Guide d'installation et de mise à niveau de vShield

vShield Manager 5.1
vShield App 5.1
vShield Edge 5.1
vShield Endpoint 5.1

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-000868-03

vmware®

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

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

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

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

docfeedback@vmware.com

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 ce guide 5

1 Introduction à vShield 7
- Composants vShield d'un coup d'œil 7
- Scénarios de déploiement 10

2 Préparation à l'installation 13
- Spécifications système 13
- Considérations relatives au déploiement 14

3 Installation de vShield Manager 19
- Obtenir le fichier OVA de vShield Manager 19
- Installer le dispositif virtuel vShield Manager 19
- Configurer les paramètres réseau de vShield Manager 20
- Se connecter à l'interface utilisateur de vShield Manager 21
- Configurer vShield Manager 22
- Changer le mot de passe du compte par défaut de l'interface utilisateur vShield Manager 23
- Programmer une sauvegarde des données de vShield Manager 24

4 Installation de vShield Edge, vShield App, vShield Endpoint et vShield Data Security 25
- Exécution des composants sous licence vShield en mode d'évaluation 25
- Installer les licences des composants vShield 26
- Installer vShield App 26
- Installation de vShield Edge 28
- Installation de vShield Endpoint 33
- Installer vShield Data Security 35

5 Désinstallation des composants vShield 37
- Désinstaller un dispositif virtuel vShield App 37
- Désinstaller une instance vShield Edge 38
- Désinstaller une machine virtuelle vShield Data Security 38
- Désinstaller un module vShield Endpoint 38

6 Mise à niveau de vShield 39
- Mettre à niveau vShield Manager 39
- Mettre à niveau vShield App 45
- Mettre à niveau vShield Edge 45
- Mettre à niveau vShield Endpoint 46
- Mettre à niveau vShield Data Security 47

7 Résolution des problèmes d'installation 49
L'installation de vShield App échoue 49
Échec d'installation de vShield Data Security 50

Index 51

À propos de ce guide

Ce manuel, le *Guide d'installation et de mise à niveau de vShield*, décrit comment installer et configurer le système VMware® vShield™ avec l'interface utilisateur de vShield Manager, le plug-in vSphere Client et l'interface de ligne de commande (CLI). Il inclut des instructions de configuration pas à pas et des suggestions de meilleures pratiques.

Public cible

Ce manuel est destiné à toute personne souhaitant installer ou utiliser vShield dans un environnement VMware vCenter. Les informations qu'il contient sont destinées aux administrateurs système familiarisés avec la technologie des machines virtuelles et avec les opérations de centres de données virtuels. Ce livre suppose aussi que vous connaissez l'infrastructure VMware 5.x, notamment VMware ESX, vCenter Server et vSphere Client.

Glossaire VMware Technical Publications

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

Commentaires sur les documents

VMware prend en considérations vos suggestions pour améliorer sa documentation. Si vous avez des commentaires, envoyez-les à docfeedback@vmware.com.

Ressources de support technique et de formation

Les ressources de support technique suivantes sont à votre disposition. Pour la version actuelle de ce guide ou pour d'autres guides, rendez-vous sur http://www.vmware.com/support/pubs.

Support en ligne et support téléphonique

Pour utiliser le support en ligne afin de soumettre vos demandes de support technique, voir vos informations de produit et de contrat ou enregistrer vos produits, rendez-vous sur http://www.vmware.com/support.

Les clients ayant souscrit des contrats de support appropriés peuvent utiliser le support téléphonique pour obtenir une réponse rapide à leurs problèmes prioritaires. Allez à la http://www.vmware.com/support/phone_support.html.

Offres de support

Pour en savoir plus sur la façon dont les offres de support VMware peuvent satisfaire les besoins de votre entreprise, rendez-vous sur http://www.vmware.com/support/services.

VMware Professional Services

Les cours VMware Education Services proposent de nombreux exercices pratiques, des exemples d'étude de cas, ainsi que de la documentation destinée à servir de référence sur site. Les cours sont disponibles sur site, en salle de cours et en ligne et en direct. Pour les programmes pilotes sur site et les meilleures pratiques de mise en œuvre, VMware Consulting Services propose des offres destinées à vous aider à évaluer, planifier, élaborer et gérer votre environnement virtuel. Pour accéder aux informations sur les classes de formation, les programmes de certification et les services de conseil, rendez-vous sur http://www.vmware.com/services.

Introduction à vShield 1

Ce chapitre présente les composants VMware® vShield™ que vous installez.

Ce chapitre aborde les rubriques suivantes :

- « Composants vShield d'un coup d'œil », page 7
- « Scénarios de déploiement », page 10

Composants vShield d'un coup d'œil

VMware vShield est une suite de dispositifs virtuels de sécurité conçue pour intégration dans VMware vCenter Server. vShield est un composant de sécurité essentiel pour protéger les centres de données virtualisés contre les attaques et les utilisations abusives et pour vous aider à atteindre vos objectifs de conformité réglementaires.

vShield inclut des dispositifs et services virtuels essentiels pour la protection de vos machines virtuelles. vShield peut se configurer par une interface utilisateur web, un plug-in de vSphere Client, une interface de ligne de commande (CLI), et une API REST.

vCenter Server inclut vShield Manager. Les paquets vShield suivants nécessitent chacun une licence :

- vShield App
- vShield App avec Data Security
- vShield Edge
- vShield Endpoint

Un vShield Manager gère un seul environnement vCenter Server et plusieurs instances de vShield App, vShield Edge, vShield Endpoint et vShield Data Security.

vShield Manager

vShield Manager est le composant centralisé de gestion de réseau de vShield, il s'installe comme dispositif virtuel sur tout hôte ESX™ dans votre environnement vCenter Server. vShield Manager peut s'utiliser sur un hôte ESX différent de vos agents vShield.

Les administrateurs peuvent installer, configurer et gérer les composants vShield par l'interface utilisateur de vShield Manager ou par le plug-in de vSphere Client. L'interface utilisateur de vShield Manager tire parti du SDK VMware Infrastructure pour afficher une copie du panneau d'inventaire de vSphere Client, et inclut les vues d'hôtes et de clusters ainsi que de réseaux.

vShield App

vShield App est un pare-feu basé sur un hyperviseur qui protège les applications dans le centre de données virtuel contre les attaques provenant du réseau. Les organisations disposent d'une visibilité et d'un contrôle sur les communications réseau entre les machines virtuelles. Vous pouvez créer des stratégies de contrôle d'accès en fonction de constructions logiques, telles que des conteneurs VMware vCenter™ et des groupes de sécurité vShield et pas seulement des constructions physiques, telles que des adresses IP. En outre, l'adressage IP souple donne la possibilité d'utiliser la même adresse IP pour plusieurs zones client pour simplifier le provisionnement.

Vous devez installer vShield App sur tous les hôtes ESX d'un cluster pour que les opérations VMware vMotion puissent être exécutées et que les machines virtuelles restent protégées lors de la migration entre des hôtes ESX. Par défaut, un dispositif virtuel vShield App ne peut pas être déplacé à l'aide de vMotion.

La fonction Flow Monitoring affiche l'activité réseau entre les machines virtuelles au niveau du protocole d'application. Vous pouvez utiliser ces informations pour contrôler le trafic réseau, définir et affiner les stratégies du pare-feu et identifier les menaces que court votre réseau.

vShield Edge

vShield Edge offre des services de sécurité et de passerelle de périphérie de réseau pour isoler un réseau virtualisé, ou les machines virtuelles dans un groupe de ports, un groupe de ports vDS ou un groupe de ports Cisco Nexus 1000V. Vous installez un vShield Edge au niveau d'un centre de données et pouvez ajouter jusqu'à dix interfaces internes ou de liaison montante. vShield Edge permet de connecter des réseaux isolés ou réseaux d'extrémité sur des réseaux partagés (liaison montante) en fournissant des services communs de passerelle tels que DHCP, VPN, NAT, et équilibrage de charge. Les déploiements courants de vShield Edge s'effectuent notamment dans la DMZ, les extranets de VPN et des environnements de Cloud à plusieurs partenaires où vShield Edge assure la sécurité périmétrique pour les centres de données virtuels (VDC).

Services standard de vShield Edge (incluant Cloud Director)

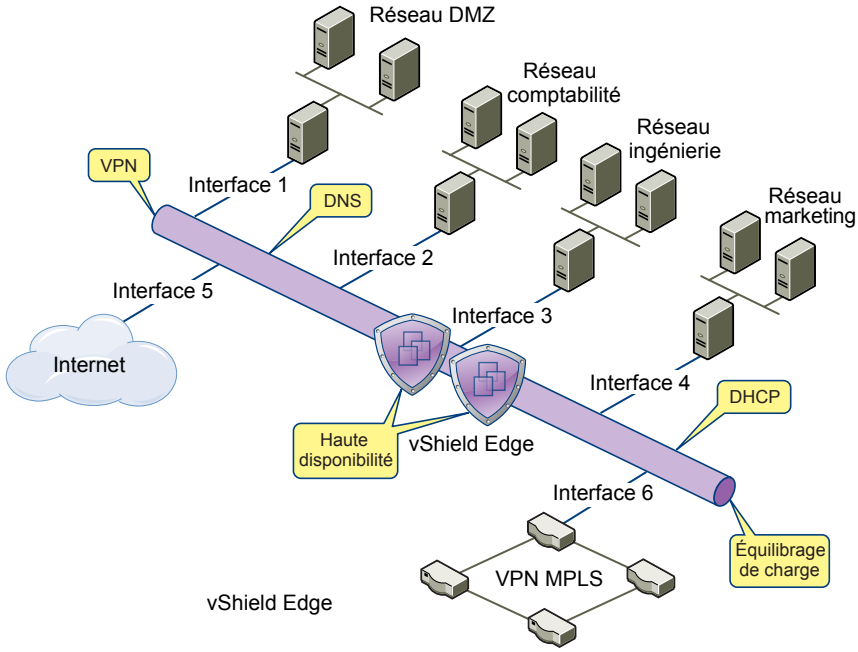
Pare-feu	Les règles prises en charge sont notamment la configuration IP 5-tuple avec plages d'adresses IP et de ports pour l'inspection d'état de tous les protocoles.
Traduction d'adresse réseau	Contrôles séparés des adresses IP source et destination, ainsi que traduction de ports.
Protocole DHCP (Dynamic Host Configuration Protocol)	Configuration de pools d'adresses IP, de passerelles, de serveurs DNS et des domaines de recherche.

Services avancés vShield Edge

Réseau privé virtuel (VPN) d'un site à l'autre	Utilise les paramètres de protocole standardisé IPsec pour l'interopérabilité avec les grands fabricants de VPN.
VPN-Plus SSL	VPN-Plus SSL autorise les utilisateurs à distance à se connecter en toute sécurité à des réseaux privés derrière une passerelvShield Edge.
Équilibrage de charge	Adresses IP et groupes de serveurs virtuels configurables de façon simple et dynamique.
Haute disponibilité	La haute disponibilité assure un vShield Edge actif sur le réseau dans le cas où la machine virtuelvShield Edge principale n'est pas disponible.

vShield Edge autorise l'exportation syslog de tous les services vers des serveurs distants.

Figure 1-1. Edge multi-interface

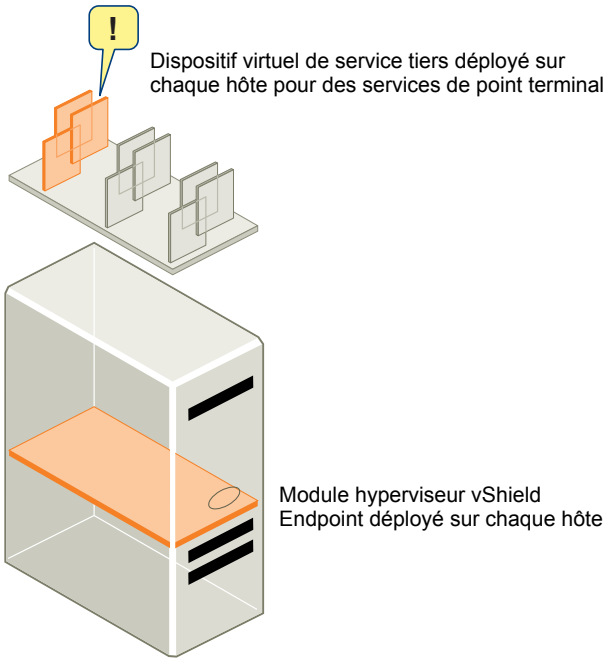


vShield Endpoint

vShield Endpoint transfère le traitement des agents antivirus et contre les logiciels malveillants vers un dispositif virtuel sécurisé et dédié, fourni par des partenaires VMware. Étant donné que le dispositif virtuel sécurisé (à la différence d'une machine virtuelle cliente) n'est pas déconnecté, il peut mettre à jour en permanence les signatures antivirus, assurant ainsi une protection ininterrompue des machines virtuelles sur l'hôte. Par ailleurs, les nouvelles machines virtuelles (ou les machines virtuelles existantes qui ont été déconnectées) sont protégées immédiatement contre la plupart des signatures antivirus actuelles lorsqu'elles sont connectées.

vShield Endpoint installe un module hyperviseur et un dispositif virtuel de sécurité d'un fournisseur antivirus tiers (partenaires VMware) sur un hôte ESX. L'hyperviseur analyse les machines virtuelles clientes depuis l'extérieur, supprimant le besoin d'agents dans chaque machine virtuelle. vShield Endpoint évite ainsi les goulots d'étranglement des ressources de manière efficace, tout en optimisant l'utilisation de la mémoire.

Figure 1-2. vShield Endpoint installé sur un hôte ESX



vShield Data Security

vShield Data Security offre une visibilité dans les données sensibles stockées dans les environnements virtualisés et de nuage de votre organisation. Selon les violations signalées par vShield Data Security, vous pouvez garantir que les données sensibles sont protégées de manière adéquate et évaluer la conformité aux réglementations mondiales.

Scénarios de déploiement

vShield permet de construire des zones sécurisées pour une grande diversité de déploiements de machines virtuelles. Vous pouvez isoler les machines virtuelles en fonction des facteurs personnalisés d'application, de segmentation du réseau ou de conformité. Dès que les stratégies de zone ont été déterminées, vous pouvez déployer vShield pour appliquer les règles d'accès à chacune de ces zones.

Protection de la zone DMZ

La DMZ est une zone de confiance mixte. Les clients y entrent depuis l'Internet pour accéder à des services web et de messagerie, alors que d'autres services dans la DMZ peuvent avoir besoin d'accéder à des services situés dans le réseau interne.

Vous pouvez placer des machines virtuelles en DMZ dans un groupe de ports pour sécuriser ce groupe de ports grâce à vShield Edge. vShield Edge permet d'accéder à des services de pare-feu, de traduction d'adresse NAT et de réseau virtuel VPN, ainsi que d'équilibrer la charge pour la sécurisation des services en DMZ.

Un exemple courant de service en DMZ nécessitant un accès à un service interne est Microsoft Exchange. Microsoft Outlook Web Access (OWA) est couramment installé dans le cluster de DMZ, alors que le serveur principal Microsoft Exchange est dans le cluster interne. Vous pouvez créer des règles de pare-feu sur le cluster interne pour n'autoriser que les requêtes associées à Exchange depuis la DMZ, en désignant des paramètres source et destination précis. Vous pouvez aussi créer des règles depuis le cluster de DMZ pour n'autoriser l'accès à cette DMZ que pour des destinations spécifiques HTTP, FTP ou SMTP.

Isolation et protection des réseaux internes

Vous pouvez utiliser un vShield Edge pour isoler un réseau interne depuis le réseau externe. vShield Edge assure une protection de pare-feu périmétrique et des services de frontière pour sécuriser des machines virtuelles dans un groupe de ports, en autorisant la communication avec le réseau externe par DHCP, la traduction d'adresse NAT et les réseaux privés virtuels VPN.

Vous pouvez installer une instance de vShield App dans le groupe de ports sécurisé sur chaque hôte ESX couvert par le vDS pour sécuriser la communication entre les machines virtuelles du réseau interne.

Si vous utilisez des étiquettes de VLAN pour segmenter le trafic, vous pouvez utiliser App Firewall pour créer des stratégies d'accès plus intelligentes. En utilisant App Firewall plutôt qu'un pare-feu physique, vous pouvez réduire ou associer des zones de confiance dans des clusters ESX partagés. Ceci permet d'assurer une utilisation et une consolidation optimale de fonctions telles que DRS et HA, plutôt que d'utiliser des clusters séparés et fragmentés. La gestion du déploiement ESX global sous forme de pool unique est moins complexe que la gestion de pools séparées.

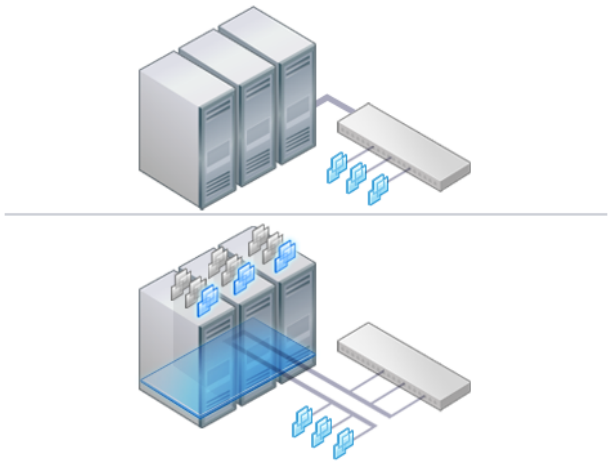
Vous pouvez par exemple utiliser des VLAN pour segmenter les zones de machines virtuelles par des frontières logiques, d'organisation ou de réseau. Grâce au SDK d'infrastructure virtuelle, le panneau d'inventaire de vShield Manager affiche une vue de vos réseaux VLAN sous la vue Réseaux. Vous pouvez construire des règles d'accès pour chaque réseau VLAN et isoler les machines virtuelles pour abandonner le trafic non étiqueté vers ces machines.

Protection des machines virtuelles dans un cluster

Vous pouvez utiliser vShield App pour protéger les machines virtuelles dans un cluster.

Dans Figure 1-3, les instances vShield App sont installées sur chaque hôte ESX dans un cluster. Les machines virtuelles sont protégées lorsqu'elles sont transférées via vMotion ou DRS entres des hôtes ESX dans le cluster. Chaque vApp partage et conserve l'état de toutes les transmissions.

Figure 1-3. Instances de vShield App installées sur chaque hôte ESX d'un cluster



Déploiements courants de vShield Edge

Vous pouvez utiliser un vShield Edge pour isoler un réseau d'extrémité en utilisant NAT pour permettre l'entrée et la sortie du trafic sur le réseau. Si vous déployez des réseaux d'extrémité internes, vous pouvez utiliser vShield Edge pour sécuriser la communication entre réseaux par chiffrement d'un réseau à l'autre avec des tunnels VPN.

vShield Edge peut être déployé comme application en libre service dans VMware Cloud Director.

Déploiements courants de vShield App

Vous pouvez utiliser vShield App pour créer des zones de sécurité dans un vDC. Vous pouvez imposer des stratégies de pare-feu sur des conteneurs vCenter ou des groupes de sécurité, qui sont des conteneurs personnalisés que vous pouvez créer depuis l'interface utilisateur vShield Manager. Les stratégies par conteneur permettent de créer des clusters de zones de confiance mixtes sans exiger de pare-feu physique externe.

Dans un déploiement n'utilisant pas de vDC, utilisez vShield App avec la fonction de groupes de sécurité pour créer des zones de confiance et appliquer les stratégies d'accès.

Les administrateurs des fournisseurs de service peuvent utiliser vShield App pour imposer des stratégies de pare-feu larges sur toutes les machines virtuelles clientes dans un réseau interne. Vous pouvez par exemple imposer une stratégie de pare-feu sur la deuxième carte réseau de toutes les machines virtuelles clientes permettant à ces machines virtuelles de se connecter à un serveur de stockage, tout en empêchant ces machines virtuelles de s'adresser à toute autre machine virtuelle.

Préparation à l'installation 2

Ce chapitre présente la configuration requise pour réussir l'installation de vShield.

Ce chapitre aborde les rubriques suivantes :

- « Spécifications système », page 13
- « Considérations relatives au déploiement », page 14

Spécifications système

Avant d'installer vShield dans l'environnement vCenter Server, tenez compte de la configuration et des ressources réseau. Vous pouvez installer un vShield Manager par vCenter Server, une vShield App ou un vShield Endpoint par hôte ESX™ et plusieurs instances vShield Edge par centre de données.

Matériel

Tableau 2-1. Spécifications du matériel

composants	Minimum
Mémoire	■ vShield Manager : 8 Go alloués, 3 Go réservés ■ vShield App : 1 Go alloué, 1 Go réservé ■ vShield Edge compact : 256 Mo, grand : 1 Go, très grand : 8 GB ■ vShield Data Security : 512 MB
space disque	■ vShield Manager : 60 GB ■ vShield App : 5 Go par vShield App par hôte ESX ■ vShield Edge compact et grand : 320 Mo, très grand : 4,4 Go (avec fichier d'échange de 4 Go) ■ vShield Data Security : 6 Go par hôte ESX
vCPU	■ vShield Manager : 2 ■ vShield App : 2 ■ vShield Edge compact : 1, grand et très grand : 2 ■ vShield Data Security : 1

Logiciel

Pour les informations d'interopérabilité les plus récentes, voir le tableau d'interopérabilité du produit surhttp://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Ci-dessous, figurent les versions minimales requises des produits VMware.

- VMware vCenter Server 5.0 ou version ultérieure

  Pour les câbles virtuels VXLAN, vous avez besoin de vCenter Server 5.1 ou version ultérieure.

- VMware ESX 4.1 ou version ultérieure pour chaque serveur

  vShield Endpoint requiert VMware ESX 4.1 Patch 3 ou une version ultérieure.

  Pour les câbles virtuels VXLAN, vous avez besoin de VMware ESX 5.1 ou version ultérieure.

- VMware Tools

  Pour vShield Endpoint et vShield Data Security, vous devez mettre à niveau les machines virtuelles vers la version matérielle 7 ou 8 et installer VMware Tools 8.6.0 publié avec ESXi 5.0 - Patch 3. Pour plus d'informations, voir « Installer VMware Tools sur les machines virtuelles invitées », page 34.

  Vous devez installer VMware Tools sur les machines virtuelles qui doivent être protégées par vShield App.

- VMware vCloud Director 1.5 ou version ultérieure
- VMware View 4.5 ou version ultérieure

Accès client et utilisateur

- PC avec VMware vSphere Client
- Si vous avez ajouté les hôtes ESX par nom à l'inventaire vSphere, assurez-vous que les serveurs DNS ont été configurés sur vShield Manager et que la résolution de nom fonctionne pour que vShield Manager puisse résoudre les adresses IP.
- Droits d'ajouter et de mettre sous tension des machines virtuelles
- Accès à la banque de données qui contient les fichiers de machine virtuelle, et droits d'accès au compte pour copier les fichiers dans cette banque de données
- Activation des cookies sur votre navigateur web pour accéder à l'interface utilisateur vShield Manager
- Depuis vShield Manager; le port 443 est accessible depuis l'hôte ESX, le vCenter Server et les dispositifs vShield à déployer. Ce port est nécessaire pour télécharger le fichier OVF sur l'hôte ESX pour le déployer.
- Connectez-vous à vShield Manager par l'un des navigateurs web pris en charge suivants :
  - Internet Explorer 6.x et version ultérieure
  - Mozilla Firefox 1.x et version ultérieure
  - Safari 1.x ou 2.x

Considérations relatives au déploiement

Prenez en compte les recommandations et restrictions ci-dessous avant de déployer des composants vShield.

Considérations relatives au déploiement de vShield

Cette rubrique décrit les considérations relatives au déploiement des composants vShield.

Préparation des machines virtuelles pour la protection vShield

Vous devez définir comment vous souhaitez protéger vos machines virtuelles avec vShield. Pour une meilleure utilisation, nous vous conseillons de préparer tous les hôtes ESX au sein d'un cluster DRS pour vShield App, vShield Endpoint et vShield Data Security en fonction des composants vShield utilisés. Vous devez mettre à niveau les machines virtuelles vers la version matérielle 7 ou 8.

Prenez en compte les questions suivantes :

Comment mes machines virtuelles sont-elles regroupées ?

Vous pouvez envisager de déplacer des machines virtuelles vers des groupes de ports sur un vDS ou un autre hôte ESX pour regrouper des machines virtuelles par fonction, par service ou autres structures d'organisation de façon à améliorer la sécurité et à faciliter la configuration des règles d'accès. Vous pouvez installer vShield Edge sur le périmètre de tout groupe de ports pour isoler les machines virtuelles du réseau externe. Vous pouvez installer vShield App sur un hôte ESX et configurer des stratégies de pare-feu par ressource de conteneur de façon à appliquer les règles en fonction de la hiérarchie des ressources.

Mes machines virtuelles sont-elles toujours protégées si j'utilise vMotion pour les transférer vers un autre hôte ESX ?

Oui, si les hôtes dans un cluster DRS sont préparés, vous pouvez migrer les machines entre les hôtes sans affaiblir la sécurité. Pour plus d'informations sur la préparation de vos hôtes ESX, consultez « Installer vShield App », page 26.

Temps de fonctionnement de vShield Manager

vShield Manager doit toujours être installé sur un hôte ESX qui ne sera pas affecté par de temps morts, par exemple redémarrages fréquents ou opérations en mode de maintenance. Vous pouvez utiliser HA ou DRS pour augmenter la résilience de vShield Manager. Si l'hôte ESX sur lequel vShield Manager réside doit subir un temps mort, déplacez le dispositif virtuel vShield Manager par vMotion sur un autre hôte ESX. Il est aussi recommandé d'utiliser plus d'un hôte ESX.

Communication entre composants vShield

Les interfaces de gestion des composants vShield doivent être placées dans un réseau commun, par exemple le réseau de gestion vSphere. vShield Manager a besoin de la connectivité avec le vCenter Server, l'hôte ESXi, ainsi qu'avec les instances vShield App et vShield Edge, le module vShield Endpoint et la machine virtuelle vShield Data Security. Les composants de vShield peuvent communiquer par des connexions routées comme sur des réseaux locaux différents.

VMware vous recommande d'installer vShield Manager sur un cluster de gestion dédié distinct du (des) cluster(s) que vShield Manager gère. Chaque vShield Manager gère un seul environnement vCenter Server .

Si le vCenter Server ou les machines virtuelles de la base de données de vCenter Server se trouvent sur l'hôte ESX sur lequel vous installez vShield App, déplacez-les vers un autre hôte avant d'installer vShield App.

Vérifiez que les ports suivants sont ouverts :

- Port 443/TCP depuis, vers et entre l'hôte ESX, le vCenter Server et vShield Data Security
- UDP123 entre vShield Manager et vShield App pour la synchronisation de l'heure
- 443/TCP à partir du client REST vers vShield Manager pour utiliser les appels API REST
- 80/TCP et 443/TCP pour utiliser l'interface utilisateur de vShield Manager et initier la connexion avec le vSphere SDK
- 22/TCP pour communiquer entre vShield Manager et vShield App et dépanner la CLI

Sécurisation renforcée de vos machines virtuelles vShield

Vous pouvez accéder à vShield Manager et à d'autres composants de vShield à l'aide d'une interface utilisateur web, par une interface de ligne de commande et par l'API REST. vShield inclut des pièces justificatives de connexion par défaut pour chacune de ces options d'accès. Après installation de la machine virtuelle vShield, vous devriez renforcer l'accès en changeant les pièces justificatives de connexion par défaut. Notez que vShield Data Security ne contient pas de données d'identification de connexion par défaut.

Interface utilisateur de vShield Manager

Vous pouvez accéder à l'interface utilisateur de vShield Manager en ouvrant une fenêtre de navigateur web pour accéder à l'adresse IP du port de gestion de vShield Manager.

Le compte d'utilisateur par défaut, admin, a un accès global à vShield Manager. Après la connexion initiale, vous devriez changer le mot de passe par défaut du compte d'utilisateur admin. Reportez-vous à la section « Changer le mot de passe du compte par défaut de l'interface utilisateur vShield Manager », page 23.

Interface de ligne de commande

Vous pouvez accéder aux dispositifs virtuels vShield Manager, vShield App et vShield Edge par l'interface de ligne de commande de la session de console de vSphere Client. Pour accéder au dispositif virtuel de vShield Endpoint, consultez les instructions du fournisseur de la solution antivirus. Vous ne pouvez pas accéder à la machine virtuelle vShield Data Security par l'interface de ligne de commande.

Chaque dispositif virtuel utilise la même combinaison de nom d'utilisateur (**`admin`**) et mot de passe (**`default`**) par défaut que l'interface utilisateur de vShield Manager. L'entrée en mode Enabled utilise aussi le mot de passe **`default`**.

Pour en savoir plus sur la sécurisation renforcée de l'interface en ligne de commande, consultez la *Référence de l'interface en ligne de commande vShield*.

Demandes REST

Toutes les requêtes de l'API REST exigent une authentification auprès de vShield Manager.

Le codage Base 64 permet d'identifier une combinaison de nom d'utilisateur-mot de passe au format suivant : nom d'utilisateur : mot de passe. Vous devez utiliser un compte d'interface utilisateur vShield Manager (nom d'utilisateur et mot de passe) disposant d'accès privilégiés pour effectuer les requêtes. Pour en savoir plus sur l'authentification des requêtes REST API, consultez le *Guide de programmation de vShield API*.

Considérations relatives au déploiement de vShield App

VMware vous recommande d'analyser votre environnement vCenter Server et de déterminer si vous voulez protéger tout l'environnement ou uniquement certains clusters.

Si vous décidez de protéger des clusters spécifiques, vous devez préparer tout le cluster et installer vShield App sur tous les hôtes ESX dans ces clusters. Si vous installez vShield App uniquement sur certains hôtes d'un cluster, il est probable que vMotion puisse déplacer les machines virtuelles d'un hôte protégé vers un hôte non protégé, compromettant ainsi la sécurité de votre réseau.

Vérifiez que vShield App est installé dans votre environnement lors de l'ouverture d'une fenêtre de maintenance. La durée d'installation totale peut varier selon votre environnement et le nombre d'hôtes dans chaque cluster, mais vous devez terminer l'installation de vShield App sur tous les clusters souhaités avant de reprendre les opérations normales.

Après l'installation, VMware vous recommande d'activer vSphere HA et de définir la fonction des clusters sur **[Surveillance des VM et applications]** sur les clusters où est installé vShield App. Cette fonction permet de surveiller le vShield App et déclenche un redémarrage s'il échoue, ce qui réduit l'indisponibilité de vShield App. Pour plus d'informations sur cette fonction, consultez *Disponibilité vSphere*.

VMware vous recommande de laisser vShield App s'exécuter pendant les opérations normales et d'utiliser l'outil vShield App Flow Monitoring pour obtenir des connaissances de référence sur le trafic entrant et sortant de votre réseau virtuel. Vous pouvez ensuite ajouter des règles selon les besoins de votre réseau.

L'activation de la fonction SpoofGuard de vShield App vous permet d'autoriser les adresses IP signalées par VMware Tools et de les modifier si nécessaire pour éviter l'usurpation. Selon le mode SpoofGuard que vous sélectionnez, vShield App fait automatiquement confiance aux affectations d'adresses IP lors de leur première utilisation ou vous demande d'approuver manuellement les affectations d'adresses IP avant de les utiliser. Cependant, sachez que l'adresse IP d'une machine virtuelle peut changer lorsque le serveur DHCP renouvelle un bail ou est redémarré. Cela signifie que vous devez approuver l'adresse IP nouvelle ou renouvelée si la fonction SpoofGuard est activée.

Familiarisez-vous avec les fonctions Flow Monitoring et SpoofGuard avant d'installer vShield App ; cela vous permettra de configurer vShield App de la manière la plus sécurisée possible. Pour plus d'informations sur ces fonctions, consultez le *Guide d'administration vShield*.

Considérations relatives au déploiement de vShield Edge

Avant d'installer vShield Edge, vous devez vous familiariser avec la topologie de votre réseau. vShield Edge peut avoir plusieurs interfaces, mais vous devez connecter au moins une interface interne à un groupe de ports ou un câble virtuel VXLAN avant de pouvoir déployer vShield Edge.

L'interface de liaison montante fournit une connectivité avec le monde extérieur. Vous devez avoir créé et configuré un groupe de ports ou un câble virtuel VXLAN ayant une connectivité externe. Vous devez aussi avoir un groupe de ports avec des machines virtuelles auxquelles vous pouvez connecter l'interface interne. Déterminez les adresses IP et sous-réseaux à fournir pour ces interfaces. Pensez également aux services que vous devez activer et configurer après avoir installer vShield Edge. Pour plus d'informations sur les services vShield Edge, consultez le *Guide d'administration vShield*.

Après avoir installé vShield Edge et avant de configurer les services vShield Edge, les machines virtuelles de ce(s) groupe(s) de ports peuvent perdre la connectivité réseau. Afin d'éviter ce problème, vous pouvez créer un nouveau groupe de ports, installer et configurer vShield Edge sur celui-ci, puis déplacer les machines virtuelles sur ce groupe de ports.

Sachez que la stratégie de pare-feu vShield Edge par défaut bloque tout le trafic entrant ; ainsi vous devez ajouter des règles d'autorisation, le cas échéant.

Installation de vShield Manager 3

VMware vShield assure des services de protection par pare-feu, d'analyse de trafic et de périmètre réseau pour protéger votre infrastructure virtuelle vCenter Server. L'installation de dispositif virtuel vShield a été automatisée pour la plupart des centres de données virtuels.

vShield Manager est le composant de gestion centralisé de vShield. Vous pouvez utiliser vShield Manager pour surveiller et pousser des configurations vers des instances de vShield App, vShield Endpoint et vShield Edge. vShield Manager s'utilise comme dispositif virtuel sur un hôte ESX.

L'installation de vShield Manager s'effectue en plusieurs étapes. Vous devez effectuer toutes les tâches suivantes dans l'ordre pour réussir l'installation de vShield Manager.

Pour améliorer votre sécurité réseau, vous pouvez obtenir des licences de vShield App, vShield Endpoint et vShield Edge.

Ce chapitre aborde les rubriques suivantes :

- « Obtenir le fichier OVA de vShield Manager », page 19
- « Installer le dispositif virtuel vShield Manager », page 19
- « Configurer les paramètres réseau de vShield Manager », page 20
- « Se connecter à l'interface utilisateur de vShield Manager », page 21
- « Configurer vShield Manager », page 22
- « Changer le mot de passe du compte par défaut de l'interface utilisateur vShield Manager », page 23
- « Programmer une sauvegarde des données de vShield Manager », page 24

Obtenir le fichier OVA de vShield Manager

La machine virtuelle vShield Manager est empaqueté dans un fichier OVA (Open Virtualization Appliance), qui permet d'utiliser vSphere Client pour importer vShield Manager dans la banque de données et l'inventaire de machine virtuelle.

Installer le dispositif virtuel vShield Manager

Vous pouvez installer la machine virtuelle vShield Manager sur un hôte ESX dans un cluster configuré par DRS.

Avec vShield 5.0 et les versions suivantes, vous pouvez installer vShield Manager dans un vCenter différent de celui avec lequel vShield Manager va interopérer. Un vShield Manager répond aux besoins d'un environnement vCenter Server.

L'installation de la machine virtuelle vShield Manager inclut VMware Tools. Ne tentez pas de mise à niveau ni d'installation de VMware Tools sur vShield Manager.

Prérequis

Le rôle Enterprise Administrator ou vShield Administrator role doit vous avoir été attribué.

Procédure

1 Connectez-vous à vSphere Client.

2 Créez un groupe de ports pour héberger l'interface de gestion de vShield Manager.

L'interface de gestion de vShield Manager, vCenter Server et les hôtes ESXi doivent être joignables par toutes les futures instances de vShield Edge, vShield App et vShield Endpoint.

REMARQUE Ne placez pas l'interface de gestion de vShield Manager dans le même groupe de ports que Service Console et VMkernel.

---

3 Sélectionnez **[File] > [Deploy OVF Template]** .

4 Cliquez sur **[Parcourir]** pour localiser sur votre PC le dossier qui contient le fichier OVA de vShield Manager.

5 Exécutez l'installation.

vShield Manager est installé comme machine virtuelle dans l'inventaire.

6 Mettez sous tension la machine virtuelle vShield Manager.

Suivant

Le CPU par défaut de vShield Manager 5.1 est 2 vCPU. Pour que vShield Manager fonctionne avec vSphere Fault Tolerance, vous devez régler le CPU sur 1 vCPU.

Configurer les paramètres réseau de vShield Manager

Vous devez utiliser l'interface de ligne de commande (CLI) de vShield Manager pour configurer une adresse IP, indiquer la passerelle par défaut et les paramètres DNS.

Vous pouvez spécifier jusqu'à deux serveurs DNS que vShield Manager utilisera pour la résolution d'adresse IP et de nom d'hôte. DNS est obligatoire si au moins un hôte ESX de votre environnement vCenter Server a été ajouté par nom d'hôte (plutôt que par adresse IP).

Procédure

1 Cliquez à droite sur la machine virtuelle vShield Manager et cliquez sur **[Open Console]** pour ouvrir l'interface de ligne de commande (CLI) de vShield Manager.

La procédure de démarrage peut prendre quelques minutes.

2 Après l'apparition de l'invite `manager login`, connectez-vous à l'interface CLI à l'aide du nom d'utilisateur **`admin`** et du mot de passe **`default`**.

3 Passez en mode Enabled à l'aide du mot de passe **`default`**.

```
manager> enable
Password:
manager#
```

4 Exécutez la commande `setup` pour ouvrir l'assistant de CLI setup.

L'assistant de CLI setup vous aide à affecter des adresses IP pour l'interface de gestion de vShield Manager et l'identification de la passerelle réseau par défaut. L'adresse IP de l'interface de gestion doit être joignable par vCenter Server, l'hôte ESXi, toutes les instances de vShield App, vShield Edge et vShield Endpoint installées, ainsi que par un navigateur Web pour la gestion du système.

```
manager# setup

Use CTRL-D to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

IP Address (A.B.C.D):
Subnet Mask (A.B.C.D):
Default gateway (A.B.C.D):
Primary DNS IP (A.B.C.D):
Secondary DNS IP (A.B.C.D):
Old configuration will be lost.

Do you want to save new configuration (y/[n]): y
```

5 (Facultatif) Si vous avez déjà défini des paramètres réseau pour vShield Manager, vous devez redémarrer le système.

6 Déconnectez-vous de l'interface CLI et reconnectez-vous à l'interface en utilisant le nom d'utilisateur **`admin`** et le mot de passe **`default`**.

7 Lancez un ping sur la passerelle par défaut pour vérifier la connectivité réseau.

```
manager> ping A.B.C.D
```

8 Sur votre PC, lancez un ping sur l'adresse IP de vShield Manager pour vérifier qu'elle est accessible.

Se connecter à l'interface utilisateur de vShield Manager

Après installation et configuration de la machine virtuelle vShield Manager, connectez-vous à l'interface utilisateur de vShield Manager.

Procédure

1 Ouvrez une fenêtre de navigateur web et tapez l'adresse IP attribuée à vShield Manager.

L'interface utilisateur vShield Manager s'ouvre dans une fenêtre de navigateur Web utilisant SSL.

2 Acceptez le certificat de sécurité.

Remarque Vous pouvez utiliser un certificat SSL pour l'authentification. Consultez le *Guide d'administration vShield*.

L'écran de connexion vShield Manager apparaît.

3 Connectez-vous à l'interface utilisateur vShield Manager à l'aide du nom d'utilisateur **`admin`** et du mot de passe **`default`**.

Vous devriez changer le mot de passe dès que possible pour éviter toute utilisation non autorisée. Reportez-vous à la section « Changer le mot de passe du compte par défaut de l'interface utilisateur vShield Manager », page 23.

4 Cliquez sur **[Log In]** .

Configurer vShield Manager

Spécifiez les détails relatifs à vCenter Server, au serveur DNS et au serveur NTP, ainsi que les détails relatifs au serveur de recherche.

Remarque La machine virtuelle vShield Manager n'apparaît pas comme ressource dans le panneau d'inventaire de l'interface utilisateur vShield Manager. L'objet **[Settings & Reports]** représente la machine virtuelle vShield Manager dans le panneau d'inventaire.

Prérequis

- Vous devez disposer d'un compte utilisateur de vCenter Server avec un accès administratif pour synchroniser vShield Manager avec vCenter Server . Si votre mot de passe comporte des caractères qui ne sont pas au format ASCII, vous devez le modifier avant de synchroniser vShield Manager avec vCenter Server.
- Pour utiliser SSO sur vShield Manager, vous devez disposer de vCenter Server 5.1 ou d'une version ultérieure. En outre, le service Single Sign On doit être installé sur vCenter Server.

Procédure

1 Connectez-vous à vShield Manager.

2 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

3 Cliquez sur l'onglet **[Configuration]** .

4 La zone **[Serveurs DNS]** affiche les adresses IP des serveurs DNS que vous avez spécifiés lorsque vous avez configuré les paramètres réseau de vShield Manager.

Vous pouvez modifier les serveurs, si nécessaire.

5 Dans **[Serveur NTP]** , cliquez sur **[Edit]** et tapez l'adresse IP de votre serveur NTP.

Le serveur NTP établit une heure réseau commune. Il est recommandé d'utiliser le serveur NTP utilisé par le serveur SSO afin que l'heure du serveur vShield Manager soit synchronisée avec celle du serveur NTP.

Important Vous devez redémarrer vShield Manager après avoir modifié les détails du serveur NTP.

6 Dans **[Lookup Service]** , cliquez sur **[Edit]** et entrez le nom d'hôte ou l'adresse IP de l'hôte qui dispose du Lookup Service.

7 Le cas échéant, modifiez le numéro du port.

L'URL de Lookup Service est affiché en fonction de l'hôte et du port spécifiés.

8 Tapez le nom d'utilisateur et le mot de passe SSO.

Cette procédure permet à vShield Manager de s'enregistrer sur le Serveur de Service d'émission de jeton de sécurité.

9 Dans **[vCenter Server]** , tapez l'adresse IP ou le nom d'hôte de vCenter Server.

10 Tapez votre nom d'utilisateur de connexion à vSphere Client.

11 Tapez le mot de passe associé au nom d'utilisateur.

12 Pour attribuer le rôle d'administrateur d'entreprise à l'utilisateur sous lequel vous vous êtes connecté, sélectionnez **[Attribuer le rôle d'administrateur d'entreprise à cet utilisateur]** .

Ce rôle confère à l'utilisateur des autorisations d'opérations et de sécurité avec vShield.

13 Pour modifier l'emplacement du téléchargement du script de plug-ins, sélectionnez **[Modifier l'emplacement du téléchargement de plug-ins]** , puis tapez l'adresse IP et le numéro de port de vShield Manager.

   Cette procédure peut être requise pour les environnements NAT. Par défaut, le rôle L'adresse utilisée pour vShield Manager est `vShield_Manager_IP:443`.

14 Cliquez sur **[Save]** .

15 (Facultatif) Sur un ordinateur Windows Server, procédez comme suit afin de charger le panneau d'inventaire vShield Manager :

   a Ouvrez Internet Explorer.

   b Sélectionnez **[Outils] > [Options Internet]** .

   c Dans la fenêtre Options Internet, sélectionnez l'onglet **[Sécurité]** .

   d Cliquez sur **[Sites de confiance]** .

   e Cliquez sur le bouton **[Sites]** .

   f Tapez l'adresse IP de vShield Manager et cliquez sur **[Ajouter]** .

   g Cliquez sur **[Fermer]** .

   h Cliquez sur **[OK]** .

   i Fermez Internet Explorer.

vShield Manager se connecte à vCenter Server, ouvre une session et utilise le SDK VMware Infrastructure pour remplir le panneau d'inventaire vShield Manager. Le panneau d'inventaire est présenté à gauche de l'écran. Cette arborescence de ressources doit correspondre à votre panneau d'inventaire VMware Infrastructure. vShield Manager n'apparaît pas dans le panneau d'inventaire vShield Manager.

Suivant

Connectez-vous à vSphere Client, sélectionnez un hôte ESX et vérifiez que vShield apparaît bien dans un onglet. Vous pouvez ensuite installer et configurer les composants vShield depuis vSphere Client.

Changer le mot de passe du compte par défaut de l'interface utilisateur vShield Manager

Vous pouvez changer le mot de passe du compte admin pour renforcer l'accès à votre vShield Manager.

Procédure

1 Connectez-vous à l'interface utilisateur vShield Manager.

2 Cliquez sur **[Modifier le mot de passe]** dans le coin supérieur droit de la fenêtre.

3 Dans le champ **[Ancien mot de passe]** , tapez **`default`** (le mot de passe actuel).

4 Tapez un nouveau de passe.

5 Confirmez le mot de passe en le tapant une deuxième fois dans le champ **[Retype Password]** .

6 Cliquez sur **[OK]** pour enregistrer vos modifications.

Programmer une sauvegarde des données de vShield Manager

Vous ne pouvez programmer les paramètres que d'un seul type de sauvegarde à la fois. Vous ne pouvez pas programmer une sauvegarde de configuration seulement et une sauvegarde complète des données pour exécution simultanée.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Backups]** .

4 Sur le menu de la liste déroulante **[Scheduled Backups]** , sélectionnez **[On]** .

5 Sur le menu déroulant **[Backup Frequency]** , sélectionnez **[Hourly]** , **[Daily]** ou **[Weekly]** .

Les menus **[Day of Week]** , **[Hour of Day]** et **[Minute]** sont désactivés en fonction de la fréquence sélectionnée. Si vous sélectionnez par exemple **[Daily]** , le menu déroulant **[Day of Week]** est désactivé car ce champ n'est pas applicable à une fréquence quotidienne.

6 (Facultatif) Cochez la case **[Exclude System Events]** pour ne pas sauvegarder les tables d'événements système.

7 (Facultatif) Cochez la case **[Exclude Audit Log]** pour ne pas sauvegarder les tables des journaux d'audit.

8 Tapez dans **[Host IP Address]** l'adresse IP du système sur lequel la sauvegarde sera enregistrée.

9 (Facultatif) Tapez le **[Host Name]** du système de sauvegarde.

10 Tapez dans **[User Name]** le nom d'utilisateur nécessaire pour se connecter au système de sauvegarde.

11 Tapez dans **[Password]** le mot de passe associé au nom d'utilisateur pour le système de sauvegarde.

12 Dans le champ **[Backup Directory]** , tapez le chemin absolu d'enregistrement des sauvegardes.

13 Tapez une chaîne de texte dans **[Filename Prefix]** .

Ce texte sera ajouté devant chaque nom de fichier de la sauvegarde pour faciliter la reconnaissance sur le système de sauvegarde. Si vous tapez par exemple **ppdb**, la sauvegarde résultante sera nommée `ppdbHH_MM_SS_JourJJMoiAAAA`.

14 Dans le menu déroulant **[Transfer Protocol]** , sélectionnez **[SFTP]** ou **[FTP]** , selon ce que la destination prend en charge.

15 Cliquez sur **[Save Settings]** .

Installation de vShield Edge, vShield App, vShield Endpoint et vShield Data Security

4

Après avoir installé vShield Manager, vous pouvez obtenir les licences pour activer les composants vShield App, vShield Endpoint, vShield Edge et vShield Data Security. Le paquet vShield Manager OVA inclut les pilotes et fichiers nécessaires pour installer ces composants supplémentaires. Une licence vShield App vous permet d'utiliser également le composant vShield Endpoint.

Les dispositifs virtuels de vShield incluent VMware Tools. Ne tentez pas de modifier ou mettre à niveau le logiciel VMware Tools sur un dispositif virtuel vShield.

Ce chapitre aborde les rubriques suivantes :

- « Exécution des composants sous licence vShield en mode d'évaluation », page 25
- « Installer les licences des composants vShield », page 26
- « Installer vShield App », page 26
- « Installation de vShield Edge », page 28
- « Installation de vShield Endpoint », page 33
- « Installer vShield Data Security », page 35

Exécution des composants sous licence vShield en mode d'évaluation

Avant d'acheter et d'activer des licences de vShield Edge, vShield App et vShield Endpoint, vous pouvez installer et exécuter des modes d'évaluation des logiciels. En mode d'évaluation, prévu pour démonstration et évaluation, vos instances de vShield Edge, vShield App et vShield Endpoint sont totalement opérationnelles juste après l'installation, ne nécessitent aucune configuration de licence et offrent des fonctionnalités complètes pendant 60 jours à compter de leur première activation.

En mode d'évaluation, les composants vShield n'autorisent qu'un nombre maximal d'instances.

Après l'expiration de la période d'évaluation de 60 jours, si vous n'obtenez pas de licence pour votre logiciel, vous ne pouvez plus utiliser vShield. Vous ne pourrez plus par exemple mettre sous tension les dispositifs virtuels vShield App ou vShield Edge ni protéger vos machines virtuelles.

Pour continuer à bénéficier des fonctionnalités de vShield App et vShield Edge sans interruptions ou pour restaurer les fonctionnalités devenues indisponibles après l'évaluation de 60 jours, vous devez obtenir et installer des fichiers de licence pour activer les fonctions appropriées du composant vShield que vous avez acheté.

Installer les licences des composants vShield

Vous devez installer une licence CIS ou vCloud Networking and Security (vCNS) avant d'installer vShield App et vShield Edge. La licence vSphere inclut une licence pour vShield Endpoint. Vous pouvez installer ces licences après l'achèvement de l'installation de vShield Manager à l'aide de vSphere Client.

Procédure

1 À partir d'un hôte vSphere Client connecté à un système vCenter Server, sélectionnez **[Page d'accueil] > [Attribution de licence]** .

2 Dans l'onglet Gestion, sélectionnez **[Ressource]** .

3 Cliquez avec le bouton droit sur un actif CIS ou vCNS, puis sélectionnez **[Changer de clé de licence]** .

4 Sélectionnez **[Assign a new license key]** et cliquez sur **[Enter Key]** .

5 Entrez la clé de licence, entrez une étiquette facultative pour la clé, et cliquez sur **[OK]** .

6 Cliquez sur **[OK]** .

7 Répétez ces opérations pour chaque licence de composant vShield dont vous disposez.

Installer vShield App

Vous pouvez installer vShield App sur un hôte ESX.

Remarque La connexion réseau d'une machine virtuelle est interrompue lorsque vous la protégez avec vShield App. Si vCenter Server s'exécute sur une machine virtuelle et se déconnecte du réseau, le processus d'installation vShield App peut s'interrompre. VMware vous recommande de placer vCenter Server, la base de données de vCenter Server ainsi que les machines virtuelles de tiers ou les machines virtuelles de service internes que vous ne souhaitez pas protéger dans la liste d'exclusion de machines virtuelles. Pour plus d'informations sur l'exclusion de machines virtuelles de la protection de vShield App, voir le *Guide d'administration de vShield*.

Important Si les machines virtuelles de vCenter Server ou de la base de données vCenter Server se trouvent sur l'hôte ESX sur lequel vous installez vShield App, migrez-les vers un autre hôte avant d'installer vShield App.

Prérequis

- Vérifiez que le port de gestion (MGT) de chaque dispositif virtuel vShield App dispose d'une adresse IP unique. Chaque adresse IP doit être accessible depuis vShield Manager et se trouver sur le réseau de gestion utilisé pour les interfaces de gestion de vCenter et d'hôte ESX. L'utilisation d'une adresse IP incorrecte nécessite que vous désinstalliez et réinstalliez vShield App sur cet hôte.
- Stockage local ou réseau pour y placer la vShield App.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez un hôte ESX dans l'arborescence d'inventaire.

3 Cliquez sur l'onglet **[vShield]** .

4 Acceptez le certificat de sécurité.

5 Cliquez sur **[Install]** pour le service **[vShield App]** .

6 Sous vShield App, entrez les informations suivantes.

Option	Description
[Banque de données]	Sélectionnez la banque de données où vous souhaitez enregistrer les fichiers de la machine virtuelle vShield App.
[Management Port Group]	Sélectionnez le groupe de ports pour héberger l'interface de gestion de vShield App. Ce groupe de ports doit pouvoir atteindre le groupe de ports de vShield Manager.
[IP Address]	Tapez l'adresse IP à attribuer à l'interface de gestion de vShield App. IMPORTANT Veillez à taper l'adresse IP exacte. Pour modifier l'adresse IP après l'installation de vShield App, vous devez désinstaller vShield App et redémarrer l'hôte ESX.
[Netmask]	Tapez le masque de sous-réseau IP associé à l'adresse IP attribuée.
[Default Gateway]	Tapez l'adresse IP de la passerelle réseau par défaut.

7 Cliquez sur **[Installer]** .

Vous pouvez suivre l'avancement de l'installation de vShield App dans le volet des tâches récentes de l'écran vSphere Client.

Suivant

Autorisez vShield App à s'exécuter pendant le fonctionnement normal, puis examinez le trafic entrant et sortant de votre réseau virtuel. Configurez les règles de pare-feu en fonction des informations ainsi obtenues. Chaque instance de vShield App hérite des règles globales de pare-feu définies dans vShield Manager. Le jeu de règles de pare-feu par défaut autorise le passage de tout le trafic. Vous devez configurer des règles de blocage pour interdire explicitement du trafic. Pour configurer des règles d'App Firewall, consultez le *Guide d'administration vShield*.

REMARQUE Si vous avez installé vShield App sur un serveur ESX sans état, vous devez effectuer les étapes suivantes dans « Installer vShield App sur un hôte ESX sans état », page 27 avant de redémarrer l'hôte.

AVERTISSEMENT Ne modifiez pas les machines virtuelles de service via vSphere client. afin de ne pas interrompre la communication entre vShield Manager et vShield App et de ne pas compromettre la sécurité du réseau.

Installer vShield App sur un hôte ESX sans état

Si vous avez installé vShield App sur un hôte ESX sans état, vous devez exécuter les étapes ci-dessous avant de redémarrer les hôtes ESX sur lesquels vShield App est installé.

Prérequis

- Installez vShield App sur l'hôte ESX sans état.
- Vérifiez que les modifications apportées à la configuration de pare-feu sur l'hôte par le VIB sont complètes.
  a Dans vCenter Client, sélectionnez l'hôte ESX sans état dans le panneau d'inventaire.
  b Cliquez sur l'onglet **[Configuration]** .
  c Vérifiez qu'une entrée DVFilter figure dans les connexions entrantes sous le panneau Pare-feu. Si aucune entrée n'apparaît, cliquez sur **[Refresh.]**
- Créez un profil d'hôte. Pour plus d'informations, voir le *Guide d'installation et de configuration de vSphere*.

Procédure

1 Modifiez le profil d'hôte.

   a Dans vCenter Client, sélectionnez **[Accueil] > [Gestion] > [Profils d'hôte.]**

   b Sélectionnez le profil à modifier.

   c Cliquez sur **[Modifier le profil d'hôte]** .

   d Sélectionnez **[Configuration de la mise en réseau] > [Groupe de ports d'hôte] > [vmservice-vmknic-pg] > [Paramètres d'adresse IP] > [Mode de détermination de l'adresse IPv4]** .

   e Tapez l'adresse sous la forme **`169.254.1.1`** et le masque de sous-réseau sous la forme **`255.255.255.0`**.

   f Sélectionnez **[Configuration de la mise en réseau] > [Groupe de ports d'hôte] > [vmservice-vmknic-pg] > [Mode de définition de l'adresse MAC de vmknic]** .

   g Sélectionnez **[L'utilisateur doit choisir explicitement l'option de politique]** .

2 Enregistrez le profil d'hôte.

3 Dans un navigateur Web, tapez https://vsm-ip/bin/offline-bundles/VMware-vShield-fastpath-esx5x-5.0.1-766127.zip et télécharger le fichier zip.

4 Utilisez le profil d'hôte que vous avez créé dans Étape 1 et le bundle hors ligne que vous avez téléchargé dans Étape 3 pour mettre à jour la configuration ESX sans état.

Installation de vShield Edge

Vous pouvez ajouter plusieurs dispositifs virtuels vShield Edge à un centre de données. Chaque dispositif virtuel vShield Edge peut disposer de dix interfaces réseau internes et de liaison montante au total. Les interfaces internes se connectent à des groupes de ports sécurisés et font office de passerelle pour toutes les machines virtuelles protégées qui se trouvent dans le groupe de ports. Le sous-réseau attribué à l'interface interne peut être un espace privé défini par la RFC 1918. Les règles de pare-feu et les autres services vShield Edge sont appliqués au trafic entre les interfaces.

Les interfaces de liaison montante de vShield Edge se connectent aux groupes de ports de liaison montante qui ont accès à un réseau d'entreprise partagé ou à un service qui propose la mise en réseau avec couche d'accès.

Il est possible de configurer plusieurs adresses IP externes pour l'équilibreur de charge, le réseau privé virtuel (VPN) de site à site et les services de traduction des adresses réseau (NAT). Les adresses IP qui se chevauchent ne sont pas autorisées avec les interfaces internes. Par ailleurs, les sous-réseaux qui se chevauchent ne sont autorisés ni avec les interfaces internes, ni avec les interfaces de liaison montante.

Prérequis

Le rôle Enterprise Administrator ou vShield Administrator role doit vous avoir été attribué.

Procédure

1 Ouvrir l'assistant Ajouter Edge page 29

   Ouvrez l'assistant Ajouter Edge pour installer et configurer une instance vShield Edge.

2 Attribuer un nom à vShield Edge page 29

   vShield Edge exige un nom descriptif qui est unique dans toutes les machines virtuelles vShield Edge d'un même locataire. Ce nom apparaît dans l'inventaire vCenter.

3 Indiquer les informations d'identification de CLI page 30

   Modifier les informations d'identification à utiliser pour se connecter à l'interface de ligne de commande (CLI).

4 Ajouter des dispositifs page 30

Vous devez ajouter un dispositif avant de pouvoir déployer un vShield Edge. Si vous n'ajoutez pas de dispositif lors de l'installation de vShield Edge, vShield Edge reste en mode déconnecté jusqu'à ce que vous ajoutiez un dispositif.

5 Ajouter des interfaces internes et de liaison montante page 31

Vous pouvez ajouter jusqu'à dix interfaces internes et de liaison montante à une machine virtuelle vShield Edge.

6 Configurer la passerelle par défaut page 32

Indiquez l'adresse IP de la passerelle par défaut de vShield Edge.

7 Configurer la stratégie de pare-feu et la haute disponibilité page 32

Vous pouvez modifier la stratégie de pare-feu qui, par défaut, bloque tout le trafic entrant.

8 Confirmer les paramètres et installer vShield Edge page 33

Avant d'installer vShield Edge, vérifiez les paramètres que vous avez entrés.

Ouvrir l'assistant Ajouter Edge

Ouvrez l'assistant Ajouter Edge pour installer et configurer une instance vShield Edge.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez une ressource de centre de données dans l'arborescence de l'inventaire.

3 Cliquez sur l'onglet **[Virtualisation réseau]** .

4 Cliquez sur **[Edges]** .

5 Cliquez sur l'icône **[Ajouter]** ( ).

L'assistant Ajouter Edge apparaît.

Attribuer un nom à vShield Edge

vShield Edge exige un nom descriptif qui est unique dans toutes les machines virtuelles vShield Edge d'un même locataire. Ce nom apparaît dans l'inventaire vCenter.

Procédure

1 Tapez le nom de la machine virtuelvShield Edge.

Ce nom apparaît dans l'inventaire vCenter. Ce nom doit être unique au sein des Edge d'un même locataire.

Si vous n'indiquez pas de nom, vShield Manager crée un nom unique pour chaque vShield Edge.

2 (Facultatif) Tapez un nom d'hôte pour la machine virtuelvShield Edge.

Ce nom apparaît dans l'interface de ligne de commande CLI. Si vous n'indiquez pas de nom d'hôte, le nom que avez indiqué au cours le l'étape 1 apparaît également dans CLI.

3 (Facultatif) Tapez une description pour ce vShield Edge.

4 (Facultatif) Entrez le locataire de ce vShield Edge.

5 (Facultatif) Sélectionnez **[Activer HA]** pour activer la haute disponibilité (HA).

6 Cliquez sur **[Suivant]** .

Indiquer les informations d'identification de CLI

Modifier les informations d'identification à utiliser pour se connecter à l'interface de ligne de commande (CLI).

Procédure

1 Sur la page des informations d'identification CLI, spécifiez les informations d'identification CLI de votre machine virtuelle vShield Edge.

Option	Action
Nom d'utilisateur CLI	Modifiez-le si nécessaire.
Mot de passe CLI	Modifiez-le si nécessaire.

2 (Facultatif) Cliquez sur **[Activer l'accès SSH]** si nécessaire.

3 Cliquez sur **[Next]** .

La page Dispositifs Edge apparaît.

Ajouter des dispositifs

Vous devez ajouter un dispositif avant de pouvoir déployer un vShield Edge. Si vous n'ajoutez pas de dispositif lors de l'installation de vShield Edge, vShield Edge reste en mode déconnecté jusqu'à ce que vous ajoutiez un dispositif.

Prérequis

Pour garantir la haute disponibilité, vérifiez que le pool de ressources dispose d'une capacité suffisante pour que les deux machines virtuelles HA puissent être déployées. Une machine virtuelvShield Edge compact nécessite 256 Mo de mémoire, une machine virtuelle de grand vShield Edge 1 Go de mémoire et une machine virtuelvShield Edge XL 8 Go de mémoire. La banque de données doit disposer d'au moins 512 Mo d'espace disque.

Procédure

1 Sur la page Dispositifs Edge, sélectionnez la taille de l'instance vShield Edge en fonction de vos ressources système.

Le **[Grand]** vShield Edge dispose de plus de CPU, de mémoire et d'espace disque que vShield Edge **[Compact]** et prend en charge un nombre plus important d'utilisateurs VPN-Plus SSL simultanés. vShield Edge **[XL]** est adapté aux environnements dont l'équilibreur de charge comporte des millions de sessions simultanées. vShield Edge XL ne prend pas en charge VPN SSL.

2 Cliquez sur **[Activer la génération automatique de règles]** pour ajouter un pare-feu, une NAT et des itinéraires de routage pour permettre au trafic de contrôle de ces services de passer.

Si vous ne sélectionnez pas **[Activer la génération automatique de règles]** , vous devrez créer manuellement des règles de pare-feu pour ajouter un pare-feu, une NAT et des itinéraires de routage afin d'autoriser le trafic du canal de contrôle pour les services vShield Edge tels que l'équilibrage de charge, VPN, etc.

Remarque La génération automatique de règles ne crée pas de règles pour le trafic du canal de données.

3 Cliquez sur **[Activer AES-NI]** afin d'activer Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI).

4 Dans **[Dispositifs Edge]** , cliquez sur l'icône **[Ajouter]** ( ) pour ajouter un dispositif.

Si vous avez sélectionné **[Activer HA]** sur la page Nom et description, vous pouvez ajouter deux dispositifs. Si vous ajoutez un dispositif unique, vShield Edge réplique sa configuration pour le dispositif en veille et s'assure que les deux machines virtuelles vShield Edge HA ne se trouvent pas sur le même hôte ESX, même après avoir utilisé DRS et vMotion (sauf si vous les déplacez manuellement sur le même hôte).

5 Dans la boîte de dialogue Ajouter un dispositif Edge, sélectionnez le cluster ou le pool de ressources et la banque de données du dispositif.

6 (Facultatif) Sélectionnez l'hôte sur lequel le dispositif doit être ajouté.

7 (Facultatif) Sélectionnez le dossier vCenter dans lequel le dispositif doit être ajouté.

8 Cliquez sur **[Add]** .

9 Cliquez sur **[Suivant]** .

La page Interfaces apparaît.

Ajouter des interfaces internes et de liaison montante

Vous pouvez ajouter jusqu'à dix interfaces internes et de liaison montante à une machine virtuelle vShield Edge.

Procédure

1 Sur la page Interfaces, cliquez sur l'icône **[Ajouter]** ( ) et tapez le nom de l'interface.

2 Sélectionnez **[Interne]** ou **[Liaison montante]** pour indiquer s'il s'agit d'une interface interne ou externe.

Pour que HA fonctionne, vous devez ajouter au moins une interface interne.

3 Sélectionnez le groupe de ports ou le câble virtuel VXLAN auquel cette interface doit être connectée.

a Cliquez sur **[Sélectionner]** en regard du champ **[Connectée à]** .

b Selon ce que vous voulez connecter à l'interface, cliquez sur l'onglet **[Câble virtuel]** , **[Groupe de ports standard]** ou **[Groupe de ports distribué]** .

c Sélectionnez le câble virtuel ou le groupe de ports approprié.

d Cliquez sur **[Sélectionner]** .

4 Sélectionnez l'état de connectivité de l'interface.

5 Dans **[Configurer les sous-réseaux]** , cliquez sur l'icône **[Ajouter]** ( ) pour ajouter un sous-réseau pour l'interface.

Une interface peut avoir plusieurs sous-réseaux qui ne se chevauchent pas.

6 Dans **[Ajouter un sous-réseau]** , cliquez sur l'icône **[Ajouter]** ( ) pour ajouter une adresse IP.

Si vous entrez plusieurs adresses IP, vous pouvez sélectionner l'adresse IP principale. Une interface peut avoir une adresse IP principale et plusieurs adresses IP secondaires. vShield Edge considère l'adresse IP principale comme étant l'adresse source du trafic généré localement.

Vous devez ajouter une adresse IP à une interface avant de l'utiliser sur une configuration des fonctionnalités.

7 Tapez le masque de sous-réseau de l'interface, puis cliquez sur **[Enregistrer]** .

8 (Facultatif) Tapez l'adresse MAC de l'interface. Si HA est activée, saisissez deux adresses IP de gestion au format CIDR.

Les pulsations des deux machines virtuelles HA vShield Edge sont communiquées via ces adresses IP de gestion. Les adresses IP de gestion doivent se trouver dans le même sous-réseau L2 et doivent pouvoir communiquer entre elles.

9 Modifiez le MTU par défaut si nécessaire.

10 Dans **[Options]** , sélectionnez les options requises.

Option	Description
Activer ARP de proxy	Prend en charge le transfert de réseaux se chevauchant entre différentes interfaces.
Envoyer ICMP Redirection	Achemine les informations de routage aux hôtes.

11 Tapez les paramètres de délimitation et cliquez sur **[Ajouter]** .

12 Répétez les étapes Étape 1 à l'aide de Étape 11 pour ajouter de nouvelles interfaces.

13 Cliquez sur **[Suivant]** .

La page Passerelle par défaut apparaît.

Configurer la passerelle par défaut

Indiquez l'adresse IP de la passerelle par défaut de vShield Edge.

Procédure

1 Sur la page Passerelle par défaut, sélectionnez **[Configurer la passerelle par défaut]** .

2 Sélectionnez l'interface qui peut communiquer avec le tronçon suivant ou l'adresse IP de la passerelle.

3 Tapez l'adresse IP de la passerelle par défaut.

4 Dans **[MTU]** , le MTU par défaut de l'interface que vous avez sélectionnée au cours de l'Étape 2 s'affiche. Vous pouvez modifier cette valeur, mais elle ne peut pas être supérieure au MTU configuré sur l'interface.

5 Cliquez sur **[Suivant]** .

La page Pare-feu et HA apparaît.

Configurer la stratégie de pare-feu et la haute disponibilité

Vous pouvez modifier la stratégie de pare-feu qui, par défaut, bloque tout le trafic entrant.

Vous devez configurer les paramètres HA pour que la haute disponibilité fonctionne sur les configurations réseau sur vShield Edge. vShield Edge prend en charge deux machines virtuelles avec haute disponibilité, toutes deux étant actualisées avec les configurations utilisateur. En cas d'échec des pulsations sur la machine virtuelle principale, l'état de la machine virtuelle secondaire devient actif. Ainsi, une machine virtuelle vShield Edge est en permanence active sur le réseau.

Procédure

1 Sur la page Pare-feu et HA, sélectionnez **[Configurer la stratégie de pare-feu par défaut]** .

2 Indiquez si vous acceptez ou refusez le trafic entrant par défaut.

Les règles de pare-feu que vous créez remplacent la stratégie par défaut.

3 Indiquez s'il faut consigner dans un journal le trafic entrant.

Si vous créez des règles de pare-feu qui remplacent qui remplacent la stratégie par défaut, ces règles déterminent la journalisation. L'activation de la journalisation par défaut peut générer un volume trop important de journaux, ce qui a une incidence sur les performances de vShield Edge. C'est pourquoi il est recommandé d'activer la journalisation par défaut uniquement lors de la résolution de problèmes ou d'un débogage.

4 Si vous avez sélectionné **[Activer HA]** sur la page Nom et description, complétez la section **[Configurer les paramètres HA]** .

vShield Edge réplique la configuration du dispositif principal pour le dispositif en standby et veille à ce que deux machines virtuelles vShield Edge HA ne se trouvent pas sur le même hôte ESX, même après avoir utilisé DRS et vMotion. Deux machines virtuelles sont déployées sur vCenter dans le même pool de ressources et la même banque de données que le dispositif que vous avez configuré. Des IP de liens locaux sont affectés aux machines virtuelles HA dans vShield Edge HA afin qu'elles soient en mesure de communiquer ensemble. Vous pouvez indiquer des adresses IP de gestion pour remplacer les liens locaux.

a Sélectionnez l'interface interne dont les paramètres HA doivent être configurés.

b (Facultatif) Tapez la période, exprimée en secondes, au cours de laquelle si le dispositif de sauvegarde ne reçoit pas de signal de pulsation du dispositif principal, ce dernier est considéré comme étant inactif et le dispositif de sauvegarde prend le relais.

L'intervalle par défaut est de 6 secondes.

c (Facultatif) Tapez deux adresses IP de gestion au format CIDR pour remplacer les IP des liens locaux attribués aux machines virtuelles HA.

Vérifiez que les adresses IP de gestion ne se chevauchent pas avec l'un des sous-réseaux de l'interface.

5 Cliquez sur **[Suivant]** .

La page Résumé apparaît.

Confirmer les paramètres et installer vShieldEdge

Avant d'installer vShield Edge, vérifiez les paramètres que vous avez entrés.

Procédure

1 Sur la page Résumé, vérifiez les paramètres de vShield Edge.

2 Cliquez sur **[Précédent]** pour modifier les paramètres

3 Cliquez sur **[Terminer]** pour accepter les paramètres et installer vShield Edge.

Installation de vShield Endpoint

Les instructions d'installation qui suivent supposent que vous disposez du système suivant :

- un centre de données avec les versions prises en charge de vCenter Server et ESXi installées sur chaque hôte du cluster. Pour plus d'informations sur les versions requises, consulter Chapitre 2, « Préparation à l'installation », page 13.
- vShield Manager 5,1 installé et en fonctionnement.
- Un serveur de gestion de solution antivirus installé et en fonctionnement.

Flux de travail d'installation de vShield Endpoint

Une fois la préparation de l'hôte ESX pour l'installation de vShield Endpoint terminée, installez vShield Endpoint en suivant les étapes suivantes :

1 Déployez et configurez une machine virtuelle de sécurité (SVM) sur chaque hôte ESX selon les instructions du fournisseur de la solution antivirus.

2 Installez VMware Tools 8.6.0 publié avec ESXi 5.0 - Correctif 1 sur toutes les machines virtuelles à protéger.

Le composant hôte vShield Endpoint ajoute deux règles de pare-feu à l'hôte ESX :

- la règle vShield-Endpoint-Mux ouvre les ports 48651 à 48666 pour la communication entre le composant hôte et les VM de sécurité partenaire.
- La règle vShield-Endpoint-Mux-Partners peut être utilisée par des partenaires pour installer un composant hôte. Elle est désactivée par défaut.

Installer VMware Tools sur les machines virtuelles invitées

VMware Tools contient vShield Thin Agent qui doit être installé sur chaque machine virtuelle invitée à protéger. Les machines virtuelles sur lesquelles VMware Tools est installé sont protégées automatiquement à chaque démarrage sur un hôte ESX sur lequel la solution de sécurité est installée. Les machines virtuelles protégées conservent donc la protection de la sécurité lors des arrêts et redémarrages, et même après un déplacement par vMotion sur un autre hôte ESX sur lequel la solution de sécurité est installée.

Prérequis

Assurez-vous que la machine virtuelle cliente dispose d'une version prise en charge de Windows installée. vShield Endpoint 5.0 est compatible avec les systèmes d'exploitation Windows suivants :

- Windows Vista (32 bits)
- Windows 7 (32/64 bits)
- Windows XP (32 bits)
- Windows 2003 (32/64 bits)
- Windows 2003 R2 (32/64 bits)
- Windows 2008 (32/64 bits)
- Windows 2008 R2 (64 bits)

Procédure

1 Sélectionnez le type d'installation pour VMware Tools.

Version ESX de l'hôte	Action
ESX 5.0 - Correctif 1	Suivez les instructions d'installation dans *Installation et configuration de VMware Tools* jusqu'à ce que l'assistant de type d'installation s'affiche.
ESX 4.1 - Correctif 3 ou suivant	Suivez les instructions d'installation dans l'article http://kb.vmware.com/kb/2008084 de la base de connaissances jusqu'à ce que l'assistant de type d'installation s'affiche.

2 Dans l'assistant, sélectionnez l'une des options suivantes :

- Complète.
- Personnalisée.
  - Dans la liste des pilotes de périphérique VMware, sélectionnez le pilote VMCI, puis le pilote vShield.

Installer vShield Data Security

Vous ne pouvez installer vShield Data Security qu'après avoir installé vShield Endpoint.

Prérequis

Vérifiez que vShield Endpoint a bien été installé sur les machines virtuelles hôtes et clientes..

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez un hôte ESX dans l'arborescence d'inventaire.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Install]** en regard de vShield Data Security.

5 Cochez la case **[vShield Data Security]** .

6 Sous vShield Data Security, entrez les informations suivantes.

Option	Description
[Datastore]	Sélectionnez la banque de données à laquelle vous voulez ajouter la machine virtuelle du service vShield Data Security.
[Management Port Group]	Sélectionnez le groupe de ports qui doit héberger l'interface de gestion de vShield Data Security. Ce groupe de ports doit pouvoir atteindre le groupe de ports de vShield Manager.

7 Pour définir une adresse IP statique, cochez la case **[Configure static IP for management interface]** .

Saisissez l' **[IP address]** , le **[Netmask]** , et la **[Default Gateway]** .

REMARQUE Si vous ne sélectionnez pas **[Configure static IP for management interface]** , une adresse IP est attribuée avec le Protocole DHCP (Dynamic Host Configuration Protocol).

8 Cliquez sur **[Install]** .

La machine virtuelle vShield Data Security est installée sur l'hôte sélectionné.

Désinstallation des composants vShield

5

Ce chapitre détaille les étapes nécessaires à la désinstallation des composants vShield de votre inventaire vCenter.

Ce chapitre aborde les rubriques suivantes :

- « Désinstaller un dispositif virtuel vShield App », page 37
- « Désinstaller une instance vShield Edge », page 38
- « Désinstaller une machine virtuelle vShield Data Security », page 38
- « Désinstaller un module vShield Endpoint », page 38

Désinstaller un dispositif virtuel vShield App

La désinstallation d'une vShield App supprime le dispositif virtuel du réseau et de vCenter Server.

AVERTISSEMENT La désinstallation d'une instance de vShield App place l'hôte ESX en mode de maintenance. L'hôte ESX redémarre pendant la désinstallation. Si une ou plusieurs des machines virtuelles actives sur l'hôte ESX cible ne peut pas être migrée vers un autre hôte ESX, ces machines virtuelles doivent être mises hors tension ou migrées manuellement avant de pouvoir poursuivre la désinstallation. Si vShield Manager se trouve sur le même hôte ESX, vShield Manager doit être migré avant la désinstallation de la vShield App.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez l'hôte ESX dans l'arborescence d'inventaire.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Uninstall]** pour le service **[vShield App]** .

Si vous désinstallez vShield App sur un hôte ESX sans état, ignorez les erreurs de désinstallation VIB.

5 Si l'hôte ESX était en mode de maintenance avant de démarrer la désinstallation de vShield App, retirez les machines virtuelles vShield App manuellement après la désinstallation automatique.

L'instance est désinstallée.

Désinstaller une instance vShield Edge

Vous pouvez désinstaller une instance vShield Edge à l'aide de vSphere Client.

Prérequis

Le rôle Enterprise Administrator ou vShield Administrator doit vous avoir été attribué.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez une ressource de centre de données dans l'arborescence de l'inventaire.

3 Cliquez sur l'onglet **[Virtualisation réseau]** .

4 Cliquez sur **[Edges]** .

5 Cliquez sur l'icône **[Delete]** ( ).

Désinstaller une machine virtuelle vShield Data Security

Après la désinstallation de la machine virtuelle vShield Data Security, vous devez désinstaller le dispositif virtuel en suivant les instructions du partenaire VMware.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez un hôte ESX dans l'arborescence d'inventaire.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Désinstaller]** pour le service vShield Data Security.

Désinstaller un module vShield Endpoint

La désinstallation d'un module vShield Endpoint supprime un module vShield Endpoint d'un hôte ESX. Vous devez exécuter ces étapes chronologiquement.

AVERTISSEMENT Si vShield Data Security est installé sur un hôte ESX, vous devez le désinstaller avant vShield Endpoint.

Désinstaller les produits qui utilisent vShield Endpoint

Avant de désinstaller un module vShield Endpoint sur un hôte, vous devez désinstaller de l'hôte tous les produits qui utilisent vShield Endpoint. Suivez les instructions du fournisseur de la solution.

Désinstaller le module vShield Endpoint depuis vSphere Client

La désinstallation d'un module vShield Endpoint supprime le module d'un hôte ESX.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez un hôte ESX dans l'arborescence d'inventaire.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Uninstall]** pour le service **[vShield Endpoint]** .

Mise à niveau de vShield 6

Pour mettre à niveau vShield, vous devez d'abord mettre à niveau vShield Manager, puis mettre à jour les autres composants pour lesquels vous disposez d'une licence.

Ce chapitre aborde les rubriques suivantes :

- « Mettre à niveau vShield Manager », page 39
- « Mettre à niveau vShield App », page 45
- « Mettre à niveau vShield Edge », page 45
- « Mettre à niveau vShield Endpoint », page 46
- « Mettre à niveau vShield Data Security », page 47

Mettre à niveau vShield Manager

Vous pouvez mettre à niveau vShield Manager vers une nouvelle version uniquement depuis l'interface utilisateur vShield Manager. Vous pouvez mettre à niveau vShield App et vShield Edge vers une nouvelle version depuis l'interface utilisateur vShield Manager ou en utilisant des API REST.

Prérequis

- Prenez un snapshot de vShield Manager de manière à pouvoir le rétablir en cas d'échec de la mise à niveau.
- Si vous utilisez vShield Endpoint 4.1, désinstallez-le avant de mettre à niveau vShield Manager.

AVERTISSEMENT Ne désinstallez pas une instance déployée du dispositif vShield Manager.

Mettre à niveau vShield Manager de la version 4.x à la version 5.1 ou ultérieure

Pour mettre à niveau vShield Manager 4.x vers la version 5.1 ou une version ultérieure, vous devez d'abord passer à la version 5.0, puis à la version 5.1.

1 Mettre à niveau vShield Manager vers la version 5.0 page 40

   Il s'agit de la première étape de la mise à niveau de vShield Manager de la version 4.x à la version 5.1 ou ultérieure.

2 Mettre à niveau vShield Manager de la version 5.0 à la version 5.1 ou ultérieure page 40

   vShield Manager version 5.1 (et versions ultérieures) nécessite au minimum 2,5 Go d'espace disque. Vous devez exécuter le bundle de maintenance pour créer suffisamment d'espace disque pour vShield Manager mis à niveau.

Mettre à niveau vShield Manager vers la version 5.0

Il s'agit de la première étape de la mise à niveau de vShield Manager de la version 4.x à la version 5.1 ou ultérieure.

Procédure

1 Téléchargez le bundle de mise à niveau vShield vers un emplacement que vShield Manager peut parcourir. Le nom du fichier de bundle de mise à niveau est de la forme `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

2 Dans le panneau d'inventaire vShield Manager, cliquez sur **[Settings & Reports]** .

3 Cliquez sur l'onglet **[Updates]** .

4 Cliquez sur **[Upload Settings]** .

5 Cliquez sur **[Browse]** et sélectionnez le fichier `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

6 Cliquez sur **[Open]** .

7 Cliquez sur **[Upload Upgrade Bundle]** .

8 Cliquez sur **[Installer]** pour commencer le processus de mise à niveau.

9 Cliquez sur **[Confirmer l'installation]** . Le processus de mise à niveau redémarre vShield Manager, vous pouvez donc de perdre la connectivité à l'interface utilisateur vShield Manager. Aucun des composants vShield n'est redémarré.

10 Après le redémarrage, connectez-vous à nouveau à vShield Manager et cliquez sur l'onglet Updates. Le volet Version installée affiche la version 5.0 que vous venez d'installer.

Suivant

Lors d'une mise à niveau à partir de vShield Manager 4.1, vous devez à nouveau enregistrer le serveur vCenter Server.

Vous pouvez désormais installer vShield Manager 5.1 ou une version ultérieure. Reportez-vous à « Mettre à niveau vShield Manager vers la version 5.0 », page 40.

Mettre à niveau vShield Manager de la version 5.0 à la version 5.1 ou ultérieure

vShield Manager version 5.1 (et versions ultérieures) nécessite au minimum 2,5 Go d'espace disque. Vous devez exécuter le bundle de maintenance pour créer suffisamment d'espace disque pour vShield Manager mis à niveau.

Reportez-vous à « Mettre à niveau vShield Manager de la version 5.0 à la version 5.1 ou ultérieure », page 40.

Mettre à niveau vShield Manager de la version 5.0 à la version 5.1 ou ultérieure

vShield Manager version 5.1 (et versions ultérieures) nécessite au minimum 2,5 Go d'espace disque. Vous devez exécuter le bundle de maintenance pour créer suffisamment d'espace disque pour vShield Manager mis à niveau.

Reportez-vous à « Mettre à niveau vShield Manager de la version 5.0 à la version 5.1 ou ultérieure », page 40.

Procédure

1 Appliquer le bundle de maintenance page 41

Il est nécessaire de disposer d'au minimum 2,5 Go d'espace disque libre dans la partition `/common` pour le processus de mise à niveau. Le bundle de maintenance de vShield crée de l'espace disque sur le vShield Manager. Celui-ci arrête le processus de vShield Manager et le relance après la fin de l'activité de nettoyage du système de fichiers.

2 Mettre à niveau vShield Manager vers la version 5.1 ou une version ultérieure page 42

3 Créer une sauvegarde post mise à niveau page 43

À partir de la version 5.1, vShield Manager nécessite une mise à niveau pour son matériel virtuel. Cette mise à niveau de matériel virtuel n'est pas effectuée automatiquement dans le cadre du processus de mise à niveau de vShield pour vShield Manager versions 5.0.x ou les versions antérieures. Les modifications architecturales pour les capacités améliorées d'évolutivité, de performance, ainsi que de journalisation et de génération de rapports requièrent la mise à niveau du matériel virtuel de vShield Manager. Certaines de ces modifications incluent la prise en charge 64 bits, 2 vCPU, 8 Go de mémoire vive, un disque virtuel d'une capacité supérieure, ainsi que d'autres propriétés de matériel virtuel.

4 Restaurer la sauvegarde post mise à niveau page 44

Restaurer la sauvegarde de vShield Manager.

Appliquer le bundle de maintenance

Il est nécessaire de disposer d'au minimum 2,5 Go d'espace disque libre dans la partition `/common` pour le processus de mise à niveau. Le bundle de maintenance de vShield crée de l'espace disque sur le vShield Manager. Celui-ci arrête le processus de vShield Manager et le relance après la fin de l'activité de nettoyage du système de fichiers.

Prérequis

Remarque Les journaux, les données de Flow Monitoring et les journaux d'audit et d'événements système existants sur le dispositif vShield Manager sont supprimés dans le cadre de cette procédure. Vous pouvez récupérer les journaux d'audit et d'événements système à l'aide de l'appel API REST approprié avant d'appliquer le bundle de maintenance. Le bundle de journaux du support technique contient les messages des journaux de cette procédure.

Procédure

1 Cliquez à droite sur la machine virtuelle vShield Manager et cliquez sur **[Open Console]** pour ouvrir l'interface de ligne de commande (CLI) de vShield Manager.

2 Passez au mode Activer.

3 Une fois connecté, tapez la commande `show filesystems`.

Vous devez disposer d'au moins 5 % d'espace disque disponible dans la partition `/common` pour installer le bundle de maintenance.

4 Tapez la commande `show manager log follow` . Gardez cette console ouverte pendant que vous suivez les autres étapes.

5 Téléchargez le bundle de maintenance vShield dans un emplacement auquel vShield Manager peut accéder. Le nom du fichier de bundle de maintenance est de la forme `VMware-vShield-Manager-upgrade-bundle-maintenance-`*bundlebuildNumber*`.tar.gz`.

6 Dans le panneau d'inventaire vShield Manager, cliquez sur **[Settings & Reports]** .

7 Cliquez sur l'onglet **[Updates]** .

8 Cliquez sur **[Upload Settings]** .

9 Cliquez sur **[Browse]** et sélectionnez le fichier `VMware-vShield-Manager-upgrade-bundle-maintenance-`*bundlebuildNumber*`.tar.gz`.

10 Cliquez sur **[Open]** .

11 Cliquez sur **[Upload File]** .

12 Cliquez sur **[Installer]** pour commencer le processus de mise à niveau.

13 Cliquez sur **[Confirmer l'installation]** .

14 Dans la CLI, suivez le résultat de la commande `show manager log`. Une fois que le message `maintenance-fs-cleanup: Filesystem cleanup successful` s'est affiché, connectez-vous à l'interface utilisateur de vShield Manager.

Le processus de mise à niveau redémarre le service vShield Manager ; ainsi vous risquez de perdre la connectivité avec l'interface utilisateur de vShield Manager. Aucun des autres composants vShield n'est redémarré.

15 Connectez-vous à la CLI de vShield Manager, passez en mode Activer et exécutez la commande `show filesystems` afin de vérifier que vous disposez d'au moins 2,5 Go d'espace disque disponible pour la mise à niveau.

Mettre à niveau vShield Manager vers la version 5.1 ou une version ultérieure

Procédure

1 Téléchargez le bundle de mise à niveau vShield vers un emplacement que vShield Manager peut parcourir. Le nom du fichier de bundle de mise à niveau est de la forme `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

2 Dans le panneau d'inventaire vShield Manager, cliquez sur **[Settings & Reports]** .

3 Cliquez sur l'onglet **[Updates]** .

4 Cliquez sur **[Upload Settings]** .

5 Cliquez sur **[Browse]** et sélectionnez le fichier `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

6 Cliquez sur **[Open]** .

7 Cliquez sur **[Upload Upgrade Bundle]** .

8 Cliquez sur **[Installer]** pour commencer le processus de mise à niveau.

9 Cliquez sur **[Confirmer l'installation]** . Le processus de mise à niveau redémarre vShield Manager, vous pouvez donc de perdre la connectivité à l'interface utilisateur vShield Manager. Aucun des composants vShield n'est redémarré.

10 Après le redémarrage, connectez-vous à nouveau à vShield Manager et cliquez sur l'onglet Updates. Le volet Version installée affiche la version 5.1.1 que vous venez d'installer.

Les règles de vShield App de la version antérieure sont mises à niveau comme décrit ci-dessous.

Fonction de pare-feu dans la version antérieure	Résultat de la mise à niveau vers la version 5.1
Règles de pare-feu autorisées aux niveaux du centre de données, du cluster et du groupe de ports	Règles de pare-feu autorisées au niveau de l'espace de noms : niveaux du centre de données, du groupe de ports avec un espace de noms indépendant et du câble virtuel Après la mise à niveau, les règles de pare-feu des contextes autres que de l'espace de noms sont déplacées vers le centre de données correspondant. Les règles migrées sont fusionnées avec les règles du centre de données dans l'ordre suivant : ■ centre de données haut ■ cluster ■ Groupe de ports ou groupe dvport autre que de l'espace de noms ■ centre de données bas ■ centre de données par défaut
Les règles de pare-feu prenaient en charge les adresses IP et MAC brutes ainsi que le protocole de ports et le sous-type de protocole	Les règles de pare-feu prenaient en charge uniquement les IPsets, les MACsets et les groupes de sécurité Après la mise à niveau, l'IPset, le MACset ou le service est créé en interne, le cas échéant. Les noms des conteneurs créés suivent ces conventions de dénomination : ■ IPset / MACset : *ip/macValue-contextName* ■ Service : *protocolName-portNumber-contextName* ou *protocolName-subtypeName-contextName*
Les règles de pare-feu incluaient les règles de haute et de basse priorité. Les règles de groupe de ports autre que de l'espace de noms n'avaient aucune priorité.	Règles de haute et de basse priorité non prises en charge. Après la mise à niveau, toutes les règles de priorité autres que par défaut sont changées à aucune priorité.
Un seul paramètre général Spoofguard a été appliqué dans tous les centres de données de l'inventaire	Les paramètres généraux Spoofguard sont appliqués à chaque espace de noms. Vous pouvez modifier les paramètres Spoofguard sur la base de l'espace ce noms après la mise à niveau.

En outre, tous les historiques et les flux de pare-feu avant la mise à niveau sont supprimés.

Suivant

Effacez le cache du navigateur sur tous les clients qui ont accédé à la version précédente du produit. Cette action efface les fichiers javascript ou les autres fichiers mis en cache de cette version qui ont pu changer dans la version en cours.

Créer une sauvegarde post mise à niveau

À partir de la version 5.1, vShield Manager nécessite une mise à niveau pour son matériel virtuel. Cette mise à niveau de matériel virtuel n'est pas effectuée automatiquement dans le cadre du processus de mise à niveau de vShield pour vShield Manager versions 5.0.x ou les versions antérieures. Les modifications architecturales pour les capacités améliorées d'évolutivité, de performance, ainsi que de journalisation et de génération de rapports requièrent la mise à niveau du matériel virtuel de vShield Manager. Certaines de ces modifications incluent la prise en charge 64 bits, 2 vCPU, 8 Go de mémoire vive, un disque virtuel d'une capacité supérieure, ainsi que d'autres propriétés de matériel virtuel.

Procédure

1 Dans le panneau d'inventaire vShield Manager, cliquez sur **[Settings & Reports]** .

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Backups]** .

4 Tapez l'adresse IP de l'hôte ou le nom du système sur lequel la sauvegarde doit être enregistrée.

5 Tapez le nom d'utilisateur et le mot de passe requis pour se connecter au système de sauvegarde (serveur ftp/sftp).

6 Dans le champ **[Backup Directory]** , tapez le chemin absolu d'enregistrement des sauvegardes.

7 Tapez une chaîne de texte dans **[Filename Prefix]** . Ce texte sera ajouté devant chaque nom de fichier de la sauvegarde pour faciliter la reconnaissance sur le système de sauvegarde. Si vous tapez par exemple `ppdb`, la sauvegarde résultante sera nommée `ppdb`*HH_MM_SS_DayDDMonYYYY*.

8 Dans le menu déroulant **[Transfer Protocol]** , sélectionnez SFTP ou FTP, selon ce que la destination prend en charge.

9 Cliquez sur **[Save Settings]** , puis cliquez sur **[Backup]** .

10 Cliquez sur **[View Backups]** pour vérifier que la sauvegarde a bien été créée.

Restaurer la sauvegarde post mise à niveau

Restaurer la sauvegarde de vShield Manager.

Procédure

1 Mettez hors tension le vShield Manager.

2 Téléchargez le package d'installation .OVA de vShield Manager 5.1.x.

3 Déployez un nouveau vShield Manager dans votre inventaire vSphere afin de remplacer le vShield Manager existant.

4 Mettez sous tension le nouveau vShield Manager et accédez à la configuration initiale, en lui donnant la même adresse IP que celui actuellement hors tension.

5 Configurez la page vShield Manager Backups (Sauvegardes vShield Manager) pour afficher les sauvegardes actuellement stockées sur le serveur ftp/sftp.

6 Identifiez la sauvegarde vShield Manager créée précédemment et cliquez sur **[Restore]** .

Mettre à niveau vShield Manager de la version 5.1 à une version ultérieure

Procédure

1 Téléchargez le bundle de mise à niveau vShield vers un emplacement que vShield Manager peut parcourir. Le nom du fichier de bundle de mise à niveau est de la forme `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

2 Dans le panneau d'inventaire vShield Manager, cliquez sur **[Settings & Reports]** .

3 Cliquez sur l'onglet **[Updates]** .

4 Cliquez sur **[Upload Settings]** .

5 Cliquez sur **[Browse]** et sélectionnez le fichier `VMware-vShield-Manager-upgrade_bundle-`*buildNumber*`.tar.gz`.

6 Cliquez sur **[Open]** .

7 Cliquez sur **[Upload Upgrade Bundle]** .

8 Cliquez sur **[Installer]** pour commencer le processus de mise à niveau.

9 Cliquez sur **[Confirmer l'installation]** . Le processus de mise à niveau redémarre vShield Manager, vous pouvez donc de perdre la connectivité à l'interface utilisateur vShield Manager. Aucun des composants vShield n'est redémarré.

10 Après le redémarrage, connectez-vous à nouveau à vShield Manager et cliquez sur l'onglet Updates. Le volet Version installée affiche la version 5.1.1 que vous venez d'installer.

Mettre à niveau vShield App

Mettez à niveau vShield App sur chaque hôte dans le centre de données.

Prérequis

Si vous utilisez vShield App version 4.1, vous devez mettre à niveau vers la version 5.0 ou 5.0.1 avant de mettre à niveau vers la version 5.1.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez **[Inventory] > [Hosts and Clusters]** .

3 Sélectionnez l'hôte sur lequel vous voulez mettre à niveau vShield App.

4 Cliquez sur l'onglet **[vShield]** .

L'onglet **[General]** affiche chaque composant vShield installé sur l'hôte sélectionné et la version disponible.

5 Sélectionnez **[Mettre à jour]** à côté de vShield App.

6 Cochez la case **[vShield App]** .

7 Cliquez sur **[Installer]** .

Suivant

Inspectez chaque règle mise à niveau afin de vous assurer qu'elle fonctionne comme prévu. Pour plus d'informations sur l'ajout de nouvelles règles de pare-feu, reportez-vous au **[Guide d'administration vShield]** .

Mettre à niveau vShield Edge

Vous devez mettre à niveau vShield Edge dans chaque groupe de ports dans votre centre de données. Vous ne pouvez pas mettre à niveau vShield Edge si la même adresse IP de serveur a été configurée sous différents ports d'écoute avec différents ports.

vShield Edge 5.1 n'a pas de compatibilité descendante et vous ne pouvez pas utiliser les appels REST 2.0 après la mise à niveau.

Prérequis

Le rôle Enterprise Administrator ou vShield Administrator doit vous avoir été attribué.

Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez **[Views] > [Inventory] > [Networking]** .

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur **[Mettre à niveau]** .

5 Affichez vShield Edge mis à niveau.

a Sélectionnez le centre de données correspondant au groupe de ports sur lequel vous avez mis à niveau vShield Edge.

b Cliquez sur l'onglet **[Virtualisation réseau]** .

c Cliquez sur **[Edges]** .

vShield Edge est mis à niveau vers la taille compacte. Un événement système est généré pour indiquer l'ID de chaque instance vShield Edge mise à niveau.

Suivant

IMPORTANT Les règles de pare-feu de la version antérieure sont mises à niveau avec certaines modifications. Inspectez chaque règle mise à niveau afin de vous assurer qu'elle fonctionne comme prévu. Pour plus d'informations sur l'ajout de nouvelles règles de pare-feu, reportez-vous au *Guide d'administration vShield*.

Si la portée d'un utilisateur dans une version antérieure était limitée à un groupe de ports qui avait un vShield Edge installé, l'utilisateur obtient automatiquement un accès à ce vShield Edge après la mise à niveau.

Mettre à niveau vShield Endpoint

La procédure de mise à niveau à exécuter dépend de la version du produit que vous utilisez.

Mettre à niveau vShield Endpoint de la version 4.1 vers la version 5.0

Pour mettre à niveau vShield Endpoint de la version 4.1 vers la version 5.0, vous devez tout d'abord désinstaller vShield Endpoint sur chaque hôte du centre de données, mettre à niveau vShield Manager, puis installer la nouvelle version.

1. Si les machines virtuelles protégées fonctionnent dans un cluster, désactivez DRS.
2. Désactivez tous les DSVA de tendance. Ceci est nécessaire pour pouvoir supprimer les entrées de filtre VFILE associées à vShield des machines virtuelles.
3. Si vous avez désactivé DRS au cours de l'étape 1, réactivez-le.
4. Désinstallez vShield Endpoint sur chaque hôte dans le centre de données. Pour plus d'informations, voir « Désinstaller le module vShield Endpoint depuis vSphere Client », page 38.
5. Mettez à niveau VMware vCenter vers la version requise. Pour plus d'informations, voir Chapitre 2, « Préparation à l'installation », page 13.
6. Mettez à niveau chaque hôte vers la version VMware ESX requise. Pour plus d'informations, voir Chapitre 2, « Préparation à l'installation », page 13.
7. Mettez à niveau vShield Manager. Pour plus d'informations, voir « Mettre à niveau vShield Manager », page 39.
8. Installez vShield Endpoint. Pour plus d'informations, voir « Installation de vShield Endpoint », page 33.

Mettre à niveau vShield Endpoint de la version 5.0 vers une version suivante

Pour mettre à niveau vShield Endpoint de la version 5.0 vers une version suivante, vous devez mettre à niveau mise à niveau vShield Manager, puis mettre à jour vShield Endpoint sur chaque hôte du centre de données.

Procédure

1. Connectez-vous à vSphere Client.
2. Sélectionnez **[Inventory] > [Hosts and Clusters]** .
3. Sélectionnez l'hôte sur lequel vous voulez mettre à niveau vShield Endpoint.
4. Cliquez sur l'onglet **[vShield]** .

   L'onglet **[General]** affiche chaque composant vShield installé sur l'hôte sélectionné et la version disponible.
5. Sélectionnez **[Update]** à côté de vShield Endpoint.

6 Cochez la case **[vShield Endpoint]** .

7 Cliquez sur **[Installer]** .

Mettre à niveau vShield Data Security

Mettez à niveau vShield Data Security sur chaque hôte dans le centre de données. Il est recommandé de mettre à niveau vShield Endpoint avant vShield Data Security.

Procédure

1 Connectez-vous à vSphere Client.

2 Allez dans **[Inventaire]** > **[Hôtes et clusters]** .

3 Sélectionnez l'hôte sur lequel vous voulez mettre à niveau vShield App.

L'onglet **[Résumé]** affiche chaque composant vShield installé sur l'hôte sélectionné et la version disponible.

4 Sélectionnez **[Mettre à jour]** à côté de vShield Data Security.

5 Cochez la case **[vShield Data Security]** .

6 Cliquez sur **[Installer]** .

Résolution des problèmes d'installation 7

Cette section décrit les problèmes d'installation.

Ce chapitre aborde les rubriques suivantes :

- « L'installation de vShield App échoue », page 49
- « Échec d'installation de vShield Data Security », page 50

L'installation de vShield App échoue

Installation de vShield App échoue.

Problème

L'installation de vShield App peut échouer du fait d'une installation antérieure incomplète ou de problèmes qui surviennent lors de la désinstallation d'une version antérieure.

Solution

1 Commencez par une désinstallation automatisée de vShield App. Reportez-vous à Chapitre 5, « Désinstallation des composants vShield », page 37.

2 Vérifiez que les modules requis sont chargés dans l'hôte ESX en vous connectant à un client SSH et en tapant la commande suivante :

```
esx01# esxcfg-module -l | grep -i dvf

dvfilter 2 72

vmkapiv1_0_0_0_dvfilter_shim0 8
```

3 Si les modules requis ne sont pas chargés, tapez les commandes suivantes afin de les charger.

```
#esxcfg-module -e /usr/lib/vmware/vmkmod/dvfilter

#esxcfg-module -v -e /usr/lib/vmware/vmkmod/vmkapiv1_0_0_0_dvfilter_shim
```

4 Connectez-vous à la ligne de commande CLI de vShield Manager en tant que qu'administrateur et réinitialisez l'interface Web en tapant la commande suivante :

enable > config t > **`no web-manager`**

5 Après avoir exécuté la commande **`no web-manager`**, redémarrez les services Web en tapant la commande suivante :

enable > config t > **`web-manager`**

Si vous étiez connecté à l'interface utilisateur de vShield Manager, reconnectez-vous après le redémarrage des services Web.

6 (Facultatif) Redémarrez l'hôte ESX si l'erreur suivante s'est produite lors de l'installation de vShield App :

`vShield App installation encountered error while installing vib`

7 Supprimer le vswitch vmservice qui a été créé lors de l'installation en suivant les étapes ci-dessous.

a Connectez-vous à vSphere Client.

b Sélectionnez l'hôte ESX dans l'arborescence d'inventaire.

c Cliquez sur l'onglet **[Configuration]** .

d Dans le volet Logiciels, cliquez sur **[Mise en réseau]** .

e Dans la zone **[Commutateur standard : vmservice-vswitch]** , cliquez sur **[Delete]** .

8 Supprimez la propriété **[Net.DVFilterBindIpAddress]** de l'hôte en suivant les étapes ci-dessous :

a Dans vSphere client, sélectionnez l'hôte ESX dans l'arborescence de l'inventaire.

b Cliquez sur l'onglet **[Configuration]** .

c Dans le volet Logiciels, cliquez sur **[Paramètres avancés]**

d Dans la boîte de dialogue Paramètres avancés, cliquez sur **[Net]** .

e Vérifiez que le champ Net. **[DVFilterBindIpAddress]** est vide.

9 Installez à nouveau vShield App. Reportez-vous à « Installer vShield App », page 26.

Échec d'installation de vShield Data Security

Problème

Lors de l'installation de vShield Data Security, j'ai une erreur quand j'installe la machine virtuelle de service et un message d'erreur sur vSphere Client.

```
NAME=deploy OVF template Target=VMWARE-Data Security-xxxx
Status=operation timed out
```

.

Cause

La configuration DNS de vShield Manager peut ne pas être cohérente avec la configuration DNS de l'hôte dans vCenter Server.

Solution

Modifiez la configuration DNS de vShield Manager afin qu'elle corresponde à la configuration de l'hôte.

Index

A

attribution de licence
- installation **26**
- mode d'évaluation **25**

B

Backups, planification **24**

C

changement de mot de passe **23**

changement du mot de passe d'interface GUI **23**

CLI
- configuration des paramètres réseau de vShield Manager **20**
- sécurisation renforcée **16**

communication entre composants **15**

configuration des paramètres réseau de vShield Manager **20**

connexion à l'interface GUI **21**

considérations relatives au déploiement
- vShield **14**
- vShield App **16**
- vShield Edge **17**

D

déploiement
- cluster **11**
- DMZ **10**

Désenregistrer une SVM vShield Endpoint **38**

désinstaller
- module vShield Endpoint **38**
- vShield App **37**
- vShield Data Security **38**
- vShield Edge **38**

DMZ **10**

données, programmation de sauvegardes **24**

E

évaluation des composants de vShield **25**

exigences sur le client **13**

G

GUI de vShield Manager **16**

GUI, connexion **21**

I

installation
- agent léger vShield Endpoint **34**
- licences **26**
- vShield Edge **29**
- vShield Manager **19**

installation d'agent léger **34**

installer
- vShield App **26**
- vShield Data Security **35**
- vShield Edge **28**
- vShield Endpoint **33**

interface de liaison montante, ajout **31**

interface de liaison montante, ajout **31**

isolement de réseaux **11**

M

mettre à niveau Endpoint
- 4.1 vers 5.0 **46**
- 5.0 vers une version suivante **46**

mise à niveau
- vShield App **45**
- vShield Edge **45**
- vShield Manager **39**

P

passerelle par défaut, configuration de l'adresse IP **32**

préparation des machines virtuelles pour la protection **14**

programmation de sauvegardes **24**

protection d'un cluster **11**

protection de cluster **11**

protection de machines virtuelles **14**

R

REST **16**

S

sans état **27**

scénarios de déploiement **10**

sécurisation renforcée
- CLI **16**
- GUI de vShield Manager **16**
- REST **16**

spécifications système **13**

synchronisation avec vCenter **22**

V

vCenter, synchronisation depuis vShield Manager **22**
vMotion **14**
vShield
  composants, communication **15**
  évaluation des composants **25**
  scénarios de déploiement **10**
  sécurisation renforcée **16**
  vShield App **8**
  vShield Edge **8**
  vShield Endpoint **9**
  vShield Manager **7**
vShield App
  à propos **8**
  attribution de licence **26**
  déploiements courants **12**
  désinstaller **37**
  installer **26**
vShield Data Security, installer **35**
vShield Edge
  à propos **8**
  attribution de licence **26**
  déploiements courants **11**
  désinstaller **38**
  installation **29**
  installer **28**
  isolement de réseaux **11**
vShield Edge, attribution de nom **29**
vShield Endpoint
  à propos **9**
  attribution de licence **26**
  Désenregistrer SVM **38**
  désinstaller **38**
  étapes d'installation **34**
  installation d'agent léger **34**
  installer **33**
vShield Manager
  à propos **7**
  changement du mot de passe d'interface GUI **23**
  connexion à l'interface GUI **21**
  installation **19**
  paramètres réseau **20**
  programmation d'une sauvegarde **24**
  synchronisation avec vCenter **22**
  temps de fonctionnement **15**
vShield Zones, vShield Manager **7**