vShield-Kurzanleitung

vShield Manager 5.0
vShield App 5.0
vShield Edge 5.0
vShield Endpoint 5.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000695-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Über dieses Handbuch

In diesem Handbuch, der *vShield-Kurzanleitung*, wird beschrieben, wie das VMware® vShield™-System unter Verwendung der vShield Manager-Benutzerschnittstelle, des vSphere-Client-Plug-Ins und der Befehlszeilenschnittstelle (CLI) installiert und konfiguriert wird. Zu den bereitgestellten Informationen gehören Schrittanleitungen für die Konfiguration sowie empfohlene Vorgehensweisen.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die vShield in einer VMware vCenter-Umgebung installieren oder verwenden möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datencenter vertraut sind. In diesem Dokument wird vorausgesetzt, dass Sie bereits mit VMware Infrastructure 4.x, einschließlich VMware ESX, vCenter Server und vSphere Client, vertraut sind.

VMware Technical Publications – Glossar

VMware Technical Publications stellt ein Glossar mit Begriffen bereit, mit denen Sie möglicherweise noch nicht vertraut sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Feedback zu diesem Dokument

VMware freut sich über Ihre Anregungen zur Verbesserung der Dokumentation. Bitte senden Sie Ihre Kommentare und Anregungen an docfeedback@vmware.com.

Technischer Support und Schulungsressourcen

Ihnen stehen die folgenden Ressourcen für die technische Unterstützung zur Verfügung. Die aktuelle Version dieses Handbuchs sowie weitere Handbücher finden Sie auf folgender Webseite: http://www.vmware.com/support/pubs.

Online- und Telefon-Support

Auf der folgenden Webseite können Sie über den Onlinesupport technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren: http://www.vmware.com/support.

Kunden mit entsprechenden Supportverträgen erhalten über den Telefonsupport schnelle Hilfe bei Problemen der Prioritätsstufe 1. Rufen Sie die folgende Webseite auf: http://www.vmware.com/support/phone_support.html.

Support-Angebote

Informationen zum Support-Angebot von VMware und dazu, wie es Ihre geschäftlichen Anforderungen erfüllen kann, finden Sie unter http://www.vmware.com/support/services.

VMware Professional Services

Die VMware Education Services-Kurse umfassen umfangreiche praktische Übungen, Fallbeispiele und Kursmaterialien, die bei der praktischen Arbeit als Nachschlagewerke dienen. Kurse werden am Kundenstandort, in einer Kursraumumgebung und live im Internet angeboten. Für Pilotprogramme vor Ort und die Best Practices für die Implementierung verfügt VMware Consulting Services über Angebote, die Sie bei der Beurteilung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung unterstützen. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting-Diensten finden Sie auf der folgenden Webseite: http://www.vmware.com/services.

1 Einführung zu vShield

In diesem Kapitel werden die VMware® vShield™-Komponenten vorgestellt, die Sie installieren.

Dieses Kapitel behandelt die folgenden Themen:

vShield-Komponenten im Überblick

VMware vShield ist eine Suite von virtuellen Sicherheits-Appliances, die für die VMware vCenter Server-Integration entwickelt wurden. vShield ist eine kritische Sicherheitskomponente zum Schutz von virtualisierten Datencentern vor Angriffen und Missbrauch, die Sie beim Erreichen Ihrer Compliance-Zielsetzungen unterstützt.

vShield umfasst virtuelle Appliances und Dienste, die für den Schutz von virtuellen Maschinen unerlässlich sind. vShield kann über eine webbasierte Benutzeroberfläche, ein vSphere Client-Plug-In, eine Befehlszeilenschnittstelle und REST API konfiguriert werden.

vCenter Server enthält vShield Manager. Die folgenden vShield-Pakete erfordern jeweils eine Lizenz:

- vShield App
- vShield App mit Data Security
- vShield Edge
- vShield Endpoint

Ein vShield Manager verwaltet mehrere vShield App-, vShield Edge-, vShield Endpoint- und vShield Data Security-Instanzen.

- vShield Manager auf Seite 8

  Der vShield Manager ist die zentralisierte Netzwerkmanagement-Komponente von vShield und wird als virtuelle Appliance auf einem beliebigen ESX™-Host in Ihrer vCenter Server-Umgebung eingesetzt. Ein vShield Manager kann von Ihren vShield-Agenten aus auf verschiedenen ESX-Hosts ausgeführt werden.

- vShield App auf Seite 8

  vShield App ist eine Hypervisor-basierte Firewall, die Anwendungen im virtuellen Datencenter vor netzwerkbasierten Angriffen schützt. Organisationen erhalten Sichtbarkeit und Kontrolle über die Netzwerkkommunikation zwischen virtuellen Maschinen. Sie können Zugriffssteuerungsrichtlinien anhand logischer Konstrukte, wie z. B. VMware vCenter™-Container und vShield-Sicherheitsgruppen, und nicht nur anhand physischer Konstrukte, wie z. B. IP-Adressen, erstellen. Außerdem bietet die flexible IP-Adressierung die Möglichkeit, dieselbe IP-Adresse in mehreren Tenant-Zonen zu verwenden, was die Bereitstellung vereinfacht.

- vShield Edge auf Seite 9

  vShield Edge bietet Netzwerk-Edge-Sicherheits- und -Gateway-Dienste zur Isolierung der virtuellen Maschinen in einer Portgruppe, vDS-Portgruppe oder einem Cisco Nexus 1000V-Switch. vShield Edge verbindet isolierte Stub-Netzwerke mit freigegebenen (Uplink-)Netzwerken durch die Bereitstellung von gängigen Gateway-Diensten wie DHCP, VPN, NAT und Lastausgleich. Gängige Implementierungen von vShield Edge umfassen in DMZ-, VPN Extranets- und Multi-Tenant-Cloud-Umgebungen, in denen vShield Edge Perimeter-Sicherheit für virtuelle Datencenter (VDCs) bietet.

- vShield Endpoint auf Seite 10

  vShield Endpoint lagert die Verarbeitung von Antivirus- und Anti-Malware-Agenten auf eine dedizierte sichere virtuelle Appliance aus, die von VMware-Partnern bereitgestellt wird. Da die sichere virtuelle Appliance (im Unterschied zu einer virtuellen Gastmaschine) nicht offline geschaltet wird, kann sie kontinuierlich Antivirus-Signaturen aktualisieren und dabei den virtuellen Maschinen auf dem Host unterbrechungsfreien Schutz bieten. Zudem werden neue virtuelle Maschinen (oder vorhandene virtuelle Offline-Maschinen) sofort durch die aktuellsten Antivirus-Signaturen geschützt, wenn sie wieder online geschaltet werden.

- vShield Data Security auf Seite 10

  vShield Data Security bietet Sichtbarkeit in vertrauliche Daten, die in den virtualisierten und Cloud-Umgebungen Ihres Unternehmens gespeichert sind. Auf Basis der von vShield Data Security gemeldeten Verstöße können Sie sicherzustellen, dass vertrauliche Daten angemessen geschützt und weltweit die jeweils geltenden Bestimmungen eingehalten werden.

vShield Manager

Der vShield Manager ist die zentralisierte Netzwerkmanagement-Komponente von vShield und wird als virtuelle Appliance auf einem beliebigen ESX™-Host in Ihrer vCenter Server-Umgebung eingesetzt. Ein vShield Manager kann von Ihren vShield-Agenten aus auf verschiedenen ESX-Hosts ausgeführt werden.

Mit der vShield Manager-Benutzeroberfläche oder dem vSphere Client-Plug-In können Administratoren vShield-Komponenten installieren, konfigurieren und warten. Die vShield Manager-Benutzeroberfläche verwendet das VMware Infrastructure SDK, um ein Exemplar der vSphere Client-Bestandsliste anzuzeigen, und umfasst die Ansichten „Hosts & Cluster“ und „Netzwerk“.

vShield App

vShield App ist eine Hypervisor-basierte Firewall, die Anwendungen im virtuellen Datencenter vor netzwerkbasierten Angriffen schützt. Organisationen erhalten Sichtbarkeit und Kontrolle über die Netzwerkkommunikation zwischen virtuellen Maschinen. Sie können Zugriffssteuerungsrichtlinien anhand logischer Konstrukte, wie z. B. VMware vCenter™-Container und vShield-Sicherheitsgruppen, und nicht nur anhand physischer Konstrukte, wie z. B. IP-Adressen, erstellen. Außerdem bietet die flexible IP-Adressierung die Möglichkeit, dieselbe IP-Adresse in mehreren Tenant-Zonen zu verwenden, was die Bereitstellung vereinfacht.

Sie sollten vShield App auf jedem ESX-Host innerhalb eines Clusters installieren, damit VMware vMotion-Vorgänge funktionieren und virtuelle Maschinen geschützt bleiben, wenn sie zwischen ESX-Hosts migriert werden. Standardmäßig kann eine virtuelle vShield App-Appliance nicht mit vMotion verschoben werden.

Die Flow Monitoring-Funktion zeigt Netzwerkaktivitäten zwischen virtuellen Maschinen auf der Anwendungsprotokollebene an. Sie können anhand dieser Informationen den Netzwerkdatenverkehr überwachen, Firewallrichtlinien definieren bzw. verfeinern und Botnets erkennen.

vShield Edge

vShield Edge bietet Netzwerk-Edge-Sicherheits- und -Gateway-Dienste zur Isolierung der virtuellen Maschinen in einer Portgruppe, vDS-Portgruppe oder einem Cisco Nexus 1000V-Switch. vShield Edge verbindet isolierte Stub-Netzwerke mit freigegebenen (Uplink-)Netzwerken durch die Bereitstellung von gängigen Gateway-Diensten wie DHCP, VPN, NAT und Lastausgleich. Gängige Implementierungen von vShield Edge umfassen in DMZ-, VPN Extranets- und Multi-Tenant-Cloud-Umgebungen, in denen vShield Edge Perimeter-Sicherheit für virtuelle Datencenter (VDCs) bietet.

Standard-vShield Edge-Dienste (einschließlich vCloud Director)

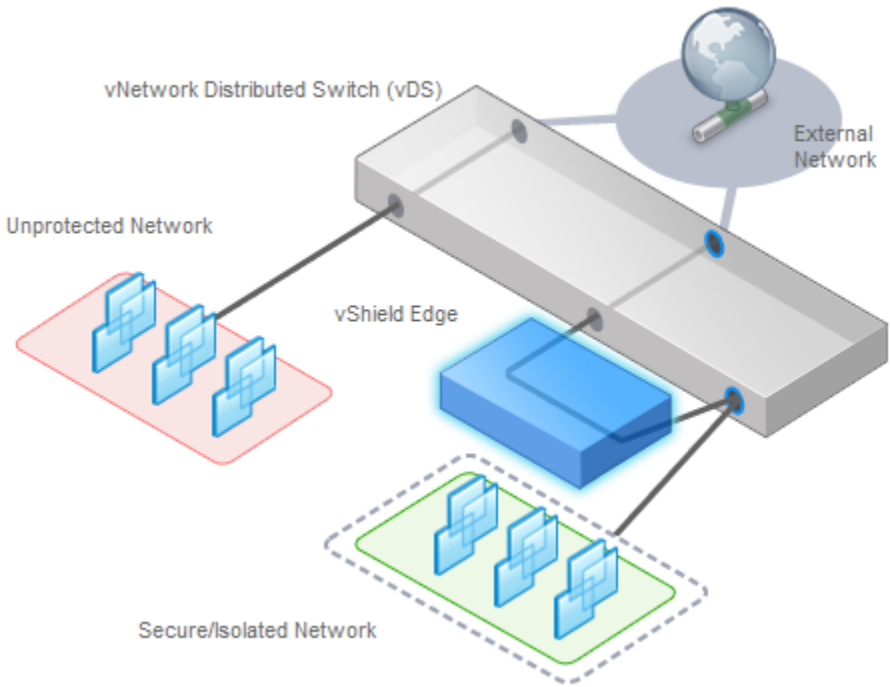
Firewall	Die unterstützten Regeln umfassen die IP 5-tuple-Konfiguration mit IP- und Port-Bereichen für die statusbehaftete Inspektion für TCP, UDP und ICMP.
Netzwerkadressübersetzung (NAT)	Separate Steuerelemente für Quell- und Ziel-IP-Adressen sowie TCP- und UDP-Portübersetzung.
Dynamic Host Configuration Protocol (DHCP)	Konfiguration von IP-Pools, Gateways, DNS-Servern und Suchdomänen.

Erweiterte vShield Edge-Dienste

Virtuelles privates Site-to-Site-Netzwerk (VPN)	Verwendet standardisierte IPsec-Protokolleinstellungen für die Interoperabilität mit allen großen Firewall-Anbietern.
Lastenausgleich	Einfach und dynamisch konfigurierbare IP-Adressen und Servergruppen.

vShield Edge unterstützt den Syslog-Export an Remote-Server für alle Dienste.

Abbildung 1-1. Installation von vShield Edge zur Sicherung einer vDS-Portgruppe

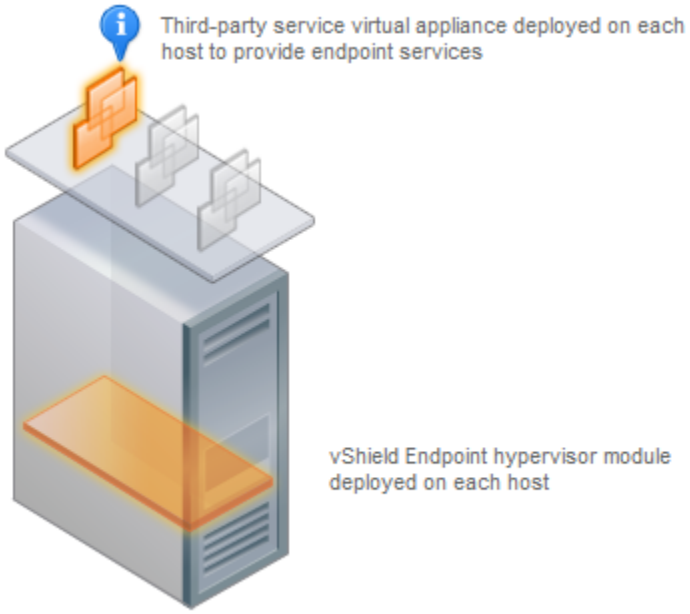


vShield Endpoint

vShield Endpoint lagert die Verarbeitung von Antivirus- und Anti-Malware-Agenten auf eine dedizierte sichere virtuelle Appliance aus, die von VMware-Partnern bereitgestellt wird. Da die sichere virtuelle Appliance (im Unterschied zu einer virtuellen Gastmaschine) nicht offline geschaltet wird, kann sie kontinuierlich Antivirus-Signaturen aktualisieren und dabei den virtuellen Maschinen auf dem Host unterbrechungsfreien Schutz bieten. Zudem werden neue virtuelle Maschinen (oder vorhandene virtuelle Offline-Maschinen) sofort durch die aktuellsten Antivirus-Signaturen geschützt, wenn sie wieder online geschaltet werden.

vShield Endpoint wird als Hypervisor-Modul und virtuelle Sicherheits-Appliance von einem Drittanbieter-Virenschutzanbieter (VMware-Partner) auf einem ESX-Host installiert. Der Hypervisor prüft virtuelle Gastmaschinen von außerhalb, wodurch keine Agenten mehr der virtuellen Maschine benötigt werden. Dies macht den Einsatz von vShield Endpoint effizient, da Ressourcenengpässe beim Optimieren der Arbeitsspeichernutzung vermieden werden.

Abbildung 1-2. Installation von vShield Endpoint auf einem ESX-Host



vShield Data Security

vShield Data Security bietet Sichtbarkeit in vertrauliche Daten, die in den virtualisierten und Cloud-Umgebungen Ihres Unternehmens gespeichert sind. Auf Basis der von vShield Data Security gemeldeten Verstöße können Sie sicherzustellen, dass vertrauliche Daten angemessen geschützt und weltweit die jeweils geltenden Bestimmungen eingehalten werden.

Bereitstellungsszenarien

Mit vShield können Sie sichere Zonen für eine Reihe von Bereitstellungen virtueller Maschinen erstellen. Sie können virtuelle Maschinen auf Grundlage von spezifischen Anwendungen, Netzwerksegmentierung oder anwenderdefinierten Compliance-Faktoren isolieren. Sobald Sie Ihre Richtlinien für die Zonenzuordnung festgelegt haben, können Sie vShield bereitstellen, um die Durchsetzung von Zugriffsregeln für jede dieser Zonen zu erzwingen.

- Schutz von DMZ auf Seite 11

  Die DMZ ist eine gemischte vertrauenswürdige Zone. Clients greifen vom Internet aus für Web- und E-Mail-Dienste darauf zu, während die Dienste innerhalb der DMZ Zugriff auf Dienste innerhalb des internen Netzwerks erfordern können.

- Isolieren und Schützen von internen Netzwerken auf Seite 12

  Sie können mit vShield Edge ein internes Netzwerk vom externen Netzwerk isolieren. Eine vShield Edge-Instanz bietet Perimeter-Firewall-Schutz und Edge-Dienste zur Sicherung von virtuellen Maschinen in einer Portgruppe, indem die Kommunikation mit dem externen Netzwerk über DHCP, NAT und VPN ermöglicht wird.

- Schutz von virtuellen Maschinen in einem Cluster auf Seite 12

  Mit vShield App können Sie virtuelle Maschinen in einem Cluster schützen.

- Gängige Bereitstellungen von vShield Edge auf Seite 12

  Sie können mit vShield Edge ein Stub-Netzwerk isolieren, wobei durch die Verwendung von NAT der Datenverkehr zu und vom Netzwerk ermöglicht wird. Wenn Sie interne Stub-Netzwerke bereitstellen, können Sie mit vShield Edge die Kommunikation zwischen Netzwerken per LAN-zu-LAN-Verschlüsselung über VPN-Tunnels sichern.

- Gängige Bereitstellungen von vShield App auf Seite 13

  Sie können vShield App verwenden, um Sicherheitszonen innerhalb eines vDC zu schaffen. Sie können Firewall-Richtlinien für vCenter-Container oder Sicherheitsgruppen festlegen, bei denen es sich um anwenderdefinierte Container handelt, die Sie mithilfe der vShield Manager-Benutzeroberfläche erstellen können. Container-basierte Richtlinien ermöglichen Ihnen die Schaffung gemischter vertrauenswürdiger Zonen, ohne dass Sie eine externe physische Firewall benötigen.

Schutz von DMZ

Die DMZ ist eine gemischte vertrauenswürdige Zone. Clients greifen vom Internet aus für Web- und E-Mail-Dienste darauf zu, während die Dienste innerhalb der DMZ Zugriff auf Dienste innerhalb des internen Netzwerks erfordern können.

Sie können virtuelle DMZ-Maschinen in einer Portgruppe platzieren und diese Portgruppe mit einer vShield Edge-Instanz sichern. vShield Edge bietet Zugriffdienste wie eine Firewall, NAT und VPN sowie den automatischen Lastausgleich zur Sicherung von DMZ-Diensten.

Ein gängiges Beispiel für einen DMZ-Dienst, der Zugriff auf einen internen Dienst benötigt, ist Microsoft Exchange. Microsoft Outlook Web Access (OWA) befindet sich in der Regel im DMZ-Cluster, das Back-End von Microsoft Exchange hingegen im internen Cluster. Für den internen Cluster können Sie Firewall-Regeln erstellen, um nur Exchanged-bezogene Anforderungen von der DMZ zu erlauben, indem bestimmte Quelle/Ziel-Parameter erkannt werden. Für den DMZ-Cluster können Sie Regeln erstellen, um den externen Zugriff auf die DMZ mithilfe von HTTP, FTP oder SMTP nur für bestimmte Zielbereiche zu erlauben.

Isolieren und Schützen von internen Netzwerken

Sie können mit vShield Edge ein internes Netzwerk vom externen Netzwerk isolieren. Eine vShield Edge-Instanz bietet Perimeter-Firewall-Schutz und Edge-Dienste zur Sicherung von virtuellen Maschinen in einer Portgruppe, indem die Kommunikation mit dem externen Netzwerk über DHCP, NAT und VPN ermöglicht wird.

Innerhalb der gesicherten Portgruppe können Sie eine vShield App-Instanz auf jedem ESX-Host installieren, den der vDS umspannt, um die Kommunikation zwischen virtuellen Maschinen im internen Netzwerk zu sichern.

Wenn Sie VLAN-Tags zur Segmentierung von Datenverkehr verwenden, können Sie mit App Firewall intelligente Zugriffsrichtlinien erstellen. Indem Sie App Firewall anstelle einer physischen Firewall verwenden, können Sie vertrauenswürdige Zonen in freigegebenen ESX-Clustern reduzieren oder mischen. Dadurch erhalten Sie eine optimale Auslastung und Konsolidierung anhand von Funktionen wie DRS und HA, anstatt mit separaten, fragmentierten Clustern arbeiten zu müssen. Das Management der gesamten ESX-Bereitstellung als einzelner Pool ist weniger komplex als separat verwaltete Pools.

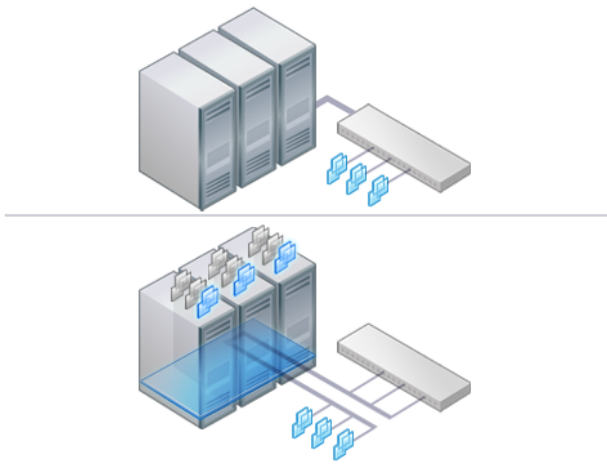
Sie verwenden z.B. VLANs, um virtuelle Maschinenzonen auf Basis von logischen, organisatorischen oder Netzwerkbegrenzungen zu segmentieren. Auf Grundlage des Virtual Infrastructure SDK zeigt die Bestandsliste von vShield Manager eine Ansicht Ihrer VLAN-Netzwerke in der Netzwerkansicht an. Sie können Zugriffsregeln für jedes VLAN-Netzwerk erstellen, um virtuelle Maschinen zu isolieren und nicht getaggten Datenverkehr auf diesen Maschinen abzulegen.

Schutz von virtuellen Maschinen in einem Cluster

Mit vShield App können Sie virtuelle Maschinen in einem Cluster schützen.

In Abbildung 1-3 sind vShield App-Instanzen auf jedem ESX-Host in einem Cluster installiert. Virtuelle Maschinen sind geschützt, wenn sie über vMotion oder DRS zwischen ESX-Hosts im Cluster verschoben werden. Jede vApp gibt den Status aller Übertragungen frei und behält ihn bei.

Abbildung 1-3. Auf jedem ESX-Host in einem Cluster installierte vShield App-Instanzen



Gängige Bereitstellungen von vShield Edge

Sie können mit vShield Edge ein Stub-Netzwerk isolieren, wobei durch die Verwendung von NAT der Datenverkehr zu und vom Netzwerk ermöglicht wird. Wenn Sie interne Stub-Netzwerke bereitstellen, können Sie mit vShield Edge die Kommunikation zwischen Netzwerken per LAN-zu-LAN-Verschlüsselung über VPN-Tunnels sichern.

vShield Edge kann als Selbstbedienungsanwendung innerhalb von VMware vCloud Director konfiguriert werden.

Gängige Bereitstellungen von vShield App

Sie können vShield App verwenden, um Sicherheitszonen innerhalb eines vDC zu schaffen. Sie können Firewall-Richtlinien für vCenter-Container oder Sicherheitsgruppen festlegen, bei denen es sich um anwenderdefinierte Container handelt, die Sie mithilfe der vShield Manager-Benutzeroberfläche erstellen können. Container-basierte Richtlinien ermöglichen Ihnen die Schaffung gemischter vertrauenswürdiger Zonen, ohne dass Sie eine externe physische Firewall benötigen.

Bei einer Bereitstellung ohne vDCs verwenden Sie eine vShield App-Instanz mit der Sicherheitsgruppenfunktion, um vertrauenswürdige Zonen zu schaffen und Zugriffsrichtlinien durchzusetzen.

Administratoren von Dienstanbietern können vShield App verwenden, um breitflächige Firewall-Richtlinien für alle virtuellen Gastmaschinen in einem internen Netzwerk festzulegen. Sie können beispielsweise eine Firewall-Richtlinie auf der zweiten vNIC für alle virtuellen Gastmaschinen festlegen, die den virtuellen Maschinen die Herstellung einer Verbindung mit einem Speicherserver erlaubt, jedoch die Kommunikation zwischen virtuellen Maschinen untereinander blockiert.

Vorbereitung für die Installation 2

Dieses Kapitel bietet einen Überblick über die Voraussetzungen für die erfolgreiche Installation von vShield.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen

Bevor Sie vShield in Ihrer vCenter Server-Umgebung installieren, prüfen Sie Ihre Netzwerkkonfiguration und -ressourcen. Sie können einen vShield Manager pro vCenter Server, eine vShield App oder einen vShield Endpoint pro ESX™-Host und eine vShield Edge-Instanz pro Portgruppe installieren.

Hardware

Tabelle 2-1. Hardwareanforderungen

Komponente	Minimal
Arbeitsspeicher	8 GB für alle vShield-Komponenten
Festplattenspeicher	■ 8 GB für den vShield Manager ■ 5 GB pro vShield App pro ESX-Host ■ 100 MB pro vShield Edge ■ 6 GB für vShield Data Security pro ESX-Host
Netzwerkkarten	2 Gigabit-Netzwerkkarten auf einem ESX-Host für alle vShield-Komponenten

Software

Die neuesten Interoperabilitätsinformationen finden Sie in der Produkt-Interoperabilitätmatrix unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Nachfolgend finden Sie eine Auflistung der Mindestversionsanforderungen für VMware-Produkte.

- VMware vCenter Server 4.0 Update 2 oder höher
- VMware ESX 4.0 Update 2 oder höher für jeden Server

Hinweis

- vShield Endpoint benötigt ESXi 4.1 Patch 3 oder höher.
- vShield Data Security benötigt ESXi 4.1 Patch 3 oder höher.
- Wenn Sie vShield App mit ESXi 5.0 verwenden, müssen Sie ESXi 5.0 Patch 1 installieren.

- VMware Tools

  Für vShield Endpoint und vShield Data Security müssen Sie ein Upgrade Ihrer virtuellen Maschinen auf Hardwareversion 7 oder 8 durchführen und VMware Tools 8.6.0 installieren, das mit ESXi 5.0 Patch 1 ausgeliefert wird.

- VMware vCloud Director 1.0 oder höher
- VMware View 4.5 oder höher

Client- und Benutzerzugriff

- PC mit dem VMware vSphere Client
- Berechtigungen zum Hinzufügen und Einschalten von virtuellen Maschinen
- Zugriff auf den Datenspeicher, in dem Dateien für virtuelle Maschinen gespeichert werden, sowie Kontoberechtigungen zum Kopieren von Dateien in diesen Datenspeicher
- Aktivieren von Cookies in Ihrem Webbrowser, um auf die vShield Manager-Benutzeroberfläche zugreifen zu können
- Stellen Sie über einen der folgenden unterstützten Webbrowser eine Verbindung zum vShield Manager her:
  - Internet Explorer 6.x und höher
  - Mozilla Firefox 1.x und höher
  - Safari 1.x oder 2.x

Erwägungen zur Bereitstellung

Beachten Sie die folgenden Empfehlungen und Einschränkungen, bevor Sie vShield-Komponenten bereitstellen.

- Vorbereiten virtueller Maschinen für den Schutz durch vShield auf Seite 17

  Sie müssen festlegen, wie Ihre virtuellen Maschinen mit vShield geschützt werden sollen. Je nachdem, welche vShield-Komponenten Sie verwenden, ist es empfehlenswert, alle ESX-Hosts innerhalb eines Ressourcenpools für vShield App, vShield Endpoint und vShield Data Security vorzubereiten. Sie müssen zudem ein Upgrade Ihrer virtuellen Maschinen auf Hardwareversion 7 oder 8 durchführen.

- Verfügbarkeit von vShield Manager auf Seite 17

  Der vShield Manager sollte auf einem ESX-Host ausgeführt werden, der nicht von Ausfallzeiten betroffen ist, z.B. häufigen Neustarts oder Arbeiten im Wartungsmodus. Sie können HA oder DRS verwenden, um die Ausfallsicherheit von vShield Manager zu steigern. Wenn eine Nichtverfügbarkeit des ESX-Hosts abzusehen ist, auf dem der vShield Manager installiert ist, verschieben Sie die virtuelle vShield Manager-Anwendung mit vMotion auf einen anderen ESX-Host. Aus diesem Grund werden mehrere ESX-Hosts empfohlen.

- Kommunikation zwischen vShield-Komponenten auf Seite 17

  Die Management-Schnittstellen von vShield-Komponenten sollten in einem gemeinsamen Netzwerk platziert werden, z.B. dem Netzwerk für das vSphere-Management. vShield Manager benötigt eine Verbindung zu vCenter Server, zu den vShield App- und vShield Edge-Instanzen, zum vShield Endpoint-Modul und zur virtuellen vShield Data Security-Maschine. vShield-Komponenten können über geroutete Verbindungen sowie über verschiedene LANs kommunizieren.

- Optimierung der Sicherheit Ihrer virtuellen vShield-Maschinen auf Seite 18

  Sie können auf den vShield Manager und andere vShield-Komponenten über eine webbasierte Benutzeroberfläche, eine Befehlszeilenschnittstelle und REST API zugreifen. vShield enthält Standardanmeldeinformationen für jede dieser Zugriffsoptionen. Nach der Installation jeder virtuellen vShield-Maschine sollten Sie die Zugriffssicherheit erhöhen, indem Sie die Standardanmeldeinformationen ändern. Beachten Sie, dass vShield Data Security keine Standard-Anmeldedaten bereitstellt.

Vorbereiten virtueller Maschinen für den Schutz durch vShield

Sie müssen festlegen, wie Ihre virtuellen Maschinen mit vShield geschützt werden sollen. Je nachdem, welche vShield-Komponenten Sie verwenden, ist es empfehlenswert, alle ESX-Hosts innerhalb eines Ressourcenpools für vShield App, vShield Endpoint und vShield Data Security vorzubereiten. Sie müssen zudem ein Upgrade Ihrer virtuellen Maschinen auf Hardwareversion 7 oder 8 durchführen.

Stellen Sie sich die folgenden Fragen:

Wie sind meine virtuellen Maschinen gruppiert?

Sie können darüber nachdenken, virtuelle Maschinen in Portgruppen auf einem vDS oder einen anderen ESX-Host zu verschieben, um sie nach Funktion, Abteilung oder nach anderen organisatorischen Aspekten zu gruppieren, um die Sicherheit zu verbessern und die Konfiguration von Zugriffsregeln zu verbessern. Sie können eine vShield Edge-Instanz im Umkreis einer beliebigen Portgruppe installieren, um virtuelle Maschinen vom externen Netzwerk zu isolieren. Sie können eine vShield App-Instanz auf einem ESX-Host installieren und Firewall-Richtlinien pro Containerressource konfigurieren, um Regeln basierend auf der Hierarchie von Ressourcen anzuwenden.

Sind meine virtuellen Maschinen weiterhin geschützt, wenn ich sie mit vMotion zu einem anderen ESX-Host verschiebe?

Ja, wenn die Hosts in einem Ressourcenpool vorbereitet sind, können Sie Maschinen zwischen Hosts migrieren, ohne die Sicherheit zu gefährden. Informationen zum Vorbereiten Ihrer ESX-Hosts finden Sie unter „Vorbereitung aller ESX-Hosts“, auf Seite 26.

Verfügbarkeit von vShield Manager

Der vShield Manager sollte auf einem ESX-Host ausgeführt werden, der nicht von Ausfallzeiten betroffen ist, z.B. häufigen Neustarts oder Arbeiten im Wartungsmodus. Sie können HA oder DRS verwenden, um die Ausfallsicherheit von vShield Manager zu steigern. Wenn eine Nichtverfügbarkeit des ESX-Hosts abzusehen ist, auf dem der vShield Manager installiert ist, verschieben Sie die virtuelle vShield Manager-Anwendung mit vMotion auf einen anderen ESX-Host. Aus diesem Grund werden mehrere ESX-Hosts empfohlen.

Kommunikation zwischen vShield-Komponenten

Die Management-Schnittstellen von vShield-Komponenten sollten in einem gemeinsamen Netzwerk platziert werden, z.B. dem Netzwerk für das vSphere-Management. vShield Manager benötigt eine Verbindung zu vCenter Server, zu den vShield App- und vShield Edge-Instanzen, zum vShield Endpoint-Modul und zur virtuellen vShield Data Security-Maschine. vShield-Komponenten können über geroutete Verbindungen sowie über verschiedene LANs kommunizieren.

Hinweis Der vShield Manager muss sich in derselben vCenter Server-Umgebung wie die zu verwalteten vShield-Komponenten befinden. Sie können den vShield Manager nicht über verschiedene vCenter Server-Umgebungen hinweg verwenden.

Optimierung der Sicherheit Ihrer virtuellen vShield-Maschinen

Sie können auf den vShield Manager und andere vShield-Komponenten über eine webbasierte Benutzeroberfläche, eine Befehlszeilenschnittstelle und REST API zugreifen. vShield enthält Standardanmeldeinformationen für jede dieser Zugriffsoptionen. Nach der Installation jeder virtuellen vShield-Maschine sollten Sie die Zugriffssicherheit erhöhen, indem Sie die Standardanmeldeinformationen ändern. Beachten Sie, dass vShield Data Security keine Standard-Anmeldedaten bereitstellt.

- vShield Manager-Benutzeroberfläche auf Seite 18

  Sie greifen auf die vShield Manager-Benutzeroberfläche zu, indem Sie ein Webbrowser-Fenster öffnen und zur IP-Adresse des Management-Ports von vShield Manager wechseln.

- Befehlszeilenschnittstelle auf Seite 18

  Sie können auf die virtuellen Appliances vShield Manager, vShield App und vShield Edge mittels einer Befehlszeilenschnittstelle über eine vSphere Client-Konsolensitzung zugreifen. Informationen zum Zugriff auf die virtuelle vShield Endpoint-Appliance finden Sie in den Anweisungen des Antivirus-Anbieters. Sie können über die Befehlszeilenschnittstelle nicht auf die virtuelle vShield Data Security-Maschine zugreifen.

- REST-Anforderungen auf Seite 18

  Alle REST API-Anforderungen erfordern eine Authentifizierung über den vShield Manager.

vShield Manager-Benutzeroberfläche

Sie greifen auf die vShield Manager-Benutzeroberfläche zu, indem Sie ein Webbrowser-Fenster öffnen und zur IP-Adresse des Management-Ports von vShield Manager wechseln.

Das Standardbenutzerkonto „admin“ besitzt globalen Zugriff auf den vShield Manager. Nach der ersten Anmeldung sollten Sie das Standardkennwort des Benutzerkontos „admin“ ändern. Siehe „Ändern des Kennworts für das Standardkonto der vShield Manager-Benutzeroberfläche“, auf Seite 22.

Befehlszeilenschnittstelle

Sie können auf die virtuellen Appliances vShield Manager, vShield App und vShield Edge mittels einer Befehlszeilenschnittstelle über eine vSphere Client-Konsolensitzung zugreifen. Informationen zum Zugriff auf die virtuelle vShield Endpoint-Appliance finden Sie in den Anweisungen des Antivirus-Anbieters. Sie können über die Befehlszeilenschnittstelle nicht auf die virtuelle vShield Data Security-Maschine zugreifen.

Jede virtuelle Appliance verwendet dieselbe Standardkombination aus Benutzername (**`admin`**) und Kennwort (**`default`**) wie die vShield Manager-Benutzeroberfläche. Zur Aktivierung des Modus Enabled wird ebenfalls das Kennwort **`default`** verwendet.

Weitere Informationen zur Optimierung der Befehlszeilenschnittstelle (CLI) finden Sie in der *vShield Command Line Interface Reference*.

REST-Anforderungen

Alle REST API-Anforderungen erfordern eine Authentifizierung über den vShield Manager.

Mit der Base 64-Verschlüsselung legen Sie eine Benutzername/Kennwort-Kombination im folgenden Format fest: Benutzername:Kennwort. Sie müssen über ein Konto für die vShield Manager-Benutzeroberfläche (Benutzername und Kennwort) mit privilegiertem Zugriff verfügen, um Anforderungen ausführen zu können. Weitere Informationen zum Authentifizieren von REST API-Anforderungen finden Sie im *vShield API-Programmierhandbuch*.

Installieren von vShield Manager 3

VMware vShield bietet Firewall-Schutz, Datenverkehrsanalysen und Netzwerk-Perimeter-Schutz zum Schutz Ihrer virtuellen vCenter Server-Infrastruktur. Die Installation der virtuellen Appliance vShield wurde für die meisten virtuellen Datencenter automatisiert.

Der vShield Manager ist die zentrale Management-Komponente von vShield. Sie verwenden den vShield Manager, um Konfigurationen zu überwachen und an Instanzen von vShield App, vShield Endpoint und vShield Edge weiterzugeben. Der vShield Manager wird als virtuelle Appliance auf einem ESX-Host ausgeführt.

VMware vShield ist in VMware ESX 4.0 und 4.1 enthalten. Das VMware vShield-Basispaket enthält den vShield Manager und vShield Zones. Sie können den vShield Zones-Firewall-Regelsatz für die Überwachung von Datenverkehr auf Basis der Kommunikation zwischen IP-Adressen konfigurieren.

Die Installation von vShield Manager umfasst mehrere Schritte. Sie müssen alle folgenden Aufgaben nacheinander ausführen, um die Installation von vShield Manager erfolgreich abzuschließen.

Um die Sicherheit Ihres Netzwerks weiter zu verbessern, können Sie Lizenzen für vShield App, vShield Endpoint und vShield Edge erwerben.

Dieses Kapitel behandelt die folgenden Themen:

Abrufen der vShield Manager OVA-Datei

Die virtuelle vShield Manager-Maschine ist als Open Virtualization Appliance (OVA)-Datei gepackt, sodass Sie den vSphere Client verwenden können, um den vShield Manager in den Datenspeicher und den virtuellen Maschinenbestand zu importieren.

Installieren der virtuellen Appliance vShield Manager

Sie können die virtuelle vShield Manager-Maschine auf einem ESX-Host in einem mit DRS konfigurierten Cluster installieren.

Sie müssen den vShield Manager in dem vCenter installieren, mit dem der vShield Manager interagieren wird. Ein einzelner vShield Manager dient als einzelne vCenter Server-Umgebung.

Die Installation der virtuellen vShield Manager-Maschine umfasst VMware Tools. Versuchen sie nicht, VMware Tools auf dem vShield Manager zu aktualisieren oder zu installieren.

Vorgehensweise

1 Melden Sie sich beim vSphere Client an.

2 Erstellen Sie eine Portgruppe als Ausgangsspeicherort für die Management-Schnittstelle von vShield Manager.

Die Management-Schnittstelle von vShield Manager muss für alle künftigen vShield Edge-, vShield App- und vShield Endpoint-Instanzen erreichbar sein.

Hinweis Platzieren Sie die Management-Schnittstelle von vShield Manager nicht in derselben Portgruppe wie die Service Console und den VMkernel.

---

3 Navigieren Sie zu **[File] > [Deploy OVF Template]** .

4 Klicken Sie auf **[Deploy from file]** und dann auf **[Browse]** , um nach dem Ordner auf Ihrem Computer zu suchen, der die vShield Manager OVA-Datei enthält.

5 Schließen Sie den Assistenten ab.

Der vShield Manager wird als virtuelle Maschine in Ihrem Bestand installiert.

6 Schalten Sie die virtuelle vShield Manager-Maschine ein.

Konfigurieren der Netzwerkeinstellungen von vShield Manager

Sie müssen die Befehlszeilenschnittstelle von vShield Manager verwenden, um eine IP-Adresse zu konfigurieren, das Standard-Gateway festzulegen und die DNS-Einstellungen anzugeben.

Sie können bis zu zwei DNS-Server festlegen, die der vShield Manager zur Auflösung von IP-Adressen und Hostnamen verwenden kann. DNS ist erforderlich, wenn ein beliebiger ESX-Host in Ihrer vCenter Server-Umgebung mithilfe des Hostnamens hinzugefügt wurde (anstatt der IP-Adresse).

Vorgehensweise

1 Klicken Sie mit der rechten Maustaste auf die virtuelle vShield Manager-Maschine und klicken Sie auf **[Open Console]** , um die Befehlszeilenschnittstelle von vShield Manager zu öffnen.

Der Startprozess kann einige Minuten in Anspruch nehmen.

2 Wenn die Eingabeaufforderung `manager login` angezeigt wird, melden Sie sich bei der Befehlszeilenschnittstelle mit dem Benutzernamen **`admin`** und dem Kennwort **`default`** an.

3 Wechseln Sie mit dem Kennwort **`default`** in den Modus Enabled.

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

4 Führen Sie den Befehl `setup` aus, um den CLI setup-Assistenten zu öffnen

Der CLI setup-Assistent führt Sie durch die IP-Adressenzuweisung für die Verwaltungsschnittstelle von vShield Manager und die Identifizierung des Standard-Netzwerk-Gateways. Die IP-Adresse der Management-Schnittstelle muss für alle installierten vShield App-, vShield Edge- und vShield Endpoint-Instanzen sowie für das Systemmanagement durch einen Webbrowser erreichbar bleiben.

```
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, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Please log out and log back in again.

manager> exit
manager login:
```

5 Melden Sie bei der Befehlszeilenschnittstelle an.

6 Senden Sie einen Ping-Befehl an den Standard-Gateway, um die Netzwerkkonnektivität zu überprüfen.

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

7 Senden Sie von Ihrem Computer aus einen Ping-Befehl an die IP-Adresse von vShield Manager, um sicherzustellen, dass die IP-Adresse erreichbar ist.

Anmelden bei der vShield Manager-Benutzeroberfläche

Nachdem Sie die virtuelle vShield Manager-Maschine installiert und konfiguriert haben, melden Sie sich bei der vShield Manager-Benutzeroberfläche an.

Vorgehensweise

1 Öffnen Sie ein Webbrowser-Fenster und geben Sie die IP-Adresse an, die dem vShield Manager zugewiesen ist.

Die vShield Manager-Benutzeroberfläche wird in einer SSL-Sitzung geöffnet.

2 Akzeptieren Sie das Sicherheitszertifikat.

Hinweis Sie können das SSL-Zertifikat zur Authentifizierung verwenden. Weitere Informationen finden Sie im *vShield-Administratorhandbuch*.

Der Anmeldebildschirm von vShield Manager wird angezeigt.

3 Melden Sie sich bei vShield Manager-Benutzeroberfläche mit dem Benutzernamen **`admin`** und dem Kennwort **`default`** an.

Sie sollten das Standardkennwort baldmöglichst ändern, um dessen unbefugtem Gebrauch vorzubeugen. Siehe „Ändern des Kennworts für das Standardkonto der vShield Manager-Benutzeroberfläche“, auf Seite 22.

4 Klicken Sie auf **[Log In]** .

Synchronisieren von vShield Manager mit Ihrer vCenter Server-Instanz

Führen Sie die Synchronisierung mit Ihrer vCenter Server-Instanz durch, um Ihren VMware-Infrastrukturbestand in der vShield Manager-Benutzeroberfläche anzuzeigen.

Sie müssen über ein vCenter Server-Benutzerkonto mit Administratorzugriff verfügen, um diese Aufgabe auszuführen.

HINWEIS Die virtuelle vShield Manager-Maschine wird nicht als Ressource in der Bestandsliste der vShield Manager-Benutzeroberfläche angezeigt. Das Objekt **[Settings & Reports]** stellt die virtuelle vShield Manager-Maschine in der Bestandsliste dar.

Vorgehensweise

1 Melden Sie sich beim vShield Manager an.

2 Klicken Sie im vShield Manager-Bestandslistenbereich auf **[Settings & Reports]** .

3 Klicken Sie auf die Registerkarte **[Configuration]** .

4 Klicken Sie auf die Registerkarte **[vCenter]** .

5 Geben Sie die IP-Adresse oder den Hostnamen Ihrer vCenter Server-Instanz in das Feld **[IP address/Name]** ein.

6 Geben Sie Ihren Benutzernamen für die vSphere Client-Anmeldung in das Feld **[User Name]** ein.

7 Geben Sie das Kennwort für den Benutzernamen in das Feld **[Password]** ein.

8 Klicken Sie auf **[Save]** .

Registrieren des vShield Manager-Plug-Ins beim vSphere Client

Mit der Option **[vSphere Plug-In]** können Sie den vShield Manager als vSphere Client-Plug-In registrieren. Nachdem das Plug-In registriert wurde, können Sie die meisten vShield-Optionen vom vSphere Client aus konfigurieren.

Vorgehensweise

1 Klicken Sie im vShield Manager-Bestandslistenbereich auf **[Settings & Reports]** .

2 Klicken Sie auf die Registerkarte **[Configuration]** .

3 Klicken Sie auf **[vSphere Plug-in]** .

4 Klicken Sie auf **[Register]** .

5 Wenn Sie beim vSphere Client angemeldet sind, melden Sie sich ab.

6 Melden Sie sich beim vSphere Client an.

7 Wählen Sie einen ESX-Host aus.

8 Stellen Sie sicher, dass die Registerkarte **[vShield]** als Option angezeigt wird.

Ändern des Kennworts für das Standardkonto der vShield Manager-Benutzeroberfläche

Sie können das Kennwort des admin-Kontos ändern, um den Zugriff auf Ihren vShield Manager zu sichern.

Vorgehensweise

1 Melden Sie sich bei der vShield Manager-Benutzeroberfläche an.

2 Klicken Sie im vShield Manager-Bestandslistenbereich auf **[Settings & Reports]** .

3 Klicken Sie auf die Registerkarte **[Users]** .

4 Wählen Sie das Konto admin aus.

5 Klicken Sie auf **[Update User]** .

6 Geben Sie ein neues Kennwort ein.

7 Geben Sie das Kennwort für den Benutzernamen in das Feld **[Retype Password]** ein.

8 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Installieren von vShield Edge, vShield App, vShield Endpoint und vShield Data Security

4

Nach der Installation von vShield Manager können Sie Lizenzen erwerben, um vShield App, vShield Endpoint, vShield Edge und vShield Data Security zu aktivieren. Das vShield Manager OVA-Paket umfasst die Treiber und Dateien, die Sie zur Installation dieser Add-On-Komponenten benötigen. Eine vShield App-Lizenz ermöglicht Ihnen zudem die Verwendung der vShield Endpoint-Komponente.

Dieses Kapitel behandelt die folgenden Themen:

Ausführen von lizenzierten vShield-Komponenten im Testmodus

Bevor Sie Lizenzen für vShield Edge, vShield App oder vShield Endpoint kaufen und aktivieren, können Sie Evaluierungsmodi der Software installieren und ausführen. Wenn Sie einen Evaluierungsmodus ausführen, der für Demonstrations- und Evaluierungszwecke bestimmt ist, ist Ihre vShield Edge-, vShield App- und vShield Endpoint-Software direkt nach der Installation vollständig betriebsbereit, erfordert keine Lizenzierungskonfiguration und bietet für einen Zeitraum von 60 Tagen nach der ersten Aktivierung volle Funktionalität.

Bei der Ausführung im Evaluierungsmodus unterstützen vShield-Komponenten eine maximal zulässige Anzahl Instanzen.

Nach Ablauf des 60-tägigen Testzeitraums können Sie vShield nicht weiter verwenden, sofern Sie keine Lizenzen für die Software erwerben. Sie können zum Beispiel keine virtuellen vShield App- oder vShield Edge-Appliances aktivieren sowie Ihre virtuellen Maschinen nicht schützen.

Um die vShield App- und vShield Edge-Funktionalität ohne Unterbrechung weiter nutzen zu können oder die Funktionen wiederherzustellen, die nach Ablauf des 60-tägigen Testzeitraums nicht mehr verfügbar sind, müssen Sie Lizenzdateien erwerben und installieren, welche die Funktionen für die von Ihnen erworbene vShield-Komponente aktivieren.

Vorbereiten der virtuellen Infrastruktur für vShield App, vShield Edge, vShield Endpoint und vShield Data Security

Vor der Installation müssen Sie für die Add-On-Komponenten Ihre ESX-Host- und vNetwork-Umgebung vorbereiten. Sie installieren vShield App, vShield Endpoint und die vShield Data Security-Funktion auf ESX-Hosts. Sie installieren vShield Edge in einer Portgruppe, vNetwork Distributed Switch (vDS)-Portgruppe oder einem Cisco® Nexus 1000V-Switch.

Installieren von Lizenzen für vShield-Komponenten

Sie müssen Lizenzen für vShield Edge, vShield App und vShield Endpoint installieren, bevor Sie die Komponenten installieren. Sie können diese Lizenzen mit dem vSphere Client installieren, nachdem die Installation von vShield Manager abgeschlossen ist. Eine vShield App-Lizenz ermöglicht Ihnen zudem die Verwendung der vShield Endpoint-Komponente.

Vorgehensweise

1 Wählen Sie in einem Host des vSphere-Clients, der mit einem vCenter Server-System verbunden ist, die Option **[Home] > [Licensing]** .

2 Wählen Sie für die Berichtansicht **[Asset]** aus.

3 Klicken Sie mit der rechten Maustaste auf ein vShield-Asset und wählen Sie **[Change license key]** aus.

4 Wählen Sie **[Assign a new license key]** aus und klicken Sie auf **[Enter Key]** .

5 Geben Sie den Lizenzschlüssel und danach eine optionale Bezeichnung für den Schlüssel ein und klicken Sie auf **[OK]** .

6 Klicken Sie auf **[OK]** .

7 Wiederholen Sie diese Schritte für jede vShield-Komponente, für die Sie über eine Lizenz verfügen.

Vorbereitung aller ESX-Hosts

Sie sollten alle ESX-Hosts in Ihrer vCenter-Umgebung für die vShield-Add-On-Funktionalität vorbereiten.

Zur Vorbereitung von ESX-Hosts werden die folgenden Informationen benötigt:

- Eine IP-Adresse für den Management (MGMT)-Port jeder virtuellen vShield App-Appliance. Jede IP-Adresse muss vom vShield Manager aus erreichbar sein und sich in dem Managementnetzwerk befinden, das für die vCenter- und ESX-Host-Managementschnittstellen verwendet wird.
- Lokaler Speicherplatz oder Speicherplatz im Netzwerk für die vShield App.

Die virtuellen vShield-Appliances umfassen VMware Tools. Versuchen sie nicht, die VMware Tools-Software auf einer virtuellen vShield-Appliance zu verändern oder aufzurüsten.

Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wählen Sie einen ESX-Host aus der Bestandslistenstruktur aus.

3 Klicken Sie auf die Registerkarte **[vShield]** .

4 Akzeptieren Sie das Sicherheitszertifikat.

5 Klicken Sie für den **[vShield App]** -Dienst auf **[Install]** .

Auf dem nächsten Bildschirm können Sie alle drei Dienste installieren.

6 Geben Sie unter vShield App die folgenden Informationen ein.

Option	Beschreibung
[Datastore]	Wählen Sie den Datenspeicher aus, in dem die Dateien für die virtuelle vShield App-Maschine gespeichert werden sollen:
[Management Port Group]	Wählen Sie die Portgruppe aus, welche die Management-Schnittstelle von vShield App hosten soll. Diese Portgruppe muss in der Lage sein, die Portgruppe von vShield Manager zu erreichen.
[IP Address]	Geben Sie die IP-Adresse ein, die der Management-Schnittstelle von vShield App zugewiesen werden soll.

Option	Beschreibung
[Netmask]	Geben Sie die IP-Subnetzmaske für die zugewiesene IP-Adresse ein.
[Default Gateway]	Geben Sie die IP-Adresse des Standard-Netzwerkgateways ein.

7 Aktivieren Sie das Kontrollkästchen **[vShield Endpoint]** .

8 Klicken Sie im oberen Bereich des Formulars auf **[Install]** .

Sie können die Schritte für die Installation von vShield App im Fenster Recent Tasks des Bildschirms vSphere Client ausführen.

9 Wenn die Installation aller Komponenten abgeschlossen ist, gehen Sie folgendermaßen vor:

- vShield App: Die Installation von vShield App ist abgeschlossen. Wechseln Sie zur Registerkarte **[vShield App] > [App Firewall]** auf der Datencenter-, Cluster- oder Portgruppencontainer-Ebene, um Firewallregeln zu konfigurieren. Jede vShield App erbt globale Firewall-Regeln, die im vShield Manager festgelegt sind. Die Standard-Firewallregel gestattet jeglichen Datenverkehr. Sie müssen Blockierungsregeln festlegen, um Datenverkehr ausdrücklich zu blockieren. Erläuterungen zur Konfiguration von App Firewall-Regeln finden Sie im *vShield-Administratorhandbuch*.
- vShield Endpoint: Um die Installation abzuschließen, siehe „Installieren von vShield Endpoint“, auf Seite 28.
- vShield Data Security: Um die Installation abzuschließen, siehe „Installieren von vShield Data Security“, auf Seite 29.

Installieren einer vShield Edge-Instanz

Jede virtuelle vShield Edge-Appliance besitzt externe und interne Netzwerkschnittstellen. Die interne Schnittstelle wird mit der gesicherten Portgruppe verbunden und fungiert als Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Das Subnetz, das der internen Schnittstelle zugewiesen ist, kann ein privater RFC 1918-Raum sein. Die externe Schnittstelle auf der vShield Edge-Instanz wird mit einer Uplink-Portgruppe verbunden, die Zugriff auf ein freigegebenes Unternehmensnetzwerk oder einen freigegebenen Service bietet, der ein Zugriffslayer-Netzwerk bereitstellt.

Jede vShield Edge-Instanz erfordert mindestens eine IP-Adresse für die externe Schnittstelle. Mehrere externe IP-Adressen können für Load Balancer-, Site-to-Site VPN- und NAT-Dienste konfiguriert werden. Die interne Schnittstelle kann einen privaten IP-Adressenblock besitzen, der die IP-Adressen von weiteren gesicherten vShield Edge-Portgruppen überlappt.

Sie können eine vShield Edge-Instanz pro Portgruppe, vDS-Portgruppe oder Cisco® Nexus 1000V-Switch installieren.

Wenn DRS und HA aktiviert sind, wird eine vShield Edge-Instanz dynamisch migriert.

Vorgehensweise

1 Melden Sie sich beim vSphere Client an.

2 Navigieren Sie zu **[View] > [Inventory] > [Networking]** .

3 Erstellen Sie auf einem vDS eine Portgruppe.

Diese Portgruppe ist die interne Portgruppe.

4 Verschieben Sie die virtuellen Maschinen eines Tenant-Gastes in die interne Portgruppe.

5 Wählen Sie die neue interne Portgruppe aus.

6 Klicken Sie auf die Registerkarte **[Edge]** .

7 Geben Sie unter **[Network Interfaces]** die folgenden Informationen ein.

Option	Beschreibung
External	
Port Group	Wählen Sie die externe Portgruppe auf dem vDS aus. Diese Portgruppe beherbergt eine physische Netzwerkkarte und ist mit dem externen Netzwerk verbunden.
IP Address	Geben Sie die IP-Adresse der externen Portgruppe ein.
Subnet Mask	Geben Sie die IP-Subnetzmaske für die angegebene externe IP-Adresse ein.
Default Gateway	Geben Sie die IP-Adresse des Standard-Netzwerkgateways ein.
Intern	
Port Group	Dies ist die ausgewählte interne Portgruppe.
IP Address	Geben Sie die IP-Adresse der internen Portgruppe ein.
Subnet Mask	Geben Sie die IP-Subnetzmaske für die angegebene interne IP-Adresse ein.

8 Geben Sie unter **[Edge deployment resource selection]** die folgenden Informationen ein.

Option	Beschreibung
[Resource Pool]	Wählen Sie den Ressourcenpool aus, in dem die vShield Edge-Instanz bereitgestellt werden soll.
[Host]	Wählen Sie den ESX-Host aus, in dem sich der Datenspeicher befindet.
[Datastore]	Wählen Sie den Datenspeicher aus, in dem die Dateien für die virtuelle vShield Edge -Maschine gespeichert werden sollen.

9 Klicken Sie auf **[Install]** .

Nachdem die Installation abgeschlossen ist, konfigurieren Sie die Dienst- und Firewallregeln, um die virtuellen Maschinen in der gesicherten Portgruppe zu schützen. Erläuterungen zur Konfiguration von vShield Edge-Instanzen finden Sie im *vShield-Administratorhandbuch*.

Installieren von vShield Endpoint

Die folgenden Installationsanweisungen setzen voraus, dass Sie über folgendes System verfügen:

- Ein Datencenter mit unterstützten Versionen von vCenter Server und ESXi, die auf jedem ESX-Host im Cluster installiert sein müssen. Weitere Informationen zu den erforderlichen Versionen finden Sie unter Kapitel 2, „Vorbereitung für die Installation“, auf Seite 15.
- vShield Manager 5.0 ist installiert und wird ausgeführt.
- Ein Management-Server für eine Virenschutzlösung ist installiert und wird ausgeführt.

Installationsworkflow für vShield Endpoint

Nachdem die Vorbereitung des ESX-Hosts für die vShield Endpoint-Installation abgeschlossen ist, installieren Sie vShield Endpoint in folgenden Schritten:

1 Stellen Sie eine sichere virtuelle Maschine (SVM) für jeden ESX-Host bereit und konfigurieren Sie sie gemäß den Anweisungen des Anbieters der Virenschutzlösung.

2 Installieren Sie VMware Tools 8.6.0, das mit ESXi 5.0 Patch 1 ausgeliefert wird, auf allen virtuellen Maschinen, die geschützt werden sollen.

Installieren von VMware Tools auf der virtuellen Gastmaschine

VMware Tools muss auf jeder virtuellen Gastmaschine installiert sein, damit diese geschützt wird. Virtuelle Maschinen, auf denen VMware Tools installiert ist, werden automatisch geschützt, wenn sie auf einem ESX-Host gestartet werden, auf dem die Sicherheitslösung installiert ist. Das bedeutet, dass geschützte virtuelle Maschinen den Sicherheitsschutz auch nach dem Herunterfahren und Neustarten und sogar nach einer vMotion-Verschiebung auf einen anderen ESX-Host, auf dem die Sicherheitslösung installiert ist, behalten.

Voraussetzungen

- Stellen Sie sicher, dass auf der virtuellen Gastmaschine eine unterstützte Version von Windows installiert ist. vShield Endpoint 5.0 unterstützt folgende Versionen von Windows-Betriebssystemen:
  - Windows Vista (32-Bit)
  - Windows 7 (32/64-Bit)
  - Windows XP (32-Bit)
  - Windows 2003 (32/64-Bit)
  - Windows 2003 R2 (32/64-Bit)
  - Windows 2008 (32/64-Bit)
  - Windows 2008 R2 (64-Bit)

Vorgehensweise

1. Das Installationspaket befindet sich auf der VMware-Kundensite, von der Sie ESXi 5.0 Patch 1 heruntergeladen haben.
2. Laden Sie das Installationspaket auf Ihren PC herunter und führen Sie es aus.
3. Öffnen Sie ein Konsolenfenster auf der virtuellen Gastmaschine.
4. Klicken Sie auf **[CD/DVD drive 1] > [Connect to ISO image on local disk]** .
5. Klicken Sie auf **[Browse]** , um den Ordner auf Ihrem PC zu suchen, der die ISO-Datei von VMware Tools enthält.
6. Schließen Sie den Assistenten ab. Wenn Sie eine benutzerdefinierte Installation durchführen möchten, müssen Sie die zu installierenden vShield-Treiber auswählen.

   VMware Tools muss auf jeder virtuellen Gastmaschine installiert sein, damit diese geschützt wird.

Die vShield Endpoint-Hostkomponente fügt dem ESX-Host zwei Firewallregeln hinzu:

- Die vShield-Endpoint-Mux-Regel öffnet die Ports 48651 bis 48666 für die Kommunikation zwischen der Hostkomponente und den Partnersicherheits-VMs.
- Anhand der vShield-Endpoint-Mux-Partnerregel können Partner eine Hostkomponente installieren. Sie ist standardmäßig deaktiviert.

Installieren von vShield Data Security

Sie können vShield Data Security erst nach der Installation von vShield Endpoint installieren.

Voraussetzungen

Stellen Sie sicher, dass vShield Endpoint auf dem Host und den virtuellen Gastmaschinen installiert wurde.

Vorgehensweise

1. Melden Sie sich beim vSphere-Client an.

2 Wählen Sie einen ESX-Host aus der Bestandslistenstruktur aus.

3 Klicken Sie auf die Registerkarte **[vShield]** .

4 Klicken Sie auf **[Install]** neben vShield Data Security.

5 Aktivieren Sie das Kontrollkästchen **[vShield Data Security]** .

6 Geben Sie unter vShield Data Security die folgenden Informationen ein.

Option	Beschreibung
[Datastore]	Wählen Sie den Datenspeicher aus, dem die virtuelle vShield Data Security-Maschine hinzugefügt werden soll.
[Management Port Group]	Wählen Sie die Portgruppe aus, die die Verwaltungsschnittstelle von vShield Data Security hosten soll. Diese Portgruppe muss in der Lage sein, die Portgruppe von vShield Manager zu erreichen.
[Control IP]	vShield füllt dies automatisch aus.

7 Um eine statische IP-Adresse zu konfigurieren, aktivieren Sie das Kontrollkästchen **[Configure static IP for management interface]** .

Geben Sie unter **[IP address]** , **[Netmask]** und **[Default Gateway]** die entsprechenden Details ein.

HINWEIS Wenn Sie die Option **[Configure static IP for management interface]** nicht auswählen, wird über DHCP eine IP-Adresse zugewiesen.

8 Klicken Sie auf **[Install]** .

Die virtuelle vShield Data Security-Maschine ist auf dem ausgewählten Host installiert.

Aktualisieren von vShield 5

Um vShield zu aktualisieren, müssen Sie zuerst ein Upgrade von vShield Manager und dann der anderen Komponenten durchführen, für die Sie über eine Lizenz verfügen.

Dieses Kapitel behandelt die folgenden Themen:

Upgrade von vShield Manager

Sie können vShield Manager nur von der vShield Manager-Benutzeroberfläche aus auf eine neue Version aktualisieren. Sie können vShield App, vShield Edge und vShield Endpoint von der vShield Manager-Benutzeroberfläche aus oder unter Verwendung von REST APIs auf eine neue Version aktualisieren.

Vorgehensweise

1. Laden Sie das vShield-Upgrade-Paket an einen Speicherort herunter, auf den vShield Manager zugreifen kann.

   Der Name des Upgrade-Pakets lautet in etwa `VMware-vShield-Manager-upgrade_bundle-`*`Build-Nummer`*`.tar.gz.`
2. Klicken Sie im vShield Manager-Bestandslistenbereich auf **[Settings & Reports]** .
3. Klicken Sie auf die Registerkarte **[Updates]** .
4. Klicken Sie auf **[Upload Settings]** .
5. Klicken Sie auf **[Browse]** und wählen Sie die Datei `VMware-vShield-Manager-upgrade_bundle-`*`Build-Nummer`*`.tar.gz.` aus.
6. Klicken Sie auf **[Open.]**
7. Klicken Sie auf **[Upload File]** .
8. Klicken Sie auf **[Install]** , um mit dem Upgrade zu beginnen.
9. Klicken Sie auf **[Confirm Install]** .

   Der Upgrade-Vorgang startet vShield Manager neu, d. h., die Verbindung zur vShield Manager-Benutzeroberfläche geht möglicherweise verloren. Keine der anderen vShield-Komponenten wird neu gestartet.

10 Klicken Sie mit der rechten Maustaste auf die virtuelle vShield Manager-Maschine und klicken Sie auf **[Open Console]** , um die Befehlszeilenschnittstelle (CLI) von vShield Manager zu öffnen.

11 Wenn Sie die Meldung **[e1000_watchdog_task: NIC Link is up]** sehen, melden Sie sich bei der vShield Manager-Benutzerschnittstelle an.

12 Klicken Sie auf die Registerkarte **[Updates]** .

Im Bereich „Installed Release“ wird die Build-Nummer der vShield-Version angezeigt, die Sie gerade installiert haben.

Weiter

Starten Sie den vSphere-Client neu.

Upgrade von vShield App

Aktualisieren Sie vShield App auf jedem Host Ihres Datencenters.

Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wechseln Sie zu **[Bestandsliste] > [Hosts und Cluster]** .

3 Wählen Sie den Host aus, auf dem Sie ein Upgrade von vShield App durchführen möchten.

Die Registerkarte **[Summary]** zeigt jede vShield-Komponente, die auf dem ausgewählten Host installiert ist, und die verfügbare Version an.

4 Wählen Sie **[Update]** neben vShield App.

5 Aktivieren Sie das Kontrollkästchen **[vShield App]** .

6 Klicken Sie auf **[Install]** .

Upgrade von vShield Edge

Aktualisieren Sie vShield Edge auf jeder Portgruppe in Ihrem Datencenter.

Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Navigieren Sie zu **[Ansichten] > [Bestandsliste] > [Netzwerk]** .

3 Klicken Sie auf die Registerkarte **[vShield Edge]** .

4 Klicken Sie auf **[Upgrade]** .

5 Wählen Sie **[vShield Edge]** .

6 Klicken Sie auf **[Install]** .

Upgrade von vShield Endpoint

Um ein Upgrade von vShield Endpoint auf eine neuere Version durchzuführen, müssen Sie zuerst vShield Endpoint auf jedem Host in Ihrem Datencenter deinstallieren und dann die neue Version installieren.

Informationen zum Deinstallieren von vShield Endpoint finden Sie im Modul „Deinstallieren eines vShield Endpoint-Moduls“ im *vShield-Administratorhandbuch*.

Informationen zum Installieren von vShield Endpoint finden Sie unter „Installieren von vShield Endpoint“, auf Seite 28.

Upgrade von vShield Data Security

Führen Sie auf jedem Host Ihres Datencenters ein Upgrade von vShield Data Security durch.

Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wechseln Sie zu **[Bestandsliste] > [Hosts und Cluster]** .

3 Wählen Sie den Host aus, auf dem Sie ein Upgrade von vShield App durchführen möchten.

Die Registerkarte **[Summary]** zeigt jede vShield-Komponente, die auf dem ausgewählten Host installiert ist, und die verfügbare Version an.

4 Wählen Sie **[Update]** neben vShield Data Security.

5 Aktivieren Sie das Kontrollkästchen **[vShield Data Security]** .

6 Klicken Sie auf **[Install]** .

Index