtual SAN. Vous pouvez configurer des adaptateurs VMkernel pour le trafic d'infrastructure standard sur des commutateurs vSphere standard et sur des vSphere Distributed Switches.

Piles TCP/IP au niveau de VMkernel

La pile TCP/IP par défaut au niveau de VMkernel assure la prise en charge de la mise en réseau pour les types de trafic d'infrastructure standard. Vous pouvez ajouter des piles TCP/IP personnalisées au niveau de VMkernel et transférer le trafic réseau via des applications personnalisées.

Types de trafic d'infrastructure sur la pile TCP/IP par défaut

Vous devez dédier un adaptateur VMkernel 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 créer des adaptateurs VMkernel supplémentaires pour le trafic de gestion.

Trafic vMotion

Pour gérer le trafic vMotion, un adaptateur VMkernel pour vMotion est requis sur l'hôte source et sur l'hôte cible. Les adaptateurs VMkernel pour vMotion doivent gérer uniquement le trafic vMotion. Pour optimiser les performances, vous pouvez attribuer plusieurs cartes réseau physiques au groupe de ports de l'adaptateur VMkernel. Plusieurs cartes réseau physiques sont alors utilisées pour vMotion, offrant ainsi une plus grande bande passante.

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

Trafic de stockage IP

Les types de stockage utilisant des réseaux TCP/IP standard et dépendant de la couche de mise en réseau VMkernel nécessitent des adaptateurs 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. NFS ne nécessite pas d'adaptateur VMkernel dédié. Ce type de stockage utilise le trafic de gestion de l'hôte pour les E/S. Les hôtes ESXi prennent uniquement en charge NFS version 3 sur TCP/IP.

Trafic Fault Tolerance	Trafic envoyé par la principale machine virtuelle avec Fault Tolerance vers la machine virtuelle avec Fault Tolerance secondaire sur 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 Virtual SAN	Tous les hôtes faisant partie d'un cluster Virtual SAN doivent disposer d'un adaptateur VMkernel pour la gestion du trafic de Virtual SAN.

Afficher les informations sur les adaptateurs VMkernel d'un hôte dans Client Web vSphere

Pour chaque adaptateur VMkernel, vous pouvez consulter les services attribués, le commutateur associé, les paramètres de port, les paramètres IP, la pile TCP/IP, l'ID VLAN et les règles.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Cliquez sur **Gérer**, puis sur **Mise en réseau**.
- 3 Pour afficher les informations sur les adaptateurs VMkernel de l'hôte, sélectionnez **Adaptateurs VMkernel**.

Pour les hôtes ESX 4.x, l'option Adaptateurs VMkernel affiche la console de service ESX.

Option	Description
Périphérique	Nom de l'adaptateur VMkernel.
Étiquette réseau	Nom du réseau auquel l'adaptateur VMkernel est connecté.
Commutateur	Commutateur vSphere standard ou vSphere Distributed Switch auquel l'adaptateur VMkernel est associé.
Adresse IP	Adresse IP de l'adaptateur VMkernel.
Pile TCP/IP	Pile TCP/IP gérant le trafic de l'adaptateur VMkernel. Si une pile TCP/IP personnalisée a été définie pour l'adaptateur VMkernel, celle-ci est répertoriée.
Trafic vMotion	Statut de vMotion sur l'adaptateur VMkernel.
Journalisation FT	Statut de journalisation Fault Tolerance sur l'adaptateur VMkernel.
Trafic de gestion	Statut du trafic de gestion sur l'adaptateur VMkernel.
Trafic Virtual SAN	Statut du trafic de Virtual SAN sur l'adaptateur VMkernel.

- 4 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. Ces informations incluent les paramètres de port et de carte réseau, les paramètres IPv4 et IPv6, la formation du trafic, l'association et le basculement et les règles 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
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.
Règles	Affiche les paramètres configurés pour la formation du trafic, l'association et le basculement et les règles de sécurité qui s'appliquent au groupe de ports auquel l'adaptateur VMkernel est connecté.

Créer un adaptateur VMkernel sur un vSphere Standard Switch dans Client Web vSphere

Créez un adaptateur réseau VMkernel sur un commutateur standard vSphere pour fournir la connectivité réseau aux hôtes et gérer le trafic de vSphere vMotion, du stockage IP, de la journalisation de Fault Tolerance ou de Virtual SAN. Il est recommandé de ne dédier un adaptateur VMkernel qu'à un seul type de trafic.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **Adaptateurs VMkernel**.
- 3 Cliquez sur **Ajouter mise en réseau d'hôte**.
- 4 Dans la page Sélectionner un type de connexion, sélectionnez **Adaptateur réseau VMkernel** et cliquez sur **Suivant**.
- 5 Dans la page Sélectionner un périphérique cible, sélectionnez un commutateur standard existant ou créez un **Nouveau commutateur standard vSphere**.
- 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. Pendant ce temps, l'hôte n'a pas de connexion réseau avec les autres hôtes du réseau physique. Les machines virtuelles de l'hôte peuvent communiquer entre elles.

- a Cliquez sur **Ajouter** 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	Tapez une valeur pour cette étiquette afin d'indiquer le type de trafic de l'adaptateur VMkernel, par exemple Trafic de gestion ou vMotion .
ID VLAN	Entrez un ID de VLAN pour identifier le VLAN que le trafic réseau de l'adaptateur VMkernel utilisera.
Paramètres IP	Sélectionnez IPv4, IPv6 ou les deux. REMARQUE L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.

Option	Description
Pile TCP/IP	Sélectionnez une pile dans la liste.
Activer les services	<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"> ■ Trafic vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Vous pouvez activer cette propriété pour un seul adaptateur VMkernel vMotion et de stockage IP par hôte. Si cette propriété n'est activée pour aucun adaptateur VMkernel, la migration avec vMotion vers l'hôte sélectionné n'est pas possible. ■ Trafic Fault Tolerance. Active la journalisation de Fault Tolerance sur l'hôte. ■ Trafic de gestion. Active le trafic de gestion pour l'hôte et vCenter Server. En principe, 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. ■ Virtual SAN. Active le trafic de Virtual SAN sur l'hôte. Chaque hôte faisant partie d'un cluster Virtual SAN doit disposer de ce type d'adaptateur VMkernel.

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

Option	Description
Obtenir automatiquement les paramètres IP	Utilisez DHCP pour obtenir les paramètres IP.
Utiliser des paramètres IP statiques	<p>Entrez l'adresse IP IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel.</p> <p>Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la tâche TCP/IP sélectionnée.</p>

- 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.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Adresses IPv6 statiques	<p>a Cliquez sur Ajouter pour ajouter une nouvelle adresse IPv6.</p> <p>b Tapez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur OK.</p> <p>c Pour modifier la passerelle par défaut de VMkernel, cliquez sur Modifier.</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 dans vSphere Web Client

Créez un adaptateur VMkernel sur un hôte associé à un commutateur distribué 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 Virtual SAN. Vous devez dédier un groupe de ports distribués pour chaque adaptateur VMkernel. Un adaptateur VMkernel doit gérer un type de trafic.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **Adaptateurs VMkernel**.
- 3 Cliquez sur **Ajouter mise en réseau d'hôte**.
- 4 Dans la page Sélectionner un type de connexion, sélectionnez **Adaptateur réseau VMkernel** et cliquez sur **Suivant**.
- 5 Sélectionnez un groupe de ports distribués 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. REMARQUE L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.
Pile TCP/IP	Si des piles personnalisées sont disponibles, sélectionnez-en une dans la liste.
Activer les services	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 : <ul style="list-style-type: none">■ Trafic vMotion. Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Vous pouvez activer cette propriété pour un seul adaptateur VMkernel vMotion et de stockage IP par hôte. Si cette propriété n'est activée pour aucun adaptateur VMkernel, la migration avec vMotion vers l'hôte sélectionné n'est pas possible.■ Trafic Fault Tolerance. Active la journalisation de Fault Tolerance sur l'hôte.■ Trafic de 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.■ Virtual SAN. Active le trafic de Virtual SAN sur l'hôte. Chaque hôte faisant partie d'un cluster de Virtual SAN doit disposer de ce type d'adaptateur VMkernel.

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

Option	Description
Obtenir automatiquement les paramètres IP	Utilisez DHCP pour obtenir les paramètres IP.
Utiliser des paramètres IP 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.

- 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.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Adresses IPv6 statiques	a Cliquez sur Ajouter pour ajouter une nouvelle adresse IPv6. b Tapez 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 Modifier .

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

Modifier la configuration d'un adaptateur VMkernel dans Client Web vSphere

Il peut s'avérer nécessaire de 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 Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **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, sélectionnez les services à activer.

Case à cocher	Description
Trafic vMotion	Permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Vous pouvez activer cette propriété pour un seul adaptateur VMkernel vMotion et de stockage IP par hôte. Si cette propriété n'est activée pour aucun adaptateur VMkernel, la migration avec vMotion vers l'hôte sélectionné n'est pas possible.
Trafic Fault Tolerance	Active la journalisation de Fault Tolerance sur l'hôte.
Trafic de gestion	Active le trafic de gestion pour l'hôte et vCenter Server. En principe, ce type d'adaptateur VMkernel est créé pour les hôtes lors de l'installation du logiciel ESXi. Vous pouvez définir un autre adaptateur VMkernel de trafic de gestion sur l'hôte pour assurer la redondance.
Virtual SAN	Active le trafic de Virtual SAN sur l'hôte. Chaque hôte faisant partie d'un cluster Virtual SAN doit disposer de ce type d'adaptateur VMkernel.

- 5 Dans la page Paramètres NIC, définissez le MTU de l'adaptateur réseau.

- 6 Vérifiez que IPv4 est activé, puis dans la section Paramètres IPv4, sélectionnez le mode d'obtention des adresses IP.

Option	Description
Obtenir automatiquement les paramètres IP	Utilisez DHCP pour obtenir les paramètres IP.
Utiliser des paramètres IP 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.

- 7 Vérifiez que IPv6 est activé, puis dans la section Paramètres IPv6, choisissez une option d'obtention des adresses IPv6.

REMARQUE 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.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Adresses IPv6 statiques	<ol style="list-style-type: none"> a Cliquez sur Ajouter pour ajouter une nouvelle adresse IPv6. b Tapez 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 Modifier.

Dans la section Paramètres avancés des paramètres IP, supprimez les adresses IPv6. Si l'annonce du routeur est activée, les adresses supprimées de cette origine peuvent réapparaître. La suppression d'adresses DHCP sur l'adaptateur VMKernel n'est pas prise en charge. Ces adresses sont supprimées uniquement lorsque l'option DHCP est activée.

- 8 Dans la page Valider les modifications, vérifiez si les modifications apportées à l'adaptateur VMKernel ne vont pas perturber d'autres opérations.
- 9 Cliquez sur **OK**.

Afficher la configuration de la pile TCP/IP d'un hôte dans Client Web vSphere

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

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Cliquez sur **Gérer**, sur **Mise en réseau**, puis sélectionnez **Configuration TCP/IP**.
- 3 Sélectionnez une pile dans la table de piles TCP/IP.

Si aucune pile TCP/IP personnalisée n'a été configurée sur l'hôte, seule la pile TCP/IP par défaut de cet hôte est affichée.

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.

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

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

Modifier la configuration d'une pile TCP/IP sur un hôte dans Client Web vSphere

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

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Cliquez sur **Gérer**, sur **Mise en réseau**, puis sélectionnez **Configuration TCP/IP**.
- 3 Sélectionnez une pile dans la table, puis cliquez sur **Modifier**.
- 4 Sur la page Nom, vous pouvez modifier le nom d'une pile TCP/IP personnalisée.
- 5 Sur la page Configuration DNS, sélectionnez le mode d'obtention des informations de serveur DNS.

Option	Description
Obtenez les paramètres automatiquement à partir de l'adaptateur réseau virtuel	Depuis le menu déroulant Adaptateur réseau VMKernel , sélectionnez un adaptateur réseau.
Entrez les paramètres manuellement	<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) Utilisez la zone de texte Rechercher les domaines pour rechercher des hôtes avec des noms spécifiques.

- 6 Sur la page Routage, modifiez les informations de passerelle VMkernel.

REMARQUE La suppression de la passerelle par défaut peut provoquer la perte de connectivité du client avec l'hôte.

- 7 Sur la page Avancé, modifiez l'algorithme de contrôle d'encombrement de la pile ainsi que le nombre maximal de connexions.
- 8 Cliquez sur **OK**.

Créer une pile TCP/IP personnalisée

Vous pouvez créer une pile TCP/IP personnalisée sur un hôte pour transférer le trafic VMkernel via une application personnalisée.

Procédure

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

- 3 Exécutez la commande vSphere CLI suivante :

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

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

Supprimer un adaptateur VMkernel dans Client Web vSphere

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 Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **Adaptateurs VMkernel**.
- 3 Sélectionnez un adaptateur VMkernel dans la liste et cliquez sur **Supprimer**.
- 4 Dans la boîte de dialogue de confirmation, cliquez sur **Analyser l'impact**.
- 5 Vérifiez les services affectés, ainsi que le niveau d'impact.

Option	Description
Aucun impact	Le service continue de fonctionner normalement une fois la nouvelle configuration de mise en réseau appliquée.
Impact important	Le fonctionnement du service peut être affecté si la nouvelle configuration de mise en réseau est appliquée.
Impact critique	Le fonctionnement du service est interrompu si la nouvelle configuration de la mise en réseau est appliquée.

- a Si l'impact sur le fonctionnement d'un service est important ou critique, cliquez sur le service et vérifiez les raisons affichées dans le volet Détails de l'analyse.
 - b Si aucun service n'est affecté, fermez la boîte de dialogue Analyser l'impact. Dans le cas contraire, annulez la suppression de l'adaptateur VMkernel, puis corrigez les problèmes entraînant un impact important ou critique sur un service.
- 6 Cliquez sur **OK**.

Règles de mise en réseau

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

- [Stratégie d'association et de basculement](#) page 84

Une stratégie d'association et de basculement vous permet de déterminer la répartition du trafic réseau entre les adaptateurs physiques et de réacheminer le trafic en cas de panne d'un adaptateur.

- [Règle VLAN](#) page 92

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

- [Règle de sécurité](#) page 95

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

- [Règle de formation du trafic](#) page 99

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.

- [Règle d'allocation des ressources](#) page 103

La règle 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.

- [Règle de surveillance](#) page 104

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

- [Règle de filtrage et de balisage du trafic](#) page 106

Dans un vSphere Distributed Switch 5.5 ou version ultérieure, les règles 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.

- [Règles de blocage des ports](#) page 124

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

- [Gérer les stratégies de plusieurs groupes de ports sur un vSphere Distributed Switch dans Client Web vSphere](#) page 125
Vous pouvez modifier les stratégies de mise en réseau de plusieurs groupes de ports sur un vSphere Distributed Switch.

Stratégie d'association et de basculement

Une stratégie d'association et de basculement vous permet de déterminer la répartition du trafic réseau entre les adaptateurs physiques et de réacheminer le trafic en cas de panne d'un adaptateur.

Vous pouvez modifier la stratégie de basculement et d'équilibrage de charge en configurant les paramètres suivants :

- L'équilibrage de charge détermine la distribution du trafic sortant entre les adaptateurs réseau associés à un commutateur ou un groupe de ports.

REMARQUE Le trafic entrant est contrôlé par la stratégie d'équilibrage de charge sur le commutateur physique.

- La détection de basculement contrôle l'état du lien et le sondage de balise. La signalisation n'est pas pris en charge par le balisage VLAN invité.
- L'ordre de basculement peut être actif ou en veille.

Lorsqu'un événement de basculement se produit, vous pouvez perdre la connectivité. Dans ce cas, les adresses MAC utilisées par les machines virtuelles qui sont associées au commutateur standard ou au commutateur distribué apparaissent sur un port de commutateur physique différent de celui auquel elles étaient précédemment associées. Pour éviter ce problème, mettez votre commutateur physique en mode PortFast ou PortFast trunk.

Modifier la stratégie d'association et de basculement d'un commutateur standard vSphere dans Client Web vSphere

La stratégie d'association et de basculement vous permet de déterminer la manière dont le trafic réseau des machines virtuelles et des adaptateurs VMkernel connectés au commutateur est réparti entre les adaptateurs physiques. Elle vous permet également de déterminer le mode de réacheminement du trafic en cas de panne d'un adaptateur.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste, cliquez sur **Modifier les paramètres**, puis sélectionnez **Association et basculement**.
- 4 Dans le menu déroulant **Équilibrage de charge**, indiquez comment le commutateur standard ou distribué sélectionne une liaison montante pour gérer le trafic provenant d'une machine virtuelle ou d'un adaptateur VMkernel.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionner une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel.
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 simplement les données de ces champs pour calculer le hachage. L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel.

Option	Description
Router en fonction du hachage de l'adresse MAC source	Sélectionner une liaison montante en fonction d'un hachage de l'Ethernet source.
Utiliser un ordre 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.

- 5 Dans le menu déroulant **Détection du basculement réseau**, indiquez la méthode de détection du basculement utilisée par le commutateur standard ou distribué.

Option	Description
État du lien uniquement	<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> <p>En revanche, elle ne détecte pas les erreurs de configuration, telles que les suivantes :</p> <ul style="list-style-type: none"> ■ 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	<p>Envoie et détecte des sondes d'incident sur toutes les adaptateurs réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. L'hôte ESX/ESXi envoie des paquets de balises toutes les 10 secondes.</p> <p>Le balisage est particulièrement utile pour les associations comportant au moins trois cartes réseau, car ESX/ESXi peut détecter les pannes d'une adaptateur 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.</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>

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

Si vous sélectionnez **Oui**, à chaque fois qu'une carte réseau virtuelle est connectée au commutateur virtuel ou que le trafic de cette carte est acheminé sur une autre carte réseau physique de l'association suite à un basculement, une notification est envoyée 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.

REMARQUE 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**, déterminez si un adaptateur physique retourne à l'état actif après la récupération d'une panne.

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 emplacement le cas échéant.

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**.

Modifier la stratégie d'association et de basculement d'un groupe de ports standard dans Client Web vSphere

Configurez la stratégie d'association et de basculement sur un groupe de ports standard pour déterminer comment le trafic réseau associé à un groupe de machines virtuelles ou à un adaptateur VMkernel est distribué entre des adaptateurs physiques et comment réacheminer le trafic en cas de panne d'un adaptateur physique.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis 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, sélectionnez le groupe de ports et cliquez sur **Modifier les paramètres**.
- 5 Dans la page Association et basculement, pour remplacer les propriétés d'association et de basculement héritées du commutateur standard, cochez les cases en regard des propriétés que vous souhaitez remplacer.
- 6 Dans le menu déroulant **Équilibrage de charge**, indiquez comment le commutateur standard ou distribué sélectionne une liaison montante pour gérer le trafic provenant d'une machine virtuelle ou d'un adaptateur VMkernel.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionner une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel.
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 simplement 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 un ordre 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.

- 7 Dans le menu déroulant **Détection du basculement réseau**, indiquez la méthode de détection du basculement utilisée par le commutateur standard ou distribué.

Option	Description
État du lien uniquement	<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> <p>En revanche, elle ne détecte pas les erreurs de configuration, telles que les suivantes :</p> <ul style="list-style-type: none"> ■ 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	<p>Envoie et détecte des sondes d'incident sur toutes les adaptateurs réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. L'hôte ESX/ESXi envoie des paquets de balises toutes les 10 secondes.</p> <p>Le balisage est particulièrement utile pour les associations comportant au moins trois cartes réseau, car ESX/ESXi peut détecter les pannes d'une adaptateur 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.</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>

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

Si vous sélectionnez **Oui**, à chaque fois qu'une carte réseau virtuelle est connectée au commutateur virtuel ou que le trafic de cette carte est acheminé sur une autre carte réseau physique de l'association suite à un basculement, une notification est envoyée 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.

REMARQUE 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.

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

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 emplacement le cas échéant.

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.

- 10 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.

- 11 Cliquez sur **OK**.

Modifier la stratégie d'association et de basculement d'un groupe de ports distribués dans Client Web vSphere

La stratégie d'association et de basculement d'un groupe de ports distribués permet de déterminer la manière dont le trafic réseau d'un groupe de machines virtuelles ou d'adaptateurs VMkernel est réparti entre les adaptateurs de liaison montante d'un vSphere Distributed Switch. Elle permet également de déterminer comment réacheminer le trafic en cas de panne d'un adaptateur.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué et sélectionnez **Gérer les groupes de ports distribués**.
- 3 Cochez la case **Association et basculement** et cliquez sur **Suivant**.
- 4 Sélectionnez le groupe de ports à configurer, puis cliquez sur **Suivant**.
- 5 Dans le menu déroulant **Équilibrage de charge**, indiquez comment le commutateur standard ou distribué sélectionne une liaison montante pour gérer le trafic provenant d'une machine virtuelle ou d'un adaptateur VMkernel.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionner une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel.
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 simplement 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 un ordre 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.

- 6 Dans le menu déroulant **Détection du basculement réseau**, indiquez la méthode de détection du basculement utilisée par le commutateur standard ou distribué.

Option	Description
État du lien uniquement	<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> <p>En revanche, elle ne détecte pas les erreurs de configuration, telles que les suivantes :</p> <ul style="list-style-type: none"> ■ 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	<p>Envoie et détecte des sondes d'incident sur toutes les adaptateurs réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. L'hôte ESX/ESXi envoie des paquets de balises toutes les 10 secondes.</p> <p>Le balisage est particulièrement utile pour les associations comportant au moins trois cartes réseau, car ESX/ESXi peut détecter les pannes d'une adaptateur 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.</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>

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

Si vous sélectionnez **Oui**, à chaque fois qu'une carte réseau virtuelle est connectée au commutateur virtuel ou que le trafic de cette carte est acheminé sur une autre carte réseau physique de l'association suite à un basculement, une notification est envoyée 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.

REMARQUE 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.

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

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 emplacement le cas échéant.

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. Si l'option **Retour en arrière** est définie sur **Non** et qu'une machine virtuelle est mise hors tension lorsque tous les adaptateurs physiques actifs sont en panne et que l'un d'eux est récupéré, après la mise sous tension de la machine virtuelle, la carte réseau virtuelle est connectée à l'adaptateur récupéré et non à un adaptateur en veille. 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.

- 9 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.

- 10 Passez vos paramètres en revue et cliquez sur **Terminer**.

Modifier les stratégies d'association et de basculement de port distribué avec Client Web vSphere

Les stratégies d'association et de basculement vous permettent de déterminer le mode de répartition du trafic réseau entre les adaptateurs physiques et le mode de réacheminement du trafic en cas de panne d'un adaptateur.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Dans Client Web vSphere, accédez au commutateur distribué.
- 2 Cliquez sur l'onglet **Gérer**, puis sélectionnez **Ports**.
- 3 Sélectionnez un port distribué dans la liste et cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Cliquez sur **Association et basculement** et cochez la case en regard des propriétés que vous souhaitez remplacer.
- 5 Dans le menu déroulant **Équilibrage de charge**, indiquez comment le commutateur standard ou distribué sélectionne une liaison montante pour gérer le trafic provenant d'une machine virtuelle ou d'un adaptateur VMkernel.

Option	Description
Route basée sur le port virtuel d'origine	Sélectionner une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel.
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 simplement 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 un ordre 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.

- 6 Dans le menu déroulant **Détection du basculement réseau**, indiquez la méthode de détection du basculement utilisée par le commutateur standard ou distribué.

Option	Description
État du lien uniquement	<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> <p>En revanche, elle ne détecte pas les erreurs de configuration, telles que les suivantes :</p> <ul style="list-style-type: none"> ■ 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	<p>Envoie et détecte des sondes d'incident sur toutes les adaptateurs réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. L'hôte ESX/ESXi envoie des paquets de balises toutes les 10 secondes.</p> <p>Le balisage est particulièrement utile pour les associations comportant au moins trois cartes réseau, car ESX/ESXi peut détecter les pannes d'une adaptateur 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.</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>

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

Si vous sélectionnez **Oui**, à chaque fois qu'une carte réseau virtuelle est connectée au commutateur virtuel ou que le trafic de cette carte est acheminé sur une autre carte réseau physique de l'association suite à un basculement, une notification est envoyée 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.

REMARQUE 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.

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

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 emplacement le cas échéant.

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. Si l'option **Retour en arrière** est définie sur **Non** et qu'une machine virtuelle est mise hors tension lorsque tous les adaptateurs physiques actifs sont en panne et que l'un d'eux est récupéré, après la mise sous tension de la machine virtuelle, la carte réseau virtuelle est connectée à l'adaptateur récupéré et non à un adaptateur en veille. 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.

- 9 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.

- 10 Cliquez sur **OK**.

Règle 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.

Modifier la règle VLAN d'un groupe de ports distribués dans Client Web vSphere

Définissez la règle VLAN sur un groupe de ports distribués afin d'appliquer l'identification VLAN globalement sur tous les ports distribués.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le navigateur et sélectionnez **Gérer groupes de ports distribués**.
- 3 Cochez la case **VLAN** et cliquez sur **Suivant**.
- 4 Sélectionnez le groupe de ports que vous voulez modifier, puis cliquez sur **Suivant**.
- 5 Sélectionnez les types de filtrage et d'identification de trafic VLAN dans le menu déroulant **Type** et cliquez sur **Suivant**.

Option	Description
Aucune	N'utilise pas de VLAN. Utilisez cette option en cas d'identification de commutateur externe (EST).
VLAN	Identifier le trafic avec l'ID du champ ID VLAN . Entrez un nombre entre 1 et 4094 pour l'identification de commutateur virtuel (VST).

Option	Description
Liaison de jonction VLAN	Passage de trafic VLAN avec ID dans la Plage de jonction VLAN . Vous pouvez définir plusieurs plages et VLAN individuels à l'aide d'une liste séparée par des virgules. Utilisez cette option pour le VGT.
VLAN privé	Associez le trafic avec un VLAN privé créé sur le commutateur distribué.

- 6 Passez vos paramètres en revue et cliquez sur **Terminer**.

Modifier la règle VLAN d'un port distribué avec Client Web vSphere

Utilisez la règle VLAN sur un port distribué afin d'intégrer le trafic virtuel à des VLAN physiques via ce port, différemment du groupe de ports distribués parent.

Prérequis

Pour remplacer la règle VLAN au niveau du port, permettez les remplacements au niveau du port. Reportez-vous à la section « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port de la liste.
- 4 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 5 Cliquez sur **VLAN** et sélectionnez **Remplacer**.

Configurez le trafic VLAN à travers le port distribué dans le menu déroulant **Type de VLAN**.

Option	Description
Aucune	N'utilise pas de VLAN. Utilisez cette option en cas d'identification de commutateur externe (EST).
VLAN	Identifier le trafic avec l'ID du champ ID VLAN . Entrez un nombre entre 1 et 4094 pour l'identification de commutateur virtuel (VST).
Liaison de jonction VLAN	Passage de trafic VLAN avec ID dans la Plage de jonction VLAN . Vous pouvez définir plusieurs plages et VLAN individuels à l'aide d'une liste séparée par des virgules. Utilisez cette option pour le VGT.
VLAN privé	Associez le trafic avec un VLAN privé créé sur le commutateur distribué.

- 6 Cliquez sur **OK**.

Modifier la règle VLAN sur un groupe de ports de liaison montante dans Client Web vSphere

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

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 avez un adaptateur réseau physique qui ne prend pas en charge le filtrage VLAN, les VLAN peuvent ne toujours pas être bloqués. Dans ce cas, configurez le filtrage VLAN sur un groupe de ports distribués ou sur un port distribué.

Consultez la documentation technique des fabricants des adaptateurs pour des informations sur la prise en charge du filtrage VLAN.

Procédure

- 1 Déterminer l'emplacement d'un groupe de ports de liaison montante dans Client Web vSphere.
 - a Pour déterminer l'emplacement d'un groupe de ports de liaison montante, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Sélectionnez l'onglet **Groupes de ports de liaison montante** et localisez le groupe de liaison montante dans la liste.
- 2 Effectuez un clic droit sur le groupe de ports de liaison montante dans la liste et sélectionnez **Modifier les paramètres**.
- 3 Cliquez sur **VLAN** et entrez une **Plage de jonctions VLAN** à propager aux adaptateurs réseau physiques.
 Pour effectuer la jonction de plusieurs plages et de VLAN individuels, séparez les entrées par des virgules.
- 4 Cliquez sur **OK**.

Modifier la règle VLAN d'un port liaison montante avec Client Web vSphere

Définissez la règle VLAN sur un port liaison montante pour prendre en charge le trafic VLAN à travers le port d'une façon différente du groupe de ports liaison montante parent.

Utilisez la règle VLAN sur le port liaison montante pour propager une plage de jonctions des ID VLAN vers l'adaptateur réseau physique pour le filtrage du trafic. L'adaptateur réseau physique abandonne les paquets provenant des autres VLAN si l'adaptateur prend en charge le filtrage par VLAN. Le paramétrage d'une plage de jonctions améliore les performances de gestion de réseau car l'adaptateur réseau physique filtre le trafic à la place du port liaison montante.

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

Consultez la documentation technique du fabricant de l'adaptateur pour des informations sur la prise en charge du filtrage VLAN.

Prérequis

Pour remplacer la règle VLAN au niveau du port, permettez les remplacements au niveau du port. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Déterminer l'emplacement d'un groupe de ports de liaison montante dans Client Web vSphere.
 - a Pour déterminer l'emplacement d'un groupe de ports de liaison montante, sélectionnez un commutateur distribué et cliquez sur l'onglet **Objets associés**.
 - b Sélectionnez l'onglet **Groupes de ports de liaison montante** et double-cliquez sur un groupe de ports de liaison montante dans la liste.
 Le groupe de ports de liaison montante apparaît au premier niveau du navigateur sur la gauche.

- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez une liaison montante de la liste et cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Cliquez sur **VLAN** et cochez la case **Remplacer**.
- 5 Entrez une **Plage de jonctions VLAN** à propager vers l'adaptateur réseau physique.
Pour effectuer la jonction de plusieurs plages et de VLAN individuels, séparez les entrées par des virgules.
- 6 Cliquez sur **OK**.

Règle 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 règle de sécurité sont le mode promiscuité, les changements d'adresse MAC et les Transmissions forgées. Pour plus d'informations sur les menaces réseau potentielles, consultez la documentation de *Sécurité vSphere*.

Modifier la règle de sécurité d'un commutateur standard vSphere dans Client Web vSphere

Sur un commutateur standard vSphere, vous pouvez configurer des règles 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 également configurer des règles de sécurité pour un groupe de ports standard spécifique.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste et cliquez sur **Modifier les paramètres**.

- 4 Sélectionnez **Sécurité**, puis 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 standard.

Par défaut, l'activation du mode promiscuité et des modifications d'adresse MAC pour le trafic entrant et sortant n'est pas acceptée.

Option	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 pour le 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	<ul style="list-style-type: none"> ■ Rejeter : Si vous configurez Modifications d'adresse MAC sur Rejeter et que le système d'exploitation invité modifie l'adresse MAC de l'adaptateur sur une valeur différente de l'adresse figurant dans le fichier de configuration de la machine virtuelle (.vmx), le commutateur ignore toutes les trames entrantes sur 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, le commutateur autorise le passage des trames vers la nouvelle adresse de l'adaptateur.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter : Le commutateur ignore toutes les trames entrantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration .vmx. ■ Accepter : Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

- 5 Cliquez sur **OK**.

Modifier l'exception de règle de sécurité de la couche 2 pour un groupe de ports standard dans Client Web vSphere

À l'aide de la règle de sécurité d'un groupe de ports, vous pouvez accepter ou rejeter le mode promiscuité et les modifications d'adresse MAC dans le système d'exploitation invité d'une machine virtuelle connectée au groupe.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste.
Le diagramme de la topologie du commutateur standard s'affiche.
- 4 Dans le diagramme de la topologie du commutateur standard, cliquez sur le nom du groupe de ports standard à configurer.
- 5 Cliquez sur **Modifier les paramètres**.

- 6 Dans la section **Sécurité**, cochez les cases en regard des règles de sécurité pour les remplacer et utilisez les menus déroulants pour configurer la sécurité du trafic des machines virtuelles via les ports du groupe.

Par défaut, l'activation du mode promiscuité et des modifications d'adresse MAC pour le trafic entrant et sortant n'est pas acceptée.

Option	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 pour le 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	<ul style="list-style-type: none"> ■ Rejeter : Si vous configurez Modifications d'adresse MAC sur Rejeter et que le système d'exploitation invité modifie l'adresse MAC de l'adaptateur sur une valeur différente de l'adresse figurant dans le fichier de configuration de la machine virtuelle (.vmx), le commutateur ignore toutes les trames entrantes sur 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, le commutateur autorise le passage des trames vers la nouvelle adresse de l'adaptateur.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter : Le commutateur ignore toutes les trames entrantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration .vmx. ■ Accepter : Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

- 7 Cliquez sur **OK**.

Modifier la règle de sécurité d'un groupe de ports distribués dans Client Web vSphere

Vous pouvez définir une règle de sécurité sur un groupe de ports distribués pour autoriser ou interdire l'activation du mode de promiscuité et les modifications d'adresse MAC pour le système d'exploitation invité d'une machine virtuelle associée au groupe de ports.

Vous pouvez également configurer une règle de sécurité pour chaque port distribué.

Procédure

- 1 Accédez à un commutateur distribué dans Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué et sélectionnez **Gérer les groupes de ports distribués**.
- 3 Cochez la case **Sécurité** et cliquez sur **Suivant**.
- 4 Sélectionnez le groupe de ports distribués à configurer et cliquez sur **Suivant**.

- 5 Modifiez les paramètres de sécurité du trafic acheminé via les ports du groupe à l'aide des menus déroulants, puis cliquez sur **Suivant**.

Par défaut, l'activation du mode promiscuité et des modifications d'adresse MAC pour le trafic entrant et sortant n'est pas acceptée.

Option	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 pour le 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	<ul style="list-style-type: none"> ■ Rejeter : Si vous configurez Modifications d'adresse MAC sur Rejeter et que le système d'exploitation invité modifie l'adresse MAC de l'adaptateur sur une valeur différente de l'adresse figurant dans le fichier de configuration de la machine virtuelle (.vmx), le commutateur ignore toutes les trames entrantes sur 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, le commutateur autorise le passage des trames vers la nouvelle adresse de l'adaptateur.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter : Le commutateur ignore toutes les trames entrantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration .vmx. ■ Accepter : Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

- 6 Passez vos paramètres en revue et cliquez sur **Terminer**.

Modifier les règles de sécurité de port distribué avec Client Web vSphere

Sur un port distribué, vous pouvez remplacer la règle héritée du groupe de ports distribués pour accepter ou rejeter le mode promiscuité et les modifications d'adresse MAC dans le système d'exploitation invité d'une machine virtuelle connectée au port.

Prérequis

Activer les remplacements au niveau du port. Reportez-vous à la section « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47

Procédure

- 1 Accédez à un commutateur distribué dans Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port de la liste.
- 4 Cliquez sur **Modifier les paramètres du port distribué**.

- 5 Cliquez sur **Sécurité** et activez la case à cocher des paramètres de trafic à remplacer via le port.

Par défaut, l'activation du mode promiscuité et des modifications d'adresse MAC pour le trafic entrant et sortant n'est pas acceptée.

Option	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 pour le 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	<ul style="list-style-type: none"> ■ Rejeter : Si vous configurez Modifications d'adresse MAC sur Rejeter et que le système d'exploitation invité modifie l'adresse MAC de l'adaptateur sur une valeur différente de l'adresse figurant dans le fichier de configuration de la machine virtuelle (.vmmx), le commutateur ignore toutes les trames entrantes sur 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, le commutateur autorise le passage des trames vers la nouvelle adresse de l'adaptateur.
Transmissions forgées	<ul style="list-style-type: none"> ■ Rejeter : Le commutateur ignore toutes les trames entrantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration .vmmx. ■ Accepter : Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.

- 6 Cliquez sur **OK**.

Règle de formation du 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 du 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.

Modifier la stratégie de formation du trafic d'un commutateur standard vSphere dans Client Web vSphere

ESXi permet de mettre en forme le trafic sortant sur des commutateurs standard. L'outil de mise en forme 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.

Une stratégie de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale.

Bande passante moyenne	Définit le nombre de bits moyen par seconde à autoriser sur un port dans le temps (charge moyenne autorisée).
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 quantité spécifiée par Bande passante moyenne , il peut être autorisé à 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 transférés à une vitesse plus élevée.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis sélectionnez **Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste et cliquez sur **Modifier les paramètres**.
- 4 Cliquez sur **Formation du trafic** et activez ou désactivez les exceptions des stratégies de formation du trafic avec le menu déroulant **Statut**.

Ici, la stratégie État est appliquée à chaque adaptateur VMkernel ou adaptateur réseau de machine virtuelle attaché au groupe de ports, et non pas au commutateur standard en tant que tel. Si vous activez l'exception de la stratégie de formation de trafic, vous limitez l'allocation de bande passante réseau pour chaque adaptateur VMkernel d'adaptateur réseau de machine virtuelle associé à ce groupe de ports particulier. Si vous désactivez la stratégie, les services bénéficient par défaut d'une connexion libre au réseau physique.

- 5 Entrez une valeur de bande passante pour chaque stratégie de formation du trafic (**Bande passante moyenne**, **Bande passante maximale** et **Ampleur du pic**).
- 6 Cliquez sur **OK**.

Modifier la règle de formation du trafic d'un groupe de ports standard dans Client Web vSphere

Utilisez les règles de formation du trafic pour contrôler la taille de la bande passante et des rafales sur un groupe de ports.

Prérequis

Activer les remplacements au niveau du port Reportez-vous à la section « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47

Procédure

- 1 Accédez à un hôte dans le navigateur Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Mise en réseau > Commutateurs virtuels**.
- 3 Sélectionnez un commutateur standard dans la liste.
Un schéma de l'infrastructure de commutation standard s'affiche.
- 4 Cliquez sur **Edit settings**.
- 5 Cliquez sur **Formation du trafic** et cochez la case **Remplacer** pour remplacer la politique de formation du trafic au niveau du groupe de ports standard et entrez les paramètres.

REMARQUE Si vous n'avez pas activé les remplacements au niveau des ports, les options ne sont pas disponibles.

Option	Description
Statut	Si vous activez l'exception à la règle dans le champ État , vous limitez l'allocation de bande passante réseau pour chaque carte virtuelle associée à ce groupes de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique.
Bande passante moyenne	Valeur mesurée sur une période de temps spécifique.
Bande passante maximale	Limite la bande passante maximale au cours de la rafale. Elle doit toujours être supérieure à la bande passante moyenne.
Taille de rafale	Spécifie la capacité d'une rafale en kilooctets (ko).

- 6 Cliquez sur **OK**.

Modifier la stratégie de formation du trafic d'un groupe de ports distribués dans Client Web vSphere

ESXi permet de configurer le trafic entrant et sortant dans les groupes de ports distribués vSphere. L'outil de mise en forme du trafic limite la bande passante réseau à la disposition d'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.

Une stratégie de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le navigateur et sélectionnez **Gérer groupes de ports distribués**.
- 3 Cochez la case **Formation du trafic** et cliquez sur **Suivant**.

- 4 Sur la page **Sélectionner groupe de ports**, sélectionnez un groupe de ports de la liste et cliquez sur **Suivant**.
- 5 Cliquez sur **Formation du trafic**, puis cochez la case **Remplacer** afin de remplacer la formation du trafic d'entrée et/ou celle du trafic de sortie.

REMARQUE 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
Statut	Si vous activez la Formation du trafic d'entrée ou la Formation du trafic de sortie en utilisant le menu déroulant État , vous limitez l'allocation de bande passante réseau pour chaque adaptateur VMkernel ou adaptateur réseau virtuel associé à ce groupe de ports particulier. Si vous désactivez la stratégie, les services bénéficient d'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 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 peut être autorisé à 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 transférés à une vitesse plus élevée.

- 6 Passez vos paramètres en revue et cliquez sur **Terminer**.
Utilisez le bouton **Précédent** pour modifier les paramètres.

Modifier la stratégie de formation du trafic d'un port distribué dans Client Web vSphere

ESXi permet de mettre en forme le trafic entrant et sortant dans les vSphere Distributed Switches. L'outil de mise en forme 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 du trafic de traverser le port à des vitesses plus élevées.

Une stratégie de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un commutateur distribué dans Client Web vSphere.
- 2 Pour accéder aux ports distribués du commutateur distribué, cliquez sur **Gérer > Ports**.
- 3 Sélectionnez un port de la liste.
- 4 Cliquez sur **Modifier les paramètres d'un port distribué**.

- 5 Cliquez sur **Formation du trafic**, puis cochez la case **Remplacer** afin de remplacer la formation du trafic d'entrée et/ou celle du trafic de sortie.

REMARQUE 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
Statut	Si vous activez la Formation du trafic d'entrée ou la Formation du trafic de sortie en utilisant le menu déroulant État , vous limitez l'allocation de bande passante réseau pour chaque adaptateur VMkernel ou adaptateur réseau virtuel associé à ce groupe de ports particulier. Si vous désactivez la stratégie, les services bénéficient d'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 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 peut être autorisé à 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 transférés à une vitesse plus élevée.

- 6 Vérifiez vos paramètres dans la section **Prêt à terminer** et cliquez sur **Terminer**.

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

Règle d'allocation des ressources

La règle 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 à la section « [Contrôle d'E/S réseau vSphere](#) », page 133.

Modifier la règle d'allocation des ressources d'un groupe de ports distribués dans Client Web vSphere

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.

Prérequis

Activez Network I/O Control sur l'hôte et créez un ou plusieurs pools de ressources réseau définis par l'utilisateur.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le navigateur et sélectionnez **Gérer groupes de ports distribués**.
- 3 Cochez la case **Allocation des ressources** et cliquez sur **Suivant**.

- 4 Sélectionnez le groupe de ports distribués à modifier 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.

Modifier la règle d'allocation des ressources d'un port distribué dans vSphere Web Client

Associez un port distribué à un pool de ressources réseau pour contrôler plus efficacement la bande passante affectée au port.

Prérequis

- Activez Network I/O Control sur l'hôte et créez un ou plusieurs pools de ressources réseau définis par l'utilisateur.
- Activer les remplacement au niveau du port. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port de la liste et cliquez sur **Modifier les paramètres du port distribué**.
- 4 Dans la section **Propriétés**, cochez la case **Remplacer** et ajoutez ou supprimez le port d'un pool de ressources réseau.

Si vous n'avez pas activé les remplacements au niveau du port, les options ne sont pas disponibles.

- Pour **Ajouter** le port distribué à un pool de ressources, sélectionnez un pool de ressources défini par un utilisateur à partir du menu déroulant **Pool de ressources réseau**.
 - Pour **supprimer** le groupe de ports distribué à partir d'un pool de ressources, sélectionnez **Par défaut** du menu déroulant **Pool de ressources réseau**.
- 5 Cliquez sur **OK**.

Règle 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 avec Client Web vSphere](#) », page 174.

Modifier la règle de surveillance d'un groupe de ports distribués dans Client Web vSphere

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

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué dans le navigateur d'objet et sélectionnez **Gérer groupes de ports distribués**.
- 3 Cochez la case **Surveiller** et cliquez sur **Suivant**.
- 4 Sélectionnez le groupe de ports distribués à modifier et cliquez sur **Suivant**.
- 5 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 de NetFlow au niveau de vSphere distributed switch. Reportez-vous à « Configurer les paramètres NetFlow avec Client Web vSphere », page 174.

- 6 Passez vos paramètres en revue et cliquez sur **Terminer**.
Utilisez le bouton **Précédent** pour modifier les paramètres.

Modifier la règle de surveillance d'un port distribué dans Client Web vSphere

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

Prérequis

Pour remplacer la règle de surveillance au niveau du port, activez les remplacements au niveau de port. Reportez-vous à la section « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port de la liste.
Les informations sur la configuration s'affiche au bas de l'écran.
- 4 Cliquez sur **Modifier les paramètres du port distribué**.
- 5 Cliquez sur **Surveillance** et cochez la case pour remplacer les paramètres NetFlow au niveau du groupe de ports.

- 6 Activer ou désactiver Netflow depuis le menu déroulant.

REMARQUE Si vous n'avez pas activé les remplacements au niveau du port, les options ne sont pas disponibles.

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 de NetFlow au niveau de vSphere distributed switch. Reportez-vous à « Configurer les paramètres NetFlow avec Client Web vSphere », page 174.

- 7 Cliquez sur OK.

Règle de filtrage et de balisage du trafic

Dans un vSphere Distributed Switch 5.5 ou version ultérieure, les règles 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 règles 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 règles 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.

Filtrage et balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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 balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 107

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.

- [Baliser le trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 107

Attribuez des balises prioritaires au trafic (par exemple, au trafic VoIP et au flux vidéo) nécessitant des capacités réseau supérieures en termes 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 d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 110

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 des règles de trafic réseau d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 111

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 balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 114

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 balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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.

REMARQUE Vous pouvez désactiver les règles 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 balisage du trafic sur un port distribué ou un port de liaison montante dans Client Web vSphere](#) », page 121.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 5 Cliquez sur **OK**.

Suivant

Configurez le filtrage et 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 à la section « [Baliser le trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) », page 107 et « [Filtrer le trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) », page 110.

Baliser le trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

Attribuez des balises prioritaires au trafic (par exemple, au trafic VoIP et au flux vidéo) nécessitant des capacités réseau supérieures en termes 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 client.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.
- 5 Cliquez sur **Nouveau** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.
- 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	Balisez le trafic correspondant à la règle à l'aide d'une balise de priorité CoS dans la couche 2 du réseau. Sélectionnez Mettre à jour la balise CoS et entrez une valeur entre 0 et 7.
Valeur DSCP	Balisez le trafic associé à la règle à l'aide d'une balise DSCP dans la couche 3 du réseau. Sélectionnez Mettre à jour la balise DSCP et entrez une valeur 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 de 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 termes 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 d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.
- 5 Cliquez sur **Nouveau** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.
- 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 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 de 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.

8 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Utilisation des règles de trafic réseau d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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.

REMARQUE Vous pouvez remplacer les règles de filtrage et balisage du trafic au niveau du port. Reportez-vous à la section « [Utilisation des règles du trafic réseau sur un port distribué ou un port de liaison montante dans Client Web vSphere](#) », page 118.

- [Afficher les règles du trafic d'un groupe de ports distribués ou d'un groupe de liaisons montantes dans Client Web vSphere](#) page 112

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 du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaisons montantes dans Client Web vSphere](#) page 112

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 des règles d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 113

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 du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere](#) page 113

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 du trafic d'un groupe de ports distribués ou d'un groupe de liaisons montantes dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.
- 5 Vérifiez l'option **Action** pour déterminer si la règle filtre le trafic (Autoriser ou Refuser) ou balise le trafic (Balise) ayant 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 du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaisons montantes dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.

- 5 Cliquez sur **Nouveau** pour créer une règle, ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.

Suivant

Attribuez un nom à la règle de trafic réseau, puis refusez, autorisez ou balisez le trafic cible.

Modifier les priorités des règles d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.
- 5 Sélectionnez une règle et utilisez les boutons fléchés pour modifier sa priorité.
- 6 Cliquez sur **OK** pour appliquer les modifications.

Supprimer une règle du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - 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 avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Si le filtrage et le balisage du trafic est désactivé, activez-le dans le menu déroulant **Statut**.
- 5 Sélectionnez la règle et cliquez sur **Supprimer**.
- 6 Cliquez sur **OK**.

Désactiver le filtrage et le balisage du trafic d'un groupe de ports distribués ou d'un groupe de ports de liaison montante dans Client Web vSphere

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.

REMARQUE Vous pouvez activer les règles 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 dans Client Web vSphere](#) », page 115.

Procédure

- 1 Recherchez un groupe de ports distribués ou un groupe de ports de liaison montante dans Client Web vSphere.
 - a Sélectionnez un commutateur distribué et cliquez sur l'onglet **Éléments associés**.
 - b Cliquez sur **Groupe de ports distribués** pour afficher la liste des groupes de ports distribués, ou cliquez sur **Groupe de ports de liaison montante** pour afficher la liste des groupes de ports de liaison montante.
- 2 Cliquez avec le bouton droit de sur le groupe de ports et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Filtrage et balisage du trafic**.
- 4 Dans le menu déroulant **Statut**, sélectionnez **Désactivé**.
- 5 Cliquez sur **OK**.

Filtrage et balisage du trafic sur un port distribué ou un port de liaison montante dans Client Web vSphere

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 dans Client Web vSphere](#) page 115
 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.
- [Baliser le trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 116
 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 d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 117
 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 du trafic réseau sur un port distribué ou un port de liaison montante dans Client Web vSphere](#) page 118

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 balisage du trafic sur un port distribué ou un port de liaison montante dans Client Web vSphere](#) page 121

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 dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un commutateur distribué dans Client Web vSphere.
- 2 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 3 Sélectionnez un port de la liste.
- 4 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 5 Sélectionnez **Filtrage et balisage du trafic**.
- 6 Cochez la case **Remplacer** et sélectionnez l'option **Activé** dans le menu déroulant **État**.
- 7 Cliquez sur **OK**.

Suivant

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 à la section « [Baliser le trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) », page 116 et « [Filtrer le trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) », page 117.

Baliser le trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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 client.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 5 Cliquez sur **Nouveau** pour créer une règle ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.

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	Balisez le trafic correspondant à la règle à l'aide d'une balise de priorité CoS dans la couche 2 du réseau. Sélectionnez Mettre à jour la balise CoS et entrez une valeur entre 0 et 7.
Valeur DSCP	Balisez le trafic associé à la règle à l'aide d'une balise DSCP dans la couche 3 du réseau. Sélectionnez Mettre à jour la balise DSCP et entrez une valeur 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 de 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.

Filtrer le trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.

- 4 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 5 Cliquez sur **Nouveau** pour créer une règle ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.

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 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 de 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.

- 8 Dans la boîte de dialogue de la règle, cliquez sur **OK** pour enregistrer la règle.

Utilisation des règles du trafic réseau sur un port distribué ou un port de liaison montante dans Client Web vSphere

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 du trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 119

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 d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 120

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 des règles d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 120

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 d'un port distribué ou d'un port de liaison montante dans Client Web vSphere](#) page 121

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 du trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Sélectionnez **Filtrage et balisage du trafic**.
- 5 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 6 Vérifiez l'option **Action** pour déterminer si la règle filtre le trafic (Autoriser ou Refuser) ou balise le trafic (Balise) ayant des demandes QoS spéciales.
- 7 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 d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Sélectionnez **Filtrage et balisage du trafic**.
- 5 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 6 Cliquez sur **Nouveau** pour créer une règle ou sélectionnez une règle et cliquez sur **Modifier** pour y apporter des modifications.

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.

Suivant

Attribuez un nom à la règle de trafic réseau, puis refusez, autorisez ou balisez le trafic cible.

Modifier les priorités des règles d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.

- 4 Sélectionnez **Filtrage et balisage du trafic**.
- 5 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 6 Sélectionnez une règle et utilisez les boutons fléchés pour modifier sa priorité.
- 7 Cliquez sur **OK** pour appliquer les modifications.

Supprimer une règle de trafic d'un port distribué ou d'un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.
- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Sélectionnez **Filtrage et balisage du trafic**.
- 5 Si le filtrage et le balisage du trafic n'est pas activé au niveau du port, cliquez sur **Remplacer** et, dans le menu déroulant **Statut**, sélectionnez **Activé**.
- 6 Sélectionnez la règle et cliquez sur **Supprimer**.
- 7 Cliquez sur **OK**.

Désactiver le filtrage et le balisage du trafic sur un port distribué ou un port de liaison montante dans Client Web vSphere

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.

Prérequis

Activez l'option des remplacements au niveau du port pour cette règle. Reportez-vous à « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47.

Procédure

- 1 Accédez à un port distribué ou un port de liaison montante.
 - Pour accéder aux ports distribués du commutateur, cliquez sur **Gérer > les ports**.
 - Pour accéder aux ports de liaison montante d'un groupe de ports de liaison montante, cliquez sur **Éléments associés > Groupes de ports de liaison montante**, double-cliquez sur un groupe de ports de liaison montante dans la liste et sélectionnez **Ports** dans l'onglet **Gérer**.
- 2 Sélectionnez un port de la liste.

- 3 Cliquez sur **Modifier les paramètres d'un port distribué**.
- 4 Sélectionnez **Filtrage et balisage du trafic**.
- 5 Cliquez sur **Remplacer** et sélectionnez **Désactivé** dans le menu déroulant **Statut**.
- 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 taper 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.

REMARQUE 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 5-1. 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 de caractère générique. Définissez des zéros à l'emplacement des bits de réseau et des uns 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 « **00:00:01:ff:ff:ff** ».

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 5-2. 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.

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 d'un groupe de ports distribués dans Client Web vSphere

Vous pouvez configurer plusieurs règles de groupe de ports distribués.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le navigateur d'objet et sélectionnez **Gérer groupes de ports distribués**.
- 3 Cochez la case **Divers** et cliquez sur **Suivant**.
- 4 Sélectionnez un groupe de ports distribués à modifier et cliquez sur **Suivant**.
- 5 Utilisez le menu déroulant **Bloquer tous les ports** pour sélectionner **Oui** ou **Non** et cliquez sur **Suivant**.

Choisir Oui arrête tous les ports dans le groupe de ports. Ceci risque de perturber les opérations normales du réseau des hôtes ou des machines virtuelles qui utilisent les ports.

- 6 Passez vos paramètres en revue et cliquez sur **Terminer**.
Utilisez le bouton **Précédent** pour modifier les paramètres.

Modifier les règles de blocage de port distribué ou de port de liaison montante avec Client Web vSphere

Vous pouvez configurer les règles de blocage de port distribué ou de port de liaison montante.

Prérequis

Pour remplacer la règle de formation de trafic au niveau du port, permettez les remplacements à niveau du port. Reportez-vous à la section « [Modifier les paramètres avancés d'un groupe de ports distribués avec Client Web vSphere](#) », page 47

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Ports**.
- 3 Sélectionnez un port de la liste.
- 4 Cliquez sur **Modifier les paramètres du port distribué**.
- 5 Dans la section **Divers**, sélectionnez le **Remplacement de blocage de port**, cocher la case et cliquez sur **Oui** ou **Non** sur le menu déroulant.

Sélectionner **Oui** arrête tous les ports dans le groupe de ports. Ceci risque de perturber les opérations normales du réseau des hôtes ou des machines virtuelles qui utilisent les ports.
- 6 Cliquez sur **OK**.

Gérer les stratégies de plusieurs groupes de ports sur un vSphere Distributed Switch dans Client Web vSphere

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

Prérequis

Créez un vSphere Distributed Switch avec un ou plusieurs groupes de ports.

Procédure

- 1 Accédez à un commutateur distribué dans le Client Web vSphere.
- 2 Cliquez avec le bouton droit sur le commutateur distribué et sélectionnez **Gérer les 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.

Option	Description
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. Cette option est disponible pour vSphere Distributed Switch 5.0 et versions ultérieures.
Surveillance	Activez ou désactivez NetFlow sur les groupes de ports sélectionnés. Cette option est disponible pour vSphere Distributed Switch 5.0.0 et versions ultérieures.
Filtrage et balisage du trafic	Configurez la stratégie de filtrage (autoriser ou annuler) et de balisage de certains types de trafic via les ports des groupes de ports sélectionnés. Cette option est disponible pour vSphere Distributed Switch 5.5 et versions ultérieures.
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. Un adaptateur invité en mode promiscuité n'a aucun effet sur la réception des trames qu'il reçoit. ■ Accepter. L'activation du mode promiscuité sur un adaptateur invité permet de détecter toutes les trames transmises au 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>.vmx</code>, toutes les trames entrantes sont abandonnées. Si le système d'exploitation invité remodifie l'adresse MAC pour qu'elle corresponde à celle figurant dans le fichier de configuration <code>.vmx</code>, les trames entrantes sont de nouveau transmises. ■ 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 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
Statut	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 stratégie, les services bénéficient d'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 dans le temps, c'est à dire la charge moyenne autorisée.

Option	Description
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.

- 7 (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.

- 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 de distribution. ■ 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 basculement de 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 adaptateurs 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.

Option	Description
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 font appel à l'équilibrage de charge réseau de Microsoft en 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>
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 attente. 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 de 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 du vSphere Distributed Switch.

- 11 (Facultatif) Sur la page Filtrage et balisage du trafic, activez ou désactivez le filtrage et le balisage du trafic dans le menu déroulant **Statut**, configurez les règles de trafic pour le filtrage ou le balisage de flux de données spécifiques, puis cliquez sur **Suivant**.

Vous pouvez définir les attributs suivants d'une règle déterminant le trafic cible et son action :

Option	Description
Nom	Nom de la règle
Action	<ul style="list-style-type: none"> ■ Autoriser. Autorisez l'accès à un certain type de trafic. ■ Annuler. Refusez l'accès à un certain type de trafic. ■ Balise. Classez le trafic en termes de qualité de service en insérant une balise ou en marquant à nouveau le trafic à l'aide d'une balise CoS et DSCP.

Option	Description
Direction de trafic	Indiquez si la règle concerne uniquement le trafic entrant ou sortant, ou les deux. Le sens influence aussi la manière dont vous allez identifier la source et la destination du trafic.
Qualificateur de trafic système	Indiquez que la règle concerne le trafic système et définissez le type de protocole d'infrastructure sur lequel appliquer la règle. Par exemple, marquez d'une balise de priorité le trafic à gérer dans vCenter Server.

Option	Description
Qualificateur MAC	<p>Qualifiez le trafic de la règle en fonction de l'en-tête de la couche 2.</p> <ul style="list-style-type: none"> ■ Type de protocole. Définissez le protocole de niveau suivant (IPv4, IPv6, etc.) consommant la charge utile. Cet attribut correspond au champ EtherType des trames Ethernet. Vous pouvez sélectionner un protocole dans le menu déroulant ou taper son code hexadécimal. Par exemple, pour localiser le trafic du protocole LLDP (Link Layer Discovery Protocol), tapez 88CC. ■ ID VLAN. Localisez le trafic par VLAN. 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 en mode VST (Virtual Switch Tagging), il est impossible de le localiser en utilisant cet ID dans une règle d'un groupe de ports distribués. 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. Pour réussir à faire correspondre le trafic à un ID VLAN, utilisez une règle d'un groupe de ports de liaison montante ou d'un port de liaison montante. ■ Filtre source. Définissez une adresse MAC unique ou un réseau MAC pour faire correspondre des paquets en fonction de l'adresse source. Pour un réseau MAC, entrez l'adresse la plus petite du réseau, ainsi qu'un masque générique. Le masque contient des 0 à l'emplacement des bits de réseau et des 1 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 « 00:00:01:ff:ff:ff ». ■ Filtre de destination. Définissez une adresse MAC unique ou un réseau MAC pour faire correspondre des paquets en fonction de l'adresse de destination. Le format pris en charge par l'adresse MAC de destination est le même que celui de l'adresse source.
Qualificateur IP	<p>Qualifiez le trafic de la règle en fonction de l'en-tête de la couche 3.</p> <ul style="list-style-type: none"> ■ Protocole. Définissez le protocole de niveau suivant (TCP, UDP, etc.) consommant la charge utile. Vous pouvez sélectionner un protocole dans le menu déroulant ou taper son code décimal en fonction de la <i>RFC 1700, Assigned Numbers</i>. Pour le protocole TCP et UDP, vous pouvez également définir le port source et le port de destination. ■ Port source. Faites correspondre les paquets TCP ou UDP à un port source. Tenez compte de la direction du trafic qui se trouve dans l'étendue de la règle lorsque vous déterminez le port source auquel faire correspondre des paquets. ■ Port de destination. Faites correspondre les paquets TCP ou UDP en fonction du port source. Tenez compte de la direction du trafic qui se trouve dans l'étendue de la règle lorsque vous déterminez le port de destination auquel faire correspondre des paquets. ■ Filtre source. Définissez la version IP, une adresse IP unique ou un sous-réseau pour faire correspondre les paquets en fonction de l'adresse source. Pour un sous-réseau, entrez la plus petite adresse et la longueur en bits du préfixe. ■ Filtre de destination. Définissez la version IP, une adresse IP unique ou un sous-réseau pour faire correspondre les paquets en fonction de l'adresse source. Le format pris en charge par l'adresse IP de destination est le même format que celui de l'adresse source.

- 12 (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

- 13 Passez en revue les paramètres sur la page Prêt à terminer et cliquez sur **Terminer**.

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

Gestion des ressources réseau

vSphere fournit différentes méthodes pour vous aider à gérer vos ressources réseau.

Ce chapitre aborde les rubriques suivantes :

- [« Contrôle d'E/S réseau vSphere », page 133](#)
- [« Délestage de segmentation TCP et trames Jumbo », page 137](#)
- [« NetQueue et performances réseau », page 140](#)
- [« DirectPath I/O », page 141](#)
- [« Virtualisation des E/S à racine unique \(SR-IOV\) », page 144](#)

Contrôle d'E/S réseau vSphere

Les pools de ressources réseau déterminent la bande passante accordée à différents types de trafics réseau sur un vSphere Distributed Switch.

Lorsque le contrôle d'E/S réseau est activé, le trafic du commutateur distribué est divisé dans les pools de ressources réseau prédéfinis suivants : Trafic de tolérance aux pannes, trafic iSCSI, trafic vMotion, trafic de gestion, trafic vSphere Replication (VR), trafic NFS et trafic de machine virtuelle.

Vous pouvez également créer des pools de ressources réseau personnalisés pour le trafic de machine virtuelle. Vous pouvez contrôler la bande passante affectée à chaque pool de ressources réseau en définissant les parts de carte physiques et les limites d'hôte de chaque pool de ressources réseau.

Les parts d'adaptateur physique assignées à un pool de ressources réseau déterminent la part de la bande passante disponible totale accordée au trafic associé au pool de ressources réseau. Le part de bande passante de transmission disponible pour un pool de ressources réseau dépend des partages du pool de ressources réseau et des données transmises par les autres pools de ressources réseau. Par exemple, si vous définissez vos pools de ressources du trafic FT et iSCSI à 100 parts, alors que chacun des autres pools de ressources est défini sur 50 partages, les pools de ressources du trafic FT et iSCSI reçoivent chacun 25 % de la bande passante disponible et les quatre pools de ressources restant. Les autres pools de ressources réseau reçoivent chacun 12,5 % de la bande passante disponible. Ces réservations s'appliquent uniquement lorsque la carte physique est saturée.

REMARQUE Les parts de pool de ressources de trafic iSCSI ne s'appliquent pas au trafic iSCSI d'un adaptateur iSCSI matérielle dépendante.

La limite d'hôte d'un pool de ressources réseau est la limite supérieure de bande passante que le pool de ressources réseau peut utiliser.

L'affectation d'une balise de priorité QoS à un pool de ressources réseau applique un balise 802.1p à tous les paquets sortants associés au pool de ressources réseau.

- [Activer Network I/O Control sur un vSphere Distributed Switch avec Client Web vSphere](#) page 134
Autorisez la gestion des ressources réseau pour donner les priorités du trafic réseau en fonction de son type à l'aide des pools de ressources réseau.
- [Créer un pool de ressources réseau avec Client Web vSphere](#) page 134
Créez des pools de ressources réseau définis par l'utilisateur pour la gestion personnalisée des ressources réseau.
- [Ajouter ou supprimer des groupes de ports distribués dans un pool de ressources réseau avec Client Web vSphere](#) page 135
Ajoutez un groupe de ports distribués à un pool de ressources réseau défini par l'utilisateur pour inclure dans le pool de ressources réseau tout le trafic réseau des machines virtuelles du groupe de ports distribués.
- [Modifier les paramètres de pool de ressources réseau avec Client Web vSphere](#) page 136
Vous pouvez changer les paramètres d'un pool de ressources réseau défini par l'utilisateur ou par le système pour changer la priorité du trafic réseau du pool de ressources réseau.
- [Supprimer un pool de ressources réseau défini par l'utilisateur avec Client Web vSphere](#) page 136
Vous pouvez supprimer les pools de ressources réseau définis par l'utilisateur qui ne sont plus utilisés.

Activer Network I/O Control sur un vSphere Distributed Switch avec Client Web vSphere

Autorisez la gestion des ressources réseau pour donner les priorités du trafic réseau en fonction de son type à l'aide des pools de ressources réseau.

Prérequis

Vérifiez que le centre de données dispose d'au moins un vSphere Distributed Switch 4.1.0 ou d'une version suivante.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres > Propriétés**.
- 3 Cliquez sur **Edit**.
- 4 Sélectionnez cette option pour **Activer** ou **Désactiver** Network I/O Control dans le menu déroulant **Network I/O Control**.
- 5 Cliquez sur **OK**.

Créer un pool de ressources réseau avec Client Web vSphere

Créez des pools de ressources réseau définis par l'utilisateur pour la gestion personnalisée des ressources réseau.

Les pools de ressources réseau définis par l'utilisateur sont disponibles uniquement dans les vSphere Distributed Switches version 5.0.0 et des versions suivantes.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, et cliquez sur **Allocation de ressources**
- 3 Cliquez sur **Nouveau**.
- 4 Entrez un **Nom** pour le pool de ressources réseau ou acceptez le nom généré.

- 5 (Facultatif) Entrez une **Description** du pool de ressources réseau.
- 6 Définissez **Limite hôte** pour le pool de ressources réseau en mégabits par seconde ou sélectionnez **Illimité**.
- 7 Sélectionnez les **Parts adaptateurs physiques** pour le pool de ressources réseau du menu déroulant.

Option	Description
Faible	Définit les parts pour ce pool de ressources sur 25.
Normal	Définit les parts pour ce pool de ressources sur 50.
Haut	Définit les parts pour ce pool de ressources sur 100.
Personnalisé	Un nombre spécifique de parts, de 1 à 100, pour ce pool de ressources réseau.

- 8 (Facultatif) Sélectionnez la **Balise QoS** du pool de ressources réseau.
 Cette balise de priorité QoS spécifie une balise IEEE 802.1p permettant d'appliquer la qualité de service au niveau du contrôle d'accès du support.
- 9 Cliquez sur **OK**.
 Le nouveau pool de ressources apparaît dans la section **Pool de ressources réseau défini par l'utilisateur**.

Suivant

Ajoutez un ou plusieurs groupes de ports distribués au pool de ressources réseau.

Ajouter ou supprimer des groupes de ports distribués dans un pool de ressources réseau avec Client Web vSphere

Ajoutez un groupe de ports distribués à un pool de ressources réseau défini par l'utilisateur pour inclure dans le pool de ressources réseau tout le trafic réseau des machines virtuelles du groupe de ports distribués.

Prérequis

Créez un ou plusieurs pools de ressources réseau définis par l'utilisateur dans vSphere Distributed Switch.

Procédure

- 1 Accédez à un commutateur distribué dans Client Web vSphere.
- 2 Cliquez avec le bouton droit de la souris sur le navigateur et sélectionnez **Gérer les groupes de ports distribués**.
- 3 Sur la page **Sélectionner les règles de groupe de ports**, cochez la case **Allocation des ressources** et cliquez sur **Suivant**.
- 4 Sur la page **Sélectionner les groupes de ports**, sélectionnez des groupes de ports à modifier et cliquez sur **Suivant**.
- 5 Sur la page **Règles de configuration - Allocation des ressources** ajoutez ou supprimez le commutateur distribué à partir du pool de ressources réseau et cliquez sur **Suivant**.
 - Pour **ajouter** le groupe de ports distribués à un pool de ressources, sélectionnez un pool de ressources défini par l'utilisateur à partir du **Pool de ressources réseau** dans le menu déroulant.
 - Pour **supprimer** le groupe de ports distribués à partir d'un pool de ressources, sélectionnez **par défaut** dans **Pool de ressources réseau** dans le menu déroulant.

REMARQUE S'il n'y a pas de pool de ressources défini par l'utilisateur sur le commutateur distribué, vous ne verrez que **par défaut** dans le menu déroulant.

- 6 Passez en revue les paramètres sur la page **Prêt à terminer** et cliquez sur **Terminer**.
Utilisez le bouton **Précédent** pour modifier vos sélections.

Modifier les paramètres de pool de ressources réseau avec Client Web vSphere

Vous pouvez changer les paramètres d'un pool de ressources réseau défini par l'utilisateur ou par le système pour changer la priorité du trafic réseau du pool de ressources réseau.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, et cliquez sur **Allocation de ressources**.
- 3 Sélectionnez un pool de ressources réseau de la liste et cliquez sur **Modifier**.
- 4 Définissez la **Limite hôte** pour le pool de ressources réseau en mégabits par seconde ou sélectionnez **Illimité**.
- 5 Vous pouvez changer les paramètres d'un pool de ressources réseau depuis le menu déroulant **Parts adaptateurs physiques**.

Option	Description
Faible	Définit les parts pour ce pool de ressources sur 25.
Normal	Définit les parts pour ce pool de ressources sur 50.
Haut	Définit les parts pour ce pool de ressources sur 100.
Personnalisé	Entrez un nombre spécifique de parts, de 1 à 100, pour ce pool de ressources réseau.

- 6 (Facultatif) Sélectionnez une **Balise QoS** du pool de ressources réseau.
Cette balise de priorité QoS spécifie une balise IEEE 802.1p permettant d'appliquer la qualité de service au niveau du contrôle d'accès du support.
- 7 Cliquez sur **OK**.

Supprimer un pool de ressources réseau défini par l'utilisateur avec Client Web vSphere

Vous pouvez supprimer les pools de ressources réseau définis par l'utilisateur qui ne sont plus utilisés.

REMARQUE Vous ne pouvez pas supprimer un pool de ressources du système réseau.

Prérequis

Supprimez tous les groupes de ports distribués du pool de ressources réseau.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, et cliquez sur **Allocation de ressources**.
- 3 Sélectionnez un pool d'allocation de ressources défini par l'utilisateur et cliquez sur **Supprimer**.
- 4 Cliquez sur **Oui** pour supprimer le pool de ressources.

Délestage de segmentation TCP et trames Jumbo

L'utilisation du délestage de segmentation TCP (TSO) dans un adaptateur réseau VMkernel et des machines virtuelles, et de trames Jumbo sur un vSphere Distributed Switch ou un commutateur standard vSphere, améliore les performances du réseau dans les charges de travail de machines virtuelles et d'infrastructure.

Activation du TSO (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.

TSO sur le chemin de transmission des cartes réseau physiques et de machine virtuelle améliore les performances des hôtes ESX/ESXi en réduisant la charge sur la CPU liée aux opérations réseau TCP/IP. Lorsque TSO est activée, la carte réseau divise les blocs de données volumineux en segments TCP au lieu de confier cette tâche à la CPU. L'hôte dispose alors d'un plus grand nombre de cycles CPU pour exécuter les applications.

Activer la prise en charge de TSO pour une machine virtuelle dans Client Web vSphere

L'activation de la prise en charge de TSO sur une machine virtuelle nécessite un adaptateur VMXNET amélioré.

Pour activer TSO au niveau de la machine virtuelle, vous devez remplacer les adaptateurs réseau virtuels flexibles ou VMXNET existants par des adaptateurs réseau virtuels VMXNET améliorés. Ce remplacement peut entraîner un changement d'adresse MAC de la carte réseau virtuelle.

Prérequis

Pour utiliser TSO, vérifiez que la machine virtuelle exécute l'un des systèmes d'exploitation invités suivants :

- Microsoft Windows Server 2003 Enterprise Edition avec Service Pack 2 (32 bits et 64 bits)
- Red Hat Enterprise Linux 4 (64 bits)
- Red Hat Enterprise Linux 5 (32 bits et 64 bits)
- SUSE Linux Enterprise Server 10 (32 bits et 64 bits)

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 3 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 4 Développez la section adaptateur réseau et notez les paramètres réseau et l'adresse MAC de l'adaptateur réseau.
- 5 Cliquez sur **Supprimer** pour supprimer la carte réseau de la machine virtuelle.
- 6 Dans le menu déroulant **Nouveau périphérique**, sélectionnez **Réseau** et cliquez sur **Ajouter**.
- 7 Dans le menu déroulant **Type d'adaptateur**, sélectionnez **VMXNET 2 (amélioré)** ou **VMXNET 3**.
- 8 Définissez le paramètre réseau et l'adresse MAC utilisés par l'ancien adaptateur réseau.
- 9 Cliquez sur **OK**.

Suivant

Si la machine virtuelle n'est pas configurée pour mettre à niveau VMware Tools à chaque mise sous tension, vous devez procéder manuellement à cette mise à niveau.

Activer le support TSO pour un adaptateur réseau VMkernel

Lors de l'utilisation du transfert de segments TCP (TSO) sur un adaptateur réseau VMkernel, la carte réseau physique fractionne les blocs de données volumineux en segments TCP à la place de la CPU. Ceci permet à la CPU de disposer de davantage de cycles pour les applications. Par défaut, un hôte est configuré pour utiliser le TSO matériel si ses cartes réseau le prennent en charge.

Si TSO est désactivé pour un adaptateur VMkernel, le seul moyen de le réactiver consiste à supprimer l'adaptateur, puis à le recréer et à activer TSO sur celui-ci.

Prérequis

Vérifiez si l'une des conditions suivantes est remplie :

- L'adaptateur VMkernel ne gère pas le trafic lié aux services de mise en réseau d'hôte du type iSCSI, vSphere vMotion, etc.
- Les services de mise en réseau peuvent envoyer du trafic à l'aide d'un adaptateur VMkernel alternatif.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **Adaptateurs VMkernel**.
- 3 Sélectionnez un adaptateur VMkernel dans la liste et notez ses paramètres.
Vous devrez définir les mêmes paramètres pour l'adaptateur VMkernel que vous allez créer.
- 4 Cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue de confirmation, cliquez sur **Analyser l'impact**, vérifiez qu'aucun service de mise en réseau n'est touché, puis cliquez sur **OK**.
- 6 Dans la liste des adaptateurs VMkernel, cliquez sur **Ajouter la mise en réseau d'un hôte**.
- 7 Dans la page Ajouter un type de connexion, sélectionnez **Adaptateur réseau VMkernel**, puis cliquez sur **Suivant**.
- 8 Dans la page Sélectionner un périphérique cible, attribuez l'adaptateur VMkernel à un commutateur standard ou à un groupe de ports distribués.
- 9 Dans la page Propriétés du port, configurez la version IP et les services de mise en réseau associés à l'ancien adaptateur, puis cliquez sur **Suivant**.
- 10 Sur les pages Paramètres IPv4 et Paramètres IPv6, configurez les paramètres IP utilisés par l'ancien adaptateur.
- 11 Passez vos paramètres en revue et cliquez sur **Terminer**.

Activation de 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 avec Client Web vSphere

Activez les trames Jumbo pour l'ensemble du trafic passant par un vSphere Distributed Switch.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres > Propriétés**.
- 3 Cliquez sur **Edit**.
- 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 vSphere standard avec Client Web vSphere

Activer les trames Jumbo pour l'ensemble du trafic via un commutateur vSphere standard sur un hôte.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau**, puis 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 des trames Jumbo pour un adaptateur VMkernel dans Client Web vSphere

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 Client Web vSphere, accédez à l'hôte.
- 2 Dans **Gérer**, sélectionnez **Mise en réseau**, puis **Adaptateurs VMkernel**.
- 3 Sélectionnez un adaptateur VMkernel dans la table des adaptateurs.
Les propriétés de l'adaptateur s'affichent.
- 4 Cliquez sur le nom de l'adaptateur VMkernel.
- 5 Cliquez sur **Edit**.
- 6 Sélectionnez **Paramètres de carte réseau** et définissez une valeur supérieure à 1 500 pour le paramètre **MTU**.
La valeur de l'unité de transmission maximale (MTU) peut aller jusqu'à 9 000 octets.

- 7 Cliquez sur **OK**.

Activer la prise en charge de trames Jumbo sur une machine virtuelle dans Client Web vSphere

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 Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 3 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 4 Cliquez sur la section **Matériel virtuel**, et développez la section adaptateur réseau. Enregistrez les paramètres réseau et l'adresse MAC utilisés par la carte réseau.
- 5 Cliquez sur **Supprimer** pour supprimer la carte réseau de la machine virtuelle.
- 6 Dans le menu déroulant **Nouveau périphérique**, sélectionnez **Réseau** et cliquez sur **Ajouter**.
- 7 Dans le menu déroulant **Type d'adaptateur**, sélectionnez **VMXNET 2 (amélioré)** ou **VMXNET 3**.
- 8 Définissez les paramètres du réseau sur ceux enregistrés pour l'ancienne carte réseau.
- 9 Définissez l'**Adresse MAC** sur **Manuel**, puis saisissez l'adresse MAC utilisée par l'ancien adaptateur réseau.
- 10 Cliquez sur **OK**.

Suivant

- 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 client, configurez la carte réseau de sorte 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.

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.

Activer NetQueue sur un hôte

NetQueue est activé par défaut. Pour pouvoir utiliser NetQueue, vous devez le réactiver s'il a été désactivé.

Prérequis

Prenez connaissance des informations sur la configuration des pilotes NIC dans *Initiation aux interfaces de ligne de commande vSphere*.

Procédure

- 1 Dans l'interface de ligne de commande VMware vSphere, utilisez la commande suivante, en fonction de la version de l'hôte :

Version d'ESX/ESXi	Commande
ESX/ESXi 4.x	<code>vicfg-advcfg --set true VMkernel.Boot.netNetQueueEnable</code>
ESXi 5.x	<code>esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"</code>

- 2 Utilisez l'interface de ligne de commande VMware vSphere afin de configurer le pilote NIC pour pouvoir utiliser NetQueue.
- 3 Redémarrez l'hôte.

Désactiver NetQueue sur un hôte

NetQueue est activé par défaut.

Prérequis

Prenez connaissance des informations sur la configuration des pilotes NIC dans *Initiation aux interfaces de ligne de commande vSphere*.

Procédure

- 1 Dans l'interface de ligne de commande VMware vSphere, utilisez la commande suivante, en fonction de la version de l'hôte :

Version d'ESX/ESXi	Commande
ESX/ESXi 4.x	<code>vicfg-advcfg --set false VMkernel.Boot.netNetQueueEnable</code>
ESXi 5.x	<code>esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"</code>

- 2 Pour désactiver NetQueue sur le pilote NIC, utilisez la commande `vicfg-module -s "" module name`. Par exemple, si vous servez du pilote s2io NIC, utilisez `vicfg-module -s "" s2io`.
- 3 Redémarrez l'hôte.

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

Les systèmes UCS (Cisco Unified Computing Systems), via les commutateurs distribués Cisco Virtual Machine Fabric Extender (VM-FEX), prennent en charge les fonctions suivantes de migration et de gestion des ressources des machines virtuelles utilisant DirectPath I/O :

- vMotion
- Retrait ou ajout à chaud de périphériques virtuels
- Interruption et reprise
- Haute disponibilité
- DRS
- Snapshots

Consultez la documentation de Cisco VM-FEX pour plus de détails sur les commutateurs compatibles et pour obtenir des informations sur la configuration des commutateurs.

- [Activer un relais pour un périphérique réseau sur un hôte dans Client Web vSphere](#) page 142

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 avec Client Web vSphere](#) page 143

Les périphériques de relais peuvent fournir les moyens d'utiliser plus efficacement les ressources et d'améliorer la performances de votre environnement. Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle dans Client Web vSphere.

- [Activer DirectPath I/O avec vMotion sur une machine virtuelle avec Client Web vSphere](#) page 143

Vous pouvez activer DirectPath I/O avec vMotion sur les machines virtuelles d'un centre de données d'un système Cisco UCS qui dispose d'au moins un commutateur distribué VM-FEX Cisco UCS compatible.

Activer un relais pour un périphérique réseau sur un hôte dans Client Web vSphere

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.



AVERTISSEMENT 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 Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans la section Matériel, cliquez sur **Périphériques PCI**.
- 4 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.

- 5 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.
- 6 Redémarrez l'hôte pour mettre à disposition le périphérique réseau PCI.

Configurer un périphérique PCI sur une machine virtuelle avec Client Web vSphere

Les périphériques de relais peuvent fournir les moyens d'utiliser plus efficacement les ressources et d'améliorer la performances de votre environnement. Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle dans Client Web vSphere.

Prérequis

Vérifiez qu'un périphérique de relais de mise en réseau soit configuré sur l'hôte de la machine virtuelle. Reportez-vous à « [Activer un relais pour un périphérique réseau sur un hôte dans Client Web vSphere](#) », page 142.

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 4 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 5 Développez la section **Mémoire** et établissez la **Limite** sur **Illimité**
- 6 Dans le menu déroulant **Nouveau périphérique**, sélectionnez **Périphérique PCI** et cliquez sur **Ajouter**.
- 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.

L'ajout d'un périphérique DirectPath à une machine virtuelle configure la réservation de mémoire sur la taille de mémoire de la machine virtuelle.

Activer DirectPath I/O avec vMotion sur une machine virtuelle avec Client Web vSphere

Vous pouvez activer DirectPath I/O avec vMotion sur les machines virtuelles d'un centre de données d'un système Cisco UCS qui dispose d'au moins un commutateur distribué VM-FEX Cisco UCS compatible.

Prérequis

Activez les E/S réseau à haute performance sur au moins un profil de port Cisco UCS d'un commutateur distribué Cisco VM-FEX compatible. Pour des commutateurs pris en charge et leur configuration, consultez la documentation sur le site Web de Cisco. [Http://www.cisco.com/go/unifiedcomputing/b-series-doc](http://www.cisco.com/go/unifiedcomputing/b-series-doc)

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.
- 3 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 4 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 5 Développez la section **Mémoire** et établissez la **Limite** sur **Illimité**
- 6 Développez la section **Adaptateur réseau** pour configurer un périphérique de relais.
- 7 Dans le menu déroulant de réseau, sélectionnez un profil de port à haute performance, puis cliquez sur **OK**.
- 8 Mettez la machine virtuelle sous tension.

Virtualisation des E/S à racine unique (SR-IOV)

vSphere 5.1 et les versions ultérieures prennent 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](#) », page 145.

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 de la CPU.

Dans vSphere 5.5 et versions ultérieures, 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 5.1 et les versions ultérieures prennent 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 5.5, votre environnement doit répondre à un certain nombre d'exigences de configuration.

Tableau 6-1. Configurations prises en charge pour l'utilisation de SR-IOV

Composant	Exigences
vSphere	<ul style="list-style-type: none"> ■ Les hôtes équipés de processeurs Intel nécessitent ESXi 5.1 ou une version ultérieure. ■ Les hôtes équipés de processeurs AMD sont pris en charge avec SR-IOV dans ESXi 5.5 ou une version ultérieure.
Hôte physique	<ul style="list-style-type: none"> ■ Doit être compatible avec la version d'ESXi. ■ Doit être équipé d'un processeur Intel si vous exécutez ESXi 5.1, ou d'un processeur Intel ou AMD si vous exécutez ESXi 5.5 et versions ultérieures. ■ 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.
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.

Tableau 6-1. Configurations prises en charge pour l'utilisation de SR-IOV (suite)

Composant	Exigences
SE client	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.x ■ Windows Server 2008 R2 avec SP2
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 relai SR-IOV

REMARQUE Les tentatives d'activation ou de configuration des fonctionnalités non prises en charge par SR-IOV dans Client Web vSphere 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. Les cartes réseau suivantes sont prises en charge pour les machines virtuelles configurées avec SR-IOV :

- Les produits basés sur la famille de contrôleurs Ethernet Intel 82599ES 10 Gigabits (Niantic)

- Les produits basés sur la famille de contrôleurs Ethernet Intel X540 (Twinville)
- Emulex OneConnect (BE3)

Mise à niveau à partir de vSphere 5.0 et versions antérieures

Si vous effectuez une mise à niveau de vSphere 5.0 ou version antérieure vers vSphere 5.5 ou version ultérieure, la prise en charge de SR-IOV sera disponible uniquement lorsque vous aurez effectué une mise à jour des pilotes de carte réseau pour la version de vSphere. Pour que la fonctionnalité SR-IOV puisse fonctionner, les microprogrammes et les pilotes prenant en charge SR-IOV doivent être activés pour les cartes réseau.

Mise à niveau à partir de vSphere 5.1

Bien que SR-IOV soit pris en charge sur les hôtes ESXi 5.1 qui répondent aux exigences, vous ne pouvez pas configurer SR-IOV sur ces derniers à l'aide de Client Web vSphere. Pour activer SR-IOV sur ces hôtes, utilisez le paramètre `max_vfs` du module du pilote de carte réseau. Reportez-vous à la section « [Activation de SR-IOV en utilisant des profils d'hôte dans Client Web vSphere ou via une commande ESXCLI](#) », page 153.

Vous ne pouvez pas non plus attribuer un adaptateur de relais SR-IOV à une machine virtuelle sur un tel hôte. L'adaptateur est disponible pour les machines virtuelles compatibles avec ESXi 5.5 et versions ultérieures. Bien que la version 5.5 de vCenter Server puisse gérer un hôte ESXi 5.1, la configuration est la même que dans la version 5.1. Vous devez ajouter un périphérique PCI au matériel de la machine virtuelle et sélectionner manuellement une fonction virtuelle pour le périphérique.

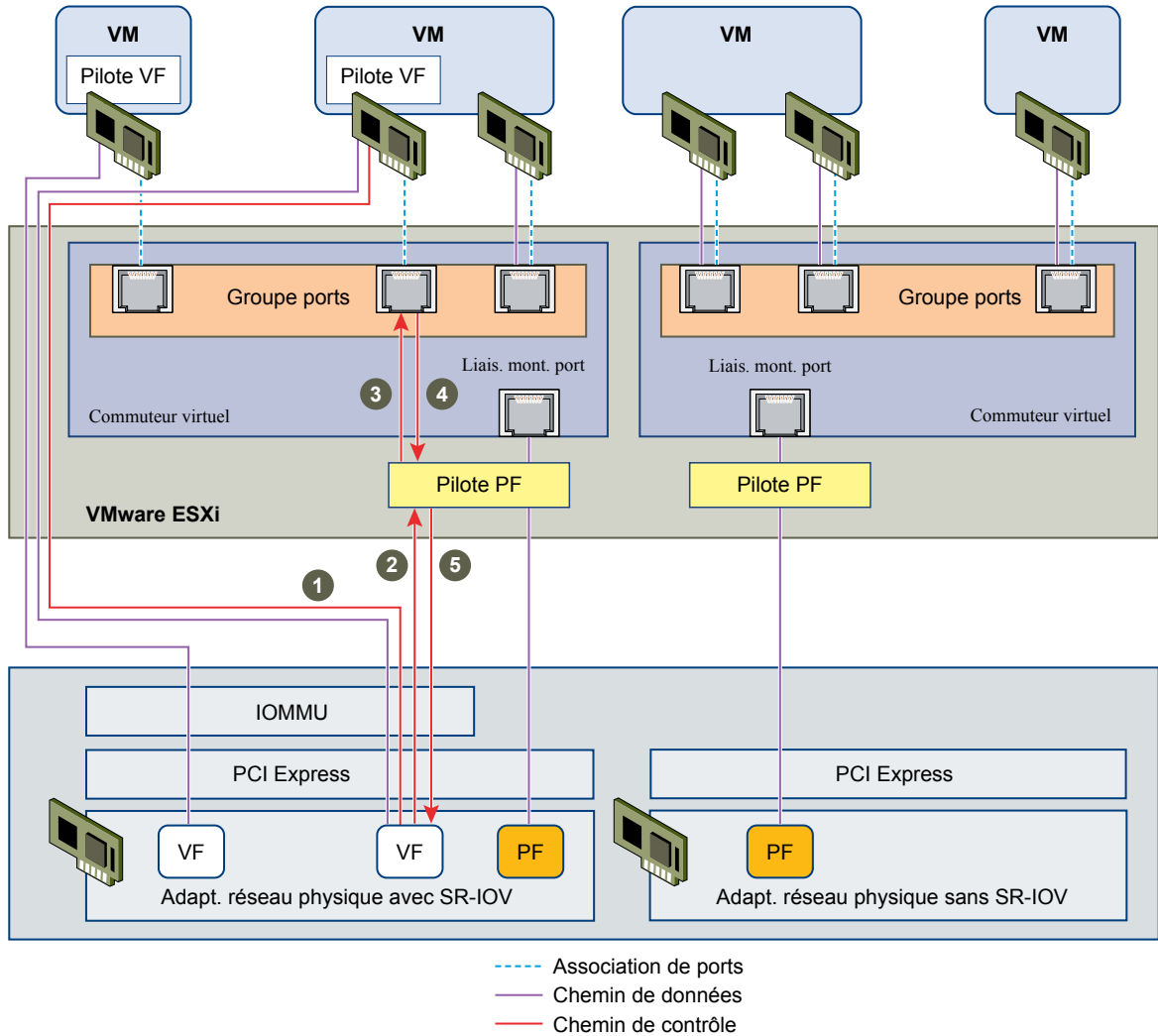
Architecture et interaction des composants SR-IOV

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 de machines virtuelles en plus des adaptateurs physiques SR-IOV, les adaptateurs des machines virtuelles 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 6-1. Chemins de données et de configuration de la prise en charge SR-IOV de vSphere



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. En conséquence, le système d'exploitation invité et le périphérique virtuel enregistrent des adresses MAC différentes. 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.

- 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.

Chaque hôte ESXi dispose d'un total de 256 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 256 vecteurs. Si ces périphériques nécessitent plus de 128 vecteurs, le nombre maximal de fonctions virtuelles potentiellement prises en charge est réduit.

Par exemple, sur les 64 fonctions virtuelles pouvant être instanciées sur une carte réseau Intel, l'hôte peut en utiliser un maximum de 43 à des fins de relais ($128 / 3 = 42,6$) si les 128 vecteurs d'interruption sont tous disponibles.

- 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 128 vecteurs d'interruption sont tous disponibles à des fins de relais :

$$3X + 2Y < 128$$

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 de 128 vecteurs d'interruption parmi les 256 vecteurs sur l'hôte.

- vSphere SR-IOV prend en charge jusqu'à 43 VF sur les cartes réseau Intel prises en charge et jusqu'à 64 VF sur les cartes réseau Emulex prises en charge.
- Si une carte réseau Intel prise en charge perd sa connexion, toutes les VF provenant de la carte réseau physique arrêtent toute communication, notamment entre les VF.

- Si une carte réseau Emulex prise en charge perd sa connexion, toutes les VF cessent de communiquer avec l'environnement externe, mais la communication entre les VF 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 dans Client Web vSphere

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.

Prérequis

Vérifiez que la configuration de votre environnement prend SR-IOV en charge. Consultez « [Prise en charge SR-IOV](#) », page 145.

Procédure

- 1 [Activer SR-IOV sur un adaptateur physique hôte dans Client Web vSphere](#) page 151
Avant de pouvoir connecter des machines virtuelles aux fonctions virtuelles, utilisez Client Web vSphere 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 à l'aide de Client Web vSphere](#) page 151
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.

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 désigne les adaptateurs de machine virtuelle qui utilisent des fonctions virtuelles avec l'icône .

Suivant

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](#) », page 152.

Activer SR-IOV sur un adaptateur physique hôte dans Client Web vSphere

Avant de pouvoir connecter des machines virtuelles aux fonctions virtuelles, utilisez Client Web vSphere pour activer SR-IOV et définissez le nombre de fonctions virtuelles sur votre hôte.

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **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.
- 6 Cliquez sur **OK**.
- 7 Redémarrez l'hôte.

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.

Suivant

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 à l'aide de Client Web vSphere

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.

Prérequis

- 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 Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Mettez la machine virtuelle hors tension.

- 3 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 4 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 5 Dans le menu déroulant **Nouveau périphérique**, sélectionnez **Réseau** et cliquez sur **Ajouter**.
- 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.

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 5.5 et versions ultérieures, vous pouvez configurer certaines fonctions 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 6-2. 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 5.5 (et versions ultérieures), 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 est indiqué par la présence de l'icône  soit dans la liste des adaptateurs physiques (pour un commutateur standard), soit dans la liste des adaptateurs de groupe de liaisons montantes (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. Si tel est le cas, l'adaptateur physique se trouve dans une liste séparée nommée Adaptateurs SR-IOV externes, à côté de 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.

Activation de SR-IOV en utilisant des profils d'hôte dans Client Web vSphere ou via 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 à l'aide de Client Web vSphere

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 vSphere*.

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 de plus amples informations concernant les commandes vCLI, consultez la *Documentation de l'interface de ligne de commande vSphere*.

Prérequis

- Vérifiez que la configuration de votre environnement prend SR-IOV en charge. Consultez « [Prise en charge SR-IOV](#) », page 145.
- 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 de Client Web vSphere, cliquez sur **Règles et Profils > Profils d'hôte**.
- 2 Sélectionnez un profil d'hôte dans la liste et cliquez sur l'onglet **Gérer**.
- 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`.

REMARQUE 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.

Les fonctions virtuelles s'affichent dans la liste des périphériques PCI dans l'onglet **Paramètres** de l'hôte.

Suivant

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 à l'aide de Client Web vSphere](#) », page 151.

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.

Prérequis

Installez le package vCLI, déployez la machine virtuelle vMA (vSphere Management Assistant) ou utilisez Shell ESXi. Reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

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.

Suivant

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 à l'aide de Client Web vSphere](#) », page 151.

Une machine virtuelle qui utilise une fonction virtuelle SR-IOV est mise hors tension, 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, une ou plusieurs machines virtuelles qui utilisent des fonctions virtuelles SR-IOV pour la mise en réseau sont mises hors tension 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
AVERTIS: IntrVector: 233: Out of interrupt vectors
```

Cause

Chaque hôte ESXi dispose d'un total de 256 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 256 vecteurs. Si ces périphériques nécessitent plus de 128 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 méthode pour 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.

Gestion des adresses MAC

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 aborde les rubriques suivantes :

- [« Attribution d'adresses MAC depuis vCenter Server », page 157](#)
- [« Génération d'adresse MAC sur des hôtes ESXi », page 161](#)
- [« Définition d'une adresse MAC statique pour une machine virtuelle », page 162](#)

Attribution d'adresses MAC depuis vCenter Server

vSphere 5.1 et les versions ultérieures offrent 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.

REMARQUE 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 de VMware OUI correspond au modèle d'attribution par défaut d'adresses MAC 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 modèle d'allocation de VMware OUI, le format d'une adresse MAC est `00:50:56:XX:YY:ZZ` où `00:50:56` représente le préfixe VMware OUI, `XX` est calculé selon la formule $(80 + \text{ID de vCenter Server})$ et `YY` et `ZZ` sont des nombres hexadécimaux à deux chiffres aléatoires.

Les adresses créées via l'allocation de VMware OUI sont comprises entre `00:50:56:80:YY:ZZ` et `00:50:56:BF:YY:ZZ`.

Allocation d'adresse MAC par préfixe

Sur les hôtes ESXi 5.1 et versions ultérieures, vous pouvez utiliser l'allocation par préfixe pour spécifier un identificateur OUI autre que celui utilisé par défaut `00:50:56` 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 se base sur les préfixes pour éviter les problèmes de duplication d'adresses MAC. Consultez la documentation de *Dépannage vSphere*.

Allocation d'adresse MAC basée sur plage

Sur les hôtes ESXi 5.1 et versions ultérieures, 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 disposant toujours d'adresses disponibles. vCenter Server vérifie l'absence de conflits d'adresses MAC dans ses plages.

Lors d'une utilisation d'une allocation basée sur plage, vous devez fournir plusieurs instances de vCenter Server avec des plages qui ne se chevauchent pas. vCenter Server ne détecte pas les plages qui peuvent entrer en conflit avec des plages utilisées par d'autres instances de vCenter Server. Pour plus d'informations sur la résolution des problèmes d'adresses MAC en double, reportez-vous à la documentation *Dépannage vSphere*.

Attribution d'une adresse MAC

Utilisez Client Web vSphere 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 Client Web vSphere. 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 dans Client Web vSphere

En basculant des OUI VMware par défaut vers l'allocation d'adresse MAC basée sur préfixe ou sur plage via Client Web vSphere, 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 Client Web vSphere.

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 », page 160.

REMARQUE Vous devez utiliser l'allocation d'adresses MAC par préfixe dans les hôtes vCenter Server 5.1 et ESXi 5.1, et versions ultérieures.

Si une instance vCenter Server 5.1 gère des hôtes qui exécutent des versions ESXi antérieures à ESXi 5.1, utilisez l'allocation d'adresses MAC par préfixe VMware OUI. Les machines virtuelles auxquelles sont attribuées des adresses MAC sans préfixe VMware OUI ne peuvent pas être mises sous tension sur les hôtes dont la version est antérieure à la version 5.1. Ces hôtes vérifient explicitement si une adresse MAC attribuée utilise le préfixe VMware OUI 00:50:56.

Procédure

- 1 Accédez à un vCenter Server dans Client Web vSphere
- 2 Cliquez sur l'onglet **Gérer**, puis sélectionnez **Paramètres > Paramètres avancés**.
- 3 Cliquez sur **Edit**.

- 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 entraînent des adresses MAC de vNIC 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 OK.

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.

Prérequis

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](#) », page 157

Procédure

- 1 Sur la machine hôte de vCenter Server, accédez au répertoire qui contient le fichier de configuration :
 - Sur un système d'exploitation Windows Server, l'emplacement du répertoire est `vCenter Server home directory\Application Data\VMware\VMware VirtualCenter`.
 - Sur vCenter Server Appliance, l'emplacement du répertoire est `/etc/vmware-vpx`.
- 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.

REMARQUE Utilisez un seul type d'allocation.

◆ Allocation de VMware OUI

```
<vpzd>
  <macAllocScheme>
    <VMwareOUI>true</VMwareOUI>
  </macAllocScheme>
</vpzd>
```

◆ allocation basée sur préfixe

```
<vpzd>
  <macAllocScheme>
    <prefixScheme>
      <prefix>005026</prefix>
      <prefixLength>23</prefixLength>
    </prefixScheme>
  </macAllocScheme>
</vpzd>
```

◆ allocation basée sur plage

```
<vpzd>
  <macAllocScheme>
    <rangeScheme>
      <range id="0">
        <begin>005067000001</begin>
        <end>005067000001</end>
      </range>
    </rangeScheme>
  </macAllocScheme>
</vpzd>
```

- 4 Enregistrez le `vpzd.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 pour 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.

REMARQUE Assurez-vous qu'aucun autre périphérique non-VMware n'utilise les adresses attribuées à des 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 Restrictions.

Si vous choisissez d'utiliser l'identificateur VMware OUI, une partie de la plage est déjà réservée pour être utilisée par vCenter Server, les cartes réseau physiques de l'hôte, les cartes réseau virtuelles et en vue d'une utilisation future.

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 à l'aide de Client Web vSphere

Vous pouvez attribuer des adresses MAC statiques à la carte réseau virtuelle d'une machine virtuelle hors tension à l'aide de Client Web vSphere.

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Désactivez la machine virtuelle.
- 3 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres > Matériel VM**.
- 4 Cliquez sur **Modifier** et sélectionnez l'onglet **Matériel virtuel**.
- 5 Dans l'onglet **Matériel virtuel**, développez la section adaptateur 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 Client Web vSphere.

Procédure

- 1 Localisez la machine virtuelle dans Client Web vSphere.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, puis cliquez sur l'onglet **Objets associés**
 - b Cliquez sur **Machines virtuelles** et sélectionnez la machine virtuelle dans la liste.
- 2 Désactivez la machine virtuelle.
- 3 Dans l'onglet **Gérer** de la machine virtuelle, sélectionnez **Paramètres**.
- 4 Dans l'onglet **Options VM**, développez **Avancé**.
- 5 Cliquez sur **Modifier la configuration**.
- 6 Pour attribuer une adresse MAC statique, ajoutez ou modifiez les paramètres requis.

Paramètre	Valeur
ethernetX.addressType	statique
ethernetX.address	MAC_address_of_the_virtual_NIC

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.

Mise en réseau avancée

Les options de configuration de mise en réseau avancée vous permettent de mieux contrôler votre environnement réseau vSphere.

Ce chapitre aborde les rubriques suivantes :

- [« Activer ou désactiver la prise en charge d'IPv6 sur un hôte à l'aide de Client Web vSphere », page 165](#)
- [« Utilisation de la mise en miroir de ports », page 166](#)
- [« Configurer les paramètres NetFlow avec Client Web vSphere », page 174](#)
- [« Switch Discovery Protocol », page 174](#)
- [« Montage de volumes NFS », page 176](#)
- [« Récupération et restauration de mise en réseau », page 176](#)
- [« Configurer les profils de protocole pour la mise en réseau des machines virtuelles », page 180](#)
- [« Déploiement de réseau sans état », page 184](#)

Activer ou désactiver la prise en charge d'IPv6 sur un hôte à l'aide de Client Web vSphere

La prise en charge d'IPv6 dans vSphere permet aux hôtes de fonctionner dans un réseau IPv6 disposant d'un très large espace d'adresses, d'une multidiffusion améliorée, d'un routage simplifié, etc.

IPv6 est désigné par le groupe de travail IETF comme le successeur de IPv4. Le bénéfice le plus évident d'IPv6 par rapport à IPv4 est la longueur de l'adresse. L'IPv6 utilise des adresses 128 bits plutôt que des adresses 32 bits utilisées par IPv4. Cette augmentation résout le problème d'épuisement d'adresses et élimine la conversion d'adresse réseau. Les autres différences incluent les adresses locales du lien qui apparaissent lors de l'initialisation de l'interface, les adresses définies par les annonces de routeur et la possibilité de disposer de plusieurs adresses IPv6 dans une interface.

Dans ESXi 5.1 et versions ultérieures, IPv6 est activé par défaut.

Prérequis

Privilège nécessaire : **Configuration.de l'hôte.Configuration.réseau.**

Procédure

- 1 Dans Client Web vSphere, accédez à l'hôte.
- 2 Dans l'onglet **Gérer**, cliquez sur **Mise en réseau** et sélectionnez **Avancé**.
- 3 Cliquez sur **Edit**.

- 4 Dans le menu déroulant **Support IPv6**, activez ou désactivez le support IPv6.
- 5 Cliquez sur **OK**.
- 6 Redémarrez l'hôte pour appliquer les modifications dans la prise en charge d'IPv6.

Suivant

Configurez les paramètres IPv6 des adaptateurs VMkernel, par exemple, du réseau de gestion. Reportez-vous à la section « [Modifier la configuration d'un adaptateur VMkernel dans Client Web vSphere](#) », page 79.

Utilisation 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 port est utilisée sur un commutateur pour envoyer une copie des paquets affichés sur un port de commutateur (ou l'intégralité d'un 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.

Compatibilité de version de mise en miroir

Certaines fonctionnalités de mise en miroir de port dans vSphere 5.1 et versions ultérieures dépendent de la version de vCenter Server, de vSphere Distributed Switch et de l'hôte que vous utilisez, ainsi que de la façon dont vous utilisez ces aspects de vSphere ensemble.

Tableau 8-1. Compatibilité de mise en miroir

Version de vCenter Server	Version de vSphere Distributed Switch	Version de l'hôte	Fonctionnalité de mise en miroir de port vSphere 5.1
vSphere 5.1 et versions ultérieures	vSphere 5.1 et versions ultérieures	vSphere 5.1 et versions ultérieures	La mise en miroir de port vSphere 5.1 est disponible et peut être utilisée. Les fonctionnalités pour la mise en miroir de port vSphere 5.0 et de version antérieure ne sont pas disponibles.
vSphere 5.1 et versions ultérieures	vSphere 5.1 et versions ultérieures	vSphere 5.0 et version antérieure	Les hôtes vSphere 5.0 et versions antérieures peuvent être ajoutés à vSphere vCenter Server 5.1, mais pas aux vSphere Distributed Switches 5.1 et versions ultérieures.
vSphere 5.1 et versions ultérieures	vSphere 5.0	vSphere 5.0	vSphere vCenter Server 5.1 et versions ultérieures peut configurer la mise en miroir de port sur un vSphere 5.0 Distributed Switch.
vSphere 5.1 et versions ultérieures	vSphere 5.0	vSphere 5.1 et versions ultérieures	Les hôtes exécutant vSphere 5.1 peuvent être ajoutés aux vSphere 5.0 Distributed Switches et prennent en charge la mise en miroir de port vSphere 5.0.

Tableau 8-1. Compatibilité de mise en miroir (suite)

Version de vCenter Server	Version de vSphere Distributed Switch	Version de l'hôte	Fonctionnalité de mise en miroir de port vSphere 5.1
vSphere 5.1 et versions ultérieures	Antérieure à vSphere 5.0	vSphere 5.5 et version antérieure	La mise en miroir n'est pas prise en charge.
vSphere 5.0 et version antérieure	vSphere 5.0 et version antérieure	vSphere 5.1	Un hôte vSphere 5.1 ne peut pas être ajouté à vCenter Server 5.0 et versions antérieures.

Si vous utilisez un profil d'hôte avec des paramètres de mise en miroir de port, le profil d'hôte doit être adapté à la nouvelle version de mise en miroir de port dans vSphere 5.1 et versions ultérieures.

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 5.1 avec d'autres fonctionnalités de vSphere.

vMotion

vMotion fonctionne différemment en fonction du type de session de mise en miroir du port vSphere 5.1 que vous sélectionnez. Pendant vMotion, un chemin de mise en miroir peut être temporairement invalide mais il est restauré lorsque vMotion s'achève.

Tableau 8-2. 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.
Mise en miroir à distance de la source	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.
Mise en miroir à distance de la destination	Source VLAN	Non	

Tableau 8-2. 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.
Encapsulated Remote Mirroring (L3) Source	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 avec Client Web vSphere

Créer une session de miroir de ports avec Client Web vSphere pour refléter le trafic de vSphere Distributed Switch aux ports, liaisons montantes et les adresses IP distantes des agents.

Prérequis

Créez un vSphere Distributed Switch version 5.0.0 ou ultérieure.

Procédure

- 1 [Sélectionner le type de session de mise en miroir des ports avec Client Web vSphere](#) page 169
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 les détails du nom et de la session de mise en miroir de ports avec Client Web vSphere](#) page 170
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 [Sélection des sources de ports de mise en miroir avec Client Web vSphere](#) page 170
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 des ports et vérification des paramètres avec Client Web vSphere](#) page 171
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 le type de session de mise en miroir des ports avec Client Web vSphere

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 Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Paramètres > Mise en miroir des ports**.
- 3 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 miroir d'un certain nombre de ports distribués à des adresses IP des agents à distance. Le trafic de la machine virtuelle se reflète vers une destination physique distante à travers un tunnel IP.
Mise en miroir de port distribué (héritage)	Paquets miroir d'un certain nombre de ports distribués à un certain nombre de ports distribués et/ou ports de liaison montante sur l'hôte correspondant.

- 5 Cliquez sur **Suivant**.

Spécifier les détails du nom et de la session de mise en miroir de ports avec Client Web vSphere

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.
Statut	Utilisez le menu déroulant pour activer ou désactiver la session.
Type de session	Affiche le type de session que vous avez sélectionné.
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 permettez pas cette option, le trafic en miroir est autorisé en sortie sur les ports de destination, mais pas le trafic entrant.
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.
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.
Description	Vous avez la possibilité d'entrer une description de la configuration de session de mise en miroir de ports.

- 2 Cliquez sur **Suivant**.

Sélection des sources de ports de mise en miroir avec Client Web vSphere

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 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 ports 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.

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 s'affiche avec une liste de ports existants. Cochez la case à côté du port distribué et cliquez sur OK . Vous pouvez choisir plus d'un port distribué.
Ajouter des ports existants par numéro de port	Cliquez sur Ajouter des ports distribués , entrez le numéro du port et cliquez sur OK .

Option	Description
Sélectionnez le sens du trafic	Après l'ajout de ports, sélectionnez le port dans la liste et cliquez sur le bouton Entrée, Sortie, ou 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 VLAN. Modifier l'ID au moyen des flèches haut et bas ou en cliquant sur le champ et en tapant l'ID VLAN manuellement.

- 2 Cliquez sur **Suivant**.

Sélectionner les destinations de mise en miroir des ports et vérification des paramètres avec Client Web vSphere

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**.

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 des ports dans Client Web vSphere

Affichez les détails de la session de mise en miroir de ports, notamment son état, ses sources et ses destinations.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres > Mise en miroir des 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 la session de mise en miroir de ports avec Client Web vSphere

Modifiez les détails d'une session de mise en miroir de ports, nom inclus, sa description, son statut, sources et destinations.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Paramètres > Mise en miroir des 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 de ports, ou accepter le nom de session généré automatiquement.
Statut	Utilisez le menu déroulant pour activer ou désactiver la session.
E/S normales sur les ports de destination	Utilisez le menu déroulant pour activer ou désactiver les E/S normales sur les ports de destination. Cette propriété n'est disponible que pour la liaison montante et les destinations 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.
ID VLAN encapsulé	Entrez un ID VLAN valide dans le champ. Cette information est nécessaire pour les sessions de mise en miroir de ports de la Source de mise en miroir distante. Cochez la case à côté de Préserver le VLAN d'origine pour créer un ID de VLAN qui encapsule tous les trames des ports de destination. 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.

Option	Description
La longueur du paquet en miroir (Octets)	Utilisez la case cocher pour activer la longueur en octets du paquet en miroir. Cela impose une 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 ports distribués... 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.
Ajouter des ports existants par numéro de port	Cliquez sur le bouton Ajouter 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 le bouton Ajouter pour ajouter un ID VLAN. Modifier l'ID au moyen des flèches haut et bas ou en cliquant sur le champ et en tapant l'ID VLAN manuellement

- 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 une destination pour le port distribué	Cliquez sur le bouton Sélectionner ports distribués... pour sélectionner les ports à partir d'une liste, ou cliquez sur le bouton Ajouter ports distribués... pour ajouter des ports par leur numéro. Vous pouvez ajouter plus d'un port distribué.
Sélectionner des liaisons montantes	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 des ports Vous pouvez sélectionner plus d'une liaison montante.
Sélectionnez les ports ou les liaisons montantes	Cliquez sur le bouton Sélectionner ports distribués pour sélectionner les ports à partir d'une liste, ou cliquez sur le bouton Ajouter ports distribués... pour ajouter des ports par leur numéro. Vous pouvez ajouter plus d'un port distribué. Cliquez sur bouton Ajouter 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 le bouton Ajouter . Une nouvelle entrée de liste est créée. Sélectionnez l'entrée et cliquez soit sur le bouton Modifier pour entrer l'adresse IP, ou cliquez directement dans le champ Adresse IP et entrez l'adresse IP. Une boîte de dialogue d'avertissement s'ouvre si l'adresse IP n'est pas valide.

- 7 Cliquez sur **OK**.

Configurer les paramètres NetFlow avec Client Web vSphere

NetFlow est un outil d'analyse de réseau que vous pouvez utiliser pour surveiller le réseau et le trafic de machine virtuelle.

NetFlow est disponible dans vSphere Distributed Switches version 5.0.0 et suivantes.

Procédure

- 1 Accédez à une version de commutateur distribué 5.0.0 ou une version ultérieure dans le navigateur Client Web vSphere
- 2 Cliquez avec le bouton droit de la souris dans le navigateur puis sélectionnez **Toutes les actions vCenter > Éditer Netflow**.
- 3 Entrez l'**Adresse IP** et le **Port** du collecteur NetFlow.
- 4 Entrez l'**adresse IP du commutateur**.

Avec une adresse IP sur vSphere Distributed Switch, le collecteur NetFlow peut interagir avec vSphere Distributed Switch en tant que commutateur unique, au lieu d'interagir avec un commutateur non associé distinct pour chaque hôte associé.

- 5 (Facultatif) Définissez le **Délai d'attente d'exportation de flux actif** et le **Délai d'attente d'exportation de flux inactif** en secondes.

- 6 (Facultatif) Définissez la **Fréquence de taux d'échantillonnage**

Ce taux d'échantillonnage détermine la partie des données que NetFlow collecte avec la valeur de taux d'échantillonnage qui détermine la fréquence de la collecte des paquets par NetFlow. Un collecteur dont le taux d'échantillonnage est 2 collecte les données tous les deux paquets. Un collecteur dont le taux d'échantillonnage est 5 collecte les données tous les 5 paquets.

- 7 (Facultatif) Activez ou désactivez **Traiter les flux internes uniquement** avec le menu déroulant.

Lorsque cette option est activée, seules les données concernant l'activité réseau entre les VM sur le même hôte sont collectées.

- 8 Cliquez sur **OK**.

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 Client Web vSphere.

Activer le protocole CDP (Cisco Discovery Protocol) sur un vSphere Distributed Switch avec Client Web vSphere

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 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres > Propriétés**.
- 3 Cliquez sur **Edit**.
- 4 Cliquez sur **Avancé**.
- 5 Dans la section **Protocole de découverte** sélectionnez **CDP (Cisco Discovery Protocol)** dans le menu déroulant **Type**.
- 6 définissez l'**opération** à partir du menu déroulant.

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 la disposition de l'administrateur du commutateur Cisco.
Annoncer	ESXi met les informations sur le vSphere Distributed Switch à la disposition de l'administrateur du commutateur Cisco, mais ne détecte, ni n'affiche d'informations 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 la disposition de l'administrateur du commutateur Cisco.

- 7 Cliquez sur **OK**.

Activer le protocole LLDP (Link Layer Discovery Protocol) sur un vSphere Distributed Switch dans Client Web vSphere

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 Client Web vSphere.

Le protocole LLDP est uniquement disponible sur vSphere Distributed Switch version 5.0.0. et les versions suivantes.

Procédure

- 1 Accédez à un commutateur distribué dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres > Propriétés**.
- 3 Cliquez sur **Edit**.
- 4 Cliquez sur **Avancé**.
- 5 Sélectionnez **Protocole LLDP (Link Layer Discovery Protocol)** dans le menu déroulant **Type**.

- 6 Assignez à **Opération** les valeurs **Écouter**, **Annoncer**, ou les deux.

Opération	Description
Écouter	ESXi détecte et affiche les informations sur le port physique associé, mais les informations sur vSphere Distributed Switch ne sont pas mises à la disposition de l'administrateur du commutateur.
Annoncer	ESXi met les informations sur vSphere Distributed Switch à la 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 vSphere Distributed Switch à la disposition de l'administrateur du commutateur.

- 7 Cliquez sur **OK**.

Afficher les informations du commutateur sur Client Web vSphere

Lorsque CDP ou LLDP a la valeur **Écouter** ou **Les deux**, vous pouvez afficher les informations des commutateurs physiques depuis Client Web vSphere.

Procédure

- 1 Accédez à un hôte dans le navigateur Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Mise en réseau > Adaptateurs physiques**.
- 3 Sélectionnez un adaptateur physique de la liste pour afficher ses informations détaillées.

Selon le protocole de découverte du commutateur activé, les propriétés du commutateur s'affichent sous Protocole découverte Cisco ou Protocole de découverte de couche de lien. Si les informations sont disponibles dans le réseau, les capacités système du commutateur s'affichent sous Fonction de périphérique homologue.

Montage de volumes NFS

ESXi prend en charge les montages NFS basés sur VMkernel pour le stockage des disques virtuels sur les banques de données NFS.

En plus du stockage des disques virtuels sur des banques de données NFS, vous pouvez employer les banques de données NFS comme référentiel central pour les images ISO et les modèles de machine virtuelle. Pour plus d'informations sur la création de banques de données NFS, voir *Stockage vSphere*.

ESXi prend en charge la version 3 de NFS sur les commutateurs réseau des couches 2 et 3. Les serveurs d'hôte et les baies de stockage NFS doivent être sur des sous-réseaux différents et le commutateur de réseau doit gérer les informations de routage.

Récupération et restauration de mise en réseau

vSphere 5.1 (et versions ultérieures) vous permet d'empêcher une mauvaise configuration du réseau et d'effectuer une récupération suite à cette erreur en utilisant la fonction de restauration, les fichiers de sauvegarde de configuration ou encore des configurations précédentes.

vSphere 5.1 (et versions ultérieures) peut restaurer la configuration de mise en réseau précédente valide si la configuration du réseau de gestion est incorrecte. Pour ce faire, vous pouvez vous connecter directement à l'hôte à travers l'interface DCUI et corriger les éventuels problèmes de mise en réseau. La restauration peut être utilisée sur des commutateurs standards et distribués.

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 version 5.1 et ultérieures, la restauration de la 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.

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 avec Client Web vSphere](#) », page 49.

Désactiver la restauration réseau à l'aide de Client Web vSphere

La restauration est activée par défaut dans vSphere 5.1 et une version ultérieure. Vous pouvez désactiver la restauration dans vCenter Server à l'aide de Client Web vSphere.

Procédure

- 1 Accédez à une instance de vCenter Server dans le navigateur de Client Web vSphere.
- 2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Paramètres**.
- 3 Sélectionnez **Paramètres avancés** puis cliquez sur **Modifier**.
- 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 en vSphere 5.1 et postérieures. 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 qui contient le fichier de configuration :
 - Sur un système d'exploitation Windows Server, l'emplacement du répertoire est *vCenter Server home directory\Application Data\VMware\VMware VirtualCenter*.
 - Sur vCenter Server Appliance, l'emplacement du répertoire est */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.

Restaurer une configuration de la mise en réseau précédente avec Client Web vSphere

Vous pouvez restaurer une configuration précédente d'un vSphere Distributed Switch ou d'un groupe de ports pour révoquer des modifications non valides.

Procédure

- 1 Dans Client Web vSphere, accédez au vSphere Distributed Switch concerné, ou à un groupe de ports distribués ou de liaisons montantes.
- 2 Cliquez avec le bouton droit sur le commutateur ou le groupe de ports concerné, puis sélectionnez **Toutes les actions vCenter > Restaurer la configuration**.
- 3 Si vous restaurez la configuration d'un commutateur distribué, fournissez un fichier de sauvegarde.
 - a Cliquez sur **Parcourir** et accédez à l'emplacement du fichier de sauvegarde du commutateur distribué.
 - b Sélectionnez **Restaurer un commutateur distribué et tous les groupes de ports** ou **Restaurer un commutateur distribué seulement**.
 - c Cliquez sur **Suivant**.
- 4 Si vous restaurez la configuration d'un groupe de ports distribués ou d'un groupe de ports de liaisons montantes :
 - a Sélectionnez **Restaurer la configuration précédente** ou **Restaurer la configuration à partir d'un fichier**.
Restaurer vers une configuration antérieure fait revenir la configuration un pas en arrière.
 - b Si la restauration s'effectue à partir d'un fichier, cliquez sur **Parcourir** pour accéder à l'emplacement du fichier de sauvegarde du groupe de ports.
 - c Cliquez sur **Suivant**.
- 5 Vérifiez vos informations de configuration et cliquez sur **Terminer**.

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

Dans vSphere 5.1 et versions ultérieures, 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 commutateur distribué.

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

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

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

Prérequis

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.

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.

Suivant

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.

Configurer les profils de protocole pour la mise en réseau des machines virtuelles

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.

REMARQUE 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](#) page 181

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6 que vCenter Server attribue 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 dans Client Web vSphere](#) page 183

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.

- [Configurer une machine virtuelle ou un vApp pour utiliser un profil de protocole réseau dans Client Web vSphere](#) page 183

Après avoir associé un profil de protocole à un groupe de ports d'un commutateur standard ou distribué, vous devez activer l'utilisation du profil sur une machine virtuelle qui est connectée au groupe de ports et associée à un vApp ou sur laquelle les options vApp sont activées.

Ajouter un profil de protocole réseau

Un profil de protocole réseau contient un pool d'adresses IPv4 et IPv6 que vCenter Server attribue aux vApp ou aux machines virtuelles disposant de la fonctionnalité vApp qui sont connectés 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.

REMARQUE 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 au vApp et cliquez sur l'onglet **Gérer**.
- 2 Cliquez sur **Profils de protocole réseau**
Les profils de protocole réseau existants sont répertoriés.
- 3 Cliquez sur l'icône Ajouter (+) pour ajouter un profil de protocole réseau.

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 dans Client Web vSphere

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 Client Web vSphere, 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.
Client Web vSphere affiche les groupes de ports distribués sous l'objet commutateur distribué parent.
- 2 Dans l'onglet **Gérer**, cliquez sur **Profils de protocole réseau**.
- 3 Cliquez sur **Associer un profil de protocole réseau au réseau sélectionné**.
- 4 Sur la page Définir un type d'association de l'assistant Associer un profil de protocole réseau, 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 Sélectionnez le profil de protocole réseau et cliquez sur **Suivant**.
- 6 Vérifiez l'association et les paramètres du profil de protocole réseau et cliquez sur **Terminer**.

Configurer une machine virtuelle ou un vApp pour utiliser un profil de protocole réseau dans Client Web vSphere

Après avoir associé un profil de protocole à un groupe de ports d'un commutateur standard ou distribué, vous devez activer l'utilisation du profil sur une machine virtuelle qui est connectée au groupe de ports et associée à un vApp ou sur laquelle les options vApp sont activées.

Prérequis

Assurez-vous que la machine virtuelle est connectée à un groupe de ports associé au profil de protocole réseau.

Procédure

- 1 Accédez à la machine virtuelle ou au vApp dans l'inventaire de Client Web vSphere.
- 2 Dans Client Web vSphere, ouvrez les paramètres du vApp ou l'onglet **Options vApp** de la machine virtuelle.
 - Cliquez avec le bouton droit sur un vApp et sélectionnez **Modifier les paramètres**.
 - Cliquez avec le bouton droit sur une machine virtuelle, sélectionnez **Modifier les paramètres**, puis dans la boîte de dialogue Modifier les paramètres, cliquez sur l'onglet **Options vApp**.
- 3 Cliquez sur **Activer les options vApp**.
- 4 Sous Création, développez **Allocation IP** et définissez le modèle d'allocation IP sur **Environnement OVF**.
- 5 Sous Déploiement, développez **Allocation IP** et définissez **Allocation IP** sur **Temporaire - Pool IP** ou **Statique - Pool IP**.

Les options **Statique - Pool IP** et **Temporaire - Pool IP** allouent toutes les deux une adresse IP figurant dans la plage du profil de protocole réseau qui est associé au groupe de ports. Si vous sélectionnez **Statique - IP Pool**, l'adresse IP est attribuée lors de la première mise sous tension de la machine virtuelle ou du vApp et elle persiste lors des redémarrages suivants. Si vous sélectionnez **Temporaire - Pool IP**, une adresse IP est attribuée à chaque mise sous tension de la machine virtuelle ou du vApp.
- 6 Cliquez sur **OK**.

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.

Déploiement de réseau sans état

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 au commutateur distribué, vCenter Server joint l'hôte ESXi aux commutateurs distribués VMware ou une solution de commutateur tiers.

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.)
- Les instances de commutateurs distribués (VMware et tiers)
- 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 vmknics, 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 règle de sélection de liaison montante, selon le nom vmnic ou le numéro de périphérique, et l'auto-découverte selon l'ID VLAN. Les informations (éventuellement modifiées) sont stockées par l'infrastructure de démarrage sans état et appliquées à l'hôte ESXi à 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 règle. Si la règle 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 vmknics 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 vmknics 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.

Surveillance des paquets réseau

Surveillez les paquets réseau qui passent par les ports d'un commutateur standard vSphere ou d'un vSphere Distributed Switch afin d'analyser le trafic entre les machines virtuelles et les hôtes.

Capture et suivi des paquets réseau à l'aide de l'utilitaire `pktcap-uw`

Surveillez 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 en utilisant l'interface utilisateur graphique des outils d'analyse réseau tels que Wireshark.

Dans vSphere 5.5 ou version ultérieure, 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.

REMARQUE 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
```

REMARQUE 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 9-1. Arguments pktpcap-uw pour la capture de paquets

Groupe d'arguments	Argument	Description
<i>switch_port_arguments</i>	<code>--uplink vmnicX</code>	<p>Capture de paquets associés à un adaptateur physique.</p> <p>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.</p> <p>Reportez-vous à « Capturer les paquets reçus sur un adaptateur physique », page 192.</p>
	<code>--vmk vmkX</code>	<p>Capture de paquets associés à un adaptateur VMKernel.</p> <p>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.</p> <p>Reportez-vous à « Capturer des paquets pour un adaptateur VMkernel », page 196.</p>
	<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>esxcli</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 « Capturer des paquets pour un adaptateur de machine virtuelle VMXNET3 », page 194.</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>

Tableau 9-1. Arguments pktcap-uw pour la capture de paquets (suite)

Groupe d'arguments	Argument	Description
	<code>--dir {0 1}</code>	Capture de paquets selon la direction du flux applicable au commutateur virtuel. 0 représente le trafic entrant et 1 le trafic sortant. Par défaut, l'utilitaire <code>pktcap-uw</code> capture le trafic d'entrée. Utilisez l'option <code>--dir</code> en même temps que l'option <code>--uplink</code> , <code>--vmk</code> ou <code>--switchport</code> .
	<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 « Capturer des paquets au niveau de DVFilter » , page 198.
	<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 » , page 200.	
<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 « Options de pktcap-uw pour le filtrage de paquets » , page 191.	
<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 « Options de pktcap-uw pour le contrôle de sortie » , page 190.	

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_options output_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 9-2. 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 pktcap-uw pour le filtrage de paquets », page 191.
<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 pktcap-uw pour le contrôle de sortie », page 190.

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](#) », page 187 et « [Syntaxe de la commande pktcap-uw pour le suivi de paquets](#) », page 189.

Tableau 9-3. 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 <i>number_of_packets</i> premiers paquets.
<code>{-s --snaplen} snapshot_length</code>	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. Pour limiter la taille du contenu capturé, définissez une valeur supérieure à 24. Pour capturer le paquet complet, définissez cette option sur 0.
<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](#) », page 187 et « [Syntaxe de la commande pktcap-uw pour le suivi de paquets](#) », page 189.

Tableau 9-4. 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 « : ».
<code>--ethtype 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 <i>EtherType</i> 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 <code>--ethtype 0x88CC</code> .
<code>--vlan VLAN_ID</code>	Capturez ou suivez les paquets appartenant à un VLAN.
<code>--srcip IP_address PI_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 0xPI_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 <code>--proto 0x11</code> .
<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.

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](#) », page 200.

Procédure

- 1 (Facultatif) Recherchez le nom de l'adaptateur physique à surveiller dans la liste des adaptateurs de l'hôte.
 - Dans Client Web vSphere, dans l'onglet **Gérer** de l'hôte, cliquez sur **Mise en réseau** et sélectionnez **Adaptateurs physiques**.
 - Dans Shell ESXi 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 Shell ESXi sur l'hôte, exécutez la commande `pktcap-uw` avec l'argument `--uplink vmnicX` 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 --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 `pktcap-uw --uplink vmnicX` se trouvent entre crochets `[]` et où les barres verticales `|` représentent des valeurs alternatives.

Si vous exécutez la commande `pktcap-uw --uplink vmnicX` sans options, vous obtenez le contenu des paquets entrants sur le commutateur standard ou distribué dans 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
```

Suivant

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 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](#) », page 200.

Prérequis

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 `esxstop`.
 - a Dans Shell ESXi sur l'hôte, pour démarrer l'utilitaire, exécutez `esxstop`.
 - b Appuyez sur N pour passer au panneau de réseau de l'utilitaire.
 - 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 `esxstop`.
- 2 Dans Shell ESXi sur l'hôte, exécutez `pktcap-uw --switchport port_ID`.
port_ID est l'ID que l'utilitaire `esxstop` affiche pour l'adaptateur de machine virtuelle dans la colonne PORT-ID.

- 3 Dans Shell ESXi sur l'hôte, exécutez la commande `pktcap-uw` avec l'argument `--switchport port_ID` 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 des valeurs alternatives.

Si vous exécutez la commande `pktcap-uw --switchport port_ID` sans option, vous obtenez le contenu des paquets entrants sur le commutateur standard ou distribué dans la sortie de la console au point auquel 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 Vmxnet3Tx</code>	Surveillez les paquets lorsqu'ils passent de la machine virtuelle au commutateur.
<code>--capture Vmxnet3Rx</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 Vmxnet3Rx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

Suivant

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](#) », page 200.

Procédure

- 1 (Facultatif) Recherchez le nom de l'adaptateur VMkernel à surveiller dans la liste des adaptateurs VMkernel.

- Dans Client Web vSphere, dans la liste Mise en réseau de l'onglet **Gérer** de l'hôte, sélectionnez **Adaptateurs VMkernel**.
- Dans Shell ESXi 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.

- 2 Dans Shell ESXi 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 `pktcap-uw--vmk vmkX` se trouvent entre crochets `[]` et où les barres verticales `|` représentent des valeurs alternatives.

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 `esxcli` 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.

Suivant

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 Shell ESXi 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.

REMARQUE 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.

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.

Suivant

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 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 Shell ESXi.

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 `--dvfilter dvfilter_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]
[--outfile pcap_file_path [--ng]] [--count number_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.

Suivant

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.

REMARQUE 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 `--capturecapture_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 vmnicX` 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 de la machine virtuelle 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
Vmxnet3Rx	Fonction du serveur principal VMXNET3 qui reçoit des paquets du commutateur virtuel.
Vmxnet3Tx	Fonction du serveur principal VMXNET3 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 de la machine virtuelle à l'adaptateur VMkernel.
PortInput	Fonction qui transmet une liste de paquets de l'adaptateur VMkernel à un port de la machine virtuelle. 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> .
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`](#) », page 200.

Procédure

- ◆ Dans Shell ESXi 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 Shell ESXi 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.

REMARQUE 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.

Suivant

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.

Meilleures pratiques de mise en réseau

10

Prenez en compte ces meilleures pratiques lors de la configuration de votre réseau.

- 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.

Attribuez un groupe de machines virtuelles à une carte réseau physique distincte. Cette séparation permet de répartir équitablement sur plusieurs CPU une partie de la charge de travail totale du réseau. Les machines virtuelles isolées peuvent ensuite mieux gérer le trafic des applications, par exemple, à partir d'un client Web.

- 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).
- 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.
- 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 tous les adaptateurs réseau VMkernel d'un vSphere Distributed Switch avec le même MTU. Lorsque plusieurs adaptateurs réseau VMkernel configurés avec différents MTU sont connectés aux vSphere Distributed Switches, vous risquez de rencontrer des problèmes de connectivité.
- Lors de la création d'un groupe de ports distribués, n'utilisez pas la liaison de port dynamique. La liaison de port dynamique est obsolète depuis ESXi 5.0.

Index

A

- adaptateur réseau physique
 - ajouter au commutateur standard **21**
 - basculement **21**
 - commutateur standard **20**
- adaptateur réseau virtuel
 - commutateur standard **40**
 - supprimer d'un commutateur distribué **82**
- adaptateur réseau VMkernel **79**
- Adaptateur réseau VMkernel, activation de TSO **138**
- adaptateur VMkernel, affichage des informations **75**
- adaptateurs de liaison montante
 - ajout à un commutateur distribué **41**
 - suppression d'un commutateur distribué **41**
- adaptateurs réseau physiques
 - ajout à un commutateur distribué **41**
 - suppression d'un commutateur distribué **41**
- adresse MAC
 - allocation basée sur préfixe **158**
 - attribuer une adresse MAC **159**
 - configuration **163**
 - génératon **157**
 - statique **163**
 - statique, VMware OUI **162**
 - vCenter Server **157**
- Adresse MAC
 - Adresse administrée localement (LAA) **159**
 - adresse MAC statique **162**
 - ajuster les paramètres d'allocation **159**
 - allocation basée sur plage **159, 160**
 - allocation basée sur préfixe **159, 160**
 - Allocation de VMware OUI **160**
 - attribuer une adresse MAC manuellement **162**
 - configuration **157, 163**
 - définir le type d'allocation **160**
 - génératon **157, 158**
 - génératon, hôte **161**
 - statique **163**
 - VMware OUI **158**
- adresse MAC statique **162**
- ajout
 - commutateur distribué **25**
 - vSphere Distributed Switch **25**
- ajouter un hôte au commutateur distribué **30**

- ajuster les paramètres d'allocation des adresses MAC **159**

- Allocation d'adresse MAC basée sur plage **159**

- allocation d'adresse MAC basée sur préfixe **159**

- allocation d'adresse MAC par préfixe **158**

- Allocation de VMware OUI **158**

- Association de cartes réseau

- commutateur standard **21**

- commutateurs standard **84**

- définition **11**

B

- balisage d'invité virtuel **13**
- balisage de commutateur externe **13**
- balisage de commutateur virtuel **13**
- bande passante
 - maximale **99**
 - moyenne **99**
- bande passante maximale, commutateur standard **100**
- bande passante moyenne, commutateur standard **100**
- basculement, commutateurs standard **84**
- blocage des ports **83**
- bloquer tous les ports
 - groupes de ports distribués **124**
 - ports distribués **125**

C

- capture d'un nombre de paquets **190**
- capture de paquets
 - adaptateur physique **192**
 - affichage de tous les points de capture **201**
 - capture dans un fichier **190**
 - capture uniquement des premiers octets d'un paquet **190**
 - commande de console **187, 190–192, 194, 196–201**
 - DVFilter **198**
 - filtrage de paquets **191**
 - liaison montante **192**
 - paquets abandonnés **197**
 - pktcap-uw **187, 192, 194, 196–201**
 - points de capture **199–201**
 - suivi de paquets **201**

- VMkernel **196**
- VMXNET3 **194**
- cartes réseau
 - ajout à un commutateur distribué **41**
 - retirer d'un vSphere Distributed Switch **42**
 - retirer d'une machine virtuelle active **42**
 - suppression d'un commutateur distribué **41**
 - système d'exploitation client **42**
- CDP **174**
- CDP (Cisco Discovery Protocol) **175**
- commutateur distribué
 - activer ou désactiver le contrôle d'intégrité **55**
 - adaptateur réseau **34**
 - adaptateur réseau de machine virtuelle **39**
 - adaptateur réseau physique **39**
 - Adaptateur réseau VMkernel **34**
 - adaptateurs de mise en réseau d'une machine virtuelle **36**
 - Adaptateurs VMkernel **34**
 - affichage des informations sur l'adaptateur réseau **75**
 - ajout **25**
 - ajout d'un adaptateur de liaison montante **41**
 - ajout d'un adaptateur réseau **41**
 - ajout d'une carte réseau **41**
 - ajouter des adaptateurs VMkernel **34**
 - ajouter des hôtes **29**
 - CDP **175, 176**
 - CDP (Cisco Discovery Protocol) **175**
 - commutateur proxy **39**
 - configurer des réseaux virtuels **29**
 - contrôle de l'intégrité **55**
 - créer un adaptateur VMkernel **78**
 - exporter la configuration **56, 57**
 - gérer la mise en réseau des hôtes **29**
 - hôte modèle **37**
 - importer la configuration **56, 57**
 - information de contact de l'administrateur **28**
 - l'onglet **28**
 - LACP **70**
 - liaisons montantes **28**
 - LLDP **175, 176**
 - machines virtuelles **51**
 - migration de VM **51**
 - migrer des adaptateurs VMkernel **34**
 - migrer la mise en réseau de machines virtuelles **36**
 - migrer les adaptateurs réseau des machines virtuelles **36**
 - mise à niveau **27**
 - mise en miroir de ports **169**
 - mise en réseau de machines virtuelles **36**
 - mise en réseau VMkernel **34**
 - modifier pool de ressources réseau **136**
 - MTU **28**
 - Network I/O Control **28, 134**
 - nom **28**
 - nombre de ports sur les hôtes **37**
 - nouveau pool de ressources réseau **134**
 - Pool de ressources réseau **134, 135**
 - ports **41**
 - prise en charge de Dump Collector **14**
 - Protocole LLDP (Link Layer Discovery Protocol) **175**
 - récupération **176, 179**
 - restauration **176, 177**
 - restaurer la configuration **56, 58, 179**
 - sans état **184**
 - suppression d'une carte réseau **41**
 - supprimer des hôtes **38**
 - supprimer un adaptateur de liaison montante **41**
 - supprimer un adaptateur réseau **41**
 - switch discovery protocol **28**
 - trafic de gestion **34**
 - Trafic de stockage IP **34**
 - Trafic de Virtual SAN **34**
 - Trafic Fault Tolerance **34**
 - Trafic vMotion **34**
 - VLAN **59**
 - VLAN privé **59**
 - commutateur distribué sans état **184**
 - commutateur standard
 - adaptateur réseau **76, 79**
 - adaptateur réseau physique **20**
 - adaptateur réseau virtuel **40**
 - adaptateur réseau VMkernel **79**
 - Adaptateur réseau VMkernel **76**
 - affichage des informations sur l'adaptateur réseau **75**
 - bande passante maximale **100**
 - bande passante moyenne **100**
 - configuration des ports **20**
 - créer un nouveau commutateur standard **17**
 - détection de basculement de réseau **86**
 - équilibre de charge **86**
 - étiquette de réseau du groupe de ports **18**
 - groupe de ports **17, 18**
 - ID VLAN groupe de ports **18**
 - IPv4 **76, 79**
 - IPv6 **76, 79**
 - journalisation de Fault Tolerance **79**
 - Journalisation de Fault Tolerance **76**
 - mode promiscuité **95**

- Modifications d'adresse MAC **95**
- MTU **79**
- notifier les commutateurs **86**
- ordre de basculement **86**
- Règle d'association et de basculement **18**
- Règle de formation du trafic **18**
- Règle de sécurité **18**
- règle de sécurité de la couche 2 **95, 96**
- retour arrière **86**
- sans état **184**
- stratégies d'association et de basculement **86**
- stratégies de formation du trafic **100**
- taille de rafale **100**
- trafic de gestion **79**
- Trafic de gestion **76**
- transmission forgée **95**
- vitesse et duplex de l'adaptateur réseau physique **20**
- vMotion **76, 79**
- commutateur standard vSphere
 - activation des trames Jumbo **139**
 - configuration **20**
 - configuration des ports **20**
 - définition **11**
 - diagramme de la topologie **21**
 - mode promiscuité **95**
 - Modifications d'adresse MAC **95**
 - propriétés **20**
 - protection contre l'emprunt d'identité d'adresse MAC **95**
 - protection contre le balayage du trafic **95**
 - règle de sécurité de la couche 2 **95**
 - règles de sécurité **95**
 - transmission forgée **95**
 - utilisation **15**
- Commutateur tiers **24**
- commutateurs Cisco **174**
- commutateurs standard
 - Association de cartes réseau **84**
 - basculement **84**
 - configuration **20**
 - équilibrage de charge **84**
 - état du lien **84**
 - prise en charge de Dump Collector **14**
 - propriétés **20**
 - récupération **176**
 - restauration **176, 177**
 - sondage de balise **84**
 - utilisation **15**
- configuration
 - commutateur distribué **57**
 - importation **57**
 - configuration d'adresse IP **181, 182**
 - configuration des ports **20**
 - configurer LACP **66**
 - conflit d'adresses MAC **159**
 - contrôle de l'intégrité
 - activer ou désactiver **55**
 - afficher les informations **56**
 - Contrôle E/S réseau **103**
 - créer un groupe d'agrégation de liens **66**
 - créer un LAG **66**
 - créer une pile TCP/IP **81**
- D**
 - DCUI, restaurer vDS **179**
 - définir le type de l'allocation des adresses MAC **160**
 - délestage de segmentation TCP, , voir TSO
 - démarrage sans état **184**
 - désactivation de la restauration **178**
 - désactivation de la restauration avec vpxd.cfg **178**
 - désactiver la restauration **178**
 - détection de basculement de réseau **86**
 - DirectPath I/O
 - activation **143**
 - machine virtuelle **143**
 - vMotion **143**
 - DNS, configuration **81**
 - Dump Collector **14**
- E**
 - équilibrage de charge
 - commutateurs standard **84**
 - groupes de ports distribués **125**
 - EST (balisage de commutateur externe) **13**
 - état du lien, commutateurs standard **84**
 - exporter la configuration
 - commutateur distribué **56, 57**
 - groupes de ports distribués **48**
- F**
 - filtrage et balisage du trafic
 - action Autoriser ou Annuler **117**
 - activation sur un groupe de ports **107**
 - activation sur un port **115**
 - affichage de règles de trafic sur un port **119**
 - affichage des règles de trafic **112**
 - balisage du trafic à l'aide de balises CoS et DSCP sur un port **116**
 - définition de règles de trafic **111**
 - définition de règles de trafic sur un port **118**
 - désactivation **114**
 - désactivation sur un port **121**

- en fonction de l'adresse IP **123**
 - en fonction de l'adresse MAC **122**
 - en fonction des propriétés de la couche 2 **122**
 - en fonction des propriétés de la couche 3 **122**
 - en fonction des propriétés de la couche de liaison de données **122**
 - en fonction des propriétés de la couche réseau **123**
 - en fonction du type de données système **122**
 - filtrage et balisage du trafic
 - en fonction de l'ID VLAN **122**
 - en fonction du protocole et du port de transport **123**
 - modification de la priorité des règles **113**
 - modification des priorités de règles sur un port **120**
 - octroi ou refus de l'accès au trafic **117**
 - ouverture d'une règle pour modification **112**
 - ouverture d'une règle sur un port en vue de la modifier **120**
 - suppression d'une règle d'un port **121**
 - filtrer le trafic, octroi ou refus de l'accès au trafic **110**
- G**
- gérer la mise en réseau des hôtes **30**
 - gestion des ressources réseau **133**
 - groupe d'agrégation de liens
 - ajouter des ports **69**
 - algorithme d'équilibrage de charge **69**
 - modifier la configuration **69**
 - modifier les paramètres **69**
 - stratégies de VLAN et NetFlow **69**
 - groupe de ports à liaison montante
 - activation du filtrage et du balisage du trafic **107**
 - affichage des règles de trafic **112**
 - balisage du trafic à l'aide de balises CoS et DSCP, groupe de ports **107**
 - configuration du filtrage et du balisage du trafic **106**
 - définition de règles de trafic **111**
 - désactivation du filtrage et du balisage du trafic **114**
 - LACP **70**
 - modification de la priorité des règles **113**
 - octroi ou refus de l'accès au trafic **110**
 - ouverture d'une règle de trafic en vue de la modifier **112**
 - suppression d'une règle de trafic **113**
 - groupe de ports distribués
 - activation du filtrage et du balisage du trafic **107**
 - affichage des règles de trafic **112**
 - balisage du trafic à l'aide de balises CoS et DSCP **107**
 - configuration du filtrage et du balisage du trafic **106**
 - connecter à une machine virtuelle **52**
 - définition de règles de trafic **111**
 - désactivation du filtrage et du balisage du trafic **114**
 - modification de la priorité des règles **113**
 - octroi ou refus de l'accès au trafic **110**
 - ouverture d'une règle de trafic en vue de la modifier **112**
 - Pool de ressources réseau **135**
 - stratégie de formation du trafic **101**
 - suppression d'une règle **113**
 - suppression d'une règle de trafic **113**
 - supprimer **48**
 - groupe de ports standard, règle de formation du trafic **101**
 - groupes de ports, définition **11**
 - groupes de ports de liaison montante, règles de VLAN **93**
 - groupes de ports distribués
 - ajouter nouveau **43**
 - allocation de port **43, 46**
 - bande passante maximale **125**
 - bande passante moyenne **125**
 - blocage des ports **43**
 - bloquer tous les ports **124**
 - configuration de masse **125**
 - équilibrage de charge **125**
 - exporter la configuration **48, 56**
 - filtrage et balisage du trafic **125**
 - importer la configuration **48, 49, 56**
 - Jonction VLAN **125**
 - liaison de port **43, 46**
 - mise en forme du trafic **125**
 - mode promiscuité **125**
 - modifications d'adresse MAC **125**
 - NetFlow **43, 125**
 - Network I/O Control **125**
 - notifier les commutateurs **125**
 - ordre de basculement **88, 125**
 - Paramètres avancés **47**
 - paramètres généraux **46**
 - pool de ressources réseau **43, 46**
 - pools de ressources réseau **103, 125**
 - ports bloqués **125**
 - règle de NetFlow **105**
 - règle de sécurité de la couche 2 **97**
 - Règle de surveillance **105**
 - règles de VLAN **92**

Règles diverses **124**
 réinitialiser au moment de la déconnexion **47**
 remplacer les règles de port **47**
 restaurer la configuration **48, 49, 56**
 stratégie de sécurité **125**
 stratégie VLAN **125**
 stratégies d'association **88, 125**
 stratégies d'association et de basculement **43**
 stratégies de basculement **88, 125**
 stratégies de formation du trafic **43**
 stratégies de port **125**
 stratégies de QoS **125**
 stratégies de sécurité **43**
 stratégies diverses **125**
 taille de rafale **125**
 transmissions forgées **125**
 VLAN **43, 46**
 VLAN privés **125**

H

hôte
 activation d'IPv6 **165**
 activation de SR-IOV **153, 154**
 désactivation d'IPv6 **165**

I

ID VLAN
 primaire **59**
 secondaire **59**
 Identificateur unique universel (UUID) **158**
 importer la configuration
 commutateur distribué **56**
 groupes de ports distribués **48, 49**
 Interface utilisateur de console directe (DCUI),
 restaurer vDS **179**
 IOMMU **144, 145, 150**
 IPv4 **76, 79**
 IPv6
 activation **165**
 désactivation **165**
 VMkernel **80**

J

Jonction VLAN, groupes de ports distribués **125**
 journalisation de Fault Tolerance **79**
 Journalisation de Fault Tolerance **76**

L

la machine virtuelle est hors tension, SR-IOV **155**
 LACP
 commutateur distribué **70, 71**
 convertir vers la prise en charge étendue du
 protocole LACP **63**

Équilibrage de charge de hachage d'IP **71**
 groupe de ports à liaison montante **70**
 hôte **71**
 iSCSI **71**
 limitations **71**
 mise à niveau **63**
 prise en charge étendue **63**

LAG

active **69**
 affecter des adaptateurs physiques **67**
 affecter des cartes réseau physiques **67**
 association et ordre de basculement **69**
 configuration intermédiaire **67**
 configurer **65**
 créer **65, 66**
 défini en mode veille **67**
 inutilisé **67**
 migrer le trafic réseau **65**
 ordre de basculement **67**

LAN virtuel

liaisons montantes actives **86**
 liaisons montantes de réserve **86**
 LLDP **174, 175**

M

machine virtuelle
 activation de TSO **137**
 adresse MAC statique **162**
 profil de protocole réseau **183**
 SR-IOV **150**
 machines virtuelles
 activation des trames Jumbo **140**
 migration depuis ou vers un commutateur
 distribué **51**
 migration vers et depuis vSphere Distributed
 Switch **51**
 mise en réseau **51**
 se connecter à un groupe de ports
 distribués **52**
 meilleures pratiques de mise en réseau **203**
 mise à niveau
 commutateur distribué **27**
 vSphere Distributed Switch **27**
 mise en forme du trafic, groupes de ports
 distribués **125**
 mise en miroir de ports
 adresse IP **171**
 ajouter des liaisons montantes **171**
 ajouter des ports **170**
 compatibilité de versions **166**
 compatibilité des fonctionnalités **166**
 créer avec vSphere Web Client **169**
 destinations **171, 172**

- E/S **170**
- éditer VLAN **172**
- état **172**
- LRO **167**
- modifier destinations **172**
- modifier le statut **172**
- modifier les sources **172**
- nom **170**
- sens du trafic **170**
- sources **170, 172**
- taux d'échantillonnage **170**
- TSO **167**
- type de session **169**
- types de sessions **167**
- vérifier les paramètres **171, 172**
- VLAN **170, 172**
- vMotion **167**
- mise en réseau
 - avancée **165**
 - introduction **11**
 - performances **140**
- mise en réseau d'hôte, affichage des
 - informations sur l'adaptateur réseau **75**
- mise en réseau d'hôte, restauration **177**
- mise en réseau de machines virtuelles **13, 17**
- mise en réseau VMkernel, créer un adaptateur
 - VMkernel **78**
- mode promiscuité **95, 125**
- modifications d'adresse MAC **125**
- Modifications d'adresse MAC **95**
- MTU, contrôle de l'intégrité **55, 56**

N

- NAS, montage **176**
- netdump **14**
- NetFlow
 - activation **104, 125, 174**
 - configurer **174**
 - désactivation **104, 125, 174**
 - groupes de ports distribués **125**
 - paramètres de collecteur **174**
- netqueue, activation **140**
- NetQueue, désactivation **141**
- Network I/O Control **28, 134**
- notifier le commutateur standard **86**
- notifier les commutateurs **125**
- nouveau pool de ressources, commutateur
 - distribué **134**

O

- ordre de basculement
 - groupes de ports distribués **88, 125**
 - ports distribués **90**

P

- paramètres d'association de réseaux **181**
- PCI, machine virtuelle **143**
- périphérique de relais
 - ajouter à un hôte **142**
 - machine virtuelle **143**
- Périphériques PCIE **144, 145, 150**
- pile TCP/IP personnalisée **81**
- pktcap-uw
 - options de suivi **189**
 - affichage de tous les points de capture **201**
 - capture de paquets **192, 194, 196–198**
 - options **190, 191**
 - options pour la capture des paquets **187**
 - points de capture **199–201**
 - suivi de paquets **201**
 - syntaxe de suivi **189**
 - syntaxe pour la capture des paquets **187**
- Pool de ressources réseau
 - balise QoS **134, 136**
 - définie par l'utilisateur **136**
 - limite d'hôte **134, 136**
 - parts de la carte physique **134, 136**
 - supprimer **136**
- pools de ressources, réseaux **133**
- pools de ressources réseau
 - groupes de ports distribués **103, 125**
 - ports distribués **104**
- port de liaison montante
 - activation du filtrage et du balisage du
 - trafic **115**
 - affichage des règles de trafic **119**
 - balisage du trafic à l'aide de balises CoS et
 - DSCP **116**
 - définition de règles de trafic **118**
 - désactivation du filtrage et du balisage du
 - trafic **121**
 - filtrage et balisage du trafic **114**
 - modification de la priorité des règles **120**
 - octroi ou refus de l'accès au trafic **117**
 - ouverture d'une règle de trafic en vue de la
 - modifier **120**
 - règles de VLAN **93**
 - suppression d'une règle **121**
- port distribué
 - activation du filtrage et du balisage du
 - trafic **115**
 - affichage des règles de trafic **119**
 - balisage du trafic à l'aide de balises CoS et
 - DSCP **116**
 - définition de règles de trafic **118**
 - désactivation du filtrage et du balisage du
 - trafic **121**
 - état du port **50**

- filtrage et balisage du trafic **114**
- modification de la priorité des règles **120**
- modifier le nom **51**
- modifier les paramètres **51**
- octroi ou refus de l'accès au trafic **117**
- ouverture d'une règle de trafic en vue de la modifier **120**
- Règle de sécurité **98**
- règles de VLAN **93**
- stratégie de formation du trafic **102**
- suppression d'une règle **121**
- surveiller l'état du port **50**
- ports, commutateur distribué **41**
- ports bloqués, groupes de ports distribués **125**
- ports de liaison montante, règles de VLAN **94**
- ports distribués
 - bloquer tous les ports **125**
 - bloqués **124**
 - mise en miroir de ports **169**
 - ordre de basculement **90**
 - pools de ressources réseau **104**
 - règle de NetFlow **105**
 - Règle de surveillance **105**
 - Règles diverses **125**
 - stratégies d'association **90**
 - stratégies de basculement **90**
- prise en charge du protocole LACP **61**
- profil d'hôte
 - activation de SR-IOV **153**
 - SR-IOV **153**
- profil de protocole réseau
 - association à un groupe de ports **183**
 - configuration d'un vApp **183**
 - configuration d'une machine virtuelle **183**
- profils de protocole, configuration **180**
- profils de protocole réseau, , voir profils de protocole
- Protocole LLDP (Link Layer Discovery Protocol) **174, 175**

R

- récupération, commutateur distribué **179**
- règle de NetFlow
 - groupes de ports distribués **105**
 - ports distribués **105**
- Règle de sécurité, port distribué **98**
- règle de sécurité de la couche 2, groupes de ports distribués **97**
- Règle de surveillance
 - groupes de ports distribués **105**
 - ports distribués **105**
- règle de VLAN **92**
- règles d'association, contrôle de l'intégrité **55, 56**

- règles de formation du trafic, groupe de ports standard **101**
- règles de sécurité
 - commutateur standard vSphere **95**
 - exceptions à la règle **95**
 - mode promiscuité **95**
 - Modifications d'adresse MAC **95**
 - Transmissions forgées **95**
- règles de trafic, ajout **112, 120**
- règles de VLAN
 - groupes de ports de liaison montante **93**
 - groupes de ports distribués **92**
 - port de liaison montante **93**
 - port distribué **93**
 - ports de liaison montante **94**
- Règles diverses
 - groupes de ports distribués **124**
 - ports distribués **125**
- réseau de gestion **179**
- réseaux
 - configuration d'adresse IP **181, 182**
 - pools de ressources **133**
 - ports distribués **50**
- restauration
 - commutateur distribué **176, 177, 179**
 - commutateur standard **176, 177**
 - désactivation **178**
 - fichier vpxd.cfg **178**
 - mise en réseau d'hôte **177**
 - restaurer la configuration **179**
- restaurer la configuration
 - commutateur distribué **56, 58**
 - groupes de ports distribués **48, 49**
- retour arrière **86, 125**

S

- sécurité de la couche 2 **95**
- sondage de balise, commutateurs standard **84**
- SR-IOV
 - activation **153, 154**
 - activation sur un adaptateur physique hôte **151**
 - activation via un profil d'hôte **153**
 - activation via une commande vCLI **153**
 - association à une machine virtuelle en tant qu'adaptateur réseau **151**
 - chemin de contrôle **147**
 - chemin de données **147**
 - commande ESXCLI **154**
 - composants **147**
 - fonction physique **150**
 - fonction virtuelle **149**
 - interaction de carte réseau physique **149**
 - machine virtuelle **150**

- modes de prise en charge **153**
- nombre de VF disponibles **149**
- options de mise en réseau **152**
- présentation **147**
- profil d'hôte **153**
- Stratégie VLAN **152**
- stratégies de sécurité **152**
- taux de contrôle des VF **149**
- vecteurs d'interruption épuisés **155**
- VF **149**
- SR-IOV, la machine virtuelle est hors tension **155**
- stratégie de sécurité, groupes de ports distribués **125**
- stratégie VLAN, groupes de ports distribués **125**
- Stratégie VLAN, SR-IOV **152**
- stratégies d'association
 - commutateur standard **86**
 - groupes de ports distribués **125**
- stratégies de basculement
 - commutateur standard **86**
 - groupes de ports distribués **88, 125**
 - ports distribués **90**
- stratégies de formation du trafic
 - bande passante maximale **100**
 - bande passante moyenne **100**
 - commutateur standard **100**
 - groupe de ports distribués **101**
 - port distribué **102**
 - taille de rafale **100**
- stratégies de port, groupes de ports distribués **125**
- stratégies de QoS, groupes de ports distribués **125**
- stratégies diverses, groupes de ports distribués **125**
- supprimer un groupe de ports **19**
- supprimer un groupe de ports distribués **48**
- supprimer un groupe de ports standard **19**
- surveillance de paquets **187**
- système d'exploitation client, supprimer une carte réseau **42**

T

- taille de rafale, commutateur standard **100**
- topologie de commutation, SR-IOV **153**
- trace de paquet
 - commande de console **189**
 - pktcap-uw **189**
- trafic
 - afficher les règles **112**
 - balisage avec CoS **107**
 - balisage avec DSCP **107**
 - filtrage et balisage **106, 122, 125**

- filtrage et balisage en fonction de l'adresse MAC **122**
- filtrage et balisage en fonction de l'ID VLAN **122**
- filtrage et balisage en fonction des propriétés de la couche de liaison de données **122**

- trafic de gestion **74, 79**
- Trafic de gestion **76**
- trafic de stockage IP **74**
- trafic Fault Tolerance **74**
- trafic iSCSI **74**
- trafic NFS **74**
- trafic Virtual SAN **74**
- trafic vMotion **74**
- trames Jumbo
 - activation dans le commutateur standard vSphere **139**
 - activation dans les machines virtuelles **140**
 - activation dans vSphere Distributed Switch **139**
 - activation sur un commutateur vSphere standard **139**
- trames Jumbo, activation **139**
- transmissions forgées **125**
- Transmissions forgées **95**
- TSO
 - Adaptateur réseau VMkernel **138**
 - machine virtuelle **137**

V

- vApp
 - configuration de IPv4 **181**
 - configuration de IPv6 **182**
 - profil de protocole réseau **183**
 - sélection d'associations réseau **181**
- VDS
 - affecter des cartes réseau physiques **33**
 - ajouter un hôte **31**
 - attribution de vmnics **33**
 - migration de cartes réseau physiques **33**
 - migration de vmnics **33**
- VGT **13**
- Virtualisation des E/S à racine unique
 - activation sur un adaptateur physique hôte **151**
 - Voir aussi* SR-IOV
- VLAN
 - contrôle de l'intégrité **55, 56**
 - définition **11**
 - mise en miroir de ports **172**
 - privé **59, 60**
 - secondaire **60**
 - type **59**

- VLAN privé
 - créer **59**
 - primaire **59, 60**
 - secondaire **59, 60**
 - suppression **60**
 - supprimer **60**
- VMkernel
 - configuration **73**
 - définition **11**
 - DNS **80**
 - IPv6 **80**
 - passerelle **80**
- vMotion
 - compatibilité **141**
 - configuration réseau **73**
 - définition **11**
 - mise en miroir de ports **167**
- VMware OUI
 - adresse MAC, hôte **161**
 - adresse MAC, statique **162**
 - attribution de vCenter Server **158**
- vpxd.cfg **160, 178**
- vSphere distributed switch
 - LLDP **175**
 - machines virtuelles **51**
 - migrer des machines virtuelles vers ou depuis **51**
 - miroir **166**
 - mise en miroir de ports **166**
 - modifier pool de ressources réseau **136**
 - Protocole LLDP (Link Layer Discovery Protocol) **175**
- vSphere Distributed Switch
 - ajout **25**
 - CDP **175**
 - CDP (Cisco Discovery Protocol) **175**
 - configuration du filtrage et du balisage du trafic sur un groupe de ports **106**
 - diagramme de la topologie, tous les hôtes **53**
 - diagramme de topologie, commutateur de proxy hôte **54**
 - diagrammes de la topologie **52**
 - filtrage et balisage du trafic **106**
 - filtrage et balisage du trafic sur un port **114**
 - mise à niveau **27**
 - ports **41**
 - protection contre l'emprunt d'identité d'adresse MAC **95**
 - protection contre le balayage du trafic **95**
 - règles de sécurité **95**
 - tiers **24**
 - trames Jumbo, activation **139**
 - Voir aussi* commutateur distribué
- VST (balisage de commutateur virtuel) **13**

