Guide de démarrage rapide de vShield

vShield Manager 5.0.1
vShield App 5.0.1
vShield Edge 5.0.1
vShield Endpoint 5.0.1

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-000839-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

Ce manuel, *Guide de démarrage rapide vShield*, décrit l'installation et la configuration du système VMware® vShield™ en utilisant l'interface utilisateur 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 4.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/fr/support/support-resources/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/fr/support/support-resources/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/fr/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/france.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/fr/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/fr/services.

1 Introduction à vShield

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

Ce chapitre aborde les rubriques suivantes :

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 plusieurs instances vShield App, vShield Edge, vShield Endpoint et vShield Data Security.

- vShield Manager page 8

  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.

- vShield App page 8

  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.

- vShield Edge page 9

  vShield Edge fournit des services de sécurité de frontière et de passerelle pour isoler les machines virtuelles dans un groupe de ports, un groupe de ports vDS ou Cisco Nexus 1000V. 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).

- vShield Endpoint page 10

  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 Data Security page 11

  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.

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 cette information pour auditer le trafic du réseau, définir et optimiser des stratégies de pare-feu et identifier les botnets (réseaux de machines zombies).

vShield Edge

vShield Edge fournit des services de sécurité de frontière et de passerelle pour isoler les machines virtuelles dans un groupe de ports, un groupe de ports vDS ou Cisco Nexus 1000V. 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)

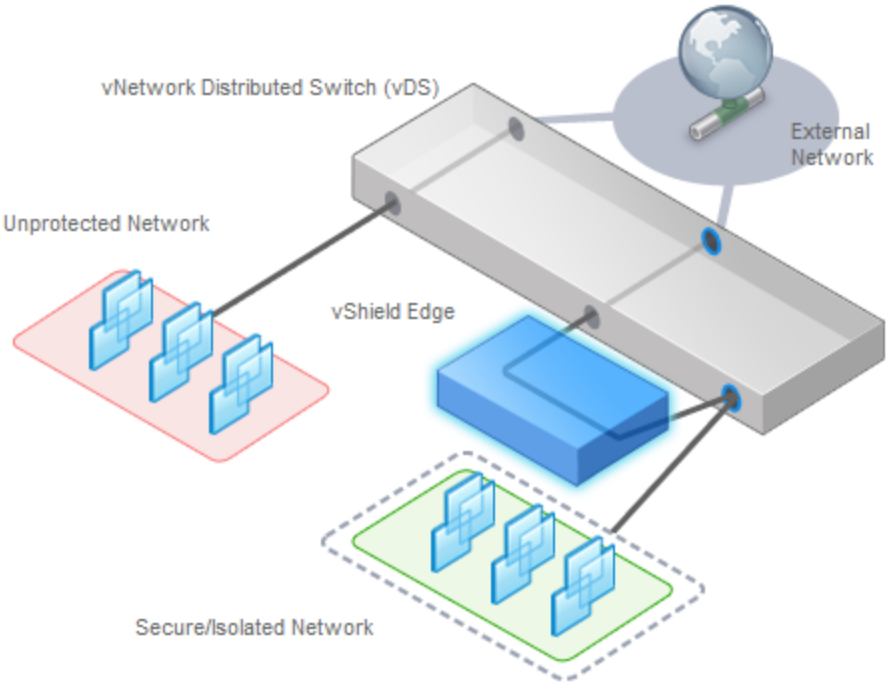
Pare-feu	Les règles prises en charge sont notamment la configuration IP 5-tuple avec plages d'adresses IP et de ports pour l'inspection d'état des protocoles TCP, UDP et ICMP.
Traduction d'adresse réseau	Contrôles séparés des adresses IP source et destination, ainsi que traduction de ports TCP et UDP.
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 pare-feux.
Équilibrage de charge	Adresses IP et groupes de serveurs virtuels configurables de façon simple et dynamique.

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

Figure 1-1. vShield Edge installé pour sécuriser un groupe de ports vDS

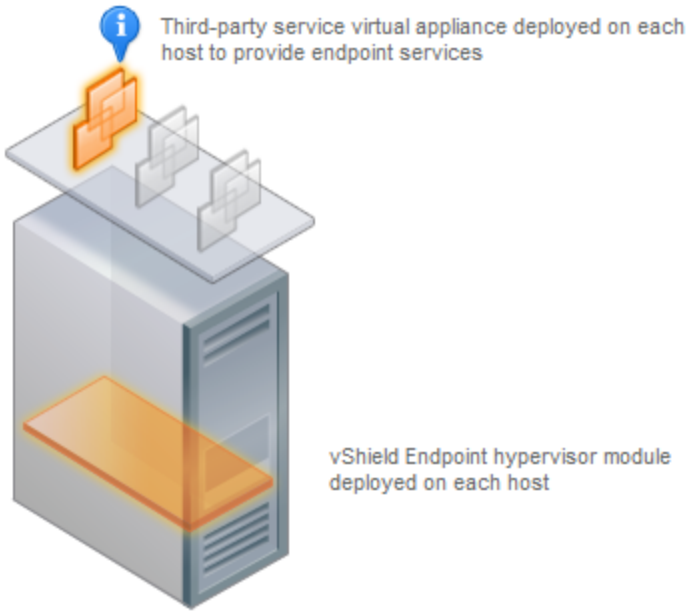


vShield Endpoint

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 page 12

  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.

- Isolation et protection des réseaux internes page 12

  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.

- Protection des machines virtuelles dans un cluster page 13

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

- Déploiements courants de vShield Edge page 13

  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.

- Déploiements courants de vShield App page 13

  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.

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.

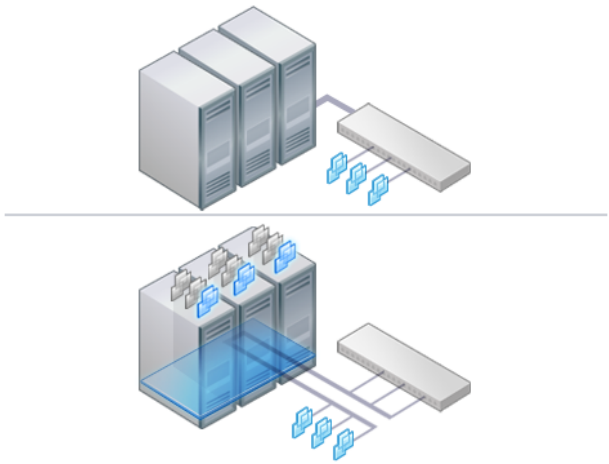
Vous pouvez par exemple utiliser des VLAN pour segmenter les zones de machines virtuelles par des frontières logiques, d'organisation ou de réseau. Grâce au SDK d'infrastructure virtuelle, le panneau d'inventaire de vShield Manager affiche une vue de vos réseaux VLAN sous la vue Réseaux. Vous pouvez 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 une vue générale des préalables à une installation réussie de vShield.

Ce chapitre aborde les rubriques suivantes :

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 un vShield Edge par groupe de ports.

Matériel

Tableau 2-1. Spécifications du matériel

Composant	Minimum
Mémoire	8 Go pour tous les composants vShield
Espace disque	■ 8 Go pour vShield Manager ■ 5 Go par vShield App par hôte ESX ■ 200 Mo par vShield Edge ■ 6 Go pour vShield Data Security par hôte ESX
Cartes réseau	Cartes réseau 2 gigabits sur un hôte ESX pour tous les composants vShield

Logiciel

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

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

- VMware vCenter Server 4.0 Update 2 ou ultérieure
- VMware ESX 4.0 Update 2 ou ultérieure pour chaque serveur

  REMARQUE vShield Endpoint et vShield Data Security nécessitent ESXi 5.0 - Correctif 1 et suivants ou ESXi 4.1 Correctif 3 et suivants.

- 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 - Correctif 1. Pour plus d'informations, voir « Installer VMware Tools sur les machines virtuelles invitées », page 30.

- VMware vCloud Director 1.0 ou ultérieure
- VMware View 4.5 ou ultérieure

Accès client et utilisateur

- PC avec VMware vSphere Client

  Remarque Si vous avez ajouté des hôtes ESX par leur nom à l'inventaire vSphere, veillez à fournir des noms DNS 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
- Port 443 vShield Manager accessible depuis l'hôte ESX. 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 ultérieur
  - Mozilla Firefox 1.x et ultérieur
  - 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.

- Préparation des machines virtuelles pour la protection vShield page 17

  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 pool de ressources 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.

- Temps de fonctionnement de vShield Manager page 17

  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 page 17

  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, ainsi qu'avec toutes 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.

- Sécurisation renforcée de vos machines virtuelles vShield page 18

  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.

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 pool de ressources 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 pool de ressources 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 « Préparer tous les hôtes ESX », 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, ainsi qu'avec toutes 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 recommande d'installer vShield Manager dans un environnement vCenter différent de celui que vShield Manager gère. Chaque vShield Manager gère un seul environnement vCenter Server .

AVERTISSEMENT Vérifiez que vCenter ne s'exécute pas sur un hôte vShield App protégé qu'il gère.

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 page 18

  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.

- Interface de ligne de commande page 18

  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.

- Demandes REST page 18

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

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*.

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.

VMware vShield est inclus avec VMware ESX 4.0 et 4.1. Le package VMware vShield de base inclut vShield Manager et vShield App. Vous pouvez configurer le groupe de règles de pare-feu vShield App pour surveiller le trafic en fonction des communications d'adresse IP à adresse IP.

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

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.

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 doit être accessible par toutes les instances à venir 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 **[Deploy from file]** et cliquez sur **[Browse]** pour rechercher le dossier du PC qui contient le fichier vShield Manager OVA.

5 Exécutez l'installation.

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

6 Mettez sous tension la machine virtuelle vShield Manager.

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 accessible par toutes les instances de vShield App, vShield Edge et vShield Endpoint, 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]** .

Synchroniser vShield Manager avec vCenter Server

Synchronisez votre vCenter Server pour afficher votre inventaire d'infrastructure VMware dans l'interface utilisateur de vShield Manager.

Vous devez disposer d'un compte d'utilisateur vCenter Server avec accès d'administration pour cette opération. Si votre mot de passe vCenter contient des caractères non-ASCII, vous devez le modifier avant de synchroniser vShield Manager avec vCenter Server.

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.

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 Cliquez sur l'onglet **[vCenter]** .

5 Tapez l'adresse IP ou le nom d'hôte de votre vCenter Server dans le champ **[IP address/Name]** .

6 Tapez votre nom d'utilisateur de connexion vSphere Client dans le champ **[User Name]** .

7 Tapez le mot de passe associé à ce nom d'utilisateur dans le champ **[Password]** .

8 Cliquez sur **[Save]** .

Enregistrer le plug-in vShield Manager avec vSphere Client

L'option **[vSphere Plug-in]** permet d'enregistrer vShield Manager comme plug-in de vSphere Client. Après enregistrement du plug-in, vous pouvez configurer la plupart des options de vShield depuis vSphere Client.

Procédure

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

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

3 Cliquez sur **[vSphere Plug-in]** .

4 Cliquez sur **[Register]** .

Pour les environnements NAT, il peut être nécessaire de modifier l'emplacement de téléchargement du script de plug-in. Par défaut, l'adresse vShield Manager est utilisée sous la forme *vShield_Manager_IP* **[:443]** .

5 Si vous êtes connecté à vSphere Client, déconnectez-vous.

6 Connectez-vous à vSphere Client.

7 Sélectionnez un hôte ESX.

8 Vérifiez que l'onglet **[vShield]** apparaît comme option.

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

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

4 Sélectionnez le compte admin.

5 Cliquez sur **[Update User]** .

6 Entrez un nouveau mot de passe.

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

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

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.

Ce chapitre aborde les rubriques suivantes :

Exécution des composants sous licence vShield en mode d'évaluation

Avant d'acheter et d'activer des licences pour vShield Edge, vShield App et vShield Endpoint, vous pouvez installer et utiliser les modes d'évaluation du logiciel. 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.

Préparation de votre infrastructure virtuelle pour vShield App, vShield Edge, vShield Endpoint et vShield Data Security

Avant d'installer des composants complémentaires, vous devez préparer les environnements d'hôte ESX et vNetwork. Vous avez installé vShield App, vShield Endpoint et la fonction vShield Data Security sur des hôtes ESX. Vous installez vShield Edge dans un groupe de ports, un groupe de ports vNetwork Distributed Switch (vDS) ou un Cisco® Nexus 1000V.

Installer les licences des composants vShield

Vous devez installer des licences pour vShield Edge, vShield App et vShield Endpoint avant d'installer ces composants. Vous pouvez installer ces licences après l'achèvement de l'installation de vShield Manager à l'aide de vSphere Client. Une licence vShield App vous permet d'utiliser également le composant vShield Endpoint.

Procédure

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

2 Pour la vue de rapport, sélectionnez **[Asset]** .

3 Cliquez à droite sur une ressource vShield et sélectionnez **[Change license key]** .

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.

Préparer tous les hôtes ESX

Préparez tous les hôtes ESX de votre environnement vCenter pour les fonctions supplémentaires vShield.

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.

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. N'installez pas vShield App sur le même hôte que la machine virtuelle VMware vCenter Server.

Prérequis

- Vérifiez que vous disposez d'une adresse IP pour le port de gestion (MGMT) de chaque dispositif virtuel vShield App. 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.
- 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
[Datastore]	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.
[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 Cochez la case **[vShield Endpoint]** .

8 Cliquez sur **[Install]** .

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

9 Après l'achèvement de l'installation de tous les composants, procédez comme suit :

- vShield App : À ce point, l'installation de vShield App est terminée. Accédez à l'onglet **[vShield App] > [App Firewall]** dans le centre de données, le cluster ou le conteneur de groupe de ports pour configurer des règles de pare-feu. 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 28 avant de redémarrer l'hôte.

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

- vShield Endpoint : Pour terminer l'installation, voir « Installation de vShield Endpoint », page 30.
- vShield Data Security : Pour terminer l'installation, consultez « Installation de vShield Data Security », page 31.

Suivant

Lorsque tous les composants sont installés, effectuez l'une des opérations suivantes.

- vShield App. À ce point, l'installation de vShield App est terminée. Sélectionnez **[vShield App] > [App Firewall]** au niveau du centre de données, du cluster ou du conteneur de groupe de ports pour définir des règles de pare-feu. Chaque 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 App Firewall, voir 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 28 avant de redémarrer l'hôte.

- vShield Endpoint : Pour terminer l'installation, voir « Installation de vShield Endpoint », page 30.
- vShield Data Security : Pour terminer l'installation, consultez « Installation de vShield Data Security », page 31.

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-5.0.1-556798.zip et télécharger le fichier zip.
4 Utilisez le profil d'hôte que vous avez créé au cours de l'étape 1 et le bundle hors ligne que vous avez téléchargé au cours de l'Étape 3 pour mettre à jour la configuration ESX sans état.

Installer un vShield Edge

Chaque dispositif virtuel vShield Edge a des interfaces réseau externe et interne. L'interface interne se connecte au groupe de ports sécurisé et sert de passerelle pour toutes les machines virtuelles protégées du groupe de ports. Le sous-réseau affecté à l'interface interne peut être un espace privé selon RFC 1918. L'interface externe du vShield Edge se connecte à un groupe de ports de liaison montante permettant d'accéder à un réseau d'entreprise partagé ou à un service permettant d'accéder à un réseau en couches.

Chaque vShield Edge nécessite au moins une adresse IP pour l'interface externe. Il est possible de configurer plusieurs adresses IP externes pour les services d'équilibrage de charge, de VPN d'un site à l'autre et NAT. L'interface interne peut avoir un bloc d'adresses IP privées recouvrant d'autres groupes de ports sécurisés vShield Edge.

Vous pouvez installer un vShield Edge par groupe de ports, groupe de ports vDS ou Cisco® Nexus 1000V.

Si DRS et HA sont activés, un vShield Edge sera migré dynamiquement.

Procédure

1 Connectez-vous à vSphere Client.

2 Allez à la **[Affichage] > [Inventaire] > [Networking]** .

3 Sur vDS, créez un groupe de ports.

Ce groupe de ports est le groupe de ports interne.

4 Déplacez les machines virtuelles clientes par un propriétaire dans le groupe de ports interne.

5 Sélectionnez le nouveau groupe de ports interne.

6 Cliquez sur l'onglet **[Edge]** .

7 Sous **[Network Interfaces]** , entrez les informations suivantes.

Option	Description
Externe	
Port Group	Sélectionnez le groupe de ports externe dans le vDS. Ce groupe de ports héberge une carte réseau physique et se connecte au réseau externe.
IP Address	Tapez l'adresse IP du groupe de ports externe.
Subnet Mask	Tapez le masque de sous-réseau IP associé à l'adresse IP externe spécifiée.
Default Gateway	Tapez l'adresse IP de la passerelle réseau par défaut.
Interne	
Port Group	C'est le groupe de ports interne sélectionné.
IP Address	Tapez l'adresse IP du groupe de ports interne.
Subnet Mask	Tapez le masque de sous-réseau IP associé à l'adresse IP interne spécifiée.

8 Sous **[Edge deployment resource selection]** , entrez les informations suivantes.

Option	Description
[Resource Pool]	Sélectionnez le pool de ressources dans lequel vShield Edge doit être déployé si vous installez vShield Edge dans un groupe dvPort qui couvre plusieurs pools de ressources. Si le groupe de ports sélectionné se trouve dans un seul pool de ressources, l'adresse IP du pool de ressources est définie automatiquement.
[Host]	Sélectionnez l'hôte ESX où se trouve la banque de données si vous installez vShield Edge dans un groupe dvPort qui couvre plusieurs hôtes. Si le groupe de ports sélectionné se trouve sur un seul hôte, l'adresse IP de l'hôte est définie automatiquement.
[Datastore]	Sélectionnez la banque de données où vous souhaitez enregistrer les fichiers de la machine virtuelle vShield Edge.

9 Cliquez sur **[Install]** .

Après l'achèvement de l'installation, configurez les services et règles de pare-feu pour protéger les machines virtuelles du groupe de ports sécurisé. Pour configurer un vShield Edge, consultez le *Guide d'administration vShield*.

AVERTISSEMENT Ne modifiez pas les machines virtuelles vShield Edge via vCenter Client afin de ne pas interrompre la communication entre vShield Edge et vShield Manager. Pour supprimer une machine virtuelle vShield Edge, désinstallez vShield Edge de vShield Manager

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 15.
- vShield Manager 5.0 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.

Installation de 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

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. Après l'achèvement de la désinstallation, l'hôte ESX redémarre. 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 depuis un groupe de ports

Vous pouvez désinstaller une instance vShield Edge depuis un groupe de ports sécurisés à l'aide de vSphere Client.

Procédure

1 Connectez-vous à vSphere Client.

2 Allez à l' **[Affichage] > [Inventaire] > [Networking]** .

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

4 Cliquez sur **[Uninstall]** .

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

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.

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

Si vous utilisez vShield Endpoint, désinstallez vShield Endpoint avant de mettre à jour vShield Manager.

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

Procédure

1 Téléchargez le bundle de mise à niveau vShield vers un emplacement que vShield Manager peut parcourir.

Le nom du fichier de lot 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 **[Parcourir]** et sélectionnez le fichier `VMware-vShield-Manager-upgrade_bundle-`*`buildNumber`*`.tar.gz`..

6 Cliquez sur **[Open.]**

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

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 Cliquez avec le bouton droit sur la machine virtuelle vShield Manager et cliquez sur **[Open Console]** pour ouvrir l'interface de ligne de commande (CLI) vShield Manager.

11 Après avoir lu le message **[e1000_watchdog_task: Message Lien NIC activé]** , connectez-vous à l'interface utilisateur vShield Manager.

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

Le panneau Installed Release affiche le numéro de compilation de la version que vous venez d'installer.

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.
- Reconnectez-vous à l'interface utilisateur vShield Manager.

Mettre à niveau vShield App

Mettez à niveau vShield App sur chaque hôte dans le 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 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 **[Install]** .

Mettre à niveau vShield Edge

Mettez à niveau vShield Edge dans chaque groupe de ports dans le centre de données.

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]** .

Suivant

Lorsque vous mettez à niveau vShield Edge depuis une version antérieure, vShield Edge fonctionne en mode de compatibilité. Vous pouvez passer au mode normal.

En mode de compatibilité, la règle de pare-feu par défaut est appliquée uniquement sur l'interface interne. Tout le trafic dans les deux directions les interfaces externes et VPN est autorisé. Lorsque vous activez le mode normal, les règles de politique de pare-feu par défaut ne sont pas modifiées initialement. Lorsque vous changez la configuration du pare-feu, les règles de pare-feu par défaut de vShield Edge 5.0.1 sont appliquées lorsque le trafic entrant est bloqué et que le trafic sortant est autorisé. Pour plus d'informations, consultez le Guide d'administration vShield.

Après la mise à niveau de vShield Edge, les informations d'identification CLI (Command Line Interface) sur le dispositif vShield Edge sont réinitialisées. Pour vous connecter à l'interface CLI, utilisez le nom d'utilisateur et le mot de passe par défaut et réinitialisez le mot de passe.

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

Pour mettre à niveau vShield Endpoint de la version 4.1 vers une version suivante, vous devez d'abors 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 34.

5 Mettez à niveau VMware vCenter vers la version requise. Pour plus d'informations, voir Chapitre 2, « Préparation à l'installation », page 15.

6 Mettez à niveau chaque hôte vers la version VMware ESX requise. Pour plus d'informations, voir Chapitre 2, « Préparation à l'installation », page 15.

7 Mettez à niveau vShield Manager. Pour plus d'informations, voir « Mettre à niveau vShield Manager », page 35.

8 Installez vShield Endpoint. Pour plus d'informations, voir « Installation de vShield Endpoint », page 30.

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 préalablement 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 **[Install]** .

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]** .

Échec de l'installation vShield 7

Installation de vShield App échoue.

Problème

Lorsque l'installation de vShield App échoue, vous recevez une invite de désinstallation du produit.

Cause

Lorsque vous désinstallez vShield vApp, les composants peuvent ne pas être tous désinstallés.

Solution

1 Cliquez sur **[Uninstall]** pour désinstaller tous les composants vShield. Pour plus d'informations, voir Chapitre 5, « Désinstallation des composants vShield », page 33.

2 Si le message d'erreur indiquait un problème d'installation du VIB, redémarrez l'hôte ESX.

3 Réinstallez vShield App.

Index