

vSphere Mise en réseau

ESXi 5.0.0

vCenter Serveur 5.0.0

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-000599-00

vmware®

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

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

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 © 2009–2011 VMware, Inc. Tous droits réservés. Ce produit est protégé par les lois américaines et internationales relatives au copyright et à la propriété intellectuelle. Les produits VMware sont protégés par un ou plusieurs brevets répertoriés à l'adresse <http://www.vmware.com/go/patents-fr>.

VMware est une marque déposée ou une marque de VMware, Inc. aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et noms mentionnés sont des marques déposées par leurs propriétaires respectifs.

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	5
1 Introduction à la mise en réseau	7
Présentation des concepts de mise en réseau	7
Services de réseau	8
Afficher les informations de mise en réseau dans vSphere Client	8
Afficher les informations de carte réseau dans vSphere Client	9
2 Configurer les communications réseau avec des commutateurs standard vSphere	11
commutateur standard vSphere	11
Groupes de ports standard	12
Configuration du groupes de ports pour des machines virtuelles	12
Configuration de réseau VMkernel	13
Propriétés des commutateurs standard vSphere	16
3 Configuration des communications réseau avec des vSphere Distributed Switches	19
vSphere Distributed Switch Architecture	20
Configurer un vSphere Distributed Switch	21
Groupes de ports distribués	26
Utilisation des ports distribués	27
VLAN privés	28
Configurer des adaptateurs réseau vSphere Distributed Switch	30
Configurer les communications réseau virtuelles sur un vSphere Distributed Switch	34
4 Gestion des ressources réseau	37
Contrôle d'E/S réseau vSphere	37
Délestage de segmentation TCP et Trames jumbo	41
NetQueue et performances réseau	43
DirectPath I/O	44
5 Règles de mise en réseau	47
Règle de basculement et d'équilibrage de charge	47
Règle VLAN	55
Règle de sécurité	56
Règle de formation du trafic	60
Règle d'allocation des ressources	64
Règle de surveillance	65
Règles de blocage des ports	66
Gérer les règles pour plusieurs groupes de ports sur un commutateur distribué vSphere	66

6	Mise en réseau avancée	71
	Activer la prise en charge d'Internet Protocol Version 6	71
	Configuration VLAN	72
	Utilisation de la mise en miroir de ports	72
	Configurer les paramètres NetFlow	76
	Switch Discovery Protocol	77
	Changer les configurations de routage et DNS	79
	Adresses MAC	79
	Montage de volumes NFS	80
7	Meilleures pratiques de mise en réseau	81
	Index	83

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 7](#)
- [« Services de réseau », page 8](#)
- [« Afficher les informations de mise en réseau dans vSphere Client », page 8](#)
- [« Afficher les informations de carte réseau dans vSphere Client », page 9](#)

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 de ESXi, il peut s'avérer utile consulter ces concepts.

Un réseau physique est un réseau de machines physiques connectées de sorte qu'elles puissent s'envoyer des données et en recevoir entre elles. VMware ESXi s'exécute sur une machine physique.

Un réseau virtuel est un réseau de machines virtuelles fonctionnant sur une machine physique unique, qui sont connectées logiquement entre elles de sorte qu'elles puissent envoyer des données et en recevoir entre elles. Des machines virtuelles peuvent être connectées à des réseaux virtuels que vous créez lorsque vous ajoutez un réseau.

Un commutateur Ethernet physique gère le trafic du réseau entre les machines sur le réseau physique. un commutateur possède plusieurs ports, et chacun peut être connecté à une machine unique ou à un autre commutateur sur le réseau. Chaque port peut être configuré pour se comporter de certaines manières, selon les besoins de la machine à laquelle il est connecté. Le commutateur connaît les hôtes qui sont connectés à ces ports et utilise ces informations pour acheminer le trafic aux machines physiques appropriées. Les commutateurs constituent le cœur d'un réseau physique. Plusieurs commutateurs peuvent être reliés entre eux pour former des réseaux plus grands.

Un commutateur standard vSphere fonctionne de façon similaire à 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.

Un vSphere Distributed Switch fait office de commutateur unique sur tous les hôtes associés dans un centre de données. Ceci permet à des machines virtuelles de conserver une configuration réseau cohérente pendant qu'elles migrent sur plusieurs hôtes.

Un port distribué est un port sur un vSphere Distributed Switch qui se connecte au VMkernel d'un hôte ou à un adaptateur réseau d'une machine virtuelle.

Un groupe de ports spécifie les options de configuration de ports, telles que les restrictions de bande passante et les stratégies de balisage VLAN pour chaque port membre. Les services réseau se connectent aux commutateurs standard via des groupes de ports. Les groupes de ports définissent la manière dont une connexion à un réseau est établie via le commutateur. Généralement, un seul commutateur standard est associé à un ou plusieurs groupes de ports.

Un groupe de ports distribués est un groupe de ports associés à un vSphere Distributed Switch et 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.

L'association NIC 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.

Les VLAN permettent 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.

La pile de communication réseau TCP/IP VMkernel prend en charge iSCSI, NFS et Fault Tolerance Logging. Les machines virtuelles exécutent leurs propres piles TCP/IP et se connectent au VMkernel au niveau de l'Ethernet via des commutateurs standard et distribués.

Le stockage IP se réfère à toute forme de stockage utilisant la communication de réseau TCP/IP comme sa fondation. iSCSI peut être utilisé comme banque de données de machine virtuelle, et NFS peut être employé comme banque de données de machine virtuelle ainsi que pour le montage direct de fichiers .ISO, présentés comme CD-ROM aux machines virtuelles.

TSO (TCP Segmentation Offload) permet à une pile TCP/IP d'émettre de très grandes trames (jusqu'à 64 Ko), même si l'unité de transmission maximale (MTU) de l'interface est plus petite. La carte réseau sépare alors la grande trame en trames adaptées à la taille MTU, et ajoute une copie ajustée des en-têtes initiaux TCP/IP.

La migration avec vMotion permet à une machine virtuelle sous tension d'être transférée d'un hôte ESXi vers un autre sans arrêter la machine virtuelle. La fonctionnalité facultative vMotion requiert une clé de licence.

Services de réseau

Un réseau virtuel fournit plusieurs services différents à l'hôte et aux machines virtuelles.

Vous pouvez activer trois types de service de 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.

Afficher les informations de mise en réseau dans vSphere Client

vSphere Client affiche les informations de mise en réseau générales ainsi que des informations spécifiques aux adaptateurs réseau.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.

- 3 (Facultatif) Choisissez le type de mise en réseau que vous souhaitez voir.

Option	Description
commutateur standard vSphere	Affiche les connexions réseau des commutateurs standard vSphere sur l'hôte.
vSphere Distributed Switch	Affiche les connexions réseau des vSphere Distributed Switchs sur l'hôte.

L'option **[vSphere Distributed Switch]** apparaît uniquement sur les hôtes connectés à un ou plusieurs vSphere Distributed Switchs.

Les informations de mise en réseau sont affichées pour chaque commutateur virtuel sur l'hôte.

Afficher les informations de carte réseau dans vSphere Client

Pour chaque carte réseau physique sur l'hôte, vous pouvez afficher des informations, telles que la vitesse, le duplex et les plages IP observées.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Cliquez sur l'onglet **[Configuration]**, puis sur **[Adaptateurs réseau]**.

Le panneau de adaptateurs réseau affiche les informations suivantes.

Tableau 1-1. Paramètres de carte réseau

Option	Description
[Périphérique]	Nom de l'adaptateur réseau.
[Vitesse]	Vitesse et duplex réels de la carte réseau.
[Configuré]	Vitesse et duplex configurés de la carte réseau.
[Commutateur]	Commutateur standard vSphere ou vSphere Distributed Switch associé à l'adaptateur réseau.
[Plages IP observées]	Adresses IP auxquelles l'adaptateur réseau peut vraisemblablement accéder.
[Réveil sur réseau local LAN pris en charge]	Possibilité pour l'adaptateur réseau de prendre en charge la fonction Wake on the LAN.

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 environnement vSphere.

Utilisez vSphere Client pour ajouter des communications réseau en fonction des catégories qui reflètent les types de services réseau.

- Machines virtuelles
- VMkernel

Ce chapitre aborde les rubriques suivantes :

- [« commutateur standard vSphere », page 11](#)
- [« Groupes de ports standard », page 12](#)
- [« Configuration du groupes de ports pour des machines virtuelles », page 12](#)
- [« Configuration de réseau VMkernel », page 13](#)
- [« Propriétés des commutateurs standard vSphere », page 16](#)

commutateur standard vSphere

Vous pouvez créer des périphériques réseau abstraits appelés commutateurs standard vSphere. Un commutateur standard peut router le trafic en interne entre les machines virtuelles et se connecter à des réseaux externes.

Vous pouvez utiliser des commutateurs standard pour combiner la bande passante de plusieurs adaptateurs réseau et équilibrer le trafic de communications entre eux. Vous pouvez également configurer un commutateur standard pour gérer le basculement NIC physique.

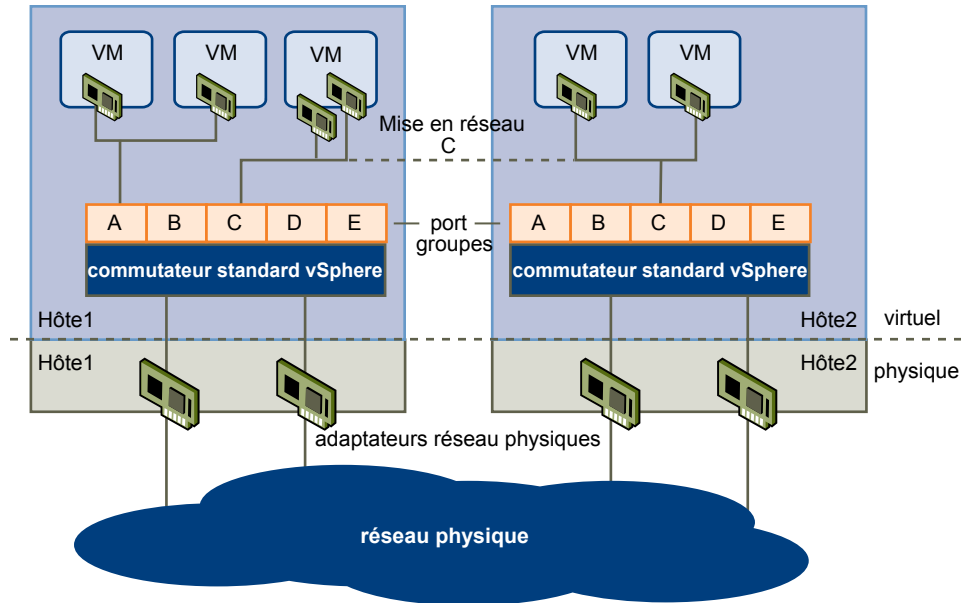
Un commutateur standard vSphere modélise un commutateur Ethernet physique. Le nombre par défaut de ports logiques pour un commutateur standard est 120. Vous pouvez connecter un adaptateur réseau de machine virtuelle à chaque port. Chaque carte de liaison montante associée à un commutateur standard utilise un port. Chaque port logique dans le commutateur standard est membre d'un seul groupe de ports. Chaque commutateur standard peut être également affecté d'un ou de plusieurs groupes de ports. Pour plus d'informations sur le nombre maximum de ports et de groupes de ports autorisés, voir *Maxima de configuration*.

Si au moins deux machines virtuelles sont connectées au même commutateur standard, le trafic réseau entre elles est routé localement. Si un adaptateur de liaison montante est connecté au commutateur standard, chaque machine virtuelle peut accéder au réseau externe auquel l'adaptateur est connecté.

Groupes de ports standard

Les groupes de ports regroupent plusieurs ports sous une configuration commune et fournissent un point d'ancrage stable pour les machines virtuelles qui se connectent à des réseaux étiquetés.

Figure 2-1. Réseau de commutateurs standard vSphere



Chaque groupe de ports est identifié par une étiquette de réseau, unique à l'hôte actuel. Les étiquettes réseau sont utilisées pour rendre compatible la configuration des machines virtuelles sur les hôtes. Tous les groupes de ports dans le centre de données qui sont physiquement connectés au même réseau (dans le sens que chacun peut recevoir des diffusions des autres) reçoivent le même nom. Au contraire, si deux groupes de ports ne peuvent pas recevoir des diffusions l'un de l'autre, ils ont des étiquettes distinctes.

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. Afin que chaque groupe de ports atteigne des groupes de ports situés sur d'autres VLAN, l'ID de VLAN doit être défini sur 4095. Si vous utilisez des ID de VLAN, vous devez modifier les étiquettes de groupes et les ID de VLAN en même temps afin que les étiquettes représentent correctement la connectivité.

Configuration du groupe de ports pour des machines virtuelles

Vous pouvez ajouter ou modifier un groupe de ports de machines virtuelles à partir de vSphere Client.

L'assistant Ajouter réseau de vSphere Client vous aide à créer un réseau virtuel auquel les machines virtuelles peuvent se connecter, y compris un commutateur standard vSphere et 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 dans 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

Les groupes de ports de machine virtuelle fournissent un réseau pour les machines virtuelles.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 4 Sélectionnez la vue Commutateur standard vSphere.

Les commutateurs standard apparaissent dans une présentation détaillée.

- 5 Sur le côté droit de la page, cliquez sur **[Ajouter gestion réseau]**.
- 6 Acceptez le type de connexion par défaut, **[Machines virtuelles]**, puis cliquez sur **[Suivant]**.
- 7 Sélectionnez **[Créer un commutateur vSphere standard]** ou l'un des commutateur standard existants listés et les adaptateurs physiques associés à utiliser pour ce groupes de ports.

Vous pouvez créer un commutateur standard avec ou sans adaptateurs Ethernet.

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.

- 8 Cliquez sur **[Suivant]**.
- 9 Dans le groupes Propriétés groupes de ports, entrez une étiquette de réseau qui identifie le groupes de ports que vous créez.

Utilisez des étiquettes réseau pour identifier les connexions compatibles pour la migration communes à deux hôtes ou plus.

- 10 (Facultatif) Si vous utilisez un VLAN, pour **[ID VLAN]**, entrez un nombre entre 1 et 4 094. Si vous n'utilisez pas un VLAN, laissez ce champ vide.

Si vous entrez 0 ou laissez ce champ vide, le groupes de ports peut uniquement voir le trafic non balisé (non VLAN). Si vous entrez 4 095, le groupes de ports peut voir le trafic sur n'importe quel VLAN tout en laissant les balises VLAN intactes.

- 11 Cliquez sur **[Suivant]**.
- 12 Après avoir déterminé que le commutateur est configuré correctement, cliquez sur **[Terminer]**.

Configuration de réseau VMkernel

Une interface réseau VMkernel fournit la connectivité réseau pour l'hôte et la gestion VMware vMotion, Stockage IP et Tolérance aux pannes.

Le déplacement d'une machine virtuelle d'un hôte à un autre est appelé migration. vMotion vous permet de migrer des machines virtuelles sous tension sans temps d'arrêt. Votre pile réseau VMkernel doit être configurée correctement pour recevoir vMotion.

Le stockage IP fait référence à n'importe quelle forme de stockage qui utilise les communications ESXi TCP/IP. Comme ces types de stockages reposent sur le réseau, ils peuvent utiliser la même interface VMkernel et le même groupes de ports.

Pile TCP/IP au niveau de VMkernel

La pile réseau TCP/IP VMkernel de VMware fournit la prise en charge réseau de plusieurs manières pour chaque service qu'elle traite.

La pile TCP/IP VMkernel traite iSCSI, NFS et vMotion des manières suivantes.

- iSCSI comme banque de données de machine virtuelle.
- iSCSI pour le montage direct de fichiers .ISO, qui sont présentés comme des CD-ROM virtuels aux machines virtuelles.
- NFS comme banque de données de machine virtuelle.
- NFS pour le montage direct de fichiers .ISO, qui sont présentés comme des CD-ROM virtuels aux machines virtuelles.
- Migration avec vMotion.
- Journalisation de la tolérance aux pannes.
- Liaison de port pour les interfaces vMotion.
- Fournit des informations réseau aux cartes matérielles iSCSI dépendantes.

Si vous avez deux adaptateurs réseau iSCSI physiques ou plus, vous pouvez créer plusieurs chemins pour le logiciel iSCSI en configurant les chemins multiples iSCSI. Pour plus d'informations sur les chemins multiples iSCSI, voir la documentation *Stockage vSphere*.

REMARQUE ESXi prend uniquement en charge NFS version 3 sur TCP/IP.

Configurer les communications réseau VMkernel sur un commutateur standard vSphere

Créez un adaptateur réseau VMkernel utilisable en tant qu'interface vMotion ou que groupes de ports de stockage d'IP.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.
- 4 Dans la vue Commutateur standard vSphere, cliquez sur **[Ajouter mise en réseau]**.
- 5 Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]**.
- 6 Sélectionnez le commutateur standard vSphere à utiliser ou **[Créer un commutateur standard vSphere]** pour créer un commutateur standard vSphere.
- 7 Cochez les cases des adaptateurs réseau du commutateur standard vSphere à utiliser.

Sélectionnez les adaptateurs de chaque commutateur standard vSphere afin que les machines virtuelles ou les autres services qui se connectent via l'adaptateur puissent atteindre le segment Ethernet correct. Si aucun adaptateur n'apparaît dans *Créer un commutateur standard vSphere*, tous les adaptateurs réseau du système sont utilisés par les commutateurs standard vSphere ou les vSphere Distributed Switches. Vous pouvez créer un commutateur standard vSphere sans adaptateur réseau ou sélectionner un adaptateur réseau utilisé par un commutateur standard vSphere existant.

8 Cliquez sur **[Suivant]** .

9 Sélectionnez ou entrez une étiquette réseau ou un ID de VLAN.

Option	Description
[Étiquette de réseau]	Nom identifiant le groupes de ports que vous créez. Il s'agit de l'étiquette que vous définissez lorsque vous configurez des services VMkernel, tels que vMotion et le stockage IP, et configurez un adaptateur virtuel à associer au groupe de ports.
[ID VLAN]	Identifie le VLAN que le trafic réseau du groupe de ports utilisera.

10 (Facultatif) Sélectionnez **[Utiliser ce groupe de ports pour vMotion]** pour permettre au groupes de ports de s'annoncer à un autre hôte comme connexion réseau via laquelle le trafic de vMotion doit être envoyé.

11 (Facultatif) Sélectionnez **[Utiliser ce groupe de ports pour la journalisation de la tolérance aux pannes]** .

12 (Facultatif) Sélectionnez **[Utiliser ce groupe port pour trafic gestion]** .

13 Si IPv6 est activé sur l'hôte, sélectionnez **[IP (valeur par défaut)]** , **[IPv6]** ou **[Communications réseau IP et IPv6]** .

Cette option n'apparaît pas sur les hôtes sur lesquels IPv6 n'est pas activé. La configuration IPv6 ne peut pas être utilisée avec les adaptateurs iSCSI matériels dépendants.

14 Cliquez sur **[Suivant]** .

15 Sélectionnez le mode d'obtention des paramètres IP.

Option	Description
[Obtenez les paramètres d'IP automatiquement]	Utilisez DHCP pour obtenir les paramètres IP.
[Utilisez les paramètres d'IP suivants]	<p>Définissez les paramètres IP manuellement.</p> <ul style="list-style-type: none"> a Entrez l'adresse IP et un masque de sous-réseau pour l'interface VMkernel. b Cliquez sur [Modifier] pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI. <p>Dans l'onglet [Config. DNS] , le nom de l'hôte est entré par défaut. Les adresses de serveur DNS spécifiées pendant l'installation sont également présélectionnées, de même que le domaine.</p> <ul style="list-style-type: none"> c Cliquez sur [OK] , puis sur [Suivant] .

16 Si vous utilisez IPv6 pour l'interface VMkernel, sélectionnez une option pour obtenir les adresses IPv6.

Option	Description
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6.
Obtenir l'adresse IPv6 automatiquement via publicité routeur	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Adresses IPv6 statiques	<ul style="list-style-type: none"> a Cliquez sur [Ajouter] pour ajouter une nouvelle adresse IPv6. b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur [OK] . c Pour modifier la passerelle par défaut de VMkernel, cliquez sur [Modifier] .

17 Cliquez sur **[Suivant]** .

- 18 Vérifiez les informations, cliquez sur **[Retour]** pour modifier des entrées, puis cliquez sur **[Terminer]** .

Afficher les informations de routage VMkernel sur un commutateur standard vSphere

Vous pouvez afficher les informations de routage IP et IPv6, telles que le réseau, le préfixe et la passerelle, d'une interface réseau VMkernel sur un commutateur standard vSphere.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]** .
- 2 Dans l'onglet **[Configuration]** , cliquez sur **[Mise en réseau]** .
- 3 Cliquez sur les **[Propriétés]** du commutateur standard associé à l'interface VMkernel que vous souhaitez afficher.
- 4 Dans l'onglet Ports, sélectionnez l'adaptateur réseau VMkernel à afficher et cliquez sur **[Afficher le tableau de routage]** sous les paramètres IP ou les paramètres IPv6.

Un tableau de routage comprenant des informations sur le réseau, le préfixe et la passerelle de l'adaptateur réseau VMkernel sélectionné apparaît.

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

Un commutateur standard vSphere fait office de conteneur pour les configurations de ports qui utilisent un ensemble commun d'adaptateurs réseau, y compris les ensembles qui ne contiennent aucun adaptateur réseau. Chaque commutateur virtuel fournit un nombre déterminé de ports à travers lesquels les machines virtuelles et les services réseau peuvent atteindre un ou plusieurs réseaux.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .
- 3 Dans la partie droite de la page, cliquez sur **[Propriétés]** pour le commutateur standard à modifier.
- 4 Cliquez sur l'onglet **[Ports]** .
- 5 Sélectionnez le commutateur standard dans la liste Configuration et cliquez sur **[Modifier]** .
- 6 Cliquez sur l'onglet **[Général]** .
- 7 Choisissez le nombre de ports que vous souhaitez utiliser dans le menu déroulant.
- 8 Cliquez sur **[OK]** .

Suivant

Les modifications entreront en vigueur au redémarrage du système.

Modification de la vitesse d'un adaptateur de liaison montante

Vous pouvez modifier la vitesse de connexion et le duplex d'un adaptateur de liaison montante.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Sélectionnez un commutateur standard et cliquez sur **[Propriétés]**.
- 4 Cliquez sur l'onglet **[Adaptateurs réseau]**.
- 5 Pour modifier la vitesse configurée et la valeur de duplex d'un adaptateur réseau, sélectionnez l'adaptateur réseau et cliquez sur **[Modifier]**.
- 6 Pour sélectionner la vitesse de connexion manuellement, sélectionnez la vitesse et le duplex dans le menu déroulant.

Choisissez la vitesse de connexion manuellement si la carte réseau et le commutateur physique risquent d'échouer dans la négociation de la vitesse de connexion correcte. Les symptômes de non-correspondance de vitesse et de duplex comprennent une bande passante faible ou aucune connectivité de liaison.

L'adaptateur et le port du commutateur physique auquel il est connecté doivent être définis sur la même valeur, telle que auto et auto ou ND et ND, où ND correspond à une certaine vitesse et à un duplex, mais pas à auto et ND.

- 7 Cliquez sur **[OK]**.

Ajout d'adaptateurs de liaison montante

Vous pouvez associer plusieurs adaptateurs à un seul commutateur standard vSwitch pour fournir l'association NIC. L'association peut partager du trafic et fournir un basculement.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Sélectionnez un commutateur standard et cliquez sur **[Propriétés]**.
- 4 Cliquez sur l'onglet **[Adaptateurs réseau]**.
- 5 Cliquez sur **[Ajouter]** pour lancer l'assistant Ajouter adaptateur.
- 6 Sélectionnez un ou plusieurs adaptateurs dans la liste et cliquez sur **[Suivant]**.
- 7 (Facultatif) Pour réorganiser les adaptateurs réseau dans une catégorie différente, sélectionnez un adaptateur et cliquez sur **[Monter]** et **[Descendre]**.

Option	Description
Adaptateurs actifs	Les adaptateurs qu'utilise le commutateur standard.
Adaptateurs standby	Adaptateurs qui deviennent actifs si un ou plusieurs adaptateurs actifs sont défectueux.

- 8 Cliquez sur **[Suivant]**.
- 9 Vérifiez les informations sur la page Résumé d'adaptateur, cliquez sur **[Retour]** pour modifier des entrées, puis cliquez sur **[Terminer]**.

La liste des adaptateurs réseau réapparaît avec les adaptateurs que le commutateur standard demande.

- 10 Cliquez sur **[Fermer]** pour quitter la boîte de dialogue.

La section Mise en réseau de l'onglet **[Configuration]** montre les adaptateurs réseau dans l'ordre et les catégories désignés.

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.

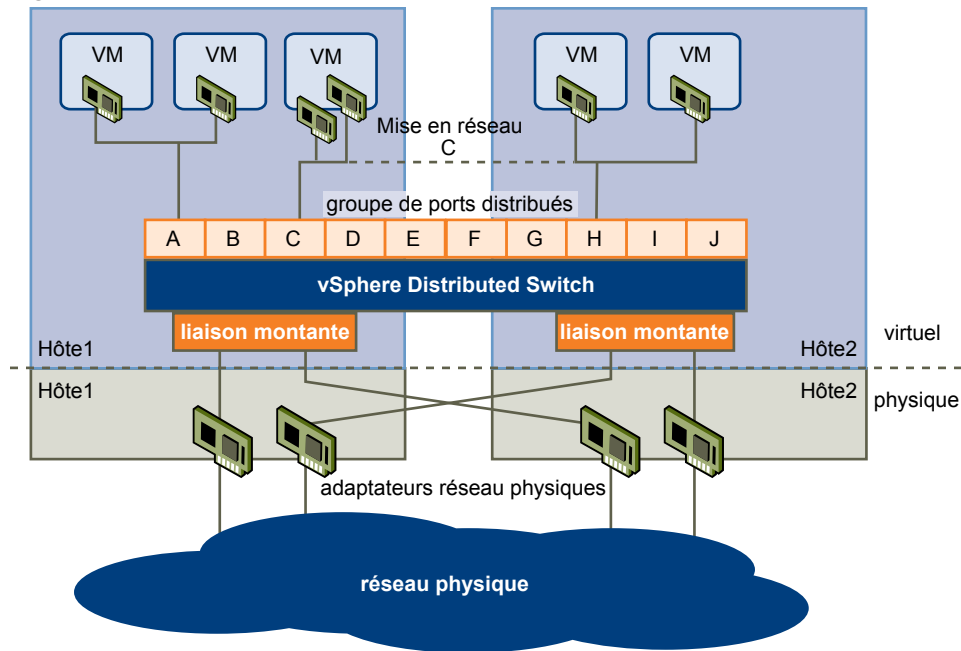
Ce chapitre aborde les rubriques suivantes :

- [« vSphere Distributed Switch Architecture », page 20](#)
- [« Configurer un vSphere Distributed Switch », page 21](#)
- [« Groupes de ports distribués », page 26](#)
- [« Utilisation des ports distribués », page 27](#)
- [« VLAN privés », page 28](#)
- [« Configurer des adaptateurs réseau vSphere Distributed Switch », page 30](#)
- [« Configurer les communications réseau virtuelles sur un vSphere Distributed Switch », page 34](#)

vSphere Distributed Switch Architecture

Un vSphere Distributed Switch fonctionne comme un commutateur unique sur tous les hôtes associés. Cela permet de régler les configurations réseau qui s'étendent sur tous les hôtes membres et permet aux machines virtuelles de conserver une configuration réseau cohérente lorsqu'elles migrent à travers plusieurs hôtes.

Figure 3-1. Réseau de vSphere Distributed Switchs



À l'instar d'un commutateur standard vSphere, chaque vSphere Distributed Switch est un hub de réseau que peuvent utiliser les machines virtuelles. Un commutateur distribué peut acheminer le trafic en interne entre les machines virtuelles ou se lier à un réseau externe en se connectant à des cartes Ethernet physiques, également appelées cartes de liaison montante.

Chaque commutateur distribué peut être également affecté à un ou plusieurs groupes de ports. Les groupes de ports distribués regroupent plusieurs ports dans une configuration commune et fournissent un point d'ancrage stable pour les machines virtuelles qui se connectent à des réseaux étiquetés. Chaque groupe de ports distribués est identifié par une étiquette réseau qui est unique dans le centre de données actuel. L'ID de VLAN est facultative. Elle permet de limiter le trafic du groupes de ports à un segment Ethernet logique dans le réseau physique.

Les pools de ressources réseau permettent de gérer le trafic réseau par type de trafic réseau.

Outre les vSphere Distributed Switch, vSphere 5 fournit également le support pour des commutateurs virtuels tiers. Pour plus d'informations sur la configuration du commutateur Cisco Nexus 1000v, accédez à <http://www.cisco.com/go/1000vdocs>.

Configurer un vSphere Distributed Switch

Vous pouvez créer un vSphere Distributed Switch sur un centre de données vCenter Server. Après avoir créé un vSphere Distributed Switch, vous pouvez ajouter des hôtes, créer des groupes de ports distribués et modifier les règles et propriétés du commutateur distribué.

Ajouter un vSphere Distributed Switch

Créez un commutateur distribué vSphere dans un centre de données vCenter Server pour gérer le trafic réseau de tous les hôtes associés dans le centre de données.

Si votre système a besoin de groupes de ports complexes, créez un groupe de ports distribués au lieu d'un groupe de ports par défaut.

Procédure

- 1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le centre de données.
- 2 Sélectionnez **[Inventaire] > [Centre de données] > [Nouveau vSphere Distributed Switch]**.
- 3 Sélectionnez une version de commutateur distribué vSphere.

Option	Description
Version de vSphere Distributed Switch : 4.0	Compatible avec la version ESX/ESXi 4,0 et ultérieure. Les fonctions publiées avec les versions ultérieures du commutateur distribué vSphere ne sont pas prises en charge.
Version de vSphere Distributed Switch : 4.1.0	Compatible avec la version ESX/ESXi 4.1 et ultérieure. Les fonctions publiées avec les versions ultérieures du commutateur distribué vSphere ne sont pas prises en charge.
Version de vSphere Distributed Switch : 5.0.0	Compatible avec la version ESXi 5.0 et les versions ultérieures.

- 4 Cliquez sur **[Suivant]**.
- 5 Dans la zone de texte **[Nom]**, entrez le nom du nouveau commutateur distribué vSphere.
- 6 Utilisez les boutons fléchés pour sélectionner le **[Nombre de ports de liaison montante]** et cliquez sur **[Suivant]**.

Les ports de liaison montante connectent le distributed switch aux cartes NIC physiques sur les hôtes associés. Le nombre de ports de liaison montante est le nombre maximum de connections physiques autorisées au distributed switch par hôte.

- 7 Indiquez si vous voulez ajouter des hôtes et leurs adaptateurs physiques au commutateur distribué vSphere maintenant ou plus tard.

Si vous choisissez **[Ajouter maintenant]**, sélectionnez les hôtes et les adaptateurs physiques à utiliser en cochant la case correspondant à chaque hôte ou adaptateur. Vous pouvez libérer des adaptateurs physiques uniquement pour un vSphere Distributed Switch au cours de la création du distributed switch.

- 8 (Facultatif) Définissez le nombre maximal de ports sur un hôte.
 - a Cliquez sur **[Afficher détails]** pour l'hôte.
 - b Sélectionnez le nombre maximal de ports de l'hôte dans le menu déroulant.
 - c Cliquez sur **[OK]**.
- 9 Cliquez sur **[Suivant]**.
- 10 (Facultatif) Choisissez s'il faut **[Créer automatiquement un groupe de ports par défaut]**.

Cette option crée un groupe de ports distribués avec les paramètres par défaut.

- 11 Cliquez sur **[Terminer]** .

Suivant

Si vous choisissez d'ajouter les hôtes plus tard, vous devez les ajouter au distributed switch avant d'ajouter les adaptateurs réseau.

Vous pouvez ajouter des adaptateurs réseau depuis la page de configuration d'hôte de vSphere Client en utilisant Gérer les hôtes ou Profils d'hôte.

Ajouter des hôtes à un vSphere Distributed Switch

Vous pouvez ajouter des hôtes et des adaptateurs physiques à un vSphere distributed switch au niveau du commutateur distribué après sa création.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Ajouter un hôte]** .
- 3 Sélectionnez les hôtes à ajouter.
- 4 Sous les hôtes sélectionnés, sélectionnez les adaptateurs physiques à ajouter et cliquez sur **[Suivant]** .

Vous pouvez sélectionner des adaptateurs physiques inutilisés et utilisés.

REMARQUE Le transfert d'un adaptateur physique vers un commutateur distribué sans déplacer d'adaptateur virtuel associé peut entraîner la perte de connexion réseau de ces adaptateurs virtuels.

- 5 Pour chaque adaptateur virtuel, sélectionnez **[Groupes de ports destination]** et un groupe de ports dans le menu déroulant pour faire migrer l'adaptateur virtuel vers le commutateur distribué ou **[Ne pas migrer]** .
- 6 (Facultatif) Définissez le nombre maximal de ports sur un hôte.
 - a Cliquez sur **[Afficher détails]** pour l'hôte.
 - b Sélectionnez le nombre maximal de ports de l'hôte dans le menu déroulant.
 - c Cliquez sur **[OK]** .
- 7 Cliquez sur **[Suivant]** .
- 8 (Facultatif) Faites migrer la gestion de réseau des machines virtuelles vers le commutateur distribué.
 - a Sélectionnez **[Migrer mise en réseau VM]** .
 - b Pour chaque machine virtuelle, sélectionnez **[Groupe de ports destination]** et un groupe de ports dans le menu déroulant ou **[Ne pas migrer]** .
- 9 Cliquez sur **[Suivant]** .
- 10 (Facultatif) Si vous devez apporter des modifications, cliquez sur **[Retour]** pour revenir à l'écran approprié.
- 11 Vérifiez les paramètres du commutateur distribué et cliquez sur **[Terminer]** .

Gérer les hôtes dans un vSphere Distributed Switch

Vous pouvez modifier la configuration des hôtes et des adaptateurs physiques dans un commutateur distribué vSphere après leur ajout au commutateur distribué.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué et sélectionnez **[Gérer les hôtes]**.
- 3 Sélectionnez les hôtes à gérer et cliquez sur **[Suivant]**.
- 4 Sélectionnez les adaptateurs physiques à ajouter, désélectionnez les adaptateurs physiques à supprimer, et cliquez sur **[Suivant]**.
- 5 Pour chaque adaptateur virtuel, sélectionnez le **[groupe de ports destination]** dans le menu déroulant pour migrer l'adaptateur virtuel vers le commutateur distribué ou sélectionnez **[Ne pas migrer]**.
- 6 Cliquez sur **[Suivant]**.
- 7 Migrer la gestion de réseau des machines virtuelles vers le commutateur distribué vSphere.
 - a Sélectionnez **[Migrer mise en réseau VM]**.
 - b Pour chaque machine virtuelle, sélectionnez le groupes de ports de destination **[groupes ports destination]** dans le menu déroulant ou sélectionnez **[Ne pas migrer]**.
- 8 Cliquez sur **[Suivant]**.
- 9 (Facultatif) Si vous devez apporter des modifications, cliquez sur **[Retour]** pour revenir à l'écran approprié.
- 10 Vérifiez les paramètres du commutateur distribué et cliquez sur **[Terminer]**.

Définir le nombre de ports par hôte sur un vSphere Distributed Switch

Définissez le nombre maximum de ports sur un hôte pour limiter le nombre de ports distribués qui peuvent exister sur un ou plusieurs hôtes associés à un commutateur distribué vSphere.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte à modifier dans le panneau d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.
- 4 Sélectionnez la vue **[vSphere Distributed Switch]**.
- 5 Cliquez sur **[Propriétés]** à côté du commutateur distribué vSphere pour modifier.
- 6 Sélectionnez le nombre maximum de ports dans le menu déroulant 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.

Modifier les paramètres généraux de vSphere Distributed Switch

Vous pouvez modifier les paramètres généraux d'un vSphere Distributed Switch, tels que le nom du commutateur distribué et le nombre de ports de liaison montante sur le commutateur distribué.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Général]** pour modifier les paramètres de vSphere Distributed Switch.

Option	Description
Nom	Entrez le nom du commutateur distribué.
Nombre de ports de liaison montante	Sélectionnez le nombre de ports de liaison montante du commutateur distribué.
Remarques	Entrez des remarques éventuelles sur le commutateur distribué.

- 4 (Facultatif) Modifiez les noms des ports de liaison montante.
 - a Cliquez sur **[Modifier noms liaison montante]**.
 - b Tapez le nouveau nom du ou des ports de liaison montante.
 - c Cliquez sur **[OK]**.
- 5 Cliquez sur **[OK]**.

Modifier les paramètres avancés de vSphere Distributed Switch

Vous pouvez changer les paramètres avancés vSphere Distributed Switch, tels que le protocole de découverte Cisco et la taille maximale MTU de vSphere Distributed Switch.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Avancé]** pour modifier les paramètres vSphere Distributed Switch suivants.

Option	Description
MTU maximal	Taille de MTU maximale pour le vSphere Distributed Switch.
État du protocole de découverte	<p>Choisissez l'état du protocole de découverte dans le vSphere Distributed Switch.</p> <ul style="list-style-type: none"> ■ [Activé]. Protocole de découverte activé pour le vSphere Distributed Switch. <ol style="list-style-type: none"> 1 Sélectionnez [Protocole découverte Cisco] ou [Protocole de découverte de couche de lien] dans le menu déroulant [Type]. 2 Affectez à [Opération] la valeur [Écouter], [Annoncer] ou [Les deux]. ■ [Désactivé].
Informations de contact admin	Entrez le [Nom] et les [Autres détails] de l'administrateur de vSphere Distributed Switch.

- 4 Cliquez sur **[OK]**.

Afficher les informations de l'adaptateur réseau pour un vSphere Distributed Switch

Affichez les adaptateurs réseau physiques et les affectations de liaison montante d'un vSphere Distributed Switch depuis la vue d'inventaire des connexions réseau de vSphere Client.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Dans l'onglet **[Adaptateurs réseau]** , vous pouvez afficher la carte réseau et les attributions de liaison montante des hôtes associés.

Cet onglet est accessible en lecture seule. Les adaptateurs réseau des commutateurs distribués doivent être configurés au niveau de l'hôte.
- 4 Cliquez sur **[OK]** .

Mettre à niveau un vSphere Distributed Switch vers une nouvelle version

Un commutateur distribué Sphere 4.0 ou 4.1 peut être une mise à niveau vers une version suivante pour lui permettre de tirer parti des fonctions disponibles uniquement dans la nouvelle version.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Résumé]** , en regard de **[Version]** , sélectionnez **[Mise à niveau]** .

L'assistant de mise à niveau répertorie les fonctions disponibles pour le commutateur distribué mis à niveau qui ne l'étaient pas dans la version précédente.

- 4 Sélectionnez la version de commutateur distribué vSphere à mettre à niveau.

Option	Description
Version de vSphere Distributed Switch : 4.1.0	Compatible avec la version ESX/ESXi 4.1 et ultérieure. Les fonctions publiées avec les versions ultérieures du commutateur distribué vSphere ne sont pas prises en charge.
Version de vSphere Distributed Switch : 5.0.0	Compatible avec la version ESXi 5.0 et les versions ultérieures.

- 5 Cliquez sur **[Suivant]** .

L'assistant de mise à niveau répertorie les hôtes associés au commutateur distribué vSphere et indique s'ils sont compatibles avec la version de commutateur distribué vSphere mise à niveau. Vous ne pouvez effectuer la mise à niveau que si tous les hôtes sont compatibles avec la nouvelle version du commutateur distribué vSphere.

La raison de la compatibilité figure à côté de chaque hôte compatible.

- 6 Cliquez sur **[Suivant]** .
- 7 Vérifiez l'exactitude des informations de mise à niveau répertoriées et cliquez sur **[Terminer]** .

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

Ajoutez un groupe de ports distribués à un vSphere Distributed Switch pour créer un réseau de commutation distribué pour les machines virtuelles.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez **[Inventaire] > [vSphere Distributed Switch] > [Nouveau groupe de ports]**.
- 3 Entrez un **[Nom]** et le **[Nombre de ports]** du nouveau groupe de ports distribués.
- 4 Sélectionnez un type de VLAN.

Option	Description
Aucune	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.

- 5 Cliquez sur **[Suivant]**.
- 6 Cliquez sur **[Terminer]**.

Modifier les paramètres généraux d'un groupe de ports distribués

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Général]** pour modifier les paramètres de groupe de ports distribués suivants.

Option	Action
Nom	Entrez le nom du groupe de ports distribués.
Description	Décrivez brièvement le groupe de ports distribués.

Option	Action
Nombre de ports	Entrez le nombre de ports dans le groupe de ports distribués.
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"> ■ Sélectionnez [Liaison statique] pour affecter un port à une machine virtuelle quand la machine virtuelle se connecte au groupe de ports distribués. Cette option n'est pas disponible lorsque vSphere Client est connecté directement à ESXi. ■ Sélectionnez [Liaison dynamique] pour affecter un port à une machine virtuelle à la première mise sous tension de la machine virtuelle une fois connectée au groupe de ports distribués. La liaison dynamique est obsolète dans ESXi 5.0. ■ Sélectionnez [Éphémère] pour aucune liaison de port. Cette option n'est pas disponible lorsque vSphere Client est connecté directement à ESXi.

- 4 Cliquez sur **[OK]**.

Modifier les paramètres avancés d'un groupe de ports distribués

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Avancé]** pour modifier les propriétés de groupes de ports distribués.

Option	Description
Autoriser le remplacement des règles de port	Sélectionnez cette option pour autoriser le remplacement des règles de groupes de ports distribués au niveau de chaque port. Cliquez sur [Modifier paramètres remplacement] pour sélectionner les règles qui peuvent être remplacées au niveau du port.
Modifier paramètres remplacement	Sélectionnez les règles qui peuvent être remplacées au niveau du port.
Configurez la réinitialisation à la déconnexion	Quand un port distribué est déconnecté d'une machine virtuelle, la configuration de ports distribués devient identique au paramétrage de groupe de ports distribués. Tous les remplacements par port sont ignorés.

- 4 Cliquez sur **[OK]**.

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.

Contrôle de l'état des ports distribués

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.

- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]**, cliquez sur **[Commencer à surveiller l'état du port]**.

Le tableau dans l'onglet Ports du commutateur distribué affiche maintenant les statistiques d'exécution de chaque port distribué, y compris le trafic et les paquets de diffusion, multidiffusion et entrant et sortant de monodiffusion.

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

Tableau 3-1. États des ports distribués

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

Définir les paramètres de ports distribués

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]**, cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]**.
- 4 Cliquez sur **[Général]**.
- 5 Modifiez la description et le nom du port.
- 6 Cliquez sur **[OK]**.

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

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez l'onglet **[VLAN privé]**.
- 4 Sous l'ID VLAN privé primaire, cliquez sur **[Saisir un ID VLAN privé ici]**, et saisissez le numéro de VLAN privé primaire.
- 5 Cliquez n'importe où dans la boîte de dialogue, puis sélectionnez le VLAN privé primaire que vous venez d'ajouter.
Ce dernier apparaît sous ID VLAN privé secondaire.
- 6 Pour chaque nouveau VLAN privé secondaire, cliquez sur **[Saisir un ID VLAN privé ici]** sous ID VLAN privé secondaire, et saisissez le numéro du VLAN privé secondaire.
- 7 Cliquez n'importe où dans la boîte de dialogue, sélectionnez le VLAN privé secondaire que vous venez d'ajouter, et sélectionnez **[Isolé]** ou **[Communauté]** comme type de port.
- 8 Cliquez sur **[OK]**.

Supprimer un VLAN privé principal

Supprimez les VLAN privés primaires non utilisés dans la vue d'inventaire de mise en réseau du vSphere Client.

Prérequis

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez l'onglet **[VLAN privé]**.
- 4 Sélectionnez le VLAN privé principal à supprimer.
- 5 Cliquez sur **[Supprimer]** sous ID VLAN privé primaire, puis cliquez sur **[OK]**.

Le retrait d'un VLAN privé primaire supprime également l'ensemble des VLAN privés secondaires associés.

Supprimer un VLAN privé secondaire

Supprimez les VLAN privés secondaires non utilisés dans la vue d'inventaire de mise en réseau du vSphere Client.

Prérequis

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sélectionnez l'onglet **[VLAN privé]** .
- 4 Sélectionnez un VLAN privé principal pour afficher l'ensemble de ses VLAN privés secondaires associés.
- 5 Sélectionnez le VLAN privé secondaire à supprimer.
- 6 Cliquez sur **[Supprimer]** sous ID VLAN privé secondaire, puis cliquez sur **[OK]** .

Configurer des adaptateurs réseau vSphere Distributed Switch

La vue des communications réseau vSphere Distributed Switch de la page de configuration de l'hôte affiche la configuration des vSphere Distributed Switchs de l'hôte et permet de configurer les adaptateurs réseau vSphere Distributed Switch et les ports montants.

Gestion des cartes physiques

Pour chaque hôte associé à un commutateur distribué vSphere, vous devez affecter des adaptateurs réseau physiques, ou liaisons montantes, au commutateur distribué vSphere. Vous pouvez affecter une liaison montante sur chaque port de liaison montante de chaque hôte dans le commutateur distribué vSphere.

Ajouter une liaison montante à un vSphere Distributed Switch

Pour chaque hôte associé à un commutateur distribué vSphere, vous devez affecter au moins un adaptateur réseau physique, ou liaison montante, au commutateur distribué vSphere.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.
La page de configuration matérielle pour l'hôte sélectionné s'affiche.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .
- 3 Sélectionnez la vue **[Commutateur distribué vSphere]** .
- 4 Cliquez sur **[Gérer adaptateurs physiques]** .
- 5 Cliquez sur **[Cliquez pour ajouter carte réseau]** pour le port de liaison montante auquel ajouter une liaison montante.
- 6 Sélectionnez la carte physique à ajouter.
Si vous choisissez un adaptateur attaché à un autre commutateur, il est retiré du commutateur et réaffecté au commutateur distribué vSphere.
- 7 Cliquez sur **[OK]** .

Supprimer une liaison montante d'un vSphere Distributed Switch

Vous pouvez supprimer une liaison montante ou l'adaptateur réseau physique d'un commutateur distribué vSphere.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
La page de configuration matérielle pour ce serveur s'affiche.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

- 3 Sélectionnez la vue **[Commutateur distribué vSphere]** .
- 4 Cliquez sur **[Gérer adaptateurs physiques]** .
- 5 Cliquez sur **[Supprimer]** pour supprimer la liaison montante du commutateur distribué vSphere.
- 6 Cliquez sur **[OK]** .

Gestion des adaptateurs réseau virtuelles

Les adaptateurs réseau virtuelles gèrent les services réseau de l'hôte sur un vSphere Distributed Switch.

Vous pouvez configurer les adaptateurs virtuels VMkernel d'un hôte via un vSphere distributed switch associé en créant des cartes virtuelles ou en migrant des adaptateurs virtuels existants.

Créer un adaptateur réseau VMkernel dans un vSphere Distributed Switch

Créez un adaptateur réseau VMkernel utilisable en tant qu'interface vMotion ou que groupes de ports de stockage d'IP.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]** .
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]** , cliquez sur **[Mise en réseau]** .
- 4 Sélectionnez la vue vSphere Distributed Switch.
- 5 Cliquez sur **[Gérer adaptateurs virtuels]** .
- 6 Cliquez sur **[Ajouter]** .
- 7 Sélectionnez **[Nouvel adaptateur virtuel]** et cliquez sur **[Suivant]** .
- 8 Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .
- 9 Choisissez une connexion de port distribué ou de groupes de ports distribués pour la carte virtuelle.

Option	Description
Sélectionnez un groupe de ports	Dans le menu déroulant, choisissez le groupe de ports distribués de la carte virtuelle à laquelle vous voulez vous connecter.
Sélectionnez le port	Tapez l'ID du port distribué de la carte réseau virtuelle à laquelle vous voulez vous connecter.

- 10 Sélectionnez **[Utiliser cet adaptateur virtuel pour vMotion]** pour permettre à ce groupe de ports de s'annoncer à un autre hôte ESXi comme connexion réseau où le trafic vMotion est envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte. Si cette propriété n'est pas activée pour un groupe de ports, la migration avec vMotion vers cet hôte n'est pas possible.

- 11 Choisissez **[Utiliser cet adaptateur virtuel pour enregistrement tolérance pannes]** .
- 12 Choisissez **[Utiliser cet adaptateur virtuel pour le trafic gestion]** , et cliquez sur **[Suivant]** .
- 13 Sous les paramètres IP, précisez l'adresse IP et le masque de sous-réseau.
IPv6 ne peut pas être utilisée avec un adaptateur iSCSI matériel dépendant.
- 14 Cliquez sur **[Modifier]** pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI.
- 15 Dans l'onglet **[Config. DNS]** , le nom de l'hôte est entré par défaut. Le domaine et les adresses de serveur DNS spécifiées pendant l'installation sont également présélectionnés.

- 16 Sous l'onglet **[Routage]**, saisissez les informations de passerelle pour VMkernel. Une passerelle est nécessaire pour la connectivité aux machines qui ne sont pas sur le même sous-réseau IP que VMkernel.
Les paramètres IP sont statiques par défaut. N'utilisez pas le routage pour les configurations logicielles des chemins multiples iSCSI ni pour les adaptateurs iSCSI matériels dépendants.
- 17 Cliquez sur **[OK]**, puis sur **[Suivant]**.
- 18 Cliquez sur **[Terminer]**.

Migrer un adaptateur virtuel existant vers un vSphere Distributed Switch

Vous pouvez migrer un adaptateur virtuel existant d'un commutateur standard vSphere vers un vSphere Distributed Switch.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.
- 4 Sélectionnez la vue vSphere Distributed Switch.
- 5 Cliquez sur **[Gérer adaptateurs virtuels]**.
- 6 Cliquez sur **[Ajouter]**.
- 7 Sélectionnez **[Migrer adaptateurs virtuels existants]** et cliquez sur **[Suivant]**.
- 8 Sélectionnez un ou plusieurs adaptateur de réseau virtuel à migrer.
- 9 Pour chaque carte sélectionnée, choisissez un groupe de ports dans le menu déroulant **[Choisir un groupe de ports]**.
- 10 Cliquez sur **[Suivant]**.
- 11 Cliquez sur **[Terminer]**.

Migrer un adaptateur virtuel vers un commutateur standard vSphere

Vous pouvez migrer une carte virtuelle existante d'un vSphere distributed switch vers un commutateur standard vSphere.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.
- 4 Sélectionnez la vue vSphere Distributed Switch.
- 5 Cliquez sur **[Gérer adaptateurs virtuels]**.
- 6 Sélectionnez l'adaptateur virtuel à migrer et cliquez sur **[Migrer]**.
- 7 Sélectionnez le commutateur standard vers lequel vous voulez migrer l'adaptateur et cliquez sur **[Suivant]**.
- 8 Entrez une **[Étiquette réseau]** et optionnellement un **[ID VLAN]** pour l'adaptateur virtuel et cliquez sur **[Suivant]**.
- 9 Cliquez sur **[Terminer]** pour migrer l'adaptateur virtuel et pour terminer l'assistant.

Modifier la configuration VMkernel dans un vSphere Distributed Switch

Vous pouvez modifier un adaptateur de réseau virtuel VMkernel dans un commutateur distribué vSphere pour modifier les paramètres IP, tels que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et la configuration DNS. Vous pouvez également indiquer si l'adaptateur virtuel est utilisé pour la journalisation vMotion ou de la tolérance aux pannes.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]** .
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]** , cliquez sur **[Mise en réseau]** .
- 4 Sélectionnez la vue vSphere Distributed Switch.
- 5 Cliquez sur **[Gérer adaptateurs virtuels]** .
- 6 Sélectionnez l'adaptateur VMkernel à modifier et cliquez sur **[Modifier]** .
- 7 Sous Connexion réseau, sélectionnez le **[vSphere Distributed Switch]** et le **[Groupe de ports]** ou le **[port]** pour y ajouter l'adaptateur virtuel.
- 8 Sélectionnez **[Utiliser cet adaptateur virtuel pour vMotion]** pour permettre à ce groupe de ports de s'annoncer à un autre hôte comme connexion réseau à laquelle le trafic de vMotion doit être envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte. Si cette propriété n'est pas activée pour un groupes de ports, la migration avec vMotion vers cet hôte n'est pas possible.
- 9 (Facultatif) Sélectionnez **[Utiliser cet adaptateur virtuel pour enregistrement tolérance pannes]** .
- 10 (Facultatif) Sélectionnez **[Utiliser cet adaptateur virtuel pour le trafic de gestion]** .
- 11 Sous les paramètres IP, spécifiez l' **[Adresse IP]** et le **[Masque de sous-réseau]** ou sélectionnez **[Obtenir les paramètres IP automatiquement]** .
- 12 Cliquez sur **[Modifier]** pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI.

Dans l'onglet **[Configuration DNS]** , le nom de l'hôte apparaît dans le champ nom par défaut. Les adresses de serveur DNS spécifiées pendant l'installation sont également présélectionnées, de même que le domaine.

Dans l'onglet **[Routage]** , une passerelle est nécessaire pour la connectivité aux machines qui ne se trouvent pas dans le même sous-réseau IP que VMkernel.

Les paramètres IP sont statiques par défaut.
- 13 Utilisez les flèches Haut et Bas pour définir la MTU de l'adaptateur VMkernel.
- 14 Cliquez sur **[OK]** .

Afficher les informations de routage VMkernel sur un vSphere Distributed Switch

Vous pouvez afficher les informations de routage IP et IPv6, telles que le réseau, le préfixe et la passerelle, d'un adaptateur réseau VMkernel sur un vSphere Distributed Switch.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]** .
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]** , cliquez sur **[Mise en réseau]** .

- 4 Dans la vue vSphere Distributed Switch, cliquez sur **[Gérer adaptateurs virtuels]** .
- 5 Sélectionnez l'adaptateur VMkernel à afficher et cliquez sur **[Afficher le tableau de routage]** sous les paramètres IP ou les paramètres IPv6.

Un tableau de routage comprenant des informations sur le réseau, le préfixe et la passerelle de l'adaptateur VMkernel sélectionné apparaît.

Supprimer un adaptateur virtuel

Supprimez un adaptateur de réseau virtuel d'un vSphere Distributed Switch dans la boîte de dialogue Gérer adaptateurs virtuels.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .
- 3 Sélectionnez la vue vSphere Distributed Switch.
- 4 Cliquez sur **[Gérer adaptateurs virtuels]** .
- 5 Sélectionnez l'adaptateur virtuel à supprimer et cliquez sur **[Supprimer]** .

Une boîte de dialogue s'affiche avec le message, Voulez-vous vraiment supprimer *adapter name* ?

- 6 Cliquez sur **[Oui]** .

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

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 commutateur distribué vSphere et un réseau commutateur standard vSphere.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris et sélectionnez **[Migrer la gestion de réseau de machines virtuelles]** .

L'assistant Migrer la mise en réseau de machines virtuelles apparaît.

- 3 Sélectionnez un **[réseau source]** de migration des adaptateurs.

Option	Description
Inclure tous les adaptateurs réseau de machine virtuelle connectés au réseau suivant (Filtre par réseau)	Migre les adaptateurs réseau de machine virtuelle depuis un réseau donné. Sélectionnez le réseau source dans le menu déroulant [Réseau] .
Inclure tous les adaptateurs réseau de machine virtuelle connectés au réseau suivant (Filtre par VDS)	Migre les adaptateurs réseau de machine virtuelle depuis un réseau dans un commutateur distribué vSphere donné. Pour migrer depuis un réseau, sélectionnez [Commutateur] et [Réseau] dans les menus déroulants.
Inclure tous les adaptateurs réseau de machine virtuelle non connectés à un réseau	Migre les adaptateurs réseau de machine virtuelle non connectés à un réseau

- 4 Sélectionnez un **[Réseau de destination]** de migration des adaptateurs.

Option	Description
Filtre par réseau	Migre les adaptateurs réseau de machine virtuelle vers un réseau donné. Sélectionnez le réseau de destination dans le menu déroulant [Réseau] .
Filtre par VDS	Migre les adaptateurs réseau de machine virtuelle vers un réseau dans un commutateur distribué vSphere donné. Pour migrer vers un réseau, sélectionnez [Commutateur] et [Réseau] dans les menus déroulants.

- 5 Cliquez sur **[Suivant]**.
- 6 (Facultatif) Sélectionnez une machine virtuelle ou un adaptateur pour afficher ses informations.
- 7 Sélectionnez les machines virtuelles et les adaptateurs à migrer vers le réseau de destination et cliquez sur **[Suivant]**.
- 8 Vérifiez que le réseau source, le réseau cible et le nombre de machines virtuelles à migrer sont corrects et cliquez sur **[OK]**.

Connecter une machine virtuelle individuelle à un groupe de ports distribués

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

Procédure

- Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.
- Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]**.
- Dans l'onglet **[Matériel]**, sélectionnez la carte réseau virtuelle.
- Dans le menu déroulant **[Étiquette réseau]**, sélectionnez le groupe de ports distribués vers lequel vous voulez effectuer la migration, puis cliquez sur **[OK]**.

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 37](#)
- [« Délestage de segmentation TCP et Trames jumbo », page 41](#)
- [« NetQueue et performances réseau », page 43](#)
- [« DirectPath I/O », page 44](#)

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 le contrôle d'E/S réseau sur un vSphere Distributed Switch](#) page 38
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](#) page 38
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](#) page 39
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](#) page 40
Vous pouvez changer les paramètres d'un pool de ressources réseau, tels que les parts allouées et les limites de chaque pool de ressources réseau, pour changer la priorité du trafic réseau du pool de ressources réseau.
- [Supprimer un pool de ressources réseau](#) page 40
Vous pouvez supprimer les pools de ressources réseau définis par l'utilisateur qui ne sont plus utilisés.

Activer le contrôle d'E/S réseau sur un vSphere Distributed Switch

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 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Sur l'onglet **[Allocation des ressources]**, cliquez sur **[Propriétés]**.
- 4 Sélectionnez **[Activer le contrôle d'E/S sur ce vSphere Distributed Switch]** et cliquez sur **[OK]**.

Créer un pool de ressources réseau

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 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Sur l'onglet **[Allocation des ressources]**, cliquez sur **[Nouveau pool de ressources réseau]**.
- 4 Entrez un **[Nom]** pour le pool de ressources réseau.
- 5 (Facultatif) Entrez une **[Description]** du pool de ressources réseau.

- 6 Sélectionnez les parts de carte physique dans **[Parts adaptateurs physiques]** pour le pool de ressources réseau.

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

- 7 Définissez **[Limite hôte]** pour le pool de ressources réseau en mégabits par seconde ou sélectionnez **[Illimité]**.
- 8 (Facultatif) Sélectionnez la **[Balise de priorité QoS]** du pool de ressources réseau.
- 9 Cliquez sur **[OK]**.

Le nouveau pool de ressources apparaît dans l'onglet **[Allocation des ressources]** sous les pools de ressources réseau définis 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

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 dans le vSphere Distributed Switch.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Allocation des ressources]**, cliquez sur **[Gérer les groupes de ports]**.
- 4 (Facultatif) Sélectionnez le pool de ressources réseau défini par l'utilisateur à associer à un groupe de ports distribués dans le menu déroulant Pool de ressources réseau ou sélectionnez **[Aucun]** pour supprimer le groupe de ports distribués d'un pool de ressources défini par l'utilisateur.
- 5 (Facultatif) Sélectionnez le pool de ressources défini par l'utilisateur à associer à des groupes de ports distribués.
 - a Maintenez la touche Ctrl enfoncée pour sélectionner plusieurs groupes de ports distribués et cliquez sur **[Affecter plusieurs]**.
 - b Sélectionnez le pool de ressources réseau défini par l'utilisateur à associer aux groupes de ports distribués dans le menu déroulant Pool de ressources réseau ou sélectionnez **[Aucun]** pour supprimer les groupes de ports distribués de tous les pools de ressources définis par l'utilisateur.
- 6 Cliquez sur **[OK]**.

Modifier les paramètres de pool de ressources réseau

Vous pouvez changer les paramètres d'un pool de ressources réseau, tels que les parts allouées et les limites de chaque pool de ressources réseau, pour changer la priorité du trafic réseau du pool de ressources réseau.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Allocation des ressources]**, cliquez avec le bouton droit sur le pool de ressources réseau à modifier et sélectionnez **[Modifier les paramètres]**.
- 4 Sélectionnez les parts de carte physique dans **[Parts adaptateurs physiques]** pour le pool de ressources réseau.

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

- 5 Définissez **[Limite hôte]** pour le pool de ressources réseau en mégabits par seconde ou sélectionnez **[Illimité]**.
- 6 (Facultatif) Sélectionnez la **[Balise de priorité QoS]** dans le menu déroulant.
Cette balise 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

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

Prérequis

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Allocation de ressources]**, cliquez avec le bouton droit de la souris sur le pool de ressources réseau à supprimer et sélectionnez **[Supprimer]**.
- 4 Cliquez sur **[Oui]**.

Délestage de segmentation TCP et Trames jumbo

Activez les trames Jumbo sur un vSphere Distributed Switch ou un commutateur standard vSphere en changeant les unités de transmission maximale (MTU). Le délestage de segmentation TCP (TSO) est activé par défaut sur l'interface VMkernel, mais doit être activé au niveau de la machine virtuelle.

Activation du TSO (délestage de segmentation TCP)

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

Le support TSO via la carte réseau vmxnet amélioré est disponible pour les machines virtuelles exécutant les systèmes d'exploitation invités suivants :

- Microsoft Windows 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)

Activer le support TSO pour une machine virtuelle

L'activation du support TSO sur une machine virtuelle requiert un adaptateur vmxnet amélioré

Procédure

- 1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Résumé]** puis sur **[Modifier les paramètres]** .
- 3 Sélectionnez la carte réseau dans la liste Matériel.
- 4 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 Cliquez sur **[Ajouter]** .
- 7 Sélectionnez **[Adaptateur Ethernet]** et cliquez sur **[Suivant]** .
- 8 Dans le groupes Type d'adaptateur, sélectionnez **[vmxnet amélioré]** .
- 9 Sélectionnez le paramètre réseau et l'adresse MAC utilisés par l'ancienne carte réseau, puis cliquez sur **[Suivant]** .
- 10 Cliquez sur **[Terminer]** , puis sur **[OK]** .
- 11 Si la machine virtuelle n'est pas configurée pour mettre VMware Tools à niveau à chaque mise sous tension, vous devez le mettre manuellement à niveau.

TSO est activé sur une interface VMkernel. Si le TSO est désactivé pour une interface VMkernel spécifique, le seul moyen de l'activer est de supprimer cette interface VMkernel et de la recréer avec un TSO activé.

Activation de trames Jumbo

Les trames jumbo permettent à ESXi d'envoyer des trames plus grandes sur le réseau physique. Le réseau doit prendre en charge des Trames jumbo de bout en bout.

Les Trames jumbo jusqu'à 9 Ko (9000 octets) sont prises en charge. 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.

Activer les trames Jumbo pour une interface VMkernel sur un commutateur standard vSphere

Les trames Jumbo réduisent la charge du processeur générée par le transfert de données. Activez les trames Jumbo sur une interface réseau VMkernel en changeant les unités MTU (Maximum Transmission Units) de l'interface VMkernel.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]** .
- 2 Dans l'onglet **[Configuration]** , cliquez sur **[Mise en réseau]** .
- 3 Cliquez sur **[Propriétés]** pour le commutateur standard vSphere associé au VMkernel que vous modifiez.
- 4 Dans l'onglet **[Ports]** , sélectionnez l'interface VMkernel et cliquez sur **[Modifier]** .
- 5 Affectez à **[MTU]** la valeur 9 000 et cliquez sur **[OK]** .

Activer les trames Jumbo sur un vSphere Distributed Switch

Activez un vSphere Distributed Switch pour les trames Jumbo en changeant la taille MTU du commutateur distribué.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sur l'onglet **[Propriétés]** , sélectionnez **[Avancé]** .
- 4 Affectez à **[MTU max.]** la taille MTU maximale parmi toutes les adaptateurs réseau virtuelles connectées au vSphere Distributed Switch, puis cliquez sur **[OK]** .

Activer la prise en charge de Trames jumbo sur une machine virtuelle

L'activation de la prise en charge de trames Jumbo sur une machine virtuelle requiert un adaptateur vmxnet amélioré.

Procédure

- 1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Résumé]** puis sur **[Modifier les paramètres]** .
- 3 Sélectionnez la carte réseau dans la liste Matériel.
- 4 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 Cliquez sur **[Ajouter]** .
- 7 Sélectionnez **[Adaptateur Ethernet]** et cliquez sur **[Suivant]** .
- 8 Dans le groupes Type d'adaptateur, sélectionnez **[vmxnet amélioré]** .
- 9 Sélectionnez le réseau utilisé par l'ancienne carte réseau, puis cliquez sur **[Suivant]** .
- 10 Cliquez sur **[Terminer]** .
- 11 Sélectionnez le nouvel adaptateur réseau dans la liste Matériel.

- 12 Sous Adresse MAC, sélectionnez **[Manuel]** , puis saisissez l'adresse MAC utilisée par l'ancienne carte réseau.
- 13 Cliquez sur **[OK]** .
- 14 Vérifiez que la carte vmxnet étendue est connectée à un commutateur standard ou distribué avec les trames Jumbo activées.
- 15 Dans le système d'exploitation invité, configurez la carte réseau de manière à autoriser les trames Jumbo. Consultez la documentation du système d'exploitation de l'invité pour plus de détails.
- 16 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 le VMware vSphere CLI, utilisez la commande `vicfg-advcfg --set true VMkernel.Boot.netNetQueueEnable`.
- 2 Utilisez l'interface de ligne de commande vSphere de VMware 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 connaissances des informations sur la configuration des pilotes NIC dans *Initiation aux interfaces de ligne de commande vSphere*.

Procédure

- 1 Dans le VMware vSphere CLI, utilisez la commande `vicfg-advcfg --set false VMkernel.Boot.netNetQueueEnable`.
- 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

vMotion est disponible pour les machines virtuelles configurées avec DirectPath uniquement sur les systèmes Cisco UCS via des commutateurs distribués Cisco compatibles. Consultez la documentation de Cisco pour obtenir plus d'informations sur les commutateurs compatibles et la configuration des commutateurs.

- [Configurer les périphériques de relais sur un hôte](#) page 44
Vous pouvez configurer des périphériques réseau de relais sur un hôte.
- [Configurer un périphérique PCI sur une machine virtuelle](#) page 44
Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle.
- [Activer DirectPath I/O avec vMotion sur une machine virtuelle](#) page 45
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 Cisco compatible.

Configurer les périphériques de relais sur un hôte

Vous pouvez configurer des périphériques réseau de relais sur un hôte.

Procédure

- 1 Sélectionnez un hôte dans le panneau d'inventaire de vSphere Client.
- 2 Dans l'onglet **[Configuration]**, cliquez sur **[Paramètres avancés]**.

La page Passthrough Configuration apparaît, énumérant tous les périphériques de relais disponibles. Une icône verte indique qu'un périphérique est activé et actif. Une icône orange indique que l'état du périphérique a changé et l'hôte doit être redémarré avant que le périphérique puisse être utilisé.
- 3 Cliquez sur **[Modifier]**.
- 4 Sélectionnez les périphériques à utiliser pour le relais et cliquez sur **[OK]**.

Configurer un périphérique PCI sur une machine virtuelle

Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle.

Procédure

- 1 Sélectionnez une machine virtuelle dans le panneau de l'inventaire du vSphere Client.
- 2 Dans le menu **[Inventaire]**, sélectionnez **[Machine virtuelle] > [Modifier les paramètres]**.

- 3 Sous l'onglet **[Matériel]**, cliquez sur **[Ajouter]**.
- 4 Sélectionnez **[Périphérique PCI]** et cliquez sur **[Suivant]**.
- 5 Sélectionnez le périphérique de relais à utiliser, et cliquez sur **[Suivant]**.
- 6 Cliquez sur **[Terminer]**.

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

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 Cisco compatible.

Prérequis

- Activez les E/S réseau de haute performance sur au moins un profil de port d'un commutateur distribué Cisco compatible. Pour obtenir des informations sur les commutateurs compatibles et la configuration des commutateurs, consultez la documentation de Cisco sur <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.
- Mettez la machine virtuelle hors tension.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire Machines virtuelles et modèles.
- 2 Faites un clic droit sur la machine virtuelle et cliquez sur **[Modifier les paramètres]**.
- 3 Dans l'onglet **[Ressources]**, sélectionnez **[Mémoire]**.
- 4 Sélectionnez **[Illimitée]**.
- 5 Dans l'onglet **[Matériel]**, sélectionnez l'adaptateur réseau à configurer en tant que périphérique de relais.
- 6 Dans le menu déroulant Étiquette de réseau, sélectionnez un profil de port à haute performance, puis cliquez sur **[OK]**.
- 7 Mettez la machine virtuelle sous tension.

Une fois la machine virtuelle sous tension, DirectPath I/O Gen. 2 apparaît comme Actif dans l'onglet **[Matériel]** de la boîte de dialogue des propriétés de la machine virtuelle.

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.

Ce chapitre aborde les rubriques suivantes :

- [« Règle de basculement et d'équilibrage de charge », page 47](#)
- [« Règle VLAN », page 55](#)
- [« Règle de sécurité », page 56](#)
- [« Règle de formation du trafic », page 60](#)
- [« Règle d'allocation des ressources », page 64](#)
- [« Règle de surveillance », page 65](#)
- [« Règles de blocage des ports », page 66](#)
- [« Gérer les règles pour plusieurs groupes de ports sur un commutateur distribué vSphere », page 66](#)

Règle de basculement et d'équilibrage de charge

Les règles de basculement et d'équilibrage de charge permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adaptateur.

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

- **[Règle d'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 règle d'équilibrage de charge sur le commutateur physique.

- **[Détection reprise]** contrôle l'état de lien et le sondage de balise. La signalisation n'est pas pris en charge par le balisage VLAN invité.
- **[Commande adaptateur réseau]** peut être actif ou en veille.

Modifier la règle de basculement et d'équilibrage de charge d'un commutateur standard vSphere

Employez les règles d'équilibrage de charge et de basculement pour déterminer la distribution du trafic réseau entre les adaptateurs et la redistribution du trafic en cas de défaillance d'un adaptateur.

Les règles de basculement et d'équilibrage de charge incluent les paramètres suivants :

- Règle d'équilibrage de charge : La règle d'équilibrage de charge détermine la distribution du trafic sortant entre les adaptateurs réseau assignés à un commutateur standard. Le trafic entrant est contrôlé par la règle d'équilibrage de charge sur le commutateur physique.
- Détection de basculement : état de lien/vérification d'incidents
- Ordre des adaptateurs réseau (actif/en standby)

Dans certains cas, la connectivité de commutateur standard peut être perdue suite à un événement de basculement ou de retour arrière. Dans ce cas, les adresses MAC utilisées par les machines virtuelles associées au commutateur standard apparaissent sur un port de commutateur différent. Pour éviter ce problème, placez votre commutateur physique en mode portfast ou portfast trunk.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez le serveur dans le panneau d'inventaire.
La page de configuration matérielle pour ce serveur s'affiche.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Sélectionnez un commutateur standard et cliquez sur **[Modifier]**.
- 4 Cliquez sur l'onglet **[Ports]**.
- 5 Pour modifier les valeurs **[Basculement et équilibrage de charge]**, sélectionnez le commutateur standard et cliquez sur **[Propriétés]**.
- 6 Cliquez sur l'onglet **[Association de cartes réseau]**.

Vous pouvez remplacer l'ordre de basculement au niveau du groupes de ports. Par défaut, les nouveaux adaptateurs sont actifs pour toutes les règles. Les nouveaux adaptateurs transportent le trafic pour le commutateur standard et son groupes de ports, sauf indication contraire.

- 7 Dans la liste **[Équilibrage de charge]**, sélectionnez une option pour le mode de sélection d'une liaison montante.

Option	Description
Router en fonction de l'ID du port d'origine	Sélectionner une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur standard.
Router en fonction du hachage d'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, les éléments présents à ces positions servent à calculer le hachage.
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	Toujours utiliser la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui vérifient les critères de détection du basculement.

- 8 Dans la liste de détection du basculement réseau, sélectionnez l'option à utiliser pour la détection du basculement.

Option	Description
État du lien uniquement	Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les pannes, telles que les débranchements et les interruptions d'alimentation du commutateur physique, mais pas les erreurs de configuration, telles qu'un port de commutateur physique bloqué par STP ou configuré sur un VLAN erroné, ou les débranchements intervenant de l'autre côté d'un commutateur physique.
Sondage de balise	Envoie et détecte des sondes d'incident sur toutes les cartes réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Cette option détecte de nombreuses Pannes parmi celles mentionnées précédemment, qui ne sont pas détectées à l'aide du seul état de lien. REMARQUE Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.

- 9 Sélectionnez **[Oui]** ou **[Non]** pour notifier les commutateurs en cas de basculement.

Si vous sélectionnez Oui, chaque fois qu'une carte NIC virtuelle est connectée au commutateur standard ou que le trafic de cette carte est acheminé sur une carte physique NIC différente dans l'association suite à un basculement, une notification est envoyée dans le réseau pour mettre à jour les tables de recherche des commutateurs physiques. Dans la grande majorité des cas, ceci permet de minimiser la latence des occurrences de basculement et des migrations avec vMotion.

N'utilisez pas cette option si les machines virtuelles utilisant le groupes de ports utilisent l'équilibrage de la charge réseau de Microsoft (NLB) en mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.

- 10 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]**, l'adaptateur est remis en service actif immédiatement après la récupération, en déplaçant l'adaptateur de réserve éventuel ayant repris son emplacement. Si le retour arrière est défini sur **[Non]**, un adaptateur ayant échoué est laissé inactif même après la récupération jusqu'à ce qu'un autre adaptateur actif échoue, exigeant un remplacement.

- 11 Définissez **[Commande de basculement]** pour spécifier la répartition de la charge de travail entre les adaptateurs.

Pour utiliser certains adaptateurs et en réserver d'autres pour des cas d'urgence, vous pouvez définir cette condition à l'aide du menu déroulant afin de les classer en groupes.

Option	Description
Adaptateurs actifs	Continuer à utiliser l'adaptateur si la connectivité de l'adaptateur réseau est disponible et en activité.
Adaptateurs standby	Utilisez cet adaptateur si la connectivité de l'adaptateur actif est indisponible.
Adaptateurs inutilisés	Ne pas utiliser cet adaptateur.

Si vous utilisez un chemins multiples iSCSI, votre interface VMKernel doit être configurée pour avoir un adaptateur actif et aucun adaptateur en attente. Voir la documentation *Stockage vSphere*.

REMARQUE En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.

Modifier la règle de basculement et d'équilibrage de charge sur un groupe de ports standard

Les règles de basculement et d'équilibrage de charge permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adaptateur.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Sélectionnez un groupe de ports et cliquez sur **[Modifier]**.
- 4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]**.
- 5 Pour éditer les valeurs **[Basculement et équilibrage de charge]** du groupe de ports, sélectionnez le groupe de ports et cliquez sur **[Propriétés]**.
- 6 Cliquez sur l'onglet **[Association de adaptateurs réseau]**.

Vous pouvez remplacer l'ordre de basculement au niveau du groupes de ports. Par défaut, les nouveaux adaptateurs sont actifs pour toutes les règles. Les nouveaux adaptateurs transportent le trafic pour le commutateur standard et son groupes de ports, sauf indication contraire.

- 7 Spécifiez les paramètres dans le groupes d'exceptions à la règle.

Option	Description
Équilibrage de charge	<p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> ■ [Route basée sur l'ID du port d'origine] . Choisissez une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel. ■ [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. ■ [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, etherchannel doit être désactivé.</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.

Option	Description
Notifier les commutateurs	<p>Sélectionnez [Oui] ou [Non] pour notifier les commutateurs en cas de basculement.</p> <p>Si vous sélectionnez [Oui], chaque fois qu'une carte NIC virtuelle est connectée au commutateur standard ou que le trafic de cette carte routé vers une carte NIC physique différente dans l'association suite à un basculement, une notification est envoyée sur le réseau pour mettre à niveau les tables de recherche dans les 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>
Retour arrière	<p>Sélectionnez [Oui] ou [Non] pour mettre hors tension ou activer le retour arrière.</p> <p>Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur [Oui], la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur [Non], un adaptateur défectueux est laissé inactif, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.</p>
ordre de basculement	<p>Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réserver d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes :</p> <ul style="list-style-type: none"> ■ [Liaisons montantes actives] . Continuez à utiliser la liaison montante 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.

8 Cliquez sur **[OK]** .

Modifier la règle d'association et de basculement d'un groupe de ports distribués

Les règles d'association et de basculement permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adaptateur.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sélectionnez **[Règles]** .

- 4 Dans le groupe association et basculement, spécifiez les éléments suivants.

Option	Description
Équilibrage de charge	<p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> ■ [Route en fonction du port virtuel originel] : choisissez une liaison montante selon le port virtuel par lequel est entré le trafic dans le commutateur distribué. ■ [Route basée sur le hachage IP] : choisissez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ [Route basée sur hachage MAC source] : choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ [Route basée sur la charge NIC physique] — Choisissez une liaison montante basée sur les charges actuelles des NIC physiques. ■ [Utiliser la commande de basculement explicite] : Utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. <p>REMARQUE L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.</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] : basée uniquement sur l'état du lien que la carte réseau fournit. Cette option détecte les pannes, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ [Sondage balise] : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. <p>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.</p> <p>Si vous sélectionnez [Oui], chaque fois qu'une carte NIC virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte NIC 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>

Option	Description
Retour arrière	<p>Sélectionnez [Oui] ou [Non] pour mettre hors tension ou activer le retour arrière.</p> <p>Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur [Oui], la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur [Non], un adaptateur défectueux est laissé inactif, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.</p>
ordre de basculement	<p>Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réserver d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes :</p> <ul style="list-style-type: none"> ■ [liaison montante active] : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ [Liaisons montantes de standby] : utilisez cette liaison montante si la connectivité de l'adaptateur actif est interrompue. ■ [Liaisons montantes inutilisées] : n'utilisez pas cette liaison montante. <p>REMARQUE En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.</p>

- 5 Cliquez sur **[OK]** .

Modifier les règles d'association et de basculement de port distribué

Les règles d'association et de basculement permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adaptateur.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .
- 4 Cliquez sur **[Règles]** pour afficher et modifier les règles de réseau des ports.

- 5 Dans le groupe association et basculement, spécifiez les éléments suivants.

Option	Description
Équilibrage de charge	<p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> ■ [Route en fonction du port virtuel originel] : choisissez une liaison montante selon le port virtuel par lequel le trafic est entré dans le vSphere distributed switch. ■ [Route basée sur le hachage IP] : choisissez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ [Route basée sur hachage MAC source] : choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ [Route basée sur la charge NIC physique] — Choisissez une liaison montante basée sur les charges actuelles des NIC physiques. ■ [Utiliser la commande de basculement explicite] : Utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. <p>REMARQUE L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.</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] : basée uniquement sur l'état du lien que la carte réseau fournit. Cette option détecte les pannes, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ [Sondage balise] : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. <p>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.</p> <p>Si vous sélectionnez [Oui], chaque fois qu'une carte NIC virtuelle est connectée au vSphere distributed switch ou que le trafic de cette carte virtuelle est acheminé sur une carte NIC 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>

Option	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 slot le cas échéant. Si le retour arrière est défini sur [Non] , un adaptateur défectueux est laissé inactif, 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. Si vous voulez 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"> ■ [Liaison montante active] : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ [Liaisons montantes de standby] : utilisez cette liaison montante si la connectivité de l'adaptateur actif est coupée. REMARQUE En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve. ■ [Liaisons montantes inutilisés] : n'utilisez pas cette liaison montante.

- 6 Cliquez sur **[OK]**.

Règle VLAN

La règle de VLAN permet aux réseaux virtuels de joindre des VLAN physiques.

Modifier la règle VLAN d'un groupe de ports distribués

La règle de VLAN permet aux réseaux virtuels de joindre des VLAN physiques.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Règles]**.
- 4 Sélectionnez le type de VLAN **[VLAN Type]** à utiliser.

Option	Description
Aucune	N'utilise pas de VLAN.
VLAN	Dans le champ [ID VLAN] , entrez un nombre entre 1 et 4094.
jonction VLAN	Entrez une ou plusieurs [Plage jonction VLAN] .
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

- 5 Cliquez sur **[OK]**.

Modifier des règles de VLAN de port distribué ou de port de liaison montante

La règle de VLAN permet aux réseaux virtuels de joindre des VLAN physiques.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.

- 3 Dans l'onglet **[Ports]**, cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]**.
- 4 Cliquez sur **[Règles]**.
- 5 Sélectionnez le type de VLAN **[Type de VLAN]** à utiliser.

Option	Action
Aucune	N'utilise pas de VLAN.
VLAN	Dans le champ [ID VLAN] , entrez un nombre entre 1 et 4094.
jonction VLAN	Entrez une ou plusieurs [Plages jonctions VLAN] .
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

- 6 Cliquez sur **[OK]**.

Règle de sécurité

Les règles de sécurité réseau déterminent la façon dont la carte filtre les trames entrantes et sortantes.

La couche 2 est la couche de liaison de données. Les trois éléments de la règle de sécurité sont le mode promiscuité, les changements d'adresse MAC et les Transmissions forgées.

En mode non-promiscuité, un adaptateur invité écoute uniquement le trafic transféré sur sa propre adresse MAC. En mode promiscuité, elle peut écouter l'ensemble des trames. Par défaut, les cartes invitées sont configurées sur le mode non-promiscuité.

Modifier la règle de sécurité d'un commutateur standard vSphere

Vous pouvez modifier les règles de sécurité de la couche 2, telles que les modifications d'adresse MAC et les transmissions frauduleuses, pour un commutateur vSphere standard.

La couche 2 est la couche de liaison de données. Les trois éléments de la règle de sécurité de la couche 2 sont le mode promiscuité, les modifications d'adresse MAC, et les Transmissions forgées. Lorsqu'il n'est pas en mode promiscuité, un adaptateur client écoute uniquement le trafic sur sa propre adresse MAC. En mode promiscuité, il peut écouter l'ensemble des paquets. Par défaut, les cartes invitées sont définies sur le mode non-promiscuité.

Vous pouvez remplacer les paramètres au niveau du commutateur pour les groupes de ports standard individuels en modifiant les paramètres du groupe de ports.

Pour plus d'informations sur la sécurité, voir la documentation *Sécurité vSphere*.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez le serveur dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Cliquez sur **[Propriétés]** pour le commutateur standard dont vous voulez modifier la règle de sécurité de la couche 2.
- 4 Dans la boîte de dialogue Propriétés du commutateur standard, cliquez sur l'onglet **[Ports]**.
- 5 Sélectionnez le commutateur standard et cliquez sur **[Modifier]**.
- 6 Cliquez sur l'onglet **[Sécurité]**.

- 7 Dans le volet Exceptions à la règle, indiquez si vous voulez rejeter ou accepter les exceptions de la règle de sécurité de la couche 2.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ [Rejeter] : l'activation du mode de promiscuité sur un adaptateur client n'a pas d'incidence sur les trames reçues par l'adaptateur. ■ [Accepter] : l'activation du mode de promiscuité sur un adaptateur client permet à l'adaptateur de détecter toutes les trames transmises au vSphere Distributed Switch qui sont autorisées par la règle VLAN du groupe de ports auquel l'adaptateur est connecté.
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ [Rejeter] : si vous affectez à [Modifications d'adresse MAC] la valeur [Rejeter] et que le système d'exploitation client remplace l'adresse MAC de l'adaptateur par une autre ne figurant pas dans le fichier de configuration .vmx, toutes les trames entrantes sont abandonnées. Si le système d'exploitation client recharge l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration.vmx, les trames entrantes sont de nouveau transmises. ■ [Accepter] : le changement d'adresse MAC depuis le système d'exploitation client a l'effet prévu : les trames pour 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.

- 8 Cliquez sur **[OK]**.

Modifier l'exception de règle de sécurité de la couche 2 pour un groupe de ports standard

Contrôlez la gestion de trames entrantes et sortantes en modifiant les règles de sécurité de la couche 2.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.
- 4 Choisissez la vue Commutateur standard vSphere et cliquez sur **[Propriétés]** pour le groupe à modifier.
- 5 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]**.
- 6 Sélectionnez l'élément de groupes de ports et cliquez sur **[Modifier]**.
- 7 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Sécurité]**.

Par défaut, **[Mode promiscuité]** est défini sur **[Rejeter]**. **[Modifications d'adresse MAC]** et **[Transmissions forcées :]** sont définis sur **[Accepter]**.

L'exception de règle remplace toute règle définie au niveau du commutateur standard.

- 8 Dans le volet Exceptions règle, choisissez de rejeter ou d'accepter les exceptions à la règle de sécurité.

Tableau 5-1. Exceptions

Mode	Rejeter	Accepter
Mode promiscuité	Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.	L'activation du mode Promiscuité sur une carte invitée permet de détecter toutes les trames transmises sur le commutateur standard qui sont autorisées par la règle VLAN pour le groupes de ports auquel la carte est connectée.
Modifications d'adresse MAC	Si le système d'exploitation invité modifie l'adresse MAC de la carte par une autre ne figurant pas dans le fichier de configuration .vmx, toutes les trames entrantes sont supprimées. Si le système d'exploitation invité rechange l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration .vmx, les trames entrantes sont de nouveau envoyées.	Si l'adresse MAC du système d'exploitation invité change, les trames pour la nouvelle adresse MAC sont reçues.
Transmissions forgées	Toutes les trames sortantes dont l'adresse MAC source diffère de celle définie sur la carte sont supprimées.	Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

- 9 Cliquez sur **[OK]**.

Modifier la règle de sécurité d'un groupe de ports distribués

Vous pouvez définir une règle de sécurité d'un groupe de ports distribués pour remplacer la règle définie pour le commutateur distribué.

Les trois éléments de la règle Sécurité sont le mode promiscuité, les changements d'adresse MAC et les transmissions forcées.

En mode non-promiscuité, un adaptateur invité écoute le trafic seulement sur sa propre adresse MAC. En mode promiscuité, il peut écouter l'ensemble des paquets. Par défaut, les cartes invitées sont définies sur le mode non-promiscuité.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Règles]**.

Par défaut, **[Mode promiscuité]** est défini sur **[Rejeter]**. **[Modifications d'adresse MAC]** et **[Transmissions forcées]** sont définis sur **[Accepter]**.

- 4 Dans le groupes **[Sécurité]** , choisissez de rejeter ou d'accepter les exceptions aux règles de sécurité.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ [Rejeter] : l'activation du mode de promiscuité sur un adaptateur client n'a pas d'incidence sur les trames reçues par l'adaptateur. ■ [Accepter] : l'activation du mode de promiscuité sur un adaptateur client permet à l'adaptateur de détecter toutes les trames transmises au commutateur standard vSphere qui sont autorisées par la règle VLAN du groupe de ports auquel l'adaptateur est connecté.
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ [Rejeter] : si vous affectez à [Modifications d'adresse MAC] la valeur [Rejeter] et que le système d'exploitation client remplace 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 client recharge l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration <code>.vmx</code>, les trames entrantes sont de nouveau transmises. ■ [Accepter] : le changement d'adresse MAC depuis le système d'exploitation client a l'effet prévu : les trames pour 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.

- 5 Cliquez sur **[OK]** .

Modifier des règles de sécurité de port distribué

Les trois éléments de la règle Sécurité sont le mode promiscuité, les changements d'adresse MAC et les transmissions forcées.

En mode non-promiscuité, un adaptateur invitée écoute le trafic seulement sur sa propre adresse MAC. En mode promiscuité, il peut écouter l'ensemble des paquets. Par défaut, les cartes invitées sont définies sur le mode non-promiscuité.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .
- 4 Cliquez sur **[Règles]** .

Par défaut, le **[Mode promiscuité]** est défini sur **[Rejeter]** ; **[Modifications d'adresse MAC]** et **[Transmissions forgées]** sont définis sur **[Accepter]** .

- 5 Dans le groupe **[Sécurité]**, choisissez de rejeter ou d'accepter les exceptions aux règles de sécurité.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ [Rejeter] : l'activation du mode promiscuité sur un adaptateur client n'a pas d'incidence sur les trames reçues par l'adaptateur. ■ [Accepter] : l'activation du mode promiscuité sur un adaptateur client permet à l'adaptateur de détecter toutes les trames transmises au vSphere Distributed Switch qui sont autorisées par la règle VLAN du groupe de ports auquel l'adaptateur est connecté.
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ [Rejeter] : si vous affectez à [Modifications d'adresse MAC] la valeur [Rejeter] et que le système d'exploitation client remplace 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 client recharge l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration <code>.vmx</code>, les trames entrantes sont de nouveau transmises. ■ [Accepter] : le changement d'adresse MAC depuis le système d'exploitation client a l'effet prévu : les trames pour 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 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 règle de formation du trafic d'un commutateur standard vSphere

ESXi permet de mettre en forme le trafic sortant sur les 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 » du trafic de traverser un port à des vitesses plus élevées.

Une règle 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).
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 ainsi transférés à une vitesse plus élevée.
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.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez le serveur dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Sélectionnez un commutateur standard et cliquez sur **[Propriétés]**.
- 4 Cliquez sur l'onglet **[Ports]**.
- 5 Sélectionnez le commutateur standard et cliquez sur **[Modifier]**.
- 6 Cliquez sur l'onglet **[Formation du trafic]**.
- 7 Sélectionnez **[Activé]** dans le menu déroulant **[État]** pour activer les exceptions à la règle de formation du trafic.

Ici, la règle d'état est appliquée à chaque adaptateur virtuel attaché au groupe de ports et non pas au commutateur standard en tant que tel. Si vous activez l'exception à la règle dans le champ **[État]**, vous limitez l'allocation de bande passante réseau pour chaque adaptateur virtuel associé à ce groupes de ports particulier. Si vous désactivez la règle, les services ont par défaut une connexion libre au réseau physique.
- 8 Entrez une valeur de bande passante pour chaque règle de formation du trafic.

Modifier la règle de formation du trafic pour un groupe de ports standard

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Hôtes et clusters]**.
- 2 Sélectionnez l'hôte dans le volet d'inventaire.
- 3 Dans l'onglet **[Configuration]**, cliquez sur **[Mise en réseau]**.

- 4 Choisissez la vue Commutateur standard vSphere et cliquez sur **[Propriétés]** pour le groupe à modifier.
- 5 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]**.
- 6 Sélectionnez l'élément de groupes de ports et cliquez sur **[Modifier]**.
- 7 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Formation du trafic]**.

Quand la formation du trafic est désactivée, les options sont grisées.

Option	Description
État	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).

Modifier la règle de formation du trafic d'un groupe de ports distribués

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 un port à des vitesses plus élevées.

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Règles]**.
- 4 Dans le groupe **[Formation du trafic]**, vous pouvez configurer **[Formation du trafic d'entrée]** et **[Formation du trafic de sortie]**.

Quand la mise en forme du trafic est désactivée, les fonctions réglables sont grisées.

État : si vous activez l'exception de règle pour **[Formation du trafic d'entrée]** et **[Formation du trafic de sortie]** dans le champ **[État]**, vous définissez des limites sur le niveau de bande passante réseau allouée à chaque adaptateur virtuel associé au groupe de ports. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique par défaut.

- 5 Spécifiez les paramètres du trafic réseau.

Option	Description
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	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 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 ainsi transférés à une vitesse plus élevée.

- 6 Cliquez sur **[OK]**.

Modifier les règles de mise en forme de trafic de port distribué ou de port de liaison montante

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 un port à des vitesses plus élevées.

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]**, cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]**.
- 4 Cliquez sur **[Règles]**.
- 5 Dans le groupe **[Formation du trafic]**, vous pouvez configurer **[Formation du trafic d'entrée]** et **[Formation du trafic de sortie]**.

Quand la mise en forme du trafic est désactivée, les fonctions réglables sont grisées.

État : si vous activez l'exception de règle pour **[Formation du trafic d'entrée]** ou **[Formation du trafic de sortie]** dans le champ **[État]**, vous définissez des limites sur le niveau de bande passante réseau allouée à chaque carte virtuelle liée à ce groupe de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique par défaut.

6 Spécifiez les paramètres du trafic réseau.

- **[Bande passante moyenne]** établit le nombre de bits par seconde à autoriser sur un port, avec valeur moyenne calculée dans le temps : la charge moyenne autorisée.
- **[Bande passante maximale]** est le 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 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 ainsi transférés à une vitesse plus élevée.

7 Cliquez sur **[OK]**.

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 37.

Modifier la règle d'allocation des ressources d'un groupe de ports distribués

Associez un groupe de ports distribués à un pool de ressources réseau pour contrôler plus efficacement la bande passante affectée au groupe de ports distribués.

Prérequis

Activez le Contrôle d'E/S réseau sur l'hôte et créez un ou plusieurs pools de ressources réseau définis par l'utilisateur.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sélectionnez **[Règles]**.
- 4 Dans le groupe Allocation des ressources, sélectionnez le **[Pool de ressources réseau]** auquel le groupe de ports distribués est associé dans le menu déroulant.
- 5 Cliquez sur **[OK]**.

Modifier la règle d'allocation des ressources d'un port distribué

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

Prérequis

Activez le Contrôle d'E/S réseau sur l'hôte et créez un ou plusieurs pools de ressources réseau définis par l'utilisateur.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .
- 4 Sélectionnez **[Règles]** .
- 5 Dans le groupe Allocation des ressources, sélectionnez le **[Pool de ressources réseau]** auquel associer le port dans le menu déroulant.
- 6 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 « [Configurer les paramètres NetFlow](#) », page 76.

Modifier la règle de surveillance d'un groupe de ports distribués

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sélectionnez **[Règles]** .
- 4 Dans le groupe de surveillance, sélectionnez **[État Netflow]** .

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 », page 76.

- 5 Cliquez sur **[OK]** .

Modifier la règle de surveillance d'un port distribué

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .
- 4 Sélectionnez **[Règles]** .

- 5 Dans le groupe de surveillance, sélectionnez **[État Netflow]** .

Option	Description
Désactivé	NetFlow est désactivé sur le port.
Activé	NetFlow est activé sur le port. Vous pouvez configurer les paramètres de NetFlow au niveau du commutateur distribué. Reportez-vous à « Configurer les paramètres NetFlow », page 76.

- 6 Cliquez sur **[OK]** .

Règles de blocage des ports

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

Modifier la règle de blocage des ports d'un groupe de ports distribués

La boîte de dialogue Règles diverses permet de configurer des règles diverses de groupe de ports distribués.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur le groupe de ports distribués dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sélectionnez **[Règles]** .
- 4 Dans le groupe **[Divers]** , indiquez si vous voulez **[Bloquer tous les ports]** du groupe de ports distribués.
- 5 Cliquez sur **[OK]** .

Modifier les règles de blocage de port distribué ou de port de liaison montante

La boîte de dialogue Règles diverses permet de définir des règles de blocage de port distribué ou de port de liaison montante.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Sélectionnez vSphere Distributed Switch dans le volet d'inventaire.
- 3 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .
- 4 Cliquez sur **[Règles]** .
- 5 Dans le groupes **[Divers]** , choisissez de bloquer ou non ce port avec **[Bloquer]** .
- 6 Cliquez sur **[OK]** .

Gérer les règles pour plusieurs groupes de ports sur un commutateur distribué vSphere

Vous pouvez modifier les règles de communication réseau de plusieurs groupes de ports ou d'un commutateur distribué.

Prérequis

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

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur le commutateur distribué et sélectionnez **[Gérer les groupes de ports]** .
- 3 Sélectionnez les catégories de règles à modifier.

Option	Description
Sécurité	Définissez les modifications d'adresse MAC, les transmissions frauduleuses et le mode promiscuité des groupes de ports sélectionnés.
Formation du trafic	Définissez la bande passante moyenne, la bande passante maximale et la taille de rafale du trafic entrant et du trafic sortant dans les groupes de ports sélectionnés.
VLAN	Indiquez comment les groupes de ports sélectionnés se connectent aux réseaux VLAN physiques.
Association et basculement	Définissez l'équilibrage de charge, la détection du basculement, la notification de commutation et l'ordre de basculement des groupes de ports sélectionnés.
Allocation de ressources	Définissez l'association de pool de ressources réseau des groupes de ports sélectionnés. Cette option est disponible pour vSphere Distributed Switch versions 5.0.0 et les versions suivantes uniquement.
Surveillance	Activez ou désactivez NetFlow sur les groupes de ports sélectionnés. Cette option est disponible pour vSphere Distributed Switch versions 5.0.0 et les versions suivantes uniquement.
Divers	Activez ou désactivez le blocage de port dans les groupes de ports sélectionnés.

- 4 Cliquez sur **[Suivant]** .
- 5 Sélectionnez un ou plusieurs groupes de ports à modifier et cliquez sur **[Suivant]** .

La page de configuration de règle s'affiche. Il n'y a que les catégories de règles que vous avez sélectionnées qui s'affichent.

- 6 (Facultatif) Dans le groupes Sécurité, indiquez si vous voulez rejeter ou accepter les exceptions de règle de sécurité.

Option	Description
Mode promiscuité	<ul style="list-style-type: none"> ■ [Rejeter] : l'activation du mode de promiscuité sur un adaptateur invité n'a pas d'incidence sur les trames reçues par l'adaptateur. ■ [Accepter] : l'activation du mode promiscuité sur un adaptateur invité permet à l'adaptateur de détecter toutes les trames transmises au vSphere Distributed Switch qui sont autorisées par la règle VLAN du groupe de ports auquel l'adaptateur est connecté.
Modifications d'adresse MAC	<ul style="list-style-type: none"> ■ [Rejeter] : si vous affectez à [Modifications d'adresse MAC] la valeur [Rejeter] et que le système d'exploitation client remplace l'adresse MAC de l'adaptateur par une autre ne figurant pas dans le fichier de configuration .vmx, toutes les trames entrantes sont abandonnées. Si le système d'exploitation invité recharge l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration.vmx, les trames entrantes sont de nouveau transmises. ■ [Accepter] : le changement d'adresse MAC depuis le système d'exploitation invité a l'effet prévu : les trames pour 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.

- 7 (Facultatif) Dans le groupe Formation du trafic, vous pouvez configurer **[Formation du trafic d'entrée]** et **[Formation du trafic de sortie]**.

Quand la mise en forme du trafic est désactivée, les fonctions réglables sont grisées.

État : si vous activez l'exception de règle pour **[Formation du trafic d'entrée]** et **[Formation du trafic de sortie]** dans le champ **[État]**, vous définissez des limites sur le niveau de bande passante allouée à chaque port distribué associé au groupe de ports sélectionné. Si vous désactivez la règle, le niveau de bande passante n'est pas limité avant l'atteinte du réseau physique .

- 8 (Facultatif) Spécifiez les paramètres du trafic réseau.

Option	Description
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	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 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 ainsi transférés à une vitesse plus élevée.

- 9 (Facultatif) Sélectionnez le type de VLAN à utiliser.

Option	Description
Aucune	N'utilise pas de VLAN.
VLAN	Dans le champ [ID VLAN] , entrez un nombre entre 1 et 4094.

Option	Description
jonction VLAN	Entrez une plage de jonctions VLAN dans [Intervalle de joncteur réseau VLAN] .
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

- 10 (Facultatif) Dans le groupe association et basculement, spécifiez les éléments suivants.

Option	Description
Équilibrage de charge	<p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> ■ [Route en fonction du port virtuel originel] : choisissez une liaison montante selon le port virtuel par lequel est entré le trafic dans le commutateur distribué. ■ [Route basée sur le hachage IP] : choisissez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ [Route basée sur hachage MAC source] : choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ [Route basée sur la charge NIC physique] — Choisissez une liaison montante basée sur les charges actuelles des NIC physiques. ■ [Utiliser la commande de basculement explicite] : Utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. <p>REMARQUE L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.</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] : basée uniquement sur l'état du lien que la carte réseau fournit. Cette option détecte les pannes, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ [Sondage balise] : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. <p>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.</p> <p>Si vous sélectionnez [Oui], chaque fois qu'une carte NIC virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte NIC 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>

Option	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 slot le cas échéant. Si le retour arrière est défini sur [Non] , un adaptateur défectueux est laissé inactif, 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. Si vous voulez 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"> ■ [liaison montante active] : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ [Liaisons montantes de standby] : utilisez cette liaison montante si la connectivité de l'adaptateur actif est interrompue. ■ [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.

- 11 (Facultatif) Dans le groupe Allocation des ressources, dans le menu déroulant, sélectionnez le **[Pool de ressources réseau]** auquel le groupe de ports distribués doit être associé.
- 12 (Facultatif) Dans le groupe de surveillance, choisissez l' **[Statut Netflow]** .

Option	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.

- 13 (Facultatif) Dans le groupe **[Divers]** , indiquez si vous voulez **[Bloquer tous les ports]** du groupe de ports distribués.
- 14 Cliquez sur **[Suivant]** .
Toutes les règles affichées sont appliquées à tous les groupes de ports sélectionnés, y compris les règles qui n'ont pas été modifiées.
- 15 (Facultatif) Si vous devez apporter des modifications, cliquez sur **[Retour]** pour revenir à l'écran approprié.
- 16 Vérifiez les paramètres des groupes de ports et cliquez sur **[Terminer]** .

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 la prise en charge d'Internet Protocol Version 6 », page 71](#)
- [« Configuration VLAN », page 72](#)
- [« Utilisation de la mise en miroir de ports », page 72](#)
- [« Configurer les paramètres NetFlow », page 76](#)
- [« Switch Discovery Protocol », page 77](#)
- [« Changer les configurations de routage et DNS », page 79](#)
- [« Adresses MAC », page 79](#)
- [« Montage de volumes NFS », page 80](#)

Activer la prise en charge d'Internet Protocol Version 6

Le support Internet Protocol IPv6 (IPv6) dans ESXi 6 permet d'utiliser les fonctions d'infrastructure virtuelle, telles que NFS dans un environnement d'IPv6. Utilisez la boîte de dialogue Propriétés mise en réseau pour activer ou mettre hors tension le support d'IPv6 sur l'hôte.

IPv6 est désigné par le groupe de travail IETF comme le successeur de IPv4. La principale différence réside dans la longueur d'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.

IPv6 est désactivé par défaut.

Prérequis

Privilège nécessaire : **Hôte.Configuration.Configuration réseau**

Procédure

- 1 Dans la page d'accueil de vSphere Client, cliquez sur **[Hôtes et clusters]**.
- 2 Choisissez l'hôte et cliquez sur l'onglet **[Configuration]**.
- 3 Cliquez sur le lien **[Mise en réseau]** sous **[Matériel]**.
- 4 Dans la vue **[Commutateur standard vSphere]**, cliquez sur le lien **[Propriétés]**.

- 5 Sélectionnez **[Activer support IPv6 sur système hôte]** et cliquez sur **[OK]**.
- 6 Redémarrez l'hôte.

Configuration VLAN

Les VLAN (LAN virtuels) permettent à un segment LAN physique unique d'être davantage segmenté de sorte que des groupes de travail 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.
- Sécurisation du trafic réseau.
- Réduction de la congestion du trafic réseau.
- Le trafic iSCSI nécessite un réseau isolé.

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. Les groupes de ports connectés au commutateur virtuel doivent avoir une ID VLAN appropriée spécifiée.

Avec VGT, tous les balisages VLAN sont exécutés par la machine virtuelle. Les balises VLAN sont conservées entre la pile réseau de la machine virtuelle et le commutateur externe quand les trames passent par les commutateurs virtuels. Les ports de commutateur physique sont réglés sur le port trunk.

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

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.

Créer une session de mise en miroir de ports

Créez une session de mise en miroir de ports pour mettre en miroir le trafic du vSphere distributed switch sur des ports de commutateur physiques.

Prérequis

Créez un commutateur distribué vSphere version 5.0.0 ou ultérieure.

Procédure

- 1 [Spécifier le nom et les informations de session de mise en miroir de ports](#) page 73
Définissez le nom, la description et les informations de la nouvelle session de mise en miroir de ports.
- 2 [Choisir les sources de mise en miroir de ports](#) page 73
Sélectionnez les sources et la direction de trafic de la nouvelle session de mise en miroir de ports.
- 3 [Choisir les destinations de mise en miroir de port](#) page 73
Sélectionnez les ports ou les liaisons montantes comme destinations de la session de mise en miroir des ports.

4 [Vérifier les nouveaux paramètres de mise en miroir de ports](#) page 74

Vérifiez et activez la nouvelle session de mise en miroir de ports.

Spécifier le nom et les informations de session de mise en miroir de ports

Définissez le nom, la description et les informations de la nouvelle session de mise en miroir de ports.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sous l'onglet de mise en miroir de ports, cliquez sur **[Ajouter]**.
- 4 Entrez le **[nom]** et la **[Description]** de la session de mise en miroir de ports.
- 5 (Facultatif) Sélectionnez **[Autoriser les E/S normales sur les ports de destination]** pour autoriser le trafic E/S sur les ports de destination.

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.
- 6 (Facultatif) Sélectionnez **[VLAN d'encapsulation]** pour créer un ID VLAN qui encapsule toutes les trames sur les 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.
- 7 (Facultatif) Sélectionnez **[Préserver le VLAN d'origine]** pour conserver le réseau VLAN d'origine dans une balise interne afin que les trames mises en miroir soient à double encapsulation.

Cette option est disponible uniquement si vous sélectionnez **[VLAN d'encapsulation]**.
- 8 (Facultatif) Sélectionnez **[Longueur du paquet en miroir]** pour limiter la taille des trames en miroir.

Si vous sélectionnez cette option, toutes les trames en miroir sont tronquées en fonction de la longueur définie.
- 9 Cliquez sur **[Suivant]**.

Choisir les sources de mise en miroir de ports

Sélectionnez les sources et la direction de trafic de la nouvelle session de mise en miroir de ports.

Procédure

- 1 Indiquez si vous voulez utiliser cette source pour le trafic **[Entrée]** ou **[Sortie]** ou choisissez **[Entrée/Sortie]** pour utiliser la source pour les deux types de trafics.
- 2 Tapez les ID de port source et cliquez sur **[>>]** pour ajouter les sources à la session de mise en miroir des ports.

Séparez les ID de port avec une virgule.
- 3 Cliquez sur **[Suivant]**.

Choisir les destinations de mise en miroir de port

Sélectionnez les ports ou les liaisons montantes comme destinations de la session de mise en miroir des ports.

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 le **[Type de source]** .

Option	Description
Port	Entrez un ou plusieurs [ID de port] à utiliser comme destination de la session de mise en miroir de ports. Séparez les ID avec une virgule.
Liaison montante	Sélectionnez une ou plusieurs liaisons montantes à utiliser comme destination pour la session de mise en miroir de ports.

- 2 Cliquez sur **[>>]** pour ajouter les destinations sélectionnées à la session de mise en miroir des ports.
- 3 (Facultatif) Répétez les étapes ci-dessus pour ajouter plusieurs destinations.
- 4 Cliquez sur **[Suivant]** .

Vérifier les nouveaux paramètres de mise en miroir de ports

Vérifiez et activez la nouvelle session de mise en miroir de ports.

Procédure

- 1 Vérifiez que le nom et les paramètres indiqués pour la nouvelle session de mise en miroir de ports sont corrects.
- 2 (Facultatif) Cliquez sur **[Retour]** pour apporter des modifications.
- 3 (Facultatif) Cliquez sur **[Activer cette session de mise en miroir du port]** pour démarrer immédiatement la session de mise en miroir de ports.
- 4 Cliquez sur **[Terminer]** .

Afficher les détails de la session de mise en miroir de ports

Affichez les détails de la session de mise en miroir de ports, notamment son état, ses sources et ses destinations.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sur l'onglet **[Mise en miroir de ports]** , sélectionnez la session de mise en miroir des ports à afficher.
Les détails de la session de mise en miroir des ports sélectionnée s'affichent sous **[Détails de la session de mise en miroir de ports]** .
- 4 (Facultatif) Cliquez sur **[Modifier]** pour modifier les informations de la session sélectionnée de mise en miroir de ports.
- 5 (Facultatif) Cliquez sur **[Supprimer]** pour supprimer la session sélectionnée de mise en miroir de ports.
- 6 (Facultatif) Cliquez sur **[Ajouter]** pour ajouter une nouvelle session de mise en miroir de ports.

Modifier le nom et les informations d'une session de mise en miroir de ports

Modifiez les informations d'une session de mise en miroir de ports, notamment son nom, sa description et son état.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .

- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Dans l'onglet **[Mise en miroir de ports]** , sélectionnez la session de mise en miroir de ports à modifier et cliquez sur **[Modifier]** .
- 4 Cliquez sur l'onglet **[Propriétés]** .
- 5 (Facultatif) Entrez un nouveau **[Nom]** pour la session de mise en miroir de ports.
- 6 (Facultatif) Entrez une nouvelle **[Description]** pour la session de mise en miroir de ports.
- 7 Indiquez si la session de mise en miroir de port doit être **[Activée]** ou **[Désactivée]** .
- 8 (Facultatif) Sélectionnez **[Autoriser les E/S normales sur les ports de destination]** pour autoriser le trafic E/S sur les ports de destination.
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.
- 9 (Facultatif) Sélectionnez **[VLAN d'encapsulation]** pour créer un ID VLAN qui encapsule toutes les trames sur les 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.
- 10 (Facultatif) Sélectionnez **[Préserver le VLAN d'origine]** pour conserver le réseau VLAN d'origine dans une balise interne afin que les trames mises en miroir soient à double encapsulation.
Cette option est disponible uniquement si vous sélectionnez **[VLAN d'encapsulation]** .
- 11 (Facultatif) Sélectionnez **[Longueur du paquet en miroir]** pour limiter la taille des trames en miroir.
Si vous sélectionnez cette option, toutes les trames en miroir sont tronquées en fonction de la longueur définie.
- 12 Cliquez sur **[OK]** .

Modifier les source de mise en miroir de port

Modifiez les sources et la direction du trafic de la session de mise en miroir de ports.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Dans l'onglet **[Mise en miroir de ports]** , sélectionnez la session de mise en miroir de ports à modifier et cliquez sur **[Modifier]** .
- 4 Cliquez sur l'onglet **[Sources]** .
- 5 (Facultatif) Indiquez si vous voulez utiliser cette source pour le trafic **[Entrée]** ou **[Sortie]** ou choisissez **[Entrée/Sortie]** pour utiliser la source pour les deux types de trafics.
- 6 (Facultatif) Tapez un ou plusieurs ID de port ou plages d'ID de port à ajouter comme source pour la session de mise en miroir de port et cliquez sur **[>>]** .
Séparez les ID avec une virgule.
- 7 (Facultatif) Sélectionnez une source dans la liste de droite et cliquez sur **[<<]** pour supprimer la source de la session de mise en miroir de port.
- 8 Cliquez sur **[OK]** .

Modifier les destinations de mise en miroir de ports

Editez les ports de destination et les liaisons montantes d'une session de mise en miroir de ports afin de changer l'emplacement où le trafic de la session est mis en miroir.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Dans l'onglet **[Mise en miroir de ports]**, sélectionnez la session de mise en miroir de ports à modifier et cliquez sur **[Modifier]**.
- 4 Cliquez sur l'onglet **[Destinations]**.
- 5 (Facultatif) Sélectionnez le **[Type de destination]** de la destination à ajouter.

Option	Description
Port	Entrez un ou plusieurs [ID de port] à utiliser comme destination de la session de mise en miroir de ports. Séparez les ID avec une virgule.
Liaison montante	Sélectionnez une ou plusieurs liaisons montantes à utiliser comme destination pour la session de mise en miroir de ports.

- 6 (Facultatif) Tapez un ou plusieurs ID de port ou plages d'ID de port à ajouter comme destination pour la session de mise en miroir de ports et cliquez sur **[>>]**.
Séparez les ID avec une virgule.
- 7 (Facultatif) Sélectionnez une destination dans la colonne de droite et cliquez sur **[<<]** pour supprimer la destination de la session de mise en miroir de ports.
- 8 Cliquez sur **[OK]**.

Configurer les paramètres NetFlow

NetFlow est un outil d'analyse de réseau que vous pouvez utiliser pour contrôler la surveillance du réseau et le trafic de machine virtuelle.

NetFlow est disponible dans le commutateur distribué vSphere version 5.0 et les versions suivantes.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Accédez à l'onglet **[NetFlow]**.
- 4 Entrez l' **[Adresse IP]** et le **[Port]** du collecteur NetFlow.
- 5 Entrez l' **[adresse IP VDS]**.

Avec une adresse IP sur le commutateur distribué vSphere, le collecteur NetFlow peut interagir avec le commutateur distribué vSphere en tant que commutateur unique, au lieu d'interagir avec un commutateur non associé distinct pour chaque hôte associé.

- 6 (Facultatif) Utilisez les flèches de menu déroulant Haut et Bas pour définir le **[Délai d'attente d'exportation de flux actif]** et le **[Délai d'attente d'exportation de flux inactif]**.

- 7 (Facultatif) Utilisez les flèches de menu déroulant Haut et Bas pour définir le **[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.
- 8 (Facultatif) Sélectionnez **[Traiter les flux internes uniquement]** pour collecter les données uniquement concernant l'activité réseau entre les machines virtuelles sur le même hôte.
- 9 Cliquez sur **[OK]** .

Switch Discovery Protocol

Les protocoles SDP (Switch Discovery Protocols) permettent aux administrateurs vSphere d'identifier le port de commutateur connecté à un commutateur standard vSphere ou vSphere Distributed Switch.

vSphere 5.0 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 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.

Activer le protocole découverte Cisco (CDP) sur un vSphere Distributed Switch

Le protocole découverte Cisco (CDP) permet aux administrateurs vSphere de déterminer quel port de commutateur Cisco est connecté à un commutateur standard vSphere ou à un vSphere Distributed Switch. Lorsque le CDP est activé pour un vSphere Distributed Switch particulier, vous pouvez afficher les propriétés du commutateur Cisco (telles que l'ID de périphérique, la version logicielle et le délai d'expiration) à partir de vSphere Client.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]** .
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]** .
- 3 Sur l'onglet **[Propriétés]** , sélectionnez **[Avancé]** .
- 4 Sélectionnez **[Activé]** dans le menu déroulant **[Statut]** .
- 5 Sélectionnez **[Protocole découverte Cisco]** dans le menu déroulant **[Type]** .
- 6 Sélectionnez le mode CDP dans le menu déroulant **[Fonctionnement]** .

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

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 vSphere Client.

Le protocole LLDP est uniquement disponible sur le vSphere Distributed Switch version 5.0.0. et les versions suivantes.

Procédure

- 1 Connectez-vous à vSphere Client et sélectionnez la vue d'inventaire **[Mise en réseau]**.
- 2 Cliquez avec le bouton droit de la souris sur vSphere Distributed Switch dans le volet d'inventaire et sélectionnez **[Modifier les paramètres]**.
- 3 Sur l'onglet **[Propriétés]**, sélectionnez **[Avancé]**.
- 4 Sélectionnez **[Activé]** dans le menu déroulant **[Statut]**.
- 5 Sélectionnez **[Protocole LLDP (Link Layer Discovery Protocol)]** dans le menu déroulant **[Type]**.
- 6 Sélectionnez le mode LLDP dans le menu déroulant **[Fonctionnement]**.

Option	Description
Écouter	ESXi détecte et affiche les informations sur le port physique associé, mais les informations sur le vSphere Distributed Switch ne sont pas mises à la disposition de l'administrateur du commutateur.
Annoncer	ESXi met les informations sur le vSphere Distributed Switch à la disposition de l'administrateur du commutateur, mais ne détecte, ni n'affiche d'informations sur le commutateur physique.
Les deux	ESXi détecte et affiche les informations sur le commutateur physique associé et met les informations sur le vSphere Distributed Switch à la disposition de l'administrateur du commutateur.

- 7 Cliquez sur **[OK]**.

Afficher les informations de commutateur sur vSphere Client

Lorsque CDP ou LLDP a la valeur **[Écouter]** ou **[Les deux]**, vous pouvez afficher les informations des commutateurs physiques depuis vSphere Client.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]**.
- 3 Cliquez sur l'icône d'information à droite du commutateur standard vSphere ou du vSphere Distributed Switch pour afficher les informations de ce commutateur.

Les informations du commutateur sélectionné apparaissent.

Changer les configurations de routage et DNS

Vous pouvez modifier les informations du serveur DNS ou de passerelle par défaut fournies lors de l'installation à la page de configuration de l'hôte dans vSphere Client.

Procédure

- 1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Configuration]**, puis sur **[DNS et routage]**.
- 3 À droite de la fenêtre, cliquez sur **[Propriétés]**.
- 4 Dans l'onglet **[Config. DNS]**, entrez un nom et un domaine.
- 5 Choisissez d'obtenir automatiquement l'adresse du serveur DNS ou d'utiliser une adresse du serveur DNS.
- 6 Spécifiez les domaines de recherche d'hôtes.
- 7 Sur l'onglet **[Routage]**, modifiez les informations de passerelle par défaut, si nécessaire.
- 8 Cliquez sur **[OK]**.

Adresses MAC

Des adresses MAC sont générées pour les adaptateurs réseau virtuelles qu'utilisent les machines virtuelles et les services réseau.

Dans la plupart des cas, les adresses MAC générées sont appropriées. Néanmoins, vous devrez peut-être configurer une adresse MAC pour un adaptateur réseau virtuelle, notamment dans les cas suivants :

- Les adaptateurs réseau virtuelles sur différents hôtes physiques partagent le même sous-réseau et se voient assigner la même adresse MAC, ce qui provoque un conflit.
- Pour garantir que la carte réseau virtuelle ait toujours la même adresse MAC.

Pour contourner la limite des 256 adaptateurs réseau virtuelles par machine physique et les conflits possibles d'adresse MAC entre machines virtuelles, les administrateurs système peuvent attribuer manuellement des adresses MAC. VMware utilise par défaut l'OUI (Organizationally Unique Identifier) 00:50:56 pour les adresses générées manuellement, mais toutes les adresses uniques générées manuellement sont prises en charge.

Vous pouvez définir les adresses en ajoutant la ligne suivante dans le fichier de configuration d'une machine virtuelle :

```
ethernetnumber.address = 00:50:56:XX:YY:ZZ
```

où *<number>* est le numéro de la carte Ethernet, XX est un nombre hexadécimal valide entre 00 et 3F, et YY et ZZ sont des numéros hexadécimaux valides entre 00 et FF. La valeur pour XX ne doit pas être supérieure à 3F afin d'éviter tout conflit avec des adresses MAC générées par VMware Workstation et les produits VMware Server. La valeur maximum pour une adresse MAC générée manuellement est la suivante :

```
ethernetnumber.address = 00:50:56:3F:FF:FF
```

Vous devez également définir l'option dans le fichier de configuration d'une machine virtuelle :

```
ethernetnumber.addressType="static"
```

Comme les machines virtuelles ESXi ne prennent pas en charge les adresses MAC arbitraires, vous devez utiliser le format ci-dessus. Tant que vous choisissez une valeur unique pour XX:YY:ZZ parmi vos adresses codées de manière irréversible, les conflits entre les adresses MAC assignées automatiquement et manuellement ne devraient jamais se produire.

Génération d'adresses MAC

Chaque carte réseau virtuelle dans une machine virtuelle se voit attribuer une adresse MAC unique. Chaque fabricant de carte réseau se voit attribuer un préfixe unique à trois octets appelé OUI (Organizationally Unique Identifier) qu'il peut utiliser pour générer des adresses MAC uniques.

VMware possède les OUI suivants :

- Adresses MAC générées
- Adresses MAC configurées manuellement
- Pour les machines virtuelles existantes qui ne sont plus utilisées avec ESXi

Les trois premiers octets de l'adresse MAC générée pour chaque carte réseau virtuelle correspondent au OUI. L'algorithme de génération d'adresse MAC produit les trois autres octets. L'algorithme garantit des adresses MAC uniques au sein d'une machine et tente de fournir des adresses MAC uniques à travers les machines.

Les adaptateurs réseau pour chaque machine virtuelle du même sous-réseau doivent disposer d'adresses MAC uniques. Sinon, leur comportement risque d'être imprévisible. L'algorithme limite le nombre de machines virtuelles en exécution et suspendues, en même temps, sur un hôte donné. Il ne gère pas non plus tous les cas où des machines virtuelles sur des machines physiques distinctes partagent un sous-réseau.

L'identificateur unique universel VMware (UUID) génère des adresses MAC contrôlées pour les conflits. Les adresses MAC générées comportent trois parties : l'OUI VMware, l'UUID SMBIOS pour la machine physique ESXi et un hachage basé sur le nom de l'entité pour laquelle l'adresse MAC est générée.

Lorsque l'adresse MAC a été générée, elle ne change pas à moins que la machine virtuelle ne soit transférée à un emplacement différent (par exemple, un chemin d'accès différent sur le même serveur). L'adresse MAC dans le fichier de configuration de la machine virtuelle est enregistrée. Toutes les adresses MAC attribuées aux adaptateurs réseau de machines virtuelles suspendues ou en exécution sur une machine physique donnée sont suivies.

L'adresse MAC d'une machine virtuelle hors tension n'est pas comparée aux adresses MAC de machines virtuelles suspendues ou en exécution. Lorsqu'une machine virtuelle est de nouveau mise sous tension, il se peut qu'elle acquière une adresse MAC différente. Cette acquisition est due à un conflit avec une machine virtuelle qui était sous tension quand cette machine virtuelle était hors tension.

Configurer une adresse MAC

Vous pouvez assigner des adresses MAC statiques aux cartes NIC virtuelles d'une machine virtuelle éteinte.

Procédure

- 1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.
- 2 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]**.
- 3 Sélectionnez la carte réseau dans la liste Matériel.
- 4 Dans un groupe d'adresses MAC, sélectionnez **[Manuel]**.
- 5 Saisissez l'adresse MAC statique, puis cliquez sur **[OK]**.

Montage de volumes NFS

ESXi prend en charge les montages NFS basés sur VMkernel.

Les volumes NFS sont montés avec des images ISO grâce à la fonctionnalité NFS de VMkernel. Tous les volumes NFS montés de cette manière apparaissent sous forme de banques de données dans vSphere Client.

Meilleures pratiques de mise en réseau

7

Prenez en compte ces meilleures pratiques lors de la configuration de votre réseau.

- Séparez les services réseau les uns des autres pour obtenir une sécurité accrue et de meilleures performances.

Placez un groupe de machines virtuelles sur une carte réseau physique séparée. 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 servir le trafic à partir d'un client Web, par exemple.

- Conservez la connexion vMotion sur un réseau séparé dédié à vMotion. 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.
- Pour séparer physiquement des services réseau et dédier un ensemble particulier de adaptateurs 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 dans le reste de votre environnement et qu'aucun routeur ne les connecte.
- 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 de meilleurs résultats, utilisez des adaptateurs réseau virtuelles vmxnet3.
- Chaque adaptateur réseau physique connecté au même commutateur standard vSphere ou au même vSphere Distributed Switch doit également être connecté au même réseau physique.
- Configurez tous les adaptateurs réseau VMkernel sur le même MTU. Lorsque plusieurs adaptateurs réseau VMkernel sont connectés aux vSphere Distributed Switches mais possèdent différents MTU configurés, il est possible que vous rencontriez des problèmes de connectivité.

Index

A

- adaptateurs actifs **17**
- adaptateurs de liaison montante
 - ajout **17**
 - ajouter à un commutateur distribué vSphere **30**
- duplex **17**
- gestion **30**
- suppression **30**
- vitesse **17**
- adaptateurs réseau
 - affichage **9, 25**
 - commutateur distribué **31**
 - vSphere distributed switch **30**
- adaptateurs réseau physiques
 - ajouter à un commutateur distribué vSphere **30**
- gestion **30**
- suppression **30**
- adaptateurs réseau virtuels, suppression **34**
- Adaptateurs réseau VMkernel
 - activation de vMotion **33**
 - ajout **14, 31**
 - enregistrement de tolérance aux pannes **33**
 - modification **33**
- adaptateurs standby **17**
- adresse IP, modification **33**
- adresse MAC
 - configuration **79, 80**
 - génération **80**
 - statique **80**
- adresses MAC **59**
- ajout
 - commutateur distribué vSphere **21**
 - groupes de ports distribués **26**
- ajout d'un adaptateur réseau VMkernel **14**
- Association de adaptateurs réseau, définition **7**
- Association de cartes réseau, commutateurs standard **48**
- attributions de liaison montante **25**

B

- bande passante
 - maximale **60, 61**
 - moyenne **60, 61**
- bande passante maximale **60–63, 66**

- bande passante moyenne **60–63, 66**
- basculement **47**
- blocage des ports **47**

C

- carte virtuelle **32**
- CDP **77, 78**
- commutateur distribué
 - adaptateurs réseau virtuels **31**
 - adresse IP **24**
 - ajout **21**
 - ajouter un hôte à **22**
 - carte réseau virtuelle **32**
 - configuration **21**
 - hôtes **23**
 - informations de contact admin **24**
 - machines virtuelles **34**
 - migration de machines virtuelles **34**
 - mise à niveau **25**
 - MTU maximal **24**
 - nombre maximum de ports **24**
 - nouveau pool de ressources **38**
 - paramètres de pool de ressources **38**
 - ports **23**
 - Protocole découverte Cisco **24**
 - Trames jumbo **42**
- commutateur distribué vSphere
 - ajout **21**
 - gérer les hôtes **23**
 - hôtes **23**
 - migration de machines virtuelles **34**
 - mise à niveau **25**
 - modification **33**
 - ports **23**
- commutateur standard **11**
- commutateur standard vSphere
 - affichage **8**
 - configuration **16**
 - configuration des ports **16**
 - définition **7**
 - propriétés **16**
 - règles d'association et de basculement **50**
 - utilisation **11**
- Commutateur virtuel **20**
- commutateurs Cisco **77**

- commutateurs standard
 - Association de cartes réseau **48**
 - bande passante maximale **61**
 - bande passante moyenne **61**
 - basculement **48**
 - configuration **16**
 - configuration des ports **16**
 - état du lien **48**
 - mode promiscuité **56**
 - Modifications d'adresse MAC **56**
 - propriétés **16**
 - règles d'équilibrage de charge **48**
 - règles de formation du trafic **61**
 - règles de sécurité **56**
 - sondage de balise **48**
 - taille de rafale **61**
 - Transmissions forgées **56**
 - utilisation **11**
- configuration des ports **16**
- Configuration DNS, commutateur distribué vSphere **33**
- Contrôle E/S réseau **64**

D

- délestage de segmentation TCP **41**
- déplacement de port actif, groupes de ports distribués **27**
- détection de basculement de réseau **50, 53**
- DirectPath I/O, vMotion **45**
- DirectPath I/O Gen. 2 **45**
- DNS **79**

E

- équilibrage de charge, groupes de ports distribués **51, 66**
- état du lien, commutateurs standard **48**
- états, ports distribués **27**

F

- format de nom de port, groupes de ports distribués **27**

G

- gestion des ressources réseau **37**
- groupe de ports standard **12**
- groupes de ports
 - définition **7**
 - détection de basculement de réseau **50**
 - équilibrage de charge **50**
 - mise en forme du trafic **61**
 - notifier les commutateurs **50**
 - ordre de basculement **50**
 - retour arrière **50**

- sécurité de la couche 2 **57**
- utilisation **12**
- groupes de ports à liaison précoce **26**
- groupes de ports à liaison tardive **26**
- groupes de ports de stockage IP, création **14, 31**
- groupes de ports distribués
 - ajout **26**
 - bande passante maximale **62, 66**
 - bande passante moyenne **62, 66**
 - Contrôle d'E/S **66**
 - Contrôle d'E/S réseau **64**
 - déplacement de port actif **27**
 - description **26**
 - équilibrage de charge **51, 66**
 - format de nom de port **27**
 - jonction VLAN **55, 66**
 - liaison sur l'hôte **27**
 - machines virtuelles **35**
 - mise en forme du trafic **62, 66**
 - mode promiscuité **58, 66**
 - Modifications d'adresse MAC **58, 66**
 - NetFlow **65, 66**
 - nom **26**
 - nombre de ports **26**
 - notifier les commutateurs **51, 66**
 - ordre de basculement **51, 66**
 - paramètres de remplacement **27**
 - pool de ressources **39**
 - pools de ressources réseau **64, 66**
 - ports bloqués **66**
 - règle de VLAN **55, 66**
 - règles d'association **51, 66**
 - règles de basculement **51, 66**
 - règles de port **66**
 - règles de QoS **55, 66**
 - règles de sécurité **58, 66**
 - règles diverses **66**
 - réinitialisation de la config à la déconnexion **27**
 - taille de rafale **62, 66**
 - Transmissions forgées **58, 66**
 - type de groupes de ports **26**
 - VLAN privés **55, 66**

H

- hôtes, ajouter à un vSphere distributed switch **22**

I

ID VLAN
 primaire **28**
 secondaire **28**
 informations de contact admin **24**
 interfaces vMotion, création **14, 31**
 IPv6 **71**
 iSCSI, mise en réseau **14, 72**

J

jonction VLAN, groupes de ports distribués **55, 66**

L

LAN virtuel **72**
 liaison sur l'hôte, groupes de ports distribués **27**
 liaisons montantes actives **50, 53**
 liaisons montantes de réserve **50, 53**
 LLDP, activation **78**

M

machines virtuelles
 migration depuis ou vers un commutateur distribué vNetwork **34**
 migration depuis ou vers un commutateur distribué vSphere **34**
 mise en réseau **34, 35**
 masque de sous-réseau, modification **33**
 meilleures pratiques de mise en réseau **81**
 mise à niveau
 commutateur distribué **25**
 commutateur distribué vSphere **25**
 mise en forme du trafic
 groupes de ports **61**
 groupes de ports distribués **62, 66**
 mise en forme du trafic entrant **63**
 mise en forme du trafic sortant **63**
 mise en miroir de ports
 créer **72**
 destinations **73, 74, 76**
 état **74**
 longueur de paquet **73**
 nom **73, 74**
 sources **73–75**
 vérifier les paramètres **74**
 VLAN **73, 74**
 mise en réseau
 avancée **71**
 introduction **7**
 performances **43**
 règles de sécurité **59**
 mise en réseau d'hôte, affichage **8**
 mise en réseau de machines virtuelles **8, 12, 13**
 mise en réseau VMkernel **8**

mode promiscuité **56, 58, 59, 66**
 Modifications d'adresse MAC **56, 58, 66**
 MTU **41, 42**
 MTU maximal **24**

N

NAS, montage **80**
 NetFlow
 activation **65, 66**
 configurer **76**
 désactivation **65, 66**
 groupes de ports distribués **65, 66**
 paramètres de collecteur **76**
 ports distribués **65**
 netqueue, activation **43**
 NetQueue, désactivation **43**
 NFS, mise en réseau **14**
 NIC
 ajouter à un commutateur distribué vSphere **30**
 suppression d'un commutateur distribué vSphere **30**
 nombre maximum de ports **24**
 notifier les commutateurs **50, 51, 53, 66**
 nouveau pool de ressources, commutateur distribué **38**

O

ordre de basculement, groupes de ports distribués **51, 66**

P

paramètres de pool de ressources
 commutateur distribué **38**
 vSphere distributed switch **40**
 paramètres de remplacement, groupes de ports distribués **27**
 passerelle par défaut, modification **33**
 PCI **44**
 périphérique de relais, ajouter une machine virtuelle **44**
 pool de ressources, groupes de ports distribués **39**
 pools de ressources, réseaux **37**
 pools de ressources réseau
 groupes de ports distribués **64, 66**
 ports distribués **64**
 ports, commutateur distribué vSphere **24**
 ports bloqués
 groupes de ports distribués **66**
 ports distribués **66**
 ports de liaison montante
 règles de formation du trafic **63**
 règles de VLAN **55**
 ports distribués
 bloqués **66**

- contrôle **27**
- Contrôle d'E/S réseau **64**
- détection de basculement de réseau **53**
- équilibrage de charge **53**
- états **27**
- NetFlow **65**
- notifier les commutateurs **53**
- ordre de basculement **53**
- pools de ressources réseau **64**
- ports bloqués **66**
- propriétés **28**
- règles d'association et de basculement **53**
- règles de formation du trafic **63**
- règles de port **66**
- règles de VLAN **55**
- retour arrière **53**
- propriétés, ports distribués **28**
- Protocole découverte Cisco **24, 77, 78**
- Protocole Internet Version 6 **71**
- Protocole LLDP (Link Layer Discovery Protocol) **77, 78**

R

- règle de sécurité de la couche 2 **56**
- règle de VLAN, groupes de ports distribués **55, 66**
- règles d'association
 - groupe de ports **50**
 - groupes de ports distribués **51, 66**
 - ports distribués **53**
- règles d'équilibrage de charge, commutateurs standard **48**
- règles de basculement
 - commutateurs standard **48**
 - groupe de ports **50**
 - groupes de ports distribués **51, 66**
 - ports distribués **53**
- règles de formation du trafic
 - ports de liaison montante **63**
 - ports distribués **63**
- règles de port, groupes de ports distribués **66**
- règles de QoS, groupes de ports distribués **55, 66**
- règles de sécurité
 - commutateurs virtuels **56**
 - exceptions à la règle **56**
 - groupes de ports distribués **58, 66**
 - ports distribués **59**
- règles de VLAN
 - ports de liaison montante **55**
 - ports distribués **55**
- règles diverses, groupes de ports distribués **66**
- réinitialisation de la config à la déconnexion, groupes de ports distribués **27**

- réseaux
 - paramètres de ressources **38–40**
 - pools de ressources **37**
 - ports distribués **27**
- retour arrière **50, 51, 53, 66**
- routage **79**

S

- sécurité de la couche 2 **56**
- sondage de balise, commutateurs standard **48**
- supprimer un pool de ressources, vSphere distributed switch **40**

T

- taille de rafale **60–63, 66**
- TCP/IP **14**
- Tolérance aux pannes, journalisation **33**
- Trames jumbo
 - activation **42**
 - machines virtuelles **41, 42**
- transmissions forcées **59**
- Transmissions forgées **56, 58, 66**
- TSO **41**
- type de VLAN **55**

V

- VLAN
 - définition **7**
 - mise en miroir de ports **73, 74**
 - privé **29**
- VLAN privé
 - créer **29**
 - primaire **29**
 - secondaire **29**
 - suppression **29**
- VLAN privés **55**
- VMkernel
 - configuration **13**
 - définition **7**
 - mise en réseau **14**
 - passerelle **16, 33**
 - préfixe **16, 33**
 - routage **16, 33**
 - Trames jumbo **42**
- vMotion
 - activation sur un adaptateur de réseau virtuel **33**
 - configuration réseau **13**
 - définition **7**
 - DirectPath I/O **45**
 - mise en réseau **14**
- vmxnet amélioré **41, 42**
- vSphere distributed switch
 - adaptateurs réseau virtuels **31**

- adresse IP **24**
- ajout d'un adaptateur réseau VMkernel **31**
- ajouter un hôte à **22**
- carte réseau virtuelle **32**
- CDP **77**
- configuration **21**
- informations de contact admin **24**
- LLDP **78**
- machines virtuelles **34**
- miroir **72**
- mise en miroir de ports **72**
- MTU maximal **24**
- nombre maximum de ports **24**
- paramètres de pool de ressources **40**
- Protocole découverte Cisco **24, 77**
- supprimer un pool de ressources **40**
- tiers **20**
- Trames jumbo **42**

