# Installations- und Upgrade-Handbuch für vShield

vShield Manager 5.5
vShield Edge 5.5
vShield Endpoint 5.5

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-001281-00

vmware®

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

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

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 5

**1** Einführung zu vShield 7
- vShield-Komponenten im Überblick 7
- Bereitstellungsszenarien 10

**2** Vorbereitung für die Installation 13
- Systemanforderungen 13
- Erwägungen zur Bereitstellung 14

**3** Installieren von vShield Manager 19
- Abrufen der vShield Manager OVA-Datei 19
- Installieren der virtuellen Appliance vShield Manager 19
- Anmelden bei der vShield Manager-Benutzeroberfläche 20
- Einrichten von vShield Manager 21
- Ändern des Kennworts für das Standardkonto der vShield Manager-Benutzeroberfläche 22
- Planen einer Sicherung von vShield Manager-Daten 23

**4** Installieren von vShield Edge, vShield App, vShield Endpoint und vShield Data Security 25
- Ausführen von lizenzierten vShield-Komponenten im Testmodus 25
- Installieren von Lizenzen für vShield-Komponenten 26
- Installieren von vShield App 26
- Installieren von vShield Edge 28
- Installieren von vShield Endpoint 34
- Installieren von vShield Data Security 35

**5** Deinstallieren von vShield-Komponenten 37
- Deinstallieren einer virtuellen vShield App-Appliance 37
- Deinstallieren von vShield Edge 38
- Deinstallieren einer virtuellen vShield Data Security-Maschine 38
- Deinstallieren eines vShield Endpoint-Moduls 38

**6** Aktualisieren von vShield 41
- Upgrade von vShield Manager 41
- Upgrade von vShield App 47
- Upgrade vShield Edge from 5.0.x to 5.5 47
- Upgrade von vShield Endpoint 48
- Upgrade von vShield Data Security 49

**7** Beheben von Installationsproblemen 51
Installation von vShield App schlägt fehl 51
Installation von vShield Data Security schlägt fehl 52

Index 53

# Über dieses Handbuch

In diesem Handbuch, dem *Installations- und Upgrade-Handbuch für vShield*, wird beschrieben, wie mithilfe der vShield Manager-Benutzeroberfläche, des vSphere-Client-Plug-Ins und der Befehlszeilenschnittstelle (CLI) das VMware® vShield™-System installiert und konfiguriert wird. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen 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 5.x, einschließlich VMware ESX, vCenter Server und dem vSphere-Client, vertraut sind.

## VMware Technical Publications - Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt 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 Vorschläge zum Verbessern der Dokumentation. Falls Sie Anmerkungen haben, senden Sie diese bitte 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 weiterer 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 Support-Verträgen erhalten über den telefonischen Support 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 Praxisübungen, Fallbeispiele und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Kurse können vor Ort, im Unterrichtsraum und live online durchgeführt werden. 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“, auf Seite 7
- „Bereitstellungsszenarien“, auf Seite 10


## 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 und unterstützt Sie beim Erreichen Ihrer Compliance-Zielsetzungen.

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 eine einzelne vCenter Server-Umgebung und mehrere vShield App-, vShield Edge-, vShield Endpoint- und vShield Data Security-Instanzen.

### 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 diese Informationen zum Überprüfen des Netzwerkverkehrs, zum Definieren und zum Verfeinern von Firewallrichtlinien und zum Identifizieren von Netzwerkbedrohungen verwenden.

## vShield Edge

vShield Edge bietet Netzwerk-Edge-Sicherheits- und Gateway-Dienste, um ein virtualisiertes Netzwerk oder virtuelle Maschinen in einer Portgruppe, einer vDS-Portgruppe oder einer Cisco Nexus 1000V-Portgruppe zu isolieren. Sie installieren eine vShield Edge-Instanz auf Datencenterebene und können bis zu zehn interne oder Uplink-Schnittstellen hinzufügen. 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)

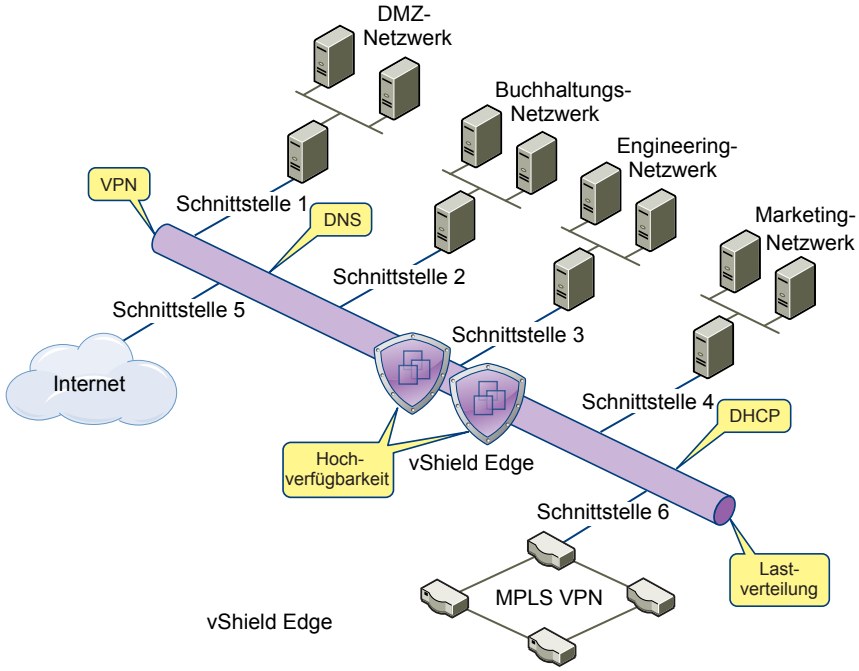
| | |
|---|---|
| **Firewall** | Die unterstützten Regeln umfassen die IP 5-tuple-Konfiguration mit IP- und Portbereichen für die statusbehaftete Inspektion für alle Protokolle. |
| **Netzwerkadressübersetzung (NAT)** | Separate Steuerelemente für Quell- und Ziel-IP-Adressen sowie Portübersetzung. |
| **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 VPN-Anbietern. |
| **SSL VPN-Plus** | SSL VPN-Plus ermöglicht Remotebenutzern die sichere Verbindung mit privaten Netzwerken hinter einem vShield Edge-Gateway. |
| **Lastausgleich** | Einfach und dynamisch konfigurierbare IP-Adressen und Servergruppen. |
| **High Availability** | High Availability stellt für den Fall, dass die primäre virtuelle vShield Edge-Maschine nicht zur Verfügung steht, sicher, dass eine aktive vShield Edge-Instanz im Netzwerk verfügbar ist. |

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

**Abbildung 1-1.** Multi-Interface Edge

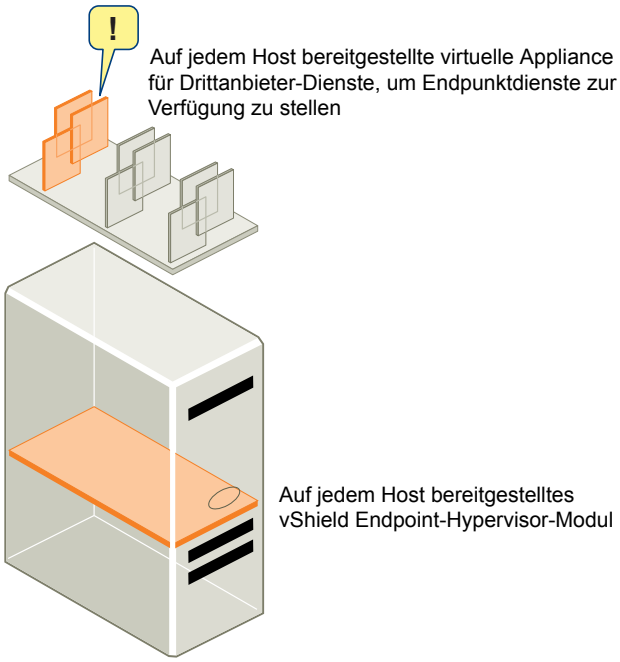



## vShield Endpoint

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

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.

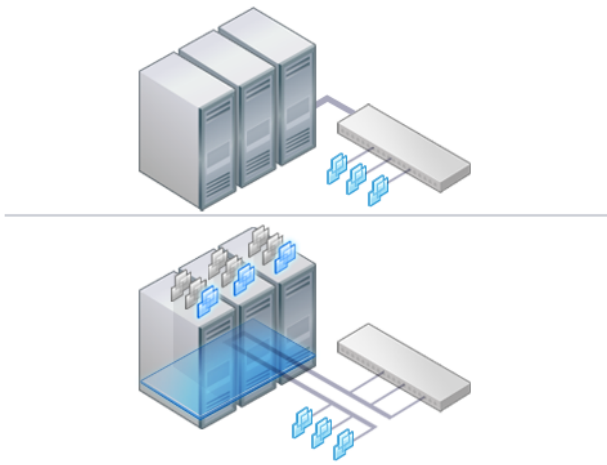
Sie verwenden z.B. VLANs, um virtuelle Maschinenzonen auf Basis von logischen, organisatorischen oder Netzwerkbegrenzungen zu segmentieren. Auf Grundlage des Virtual Infrastructure SDK zeigt die Bestandsliste von vShield Manager eine Ansicht Ihrer VLAN-Netzwerke in der Netzwerkansicht an. Sie können 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 eine erfolgreiche vShield-Installation.

Dieses Kapitel behandelt die folgenden Themen:


- „Systemanforderungen“, auf Seite 13
- „Erwägungen zur Bereitstellung“, auf Seite 14


## 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 mehrere vShield Edge-Instanzen pro Datencenter installieren.

### Hardware

**Tabelle 2-1.** Hardwareanforderungen

| Komponente | Minimal |
|---|---|
| Arbeitsspeicher | ■ vShield Manager: 8GB zugeteilt, 3GB reserviert<br>■ vShield App: 1GB zugeteilt, 1 GB reserviert<br>■ vShield Edge Compact: 256 MB, Large und Quad Large: 1 GB, X-Large: 8 GB<br>■ vShield Data Security: 512 MB |
| Festplattenspeicher | ■ vShield Manager: 60 GB<br>■ vShield App: 5 GB pro vShield App pro ESX-Host<br>■ vShield Edge Compact: 300 MB, Large, Quad Large und X-Large: 448 MB<br>■ vShield Data Security: 6 GB pro ESX-Host |
| vCPU | ■ vShield Manager: 2<br>■ vShield App: 2<br>■ vShield Edge Compact: 1, Large: 2, Quad Large und X-Large: 4<br>■ vShield Data Security: 1 |

### Software

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

Dies sind die mindestens erforderlichen Versionen der VMware-Produkte.

- VMware vCenter Server 5.0 oder höher

  Für virtuelle VXLAN-Leitungen benötigen Sie vCenter Server 5.1 oder höher.

- VMware ESX 5.1 oder höher für jeden Server

  Für virtuelle VXLAN-Leitungen benötigen Sie VMware ESX 5.1 oder höher.

- 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 3 mitgeliefert wird. Weitere Informationen hierzu finden Sie unter „Installieren von VMware Tools auf virtuellen Gastmaschinen“, auf Seite 34.

  Sie müssen auf den virtuellen Maschinen, die von vShield App geschützt werden sollen, VMware Tools installieren.

- VMware vCloud Director 5.1 oder höher

### Client- und Benutzerzugriff

- PC mit dem VMware vSphere Client
- Wenn Sie der vSphere-Bestandsliste ESX-Hosts nach Namen hinzugefügt haben, stellen Sie sicher, dass mit vShield Manager DNS-Server konfiguriert wurden und dass die Namensauflösung funktioniert. Anderenfalls kann vShield Manager die IP-Adressen nicht auflösen.
- 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
- vShield Manager-Port 443 ist vom ESX-Host, von vCenter Server und den bereitzustellenden vShield-Appliances aus erreichbar. Dieser Port wird zum Herunterladen der OVF-Datei auf dem ESX-Host für die Bereitstellung benötigt.
- 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.

## Überlegungen zur Bereitstellung von vShield

Dieses Thema befasst sich mit Überlegungen zur Bereitstellung von vShield-Komponenten.

### 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 DRS-Clusters 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 DRS-Cluster vorbereitet sind, können Sie Maschinen zwischen Hosts migrieren, ohne die Sicherheit zu gefährden. Informationen zum Vorbereiten Ihrer ESX-Hosts finden Sie unter „Installieren von vShield App“, 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, zum ESXi-Host, 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.

Es wird empfohlen, dass Sie vShield Manager auf einem dedizierten Verwaltungs-Cluster und getrennt von den Clustern, die vShield Manager verwaltet, installieren. Jeder vShield Manager verwaltet eine einzelne vCenter Server-Umgebung.

Wenn sich der vCenter Server oder die virtuellen Maschinen der vCenter Server-Datenbank auf dem ESX-Host befinden, auf dem Sie die vShield App installieren, migrieren Sie diese vor der Installation der vShield App auf einen anderen Host.

Stellen Sie sicher, dass die folgenden Ports geöffnet sind:

- Port 443/TCP von, zu und zwischen dem ESX-Host, vCenter Server und vShield Data Security
- UDP123 zwischen vShield Manager und vShield App für die Uhrzeitsynchronisierung
- 443/TCP vom REST-Client zum vShield Manager für REST API-Aufrufe
- 80/TCP und 443/TCP für die Verwendung der vShield Manager-Benutzeroberfläche und die Initiierung der Verbindung zum vSphere SDK
- 22/TCP für die Verbindung zwischen vShield Manager und vShield App sowie für die Fehlersuche beim CLI

### 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

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*.

## Überlegungen zur Bereitstellung von vShield App

Es wird empfohlen, Ihre vCenter Server-Umgebung zu analysieren und zu ermitteln, ob Sie die gesamte Umgebung oder nur bestimmte Cluster schützen möchten.

Wenn Sie nur bestimmte Cluster schützen möchten, müssen Sie den gesamten Cluster vorbereiten und vShield App auf allen ESX-Hosts in diesen Clustern installieren. Wenn Sie vShield App nur auf einigen Hosts in einem Cluster installieren, besteht die Möglichkeit, dass vMotion virtuelle Maschinen von einem geschützten auf einen nicht geschützten Host verschiebt, was die Sicherheit Ihres Netzwerks beeinträchtigt.

Stellen Sie sicher, dass Sie im Rahmen geplanter Wartungsarbeiten vShield App in Ihrer Umgebung installieren. Die Installationsdauer kann sich je nach Umgebung und der Anzahl der Hosts in jedem Cluster unterscheiden. Sie müssen vor Wiederaufnahme des normalen Betriebs die Installation von vShield App auf allen vorgesehenen Clustern abgeschlossen haben.

Nach der Installation wird empfohlen, dass Sie vSphere HA aktivieren und für die Cluster, in denen Sie vShield App installiert haben, die Clusterfunktion auf **[VM- und Anwendungsüberwachung]** festlegen. Diese Funktion überwacht die vShield App und löst einen Neustart aus, falls sie fehlschlägt, was die Ausfälle der vShield App minimiert. Weitere Informationen zu dieser Funktion finden Sie unter *vSphere-Verfügbarkeit*.

Es wird empfohlen, während des normalen Betriebs vShield App auszuführen und das Flow Monitoring-Tool der vShield App zu verwenden, um Baseline-Informationen über den ein- und ausgehenden Datenverkehr Ihres virtuellen Netzwerks zu erhalten. Anschließend können Sie anhand der Anforderungen Ihres Netzwerks Regeln hinzufügen.

Durch das Aktivieren der SpoofGuard-Funktion von vShield App können Sie die von den VMware Tools gemeldeten IP-Adressen autorisieren und diese bei Bedarf ändern, um Manipulationen (Spoofing) zu verhindern. Je nach dem von Ihnen ausgewählten SpoofGuard-Modus vertraut vShield App entweder IP-Zuweisungen bei deren ersten Verwendung automatisch oder Sie müssen IP-Zuweisungen vor deren Erstverwendung manuell genehmigen. Beachten Sie jedoch, dass sich die IP-Adresse einer virtuellen Maschine ändern kann, wenn der DHCP-Server die Lease verlängert oder neu gestartet wird. Dies bedeutet, dass Sie die neue oder erneuerte IP-Adresse genehmigen müssen, wenn die SpoofGuard-Funktion aktiviert ist.

Wenn Sie sich mit den Flow Monitoring- und SpoofGuard-Funktionen vertraut machen, bevor Sie vShield App installieren, können Sie beim Konfigurieren von vShield App die höchste Sicherheit erzielen. Weitere Informationen zu diesen Funktionen finden Sie im *vShield-Administratorhandbuch*.

## Überlegungen zur Bereitstellung von vShield Edge

Vor der Installation von vShield Edge müssen Sie sich mit Ihrer Netzwerktopologie vertraut machen. vShield Edge kann mehrere Schnittstellen haben, aber Sie müssen mindestens eine interne Schnittstelle mit einer Portgruppe oder einer virtuellen VXLAN-Leitung verbinden, bevor Sie die vShield Edge-Instanz bereitstellen können.

Die Uplink-Schnittstelle bietet Konnektivität nach außen. Sie müssen eine Portgruppe oder virtuelle VXLAN-Leitung mit externer Konnektivität erstellt und konfiguriert haben. Sie müssen auch über eine Portgruppe mit virtuellen Maschinen verfügen, mit der Sie die interne Schnittstelle verbinden können. Legen Sie die IP-Adressen und Subnetze fest, die für diese Schnittstellen gelten sollen. Bedenken Sie zudem die Dienste, die Sie nach dem Installieren von vShield Edge aktivieren und konfigurieren müssen. Weitere Informationen über die vShield Edge-Dienste finden Sie im *vShield-Administratorhandbuch*.

Nach dem Installieren von vShield Edge und vor dem Konfigurieren der vShield Edge-Dienste werden die Netzwerkverbindungen der virtuellen Maschinen in diesen Portgruppen möglicherweise unterbrochen. Um dieses Problem zu vermeiden, können Sie eine neue Portgruppe erstellen, vShield Edge darauf installieren und konfigurieren und anschließend die virtuellen Maschinen in die Portgruppe verschieben.

Beachten Sie, dass die standardmäßige vShield Edge-Firewallrichtlinie den gesamten eingehenden Datenverkehr blockiert, sodass Sie Regeln für das Zulassen des gewünschten Datenverkehrs hinzufügen müssen.

# 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.

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“, auf Seite 19
- „Installieren der virtuellen Appliance vShield Manager“, auf Seite 19
- „Anmelden bei der vShield Manager-Benutzeroberfläche“, auf Seite 20
- „Einrichten von vShield Manager“, auf Seite 21
- „Ändern des Kennworts für das Standardkonto der vShield Manager-Benutzeroberfläche“, auf Seite 22
- „Planen einer Sicherung von vShield Manager-Daten“, auf Seite 23


## 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.

Mit vShield 5.0 und höher können Sie vShield Manager in einem anderen vCenter als dem installieren, mit dem vShield Manager interagiert. 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.

### Voraussetzungen

Ihnen muss die Rolle „Enterprise Administrator“ oder „vShield Administrator“ zugewiesen worden sein.

### Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

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

Die vShield Manager-Verwaltungsschnittstelle, vCenter Server und ESXi-Hosts müssen für alle künftigen vShield Edge-, vShield App- und vShield Endpoint-Instanzen erreichbar sein.

3 Wählen Sie **[Datei] > [OVF-Vorlage bereitstellen]** .

4 Klicken Sie auf **[Browse]** , um den Ordner auf Ihrem PC auszuwählen, der die vShield Manager-OVA-Datei enthält.

5 Führen Sie die Installation durch.

vShield Manager wird als virtuelle Maschine in Ihrer Bestandsliste installiert.

6 Schalten Sie die virtuelle vShield Manager-Maschine ein.

### Weiter

Die Standard-CPU für vShield Manager 5.1 ist „2 vCPU“. Damit vShield Manager mit vSphere Fault Tolerance arbeiten kann, müssen Sie die CPU auf „1 vCPU“ festlegen.

## 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 mithilfe von SSL in einem Webbrowser-Fenster 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]** .

# Einrichten von vShield Manager

Geben Sie die Details zum vCenter Server, dem DNS- und dem NTP-Server sowie zum Lookup-Server an.

---

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

---

### Voraussetzungen

- Sie benötigen ein vCenter Server-Benutzerkonto mit Administratorzugriff, um vShield Manager mit vCenter Server synchronisieren zu können. Falls ihr vCenter-Kennwort Nicht-ASCII-Zeichen enthält, müssen Sie es ändern, bevor Sie vShield Manager mit vCenter Server synchronisieren.
- Sie benötigen zum Verwenden von SSO auf vShield Manager vCenter Server 5.1 oder höher und der Single Sign On-Dienst muss auf dem vCenter Server installiert sein.

### 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 **[Konfiguration]** .

4 Im Bereich **[DNS Servers]** werden die IP-Adressen der DNS-Server angezeigt, die Sie bei der Konfiguration der Netzwerkeinstellungen von vShield Manager angegeben haben.

   Falls erforderlich, können Sie die Server bearbeiten.

5 Klicken Sie unter **[NTP Server]** auf **[Edit]** und geben Sie die IP-Adresse Ihres NTP-Servers ein.

   Der NTP-Server legt eine einheitliche Uhrzeit für das Netzwerk fest. Es wird empfohlen, denselben NTP-Server zu verwenden, den der SSO-Server verwendet, sodass die Uhrzeit auf dem vShield Manager-Server mit der des NTP-Servers synchron ist.

   ---

   **WICHTIG** Sie müssen den vShield Manager nach dem Bearbeiten der NTP-Server-Daten neu starten.

   ---

6 Klicken Sie unter **[Lookup Service]** auf **[Edit]** und geben Sie den Hostnamen oder die IP-Adresse des Hosts ein, auf dem der Lookup-Dienst läuft.

7 Ändern Sie die Portnummer, falls erforderlich.

   Die URL des Lookup Service wird basierend auf dem angegebenen Host und Port angezeigt.

8 Geben Sie den SSO-Benutzernamen und das Kennwort ein.

   Damit kann vShield Manager sich selbst auf dem Security Token Service-Server registrieren.

9 Geben Sie im Feld **[vCenter Server]** die IP-Adresse oder den Hostnamen von Ihrem vCenter Server ein.

10 Geben Sie den Benutzernamen ein, der bei der Anmeldung zum vSphere-Client verwendet wird.

11 Geben Sie das entsprechende Kennwort für den angegebenen Benutzernamen ein.

12 Um dem angemeldeten Benutzer die Rolle „Enterprise Administrator“ zuzuweisen, wählen Sie **[Assign vShield Enterprise Administrator role to this user]** .

   Mit dieser Rolle erhält der Benutzer vShield-Berechtigungen für den Betrieb und die Sicherheit.

13 Wählen Sie zum Ändern des Speicherorts für Downloads von Plug-In-Skripts die Option **[Modify plug-in script download location]** und geben Sie die IP-Adresse und die Portnummer von vShield Manager ein.

   Dies ist möglicherweise für NAT-Umgebungen erforderlich. Die Standardadresse für vShield Manager lautet `vShield_Manager_IP:443`.

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

15 (Optional) Führen Sie auf einem Windows-Servercomputer die folgenden Schritte durch, um den Bestandslistenbereich von vShield Manager zu laden:

   a Öffnen Sie Internet Explorer.

   b Wählen Sie **[Extras] > [Internetoptionen]** .

   c Wählen Sie die Registerkarte **[Sicherheit]** .

   d Klicken Sie auf **[Vertrauenswürdige Sites]** .

   e Klicken Sie auf **[Sites]** .

   f Geben Sie die IP-Adresse von vShield Manager ein und klicken Sie auf **[Hinzufügen]** .

   g Klicken Sie auf **[Schließen]** .

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

   i Schließen Sie Internet Explorer.

vShield Manager stellt eine Verbindung mit vCenter Server her, meldet sich an und verwendet das VMware Infrastructure-SDK zum Auffüllen des vShield Manager-Bestandslistenbereichs. Der Bestandslistenbereich wird im linken Bildschirmbereich angezeigt. Diese Ressourcenstruktur sollte mit Ihrem VMware Infrastructure-Bestandslistenbereich übereinstimmen. vShield Manager erscheint nicht im vShield Manager-Bestandslistenbereich.

### Weiter

Melden Sie sich beim vSphere-Client an, wählen Sie einen ESX-Host aus und vergewissern Sie sich, dass vShield als Registerkarte angezeigt wird. Anschließend können Sie vShield-Komponenten vom vSphere-Client aus installieren und konfigurieren.

## 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 auf **[Change Password]** in der oberen rechten Ecke des Fensters.

3 Geben Sie im Feld **[Old password]** das aktuelle Kennwort **`default`** ein.

4 Geben Sie ein neues Kennwort ein.

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

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

# Planen einer Sicherung von vShield Manager-Daten

Sie können zu jedem Zeitpunkt jeweils nur die Parameter für einen Sicherungstyp planen. Es ist nicht möglich, zwei Sicherungen für eine gleichzeitige Ausführung zu planen, bei denen einmal nur Konfigurationsdaten und einmal die vollständigen Daten gesichert werden.

### Vorgehensweise

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

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

3 Klicken Sie auf **[Backups]** .

4 Wählen Sie im Dropdown-Menü **[Scheduled Backups]** die Option **[On]** .

5 Wählen Sie im Dropdown-Menü **[Backup Frequency]** die Option **[Hourly]** , **[Daily]** oder **[Weekly]** .

   Je nach ausgewählter Häufigkeit werden die Dropdown-Menüs **[Day of Week]** , **[Hour of Day]** und **[Minute]** deaktiviert. Wenn Sie beispielsweise **[Daily]** auswählen, wird das Dropdown-Menü **[Day of Week]** deaktiviert, da dieses Feld bei einer täglichen Sicherung nicht zum Tragen kommt.

6 (Optional) Aktivieren Sie das Kontrollkästchen **[Exclude System Events]** , wenn Sie die Systemereignistabellen nicht sichern möchten.

7 (Optional) Aktivieren Sie das Kontrollkästchen **[Exclude Audit Log]** , wenn Sie die Überwachungsprotokolltabellen nicht sichern möchten.

8 Geben Sie in **[Host IP Address]** die Host-IP-Adresse des Systems ein, auf dem die Sicherung gespeichert wird.

9 (Optional) Geben Sie in **[Host Name]** den Hostnamen des Sicherungssystems ein.

10 Geben Sie in **[User Name]** den erforderlichen Benutzernamen zur Anmeldung beim Sicherungssystem ein.

11 Geben Sie in **[Password]** das dem Benutzernamen für das Sicherungssystem zugeordnete Kennwort ein.

12 Geben Sie im Feld **[Backup Directory]** den absoluten Pfad zu dem Verzeichnis ein, in dem die Sicherungen gespeichert werden sollen.

13 Geben Sie in **[Filename Prefix]** eine als Präfix für den Dateinamen zu verwendende Textzeichenfolge ein.

   Dieser Text wird jedem Sicherungsdateinamen vorangestellt, um eine leichte Identifizierung auf dem Sicherungssystem zu ermöglichen. Wenn Sie beispielsweise **ppdb** als Präfix verwenden, lautet der Sicherungsname `ppdbHH_MM_SS_TagTTMonJJJJ`.

14 Wählen Sie im Dropdown-Menü **[Transfer Protocol]** basierend auf der Unterstützung durch das Zielsystem entweder das Protokoll **[SFTP]** oder das Protokoll **[FTP]** aus.

15 Klicken Sie auf **[Save Settings]** .

# 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.

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

Dieses Kapitel behandelt die folgenden Themen:


- „Ausführen von lizenzierten vShield-Komponenten im Testmodus“, auf Seite 25
- „Installieren von Lizenzen für vShield-Komponenten“, auf Seite 26
- „Installieren von vShield App“, auf Seite 26
- „Installieren von vShield Edge“, auf Seite 28
- „Installieren von vShield Endpoint“, auf Seite 34
- „Installieren von vShield Data Security“, auf Seite 35


## Ausführen von lizenzierten vShield-Komponenten im Testmodus

Bevor Sie Ihre Lizenzen für vShield Edge, vShield App und vShield Endpoint erwerben und aktivieren, können Sie Testversionen 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.

# Installieren von Lizenzen für vShield-Komponenten

Sie müssen vor der Installation von vShield App und vShield Edge eine CIS-Lizenz oder eine vCNS-Lizenz (vCloud Networking and Security) installieren. Die vSphere-Lizenz beinhaltet eine Lizenz für vShield Endpoint. Sie können diese Lizenzen mit dem vSphere-Client installieren, nachdem die Installation von vShield Manager abgeschlossen ist.

### 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 auf der Registerkarte „Management“ die Option **[Asset]** .

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

4 Wählen Sie **[Einen neuen Lizenzschlüssel zuweisen]** und klicken Sie auf **[Schlüssel eingeben]** .

5 Geben Sie den Lizenzschlüssel und 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.

# Installieren von vShield App

Sie können vShield App auf einem ESX-Host installieren.

---

**Hinweis** Die Netzwerkverbindung einer virtuellen Maschine wird unterbrochen, wenn Sie sie mit vShield App schützen. Falls vCenter Server auf einer virtuellen Maschine ausgeführt und seine Verbindung zum Netzwerk getrennt wird, wird der vShield App-Installationsvorgang möglicherweise ohne abzuschließen angehalten. Es wird empfohlen, vCenter Server, die vCenter Server-Datenbank und virtuelle Maschinen von Drittanbietern oder interne virtuelle Dienstmaschinen, die Sie nicht schützen möchten, in die „Virtual Machines Exclusion List“ aufzunehmen. Informationen über das Ausschließen von virtuellen Maschinen vom Schutz der vShield App finden Sie im *vShield-Administratorhandbuch*.

---

**Wichtig** Wenn sich der vCenter Server oder die virtuellen Maschinen der vCenter Server-Datenbank auf dem ESX-Host befinden, auf dem Sie die vShield App installieren, migrieren Sie diese vor der Installation der vShield App auf einen anderen Host.

---

### Voraussetzungen

- Stellen Sie sicher, dass Sie über eine eindeutige IP-Adresse für den Management-Port (MGT-Port) jeder virtuellen vShield App-Appliance verfügen. Jede IP-Adresse muss von vShield Manager aus erreichbar sein und sich in dem Managementnetzwerk befinden, das für die vCenter- und ESX-Host-Managementschnittstellen verwendet wird. Die Verwendung einer falschen IP-Adresse führt dazu, dass vShield App auf diesem Host deinstalliert und neu installiert werden muss.
- Lokaler oder Netzwerkspeicher, in dem die vShield App abgelegt werden soll.

### 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]** .

6 Geben Sie unter vShield App die folgenden Informationen an.

| 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, die die Verwaltungsschnittstelle 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 Verwaltungsschnittstelle von vShield App zugewiesen werden soll.<br>**WICHTIG** Vergewissern Sie sich, dass Sie die richtige IP-Adresse eingeben. Um die IP-Adresse zu ändern, nachdem vShield App installiert wurde, müssen Sie vShield App deinstallieren und den ESX-Host neu starten. |
| **[Netmask]** | Geben Sie die IP-Subnetzmaske für die zugewiesene IP-Adresse ein. |
| **[Default Gateway]** | Geben Sie die IP-Adresse des Standard-Netzwerkgateways ein. |

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

Sie können den Fortschritt der Installation von vShield App im Fenster „Aktuelle Aufgaben“ des vSphere-Clients verfolgen.

### Weiter

Führen Sie vShield App im normalen Betrieb aus und untersuchen Sie den ein- und ausgehenden Datenverkehr Ihres virtuellen Netzwerks. Konfigurieren Sie die Firewallregeln auf Basis dieser Informationen. Jede vShield App erbt globale Firewallregeln, 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*.

**HINWEIS** Wenn Sie vShield App auf einem statusfreien ESX-Host installiert haben, müssen Sie die Schritte unter „Installieren von vShield App auf einem statusfreien ESX-Host“, auf Seite 27 ausführen, bevor Sie den Host neu starten.

**VORSICHT** Ändern Sie die virtuellen Dienstmaschinen nicht mit dem vSphere-Client. Dies kann dazu führen, dass die Kommunikation zwischen vShield Manager und vShield App unterbrochen und die Sicherheit Ihres Netzwerks gefährdet wird.

## Installieren von vShield App auf einem statusfreien ESX-Host

Wenn Sie die vShield App auf einem statusfreien ESX-Host installiert haben, müssen Sie die nachfolgenden Schritte durchführen, bevor Sie einen der ESX-Hosts neu starten, auf denen die vShield App installiert ist.

### Voraussetzungen

- Installieren Sie die vShield App auf dem statusfreien ESX-Host.
- Stellen Sie sicher, dass die vom VIB auf dem Host vorgenommenen Änderungen an der Firewall-Konfiguration abgeschlossen sind.
  a Wählen Sie im vCenter-Client den statusfreien ESX-Host im Bestandslistenbereich aus.
  b Klicken Sie auf die Registerkarte **[Configuration]** .
  c Überprüfen Sie, ob unter „Eingehende Verbindungen“ im Firewall-Bereich ein DVFilter-Eintrag angezeigt wird. Falls kein DVFilter-Eintrag angezeigt wird, klicken Sie auf **[Aktualisieren.]**

- Erstellen Sie ein Hostprofil. Weitere Informationen hierzu finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.

### Vorgehensweise

1 Bearbeiten Sie das Hostprofil.

   a Wählen Sie im vCenter-Client **[Home] > [Management] > [Hostprofile.]**

   b Wählen Sie das zu bearbeitende Profil aus.

   c Klicken Sie auf **[Hostprofil bearbeiten]** .

   d Wählen Sie **[Netzwerkkonfiguration] > [Hostportgruppe] > [vmservice-vmknic-pg] > [IP-Adresseinstellungen] > [Wie wird die IPv4-Adresse festgelegt]** .

   e Geben Sie als IP-Adresse **`169.254.1.1`** und als Subnetzmaske **`255.255.255.0`** ein.

   f Wählen Sie **[Netzwerkkonfiguration] > [Hostportgruppe] > [vmservice-vmknic-pg] > [Festlegen, wie die MAC-Adresse für vmknic entschieden werden soll]** .

   g Wählen Sie **[Benutzer muss die Richtlinienoption explizit auswählen]** .

2 Speichern Sie das Hostprofil.

3 Geben Sie in einem Webbrowser https://vsm-ip/bin/offline-bundles/VMware-vShield-fastpath-esx5x-5.0.1-766127.zip ein und laden Sie die ZIP-Datei herunter.

4 Verwenden Sie das in Schritt 1 erstellte Hostprofil und das Offline-Paket, das Sie in Schritt 3 heruntergeladen haben, um die statusfreie ESX-Konfiguration zu aktualisieren.

# Installieren von vShield Edge

Sie können mehrere virtuellen vShield Edge-Appliances in einem Datencenter installieren. Jede virtuelle vShield Edge-Appliance kann über insgesamt zehn Uplink- und interne Netzwerkschnittstellen verfügen. Die internen Schnittstellen werden mit gesicherten Portgruppen verbunden und dienen als das Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Bei dem Subnetz, das der internen Schnittstelle zugewiesen ist, kann es sich um private RFC 1918-Adressbereiche handeln. Firewallregeln und andere vShield Edge-Dienste werden beim Datenverkehr zwischen Schnittstellen erzwungen.

Uplink-Schnittstellen von vShield Edge stellen Verbindungen zu Uplink-Portgruppen her, die Zugriff auf ein gemeinsam genutztes Unternehmensnetzwerk oder einen Dienst haben, das bzw. der Zugriffsebenen im Netzwerk bereitstellt.

Mehrere externe IP-Adressen können für Lastverteiler-, Site-zu-Site-VPN- und NAT-Dienste konfiguriert werden. Überlappende IP-Adressen sind bei internen Schnittstellen und überlappende Subnetze sind bei internen und IP-Uplink-Schnittstellen nicht zulässig.

### Voraussetzungen

Ihnen muss die Rolle „Enterprise Administrator“ oder „vShield Administrator“ zugewiesen worden sein.

### Vorgehensweise

1 Öffnen des Assistenten „Add Edge“ auf Seite 29

Öffnen Sie den Assistenten „Add Edge“, um eine vShield Edge-Instanz zu installieren und zu konfigurieren.

2 Benennen von vShield Edge auf Seite 29

vShield Edge benötigt einen beschreibenden Namen, der über alle virtuellen vShield Edge-Maschinen in einem einzelnen Tenant hinweg eindeutig ist. Diese Name wird in Ihrer vCenter-Bestandsliste angezeigt.

3 Angeben der CLI-Anmeldedaten auf Seite 30

Bearbeiten Sie die Anmeldedaten, die zum Anmelden bei der Befehlszeilenschnittstelle (CLI) verwendet werden sollen.

4 Hinzufügen von Appliances auf Seite 30

Sie müssen eine Appliance hinzufügen, bevor Sie vShield Edge bereitstellen können. Wenn Sie keine Appliance hinzufügen, wenn Sie vShield Edge installieren, bleibt vShield Edge so lange im Offline-Modus, bis Sie eine Appliance hinzugefügt haben.

5 Hinzufügen von internen und Uplink-Schnittstellen auf Seite 31

Sie können einer virtuellen vShield Edge-Maschine bis zu zehn interne und Uplink-Schnittstellen hinzufügen.

6 Konfigurieren des Standard-Gateways auf Seite 32

Geben Sie die IP-Adresse für das vShield Edge-Standard-Gateway an.

7 Konfigurieren der Firewallrichtlinie und High Availability (HA) auf Seite 33

Sie können die Standard-Firewallrichtlinie ändern, die den ganzen eingehenden Datenverkehr blockiert.

8 Bestätigen der Einstellungen und Installieren von vShield Edge auf Seite 34

Überprüfen Sie Ihre eingegebenen Einstellungen, bevor Sie vShield Edge installieren.

## Öffnen des Assistenten „Add Edge“

Öffnen Sie den Assistenten „Add Edge“, um eine vShield Edge-Instanz zu installieren und zu konfigurieren.

### Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wählen Sie in der Bestandslistenstruktur eine Datencenterressource aus.

3 Klicken Sie auf die Registerkarte **[Network Virtualization]** .

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

5 Klicken Sie auf das Symbol **[Add]** ( ).

Der Assistent „Add Edge“ wird angezeigt.

## Benennen von vShield Edge

vShield Edge benötigt einen beschreibenden Namen, der über alle virtuellen vShield Edge-Maschinen in einem einzelnen Tenant hinweg eindeutig ist. Diese Name wird in Ihrer vCenter-Bestandsliste angezeigt.

### Vorgehensweise

1 Geben Sie einen Namen für die virtuelle vShield Edge-Maschine ein.

Diese Name wird in Ihrer vCenter-Bestandsliste angezeigt. Der Name muss über alle Edges innerhalb eines einzelnen Tenants hinweg eindeutig sein.

Wenn Sie keinen Namen angeben, generiert vShield Manager einen eindeutigen Namen für jede vShield Edge-Instanz.

2 (Optional) Geben Sie einen Hostnamen für die virtuelle vShield Edge-Maschine ein.

Dieser Name wird in der Befehlszeilenschnittstelle angezeigt. Wenn Sie den Hostnamen nicht angeben, wird auch der Name, den Sie in Schritt 1 angegeben haben, in der Befehlszeilenschnittstelle angezeigt.

3 (Optional) Geben Sie eine Beschreibung für diese vShield Edge-Instanz ein.

4 (Optional) Geben Sie den Tenant für diese vShield Edge-Instanz ein.

5 (Optional) Wählen Sie **[Enable HA]** , um High Availability (HA) zu aktivieren.

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

## Angeben der CLI-Anmeldedaten

Bearbeiten Sie die Anmeldedaten, die zum Anmelden bei der Befehlszeilenschnittstelle (CLI) verwendet werden sollen.

### Vorgehensweise

1 Geben Sie auf der Seite „CLI Credentials“ die CLI-Anmeldedaten für Ihre virtuelle vShield Edge-Maschine an.

| Option | Aktion |
|---|---|
| **CLI-Benutzername** | Bearbeiten Sie den Eintrag, falls erforderlich. |
| **CLI-Kennwort** | Bearbeiten Sie den Eintrag, falls erforderlich. |

2 (Optional) Klicken Sie auf **[Enable SSH access]** , falls erforderlich.

3 Klicken Sie auf **[Weiter]** .

Die Seite „Edge Appliances“ wird angezeigt.

## Hinzufügen von Appliances

Sie müssen eine Appliance hinzufügen, bevor Sie vShield Edge bereitstellen können. Wenn Sie keine Appliance hinzufügen, wenn Sie vShield Edge installieren, bleibt vShield Edge so lange im Offline-Modus, bis Sie eine Appliance hinzugefügt haben.

### Voraussetzungen

Stellen Sie für High Availability sicher, dass der Ressourcenpool über ausreichend Kapazitäten für beide virtuellen HA-Maschinen verfügt, die bereitgestellt werden sollen. Eine kompakte virtuelle vShield Edge-Maschine benötigt 256 MB Arbeitsspeicher, eine große virtuelle vShield Edge-Maschine benötigt 1 GB Arbeitsspeicher und ein X-Large (sehr große) virtuelle vShield Edge-Maschine benötigt 8 GB Arbeitsspeicher. Der Datenspeicher benötigt mindestens 512 MB Festplattenspeicher.

### Vorgehensweise

1 Wählen Sie auf der Seite „Edge Appliances“ die Größe der vShield Edge-Instanz basierend auf Ihren Systemressourcen aus.

Das **[Large]** (große) vShield Edge hat mehr CPU, Arbeitsspeicher und Festplattenspeicher als das **[Compact]** (kompakte) vShield Edge und unterstützt eine größere Anzahl an gleichzeitigen SSL VPN-Plus-Benutzern. Das **[X-Large]** (sehr große) vShield Edge eignet sich für Umgebungen, die über Lastverteiler mit Millionen von gleichzeitig ausgeführten Sitzungen verfügen. Das X-Large vShield Edge unterstützt SSL VPN nicht.

2 Klicken Sie auf **[Enable auto rule generation]** um Firewall-, NAT- und Routing-Routen hinzuzufügen, die für den Fluss des Steuerungsdatenverkehrs für diese Dienste sorgen.

Wenn Sie **[Enable auto rule generation]** nicht wählen, müssen Sie Firewallregeln manuell erstellen, um Firewall-, NAT- und Routing-Routen hinzuzufügen und den Steuerungsdatenverkehr für vShield Edge-Dienste, z. B. Lastausgleich, VPN usw., zu ermöglichen.

**Hinweis** Die Option „Auto rule generation“ erstellt keine Regeln für Datenkanalverkehr.

3 Klicken Sie auf **[Enable AESNI]** , um Intel® AES-NI (Intel® Advanced Encryption Standard New Instructions) zu aktivieren.

4 Klicken Sie unter **[Edge Appliances]** auf das **[Add]** -Symbol ( ), um eine Appliance hinzuzufügen.

Wenn Sie **[Enable HA]** auf der Seite „Name and Description“ ausgewählt haben, können Sie zwei Appliances hinzufügen. Wenn Sie eine einzelne Appliance hinzufügen, repliziert vShield Edge die Konfiguration der Appliance für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA vShield Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben (es sei denn, Sie migrieren sie per vMotion manuell auf denselben Host).

5 Wählen Sie im Dialogfeld „Add Edge Appliance“ den Cluster oder den Ressourcenpool sowie den Datenspeicher für die Appliance aus.

6 (Optional) Wählen Sie den Host aus, auf dem die Appliance hinzugefügt werden soll.

7 (Optional) Wählen Sie den vCenter-Ordner aus, in dem die Appliance hinzugefügt werden soll.

8 Klicken Sie auf **[Hinzufügen]** .

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

Die Seite „Interfaces“ wird angezeigt.

## Hinzufügen von internen und Uplink-Schnittstellen

Sie können einer virtuellen vShield Edge-Maschine bis zu zehn interne und Uplink-Schnittstellen hinzufügen.

### Vorgehensweise

1 Klicken Sie auf der Seite „Interfaces“ auf das Symbol **[Add]** ) und geben Sie einen Namen für die Schnittstelle ein.

2 Wählen Sie **[Internal]** bzw. **[Uplink]** , um anzugeben, ob es sich um eine interne oder eine externe Schnittstelle handelt.

Sie müssen mindestens eine interne Schnittstelle hinzufügen, damit HA funktioniert.

3 Wählen Sie die Portgruppe oder die virtuelle VXLAN-Leitung aus, mit der diese Schnittstelle verbunden werden soll.

a Klicken Sie auf **[Select]** neben dem Feld **[Connected To]** .

b Klicken Sie je nachdem, womit die Schnittstelle verbunden werden soll, auf die Registerkarte **[Virtual Wire]** , **[Standard Portgroup]** oder **[Distributed Portgroup]** .

c Wählen Sie die entsprechende virtuelle Leitung oder Portgruppe aus.

d Klicken Sie auf **[Auswählen]** .

4 Wählen Sie den Konnektivitätsstatus für die Schnittstelle aus.

5 Klicken Sie unter **[Configure Subnets]** auf das Symbol **[Add]** ( ), um der Schnittstelle ein Subnetz hinzuzufügen.

Eine Schnittstelle kann über mehrere nicht überlappende Subnetze verfügen.

6 Klicken Sie unter **[Add Subnet]** auf das Symbol **[Add]** ( ), um eine IP-Adresse einzugeben.

Wenn Sie mehr als eine IP-Adresse eingeben, können Sie die primäre IP-Adresse auswählen. Eine Schnittstelle kann eine primäre und mehrere sekundäre IP-Adressen haben. vShield Edge betrachtet die primäre IP-Adresse als die Quelladresse für den lokal generierten Datenverkehr.

Sie müssen der Schnittstelle zuerst eine IP-Adresse hinzufügen, bevor Sie sie für jede beliebige Funktionskonfiguration verwenden können.

7 Geben Sie die Subnetzmaske für die Schnittstelle ein und klicken Sie auf **[Save]** .

8 (Optional) Geben Sie die MAC-Adresse für die Schnittstelle ein. Wenn HA aktiviert ist, geben Sie zwei Management-IP-Adressen im CIDR-Format ein.

Die Taktsignale der zwei virtuellen vShield Edge HA-Maschinen werden über diese Verwaltungs-IP-Adressen übertragen. Die Verwaltungs-IP-Adressen müssen sich in demselben L2/Subnetz befinden und müssen untereinander kommunizieren können.

9 Ändern Sie die standardmäßige MTU, falls erforderlich.

10 Wählen Sie unter **[Options]** die erforderlichen Optionen aus.

| Option | Beschreibung |
|---|---|
| **Enable Proxy ARP** | Unterstützt das Überlappen der Netzwerkweiterleitung zwischen verschiedenen Schnittstellen. |
| **Send ICMP Redirect** | Leitet Routing-Informationen an Hosts weiter. |

11 Geben Sie die Fence-Parameter ein und klicken Sie auf **[Add]** .

12 Wiederholen Sie die Schritte Schritt 1 bis Schritt 11, um weitere Schnittstellen hinzuzufügen.

13 Klicken Sie auf **[Weiter]** .

Die Seite „Default Gateway“ wird angezeigt.

## Konfigurieren des Standard-Gateways

Geben Sie die IP-Adresse für das vShield Edge-Standard-Gateway an.

### Vorgehensweise

1 Wählen Sie auf der Seite „Default Gateway“ **[Configure Default Gateway]** aus.

2 Wählen Sie die Schnittstelle aus, die mit der nächsten Hop- oder Gateway-IP-Adresse kommunizieren kann.

3 Geben Sie die IP-Adresse für das Standard-Gateway ein.

4 Unter **[MTU]** wird die Standard-MTU für die Schnittstelle angezeigt, die Sie in Schritt 2 ausgewählt haben. Sie können diesen Wert ändern, er darf jedoch nicht höher als die konfigurierte MTU für die Schnittstelle sein.

5 Klicken Sie auf **[Weiter]** .

Die Seite „Firewall & HA“ wird angezeigt.

## Konfigurieren der Firewallrichtlinie und High Availability (HA)

Sie können die Standard-Firewallrichtlinie ändern, die den ganzen eingehenden Datenverkehr blockiert.

Sie müssen HA-Parameter für die hohe Verfügbarkeit konfigurieren, um mit Netzwerkkonfigurationen auf vShield Edge arbeiten zu können. vShield Edge unterstützt zwei virtuelle Maschinen für hohe Verfügbarkeit und beide Maschinen werden mithilfe von Benutzerkonfigurationen auf dem neuesten Stand gehalten. Falls ein Taktsignalfehler auf der primären virtuellen Maschine auftritt, wird der Zustand der sekundären virtuellen Maschine in „active“ geändert. Folglich ist immer eine virtuelle vShield Edge-Maschine im Netzwerk aktiv.

### Vorgehensweise

1 Wählen Sie auf der Seite „Firewall & HA“ die Option **[Configure Firewall default policy]** aus.

2 Geben Sie an, ob der eingehende Datenverkehr standardmäßig angenommen oder abgelehnt werden soll.

Alle Firewallregeln, die Sie erstellen, haben Vorrang vor der Standardrichtlinie.

3 Geben Sie an, ob der eingehende Datenverkehr protokolliert werden soll.

Wenn Sie Firewallregeln erstellen, die Vorrang vor der Standardrichtlinie haben, wird das Protokollieren durch die von Ihnen erstellten Regeln bestimmt. Durch das Aktivieren der Standardprotokollierung werden möglicherweise zu viele Protokolle generiert und die Leistung von vShield Edge beeinträchtigt. Es wird daher empfohlen, die Standardprotokollierung nur bei der Fehlerbehebung oder beim Debuggen zu aktivieren.

4 Wenn Sie **[Enable HA]** auf der Seite „Name & Description“ ausgewählt haben, füllen Sie den Abschnitt **[Configure HA parameters]** aus.

vShield Edge repliziert die Konfiguration der primären Appliance für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA vShield Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben. Zwei virtuelle Maschinen werden auf vCenter in demselben Ressourcenpool und Datenspeicher wie die von Ihnen konfigurierte Appliance bereitgestellt. Die IP-Adressen von lokalen Links werden virtuellen HA-Maschinen in der vShield Edge HA zugewiesen, damit sie untereinander kommunizieren können. Sie können Verwaltungs-IP-Adressen angeben, um die lokalen Links zu überschreiben.

a Wählen Sie die interne Schnittstelle aus, für die HA-Parameter konfiguriert werden sollen.

b (Optional) Geben Sie den Zeitraum (in Sekunden) ein, nach dem die primäre Appliance als inaktiv betrachtet wird und die Backup-Appliance die Arbeit übernimmt, falls die Backup-Appliance kein Taktsignal von der primären Appliance erhält.

Das Standardintervall beträgt 6 Sekunden.

c (Optional) Geben Sie zwei Verwaltungs-IP-Adressen im CIDR-Format ein, die die IP-Adressen der lokalen Links überschreiben, die den virtuellen HA-Maschinen zugewiesen sind.

Vergewissern Sie sich, dass es keine Überlappungen der Management-IP-Adressen mit den Schnittstellensubnetzen gibt.

5 Klicken Sie auf **[Weiter]** .

Die Seite „Summary“ wird angezeigt.

### Bestätigen der Einstellungen und Installieren von vShieldEdge

Überprüfen Sie Ihre eingegebenen Einstellungen, bevor Sie vShield Edge installieren.

#### Vorgehensweise

1 Überprüfen Sie die Einstellungen für vShield Edge auf der Seite „Summary“.

2 Klicken Sie auf **[Previous]** , um die Einstellungen zu ändern.

3 Klicken Sie auf **[Finish]** , um die Einstellungen zu übernehmen und vShield Edge zu installieren.

## 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 Host im Cluster installiert sein müssen. Weitere Informationen zu den erforderlichen Versionen finden Sie unter Kapitel 2, „Vorbereitung für die Installation“, auf Seite 13.
- vShield Manager 5.1 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 Um sich optimal zu schützen, installieren Sie die neueste Version von VMware Tools, die für diejenige ESX-Version freigegeben wurden, die Sie auf all Ihren virtuellen Maschinen haben.

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 VMware Tools auf virtuellen Gastmaschinen

VMware Tools enthält den vShield Thin Agent, der auf jeder zu schützenden virtuellen Gastmaschine installiert werden muss. 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. Die folgenden Windows-Betriebssysteme werden für vShield Endpoint 5.0 unterstützt:

- Windows Vista (32-Bit)
- Windows 7 (32/64-Bit)
- Windows XP SP3 und höher (32-Bit)

- Windows 2003 SP2 und höher (32/64-Bit)
- Windows 2008 (32/64-Bit)
- Windows 2008 R2 (64-Bit)

### Vorgehensweise

1 Wählen Sie den Installationstyp für VMware Tools aus.

| ESX-Version des Hosts | Aktion |
|---|---|
| **ESX 5.0 Patch 1 oder höher** | Folgen Sie den Installationsanweisungen unter *Installieren und Konfigurieren von VMware Tools* bis zu dem Punkt, wo Sie den Assistenten für den Setuptyp sehen. |
| **ESX 4.1 Patch 3 oder höher** | Folgen Sie den Installationsanweisungen im Knowledgebase-Artikel http://kb.vmware.com/kb/2008084 bis zu dem Punkt, wo Sie den Assistenten für den Setuptyp sehen. |

2 Wählen Sie im Assistenten für den Setuptyp eine der folgenden Optionen aus:

- Vollständig.
- Benutzerdefiniert.
  - Wählen Sie in der Liste der VMware-Gerätetreiber „VMCI-Treiber“ und dann den vShield-Treiber aus.

## 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. |

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.

# Deinstallieren von vShield-Komponenten 5

In diesem Kapitel werden die erforderlichen Schritte zur Deinstallation von vShield-Komponenten aus Ihrer vCenter-Bestandsliste beschrieben.

Dieses Kapitel behandelt die folgenden Themen:


- „Deinstallieren einer virtuellen vShield App-Appliance“, auf Seite 37
- „Deinstallieren von vShield Edge“, auf Seite 38
- „Deinstallieren einer virtuellen vShield Data Security-Maschine“, auf Seite 38
- „Deinstallieren eines vShield Endpoint-Moduls“, auf Seite 38


## Deinstallieren einer virtuellen vShield App-Appliance

Beim Deinstallieren von vShield App wird die virtuelle Appliance vom Netzwerk und aus vCenter Server entfernt.

**Vorsicht** Bei der Deinstallation einer vShield App wird der ESX-Host in den Wartungsmodus versetzt. Der ESX-Host wird während des Deinstallationsvorgangs neu gestartet. Wenn auf dem ESX-Zielhost ausgeführte virtuelle Maschinen nicht auf einen anderen ESX-Host migriert werden können, müssen diese virtuellen Maschinen zum Fortsetzen der Deinstallation ausgeschaltet oder manuell migriert werden. Wenn vShield Manager auf demselben ESX-Host ausgeführt wird, muss vShield Manager vor der Deinstallation von vShield App migriert werden.

### Vorgehensweise

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie den ESX-Host in der Bestandslistenstruktur aus.
3. Klicken Sie auf die Registerkarte **[vShield]** .
4. Klicken Sie für den **[vShield App]** -Dienst auf **[Uninstall]** .

   Wenn Sie vShield App auf einem statusfreien ESX-Host deinstallieren, ignorieren Sie die Fehler bei der VIB-Deinstallation.
5. Wenn sich der ESX-Host im Wartungsmodus befand, bevor Sie die Deinstallation der vShield App starteten, entfernen Sie die virtuellen vShield App-Maschinen manuell, nachdem die automatische Deinstallation abgeschlossen ist.

Die Instanz wird deinstalliert.

# Deinstallieren von vShield Edge

Sie können vShield Edge mithilfe des vSphere-Clients deinstallieren.

### Voraussetzungen

Ihnen muss die Rolle „Enterprise Administrator“ oder „vShield Administrator“ zugewiesen worden sein.

### Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wählen Sie in der Bestandslistenstruktur eine Datencenterressource aus.

3 Klicken Sie auf die Registerkarte **[Network Virtualization]** .

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

5 Klicken Sie auf das Symbol **[Delete]** ( ).

# Deinstallieren einer virtuellen vShield Data Security-Maschine

Nach erfolgter Deinstallation der virtuellen vShield Data Security-Maschine müssen Sie die virtuelle Appliance entsprechend den Anweisungen des VMware-Partners deinstallieren.

### 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 für den vShield Data Security-Dienst auf **[Deinstallieren]** .

# Deinstallieren eines vShield Endpoint-Moduls

Beim Deinstallieren eines vShield Endpoint-Moduls wird ein vShield Endpoint-Modul von einem ESX-Host entfernt. Sie müssen diese Schritte in der folgenden Reihenfolge durchführen.

**VORSICHT** Wenn vShield Data Security auf dem ESX-Host installiert ist, müssen Sie es deinstallieren, bevor Sie vShield Endpoint deinstallieren.

## Deinstallieren der Produkte, die vShield Endpoint verwenden

Bevor Sie ein vShield Endpoint-Modul von einem Host deinstallieren, müssen Sie alle Produkte von diesem Host deinstallieren, die vShield Endpoint verwenden. Halten Sie sich dabei an die Anweisungen des Anbieters.

## Deinstallieren des vShield Endpoint-Moduls aus vSphere Client

Beim Deinstallieren eines vShield Endpoint-Moduls wird das vShield Endpoint-Modul von einem ESX-Host entfernt.

### 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 **[Deinstallieren]** für den **[vShield Endpoint]** -Dienst.

# Aktualisieren von vShield 6

Um ein Upgrade von vShield durchzuführen, müssen Sie zuerst ein Upgrade von vShield Manager und anschließend ein Update der anderen Komponenten durchführen, für die Sie eine Lizenz haben.

Dieses Kapitel behandelt die folgenden Themen:


- „Upgrade von vShield Manager“, auf Seite 41
- „Upgrade von vShield App“, auf Seite 47
- “Upgrade vShield Edge from 5.0.x to 5.5,” on page 47
- „Upgrade von vShield Endpoint“, auf Seite 48
- „Upgrade von vShield Data Security“, auf Seite 49


## Upgrade von vShield Manager

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

### Voraussetzungen

Erstellen Sie einen Snapshot von vShield Manager, damit Sie das Upgrade rückgängig machen können, falls es fehlschlägt.

**Vorsicht** Deinstallieren Sie keine bereitgestellte Instanz der vShield Manager-Appliance.

### Upgrade von vShield Manager von Version 5.0 auf Version 5.1.2

vShield Manager Version 5.1 und höher benötigt mindestens 2,5 GB Festplattenspeicher. Sie müssen das Wartungspaket ausführen, damit für den aktualisierten vShield Manager Festplattenspeicher zur Verfügung steht.

#### Vorgehensweise

1 Freigeben von Festplattenspeicher durch Installieren des Wartungspakets auf Seite 42

   Für den Upgrade-Vorgang ist mindestens 2,5 GB freier Festplattenspeicher auf der `/common`-Partition erforderlich. Das vShield-Wartungspaket sorgt für verfügbaren Festplattenspeicher auf dem vShield Manager. Es stoppt den vShield Manager-Vorgang und startet ihn nach Beendigung der Aktivitäten zur Bereinigung des Dateisystems neu.

2 Upgrade von vShield Manager auf Version 5.1 oder höher auf Seite 43

3 Erstellen einer Post-Upgrade-Sicherung auf Seite 44

Ab Version 5.1 benötigt vShield Manager ein Upgrade seiner virtuellen Hardware. Dieses Upgrade der virtuellen Hardware wird nicht automatisch als Teil des vShield-Upgrade-Vorgangs für vShield Manager 5.0.x oder vorherige Versionen durchgeführt. Für architektonische Änderungen zur verbesserten Skalierbarkeit, Leistung und für verbesserte Protokollierungs- und Berichtsfunktionen ist ein Upgrade der virtuellen Hardware von vShield Manager erforderlich. Zu den Änderungen gehören 64-Bit-Unterstützung, 2 vCPUs, 8 GB RAM, eine größere virtuelle Festplatte sowie weitere Eigenschaften virtueller Hardware.

4 Wiederherstellen einer Post-Upgrade-Sicherung auf Seite 45

Stellen Sie die vShield Manager-Sicherung wieder her.

5 Installieren von Wartungs-Patch 5.1.2a auf Seite 45

Wenn Sie vShield Version 5.1.2 verwenden, müssen Sie den Patch 5.1.2a installieren.

## Freigeben von Festplattenspeicher durch Installieren des Wartungspakets

Für den Upgrade-Vorgang ist mindestens 2,5 GB freier Festplattenspeicher auf der `/common`-Partition erforderlich. Das vShield-Wartungspaket sorgt für verfügbaren Festplattenspeicher auf dem vShield Manager. Es stoppt den vShield Manager-Vorgang und startet ihn nach Beendigung der Aktivitäten zur Bereinigung des Dateisystems neu.

### Voraussetzungen

**HINWEIS** Als Teil dieses Vorgangs werden vorhandene Protokolle, Flow Monitoring-Daten sowie Systemereignis- und Überwachungsprotokolle auf der vShield Manager-Appliance gelöscht. Sie können die Systemereignis- und Überwachungsprotokolle mit dem entsprechenden REST API-Aufruf abrufen, bevor Sie das Wartungspaket anwenden. Das Tech Support-Protokollpaket enthält Protokollmeldungen dieses Vorgangs.

### 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.

2 Wechseln Sie in den Aktivierungsmodus.

3 Geben Sie nach der Anmeldung den Befehl `show filesystems` ein.

Sie benötigen mindestens 5 % freien Festplattenspeicher in der `/common` -Partition, um das Wartungspaket installieren zu können.

4 Geben Sie den Befehl `show manager log follow` ein. Lassen Sie die Konsole beim Ausführen der weiteren Schritte geöffnet.

5 Laden Sie das vShield-Wartungspaket an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Name des Wartungspakets lautet in etwa `VMware-vShield-Manager-upgrade-bundle-maintenance-`*Build-Nummer des Pakets*`.tar.gz`.

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

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

8 Klicken Sie auf **[Upload Settings]** .

9 Klicken Sie auf **[Browse]** und wählen Sie die Datei `VMware-vShield-Manager-upgrade-bundle-maintenance-`*Build-Nummer des Pakets*`.tar.gz` aus.

10 Klicken Sie auf **[Öffnen]** .

11 Klicken Sie auf **[Upload File]** .

12 Klicken Sie auf **[Install]** , um mit dem Upgrade zu beginnen.

13 Klicken Sie auf **[Confirm Install]** .

14 Lesen Sie in der Befehlszeilenschnittstelle die Ausgabe des Befehls `show manager log`. Wenn Sie die Meldung `maintenance-fs-cleanup: Filesystem cleanup successful` sehen, melden Sie sich bei der vShield Manager-Benutzeroberfläche an.

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

15 Melden Sie sich bei der vShield Manager-Befehlszeilenschnittstelle an, wechseln Sie in den Aktivierungsmodus und führen Sie den Befehl `show filesystems` aus, um sicherzustellen, dass mindestens 2,5 GB freier Speicherplatz für das Upgrade vorhanden ist.

## Upgrade von vShield Manager auf Version 5.1 oder höher

### 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 **[Öffnen]** .

7 Klicken Sie auf **[Upload Upgrade Bundle]** .

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 Melden Sie sich nach dem Neustart bei vShield Manager an und klicken Sie auf die Registerkarte „Updates“. Der Bereich „Installierte Version“ zeigt Version 5.1.2 an, die Sie gerade installiert haben.

Die vShield App-Regeln der vorherigen Version werden folgendermaßen aktualisiert.

| Firewall-Funktion in vorheriger Version | Ergebnis des Upgrades auf Version 5.1 |
|---|---|
| Firewallregeln auf Datencenter-, Cluster- und Portgruppenebene erlaubt | Firewallregeln auf Namespace-Ebene erlaubt – auf der Datencenterebene, der Portgruppenebene mit unabhängigem Namespace und auf der Ebene virtueller Leitungen<br>Nach dem Upgrade werden Firewallregeln aus Nicht-Namespace-Bereichen in das entsprechende Datencenter verschoben. Beim Zusammenführen der migrierten Regeln mit den Datencenterregeln wird diese Reihenfolge eingehalten:<br>■ Datencenter – Hoch<br>■ Cluster<br>■ Nicht-Namespace-Portgruppe oder dvPort-Gruppe<br>■ Datencenter – Niedrig<br>■ Datencenter – Standard |
| Firewallregeln unterstützten Roh-IP- und MAC-Adressen sowie Portprotokoll und Protokoll-Subtyp | Firewallregeln unterstützen nur IPsets, MACsets und Sicherheitsgruppen<br>Nach dem Upgrade werden ggf. IPsets, MACsets oder Dienste intern erstellt. Die Namensvergabe für die erstellten Container unterliegt folgenden Konventionen:<br>■ IPset/MACset: *IP-/Mac-Wert-Kontextname*<br>■ Dienst: *Protokollname-Portnummer-Kontextname* oder *Protokollname-Subtypname-Kontextname* |
| Zu den Firewallregeln gehörten Regeln mit hoher und niedriger Rangordnung. Regeln für Nicht-Namespace-Portgruppen hatten die Rangordnung „None“. | Keine Unterstützung für Regeln mit hoher und niedriger Rangordnung.<br>Nach dem Upgrade erhalten alle Regeln mit einer anderen als der Standardrangordnung die Rangordnung „None“. |
| Für alle Datencenter in der Bestandsliste wurde eine einzige globale SpoofGuard-Einstellung angewendet | Für alle Namespaces werden globale SpoofGuard-Einstellungen angewendet. Nach dem Upgrade können Sie die SpoofGuard-Einstellungen auf der Namespace-Ebene ändern. |

Darüber hinaus werden alle vor dem Upgrade aufgezeichneten Firewall-Verläufe und -Flows gelöscht.

### Weiter

Löschen Sie den Cache Ihres Browsers auf allen Clients, die auf die vorherige Version des Produkts zugegriffen haben. Diese Aktion löscht die zwischengespeicherte Javascript-Datei bzw. andere Dateien dieser Version, die möglicherweise in der aktuellen Version geändert wurden.

## Erstellen einer Post-Upgrade-Sicherung

Ab Version 5.1 benötigt vShield Manager ein Upgrade seiner virtuellen Hardware. Dieses Upgrade der virtuellen Hardware wird nicht automatisch als Teil des vShield-Upgrade-Vorgangs für vShield Manager 5.0.x oder vorherige Versionen durchgeführt. Für architektonische Änderungen zur verbesserten Skalierbarkeit, Leistung und für verbesserte Protokollierungs- und Berichtsfunktionen ist ein Upgrade der virtuellen Hardware von vShield Manager erforderlich. Zu den Änderungen gehören 64-Bit-Unterstützung, 2 vCPUs, 8 GB RAM, eine größere virtuelle Festplatte sowie weitere Eigenschaften virtueller Hardware.

### Vorgehensweise

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

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

3 Klicken Sie auf **[Backups.]**

4 Geben Sie die Host-IP-Adresse oder den Namen des Systems ein, auf dem die Sicherung gespeichert werden soll.

5 Geben Sie den Benutzernamen und das Kennwort ein, die zur Anmeldung beim Sicherungssystem (ftp/sftp server) erforderlich sind.

6 Geben Sie im Feld **[Backup Directory]** den absoluten Pfad zu dem Verzeichnis ein, in dem die Sicherungen gespeichert werden sollen.

7 Geben Sie in **[Filename Prefix]** eine als Präfix für den Dateinamen zu verwendende Textzeichenfolge ein. Dieser Text wird jedem Sicherungsdateinamen vorangestellt, um eine leichte Identifizierung auf dem Sicherungssystem zu ermöglichen. Wenn Sie beispielsweise `ppdb` als Präfix verwenden, lautet der Sicherungsname `ppdb`*HH_MM_SS_TagTTMonJJJJ*.

8 Wählen Sie im Dropdown-Menü **[Transfer Protocol]** basierend auf der Unterstützung durch das Zielsystem entweder das SFTP- oder das FTP-Protokoll aus.

9 Klicken Sie auf **[Save Settings]** und dann auf **[Backup]** .

10 Klicken Sie auf **[View Backups]** , um sicherzustellen, dass die Sicherung erstellt wurde.

## Wiederherstellen einer Post-Upgrade-Sicherung

Stellen Sie die vShield Manager-Sicherung wieder her.

### Vorgehensweise

1 Schalten Sie vShield Manager aus.

2 Laden Sie das 5.1.2 vShield Manager .OVA-Installationspaket herunter.

3 Stellen Sie einen neuen vShield Manager in Ihrer vSphere-Bestandsliste bereit, um den vorhandenen vShield Manager zu ersetzen.

4 Schalten Sie den neuen vShield Manager ein und führen Sie die anfängliche Einrichtung aus. Verwenden Sie dabei dieselbe IP-Adresse wie beim aktuell ausgeschalteten vShield Manager.

5 Konfigurieren Sie die vShield Manager-Sicherungsseite, damit die Sicherungen angezeigt werden, die aktuell auf dem ftp/sftp-Server gespeichert sind.

6 Identifizieren Sie die zuvor erstellte vShield Manager-Sicherung und klicken Sie auf **[Restore]** .

## Installieren von Wartungs-Patch 5.1.2a

Wenn Sie vShield Version 5.1.2 verwenden, müssen Sie den Patch 5.1.2a installieren.

### Vorgehensweise

1 Laden Sie den vShield 5.1.2a-Wartungs-Patch an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Dateiname des Patch-Pakets lautet in etwa **[VMware-vShield-Manager-upgrade-bundle-maintenance-]** *bundlebuildNumber* **[.tar.gz]** .

2 Klicken Sie im vShield Manager-Bestandslistenbereich auf **[Einstellungen und Berichte]** .

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

4 Klicken Sie auf **[Upload Settings]** .

5 Klicken Sie auf **[Durchsuchen]** und wählen Sie die Datei aus, die Sie in Schritt 1 heruntergeladen haben.

6 Klicken Sie auf **[Öffnen]** .

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.

## Upgrade von vShield Manager Version 5.1 auf 5.1.2

### 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 **[Einstellungen und Berichte]** .

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

4 Klicken Sie auf **[Einstellungen hochladen]** .

5 Klicken Sie auf **[Durchsuchen]** und wählen Sie die Datei `VMware-vShield-Manager-upgrade_bundle-`*Build-Nummer*`.tar.gz.` aus.

6 Klicken Sie auf **[Öffnen]** .

7 Klicken Sie auf **[Upgrade-Paket hochladen]** .

8 Klicken Sie auf **[Installieren]** , um mit dem Upgrade zu beginnen.

9 Klicken Sie auf **[Installation bestätigen]** . 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 Melden Sie sich nach dem Neustart bei vShield Manager an und klicken Sie auf die Registerkarte „Updates“. Der Bereich „Installierte Version“ zeigt Version 5.1.2 an, die Sie gerade installiert haben.

11 Laden Sie den vShield 5.1.2a-Wartungs-Patch an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Dateiname des Patch-Pakets lautet in etwa **[VMware-vShield-Manager-upgrade-bundle-maintenance-]** *bundlebuildNumber* **[.tar.gz.]**

12 Folgen Sie Schritt 2 bis Schritt 4.

13 Klicken Sie auf **[Durchsuchen]** und wählen Sie die Datei aus, die Sie in Schritt 11 heruntergeladen haben.

14 Folgen Sie Schritt 6 bis Schritt 9.

## Upgrade von vShield Manager auf Version 5.5

### Voraussetzungen

Sie können ein Upgrade auf vShield Manager Version 5.5 nur von Version 5.1.2 aus ausführen. Wenn Sie eine ältere Version des vShield Manager in Ihrer Umgebung installiert haben, müssen Sie zuerst ein Upgrade auf vShield Manager Version 5.1.2 durchführen, bevor Sie das Upgrade auf vShield Manager Version 5.5 durchführen.

### 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 **[Einstellungen und Berichte]** .

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

4 Klicken Sie auf **[Einstellungen hochladen]** .

5 Klicken Sie auf **[Durchsuchen]** und wählen Sie die Datei `VMware-vShield-Manager-upgrade_bundle-`*Build-Nummer*`.tar.gz.` aus.

6 Klicken Sie auf **[Öffnen]** .

7 Klicken Sie auf **[Upgrade-Paket hochladen]** .

8 Klicken Sie auf **[Installieren]** , um mit dem Upgrade zu beginnen.

9 Klicken Sie auf **[Installation bestätigen]** . 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 Melden Sie sich nach dem Neustart bei vShield Manager an und klicken Sie auf die Registerkarte „Updates“. Der Bereich „Installed Release“ zeigt Version 5.5 an, die Sie gerade installiert haben.

# Upgrade von vShield App

Aktualisieren Sie vShield App auf jedem Host Ihres Datencenters.

### Voraussetzungen

Wenn Sie vShield App Version 4.1 verwenden, müssen Sie zuerst ein Upgrade auf Version 5.0 oder 5.0.1 durchführen, bevor Sie ein Upgrade auf Version 5.1 oder höher durchführen.

### Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wählen Sie **[Bestandsliste] > [Hosts und Cluster]** .

3 Klicken Sie auf den Host, auf dem Sie das Upgrade von vShield App durchführen wollen.

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

Auf der Registerkarte **[General]** wird jede vShield-Komponente, die auf dem ausgewählten Host installiert ist, und die verfügbare Version angezeigt.

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

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

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

**HINWEIS** Während der Durchführung des Upgrades von vShield App wird der ESXi-Host in den Wartungsmodus versetzt und neu gestartet. Um eine Versetzung des Hosts in den Wartungsmodus zu ermöglichen, stellen Sie sicher, dass die virtuellen Maschinen auf dem ESXi-Host migriert wurden (unter Verwendung von DRS oder vMotion) oder dass Sie ausgeschaltet sind.

### Weiter

Überprüfen Sie jede aktualisierte Regel, um sicherzustellen, dass sie wie vorgesehen funktioniert. Weitere Informationen zum Hinzufügen neuer Firewallregeln finden Sie im **[vShield Administration Guide]** .

# Upgrade vShield Edge from 5.0.x to 5.5

You must upgrade vShield Edge on each port group in your datacenter. You cannot upgrade vShield Edge if the same backend IP address has been configured under different listeners with different ports.

vShield Edge 5.1 and later is not backward compatible and you cannot use 2.0 REST calls after the upgrade.

During the vShield Edge upgrade, there will be a brief network disruption for the networks that are being served by the given vShield Edge instance.

### Prerequisites

You must have been assigned the Enterprise Administrator or vShield Administrator role. If you have vShield Edge 5.0.x, each 5.0.x vShield Edge instance on each portgroup in your datacenter must be upgraded to 5.5.

### Procedure

1 Log in to the vSphere Client.

2 Click the portgroup on which the vShield Edge is deployed.

3 Click the **[vShield Edge]** tab.

4 Click **[Upgrade]** .

5 View the upgraded vShield Edge.

   a Select the datacenter corresponding to the port group on which you upgraded the vShield Edge.

   b Click the **[Network Virtualization]** tab.

   c Click **[Edges]** .

   vShield Edge is upgraded to the compact size. A system event is generated to indicate the ID for each upgraded vShield Edge instance.

### What to do next

IMPORTANT Firewall rules from the previous release are upgraded with some modifications. Inspect each upgraded rule to ensure it works as intended. For information on adding new firewall rules, see the *vShield Administration Guide*.

If a user's scope in a previous release was limited to a port group which had a vShield Edge installation, the user is automatically granted access to that vShield Edge after the upgrade.

## Upgrade von vShield Endpoint

Um ein Upgrade von vShield Endpoint von Version 5.0 auf eine höhere Version durchzuführen, müssen Sie zuerst ein Upgrade von vShield Manager und dann ein Update von vShield Endpoint auf jedem Host in Ihrem Datencenter durchführen.

### Vorgehensweise

1 Melden Sie sich beim vSphere-Client an.

2 Wählen Sie **[Bestandsliste] > [Hosts und Cluster]** .

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

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

   Auf der Registerkarte **[Allgemein]** wird jede vShield-Komponente, die auf dem ausgewählten Host installiert ist, und die verfügbare Version angezeigt.

5 Wählen Sie **[Aktualisieren]** neben vShield Endpoint.

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

7 Klicken Sie auf **[Installieren]** .

# Upgrade von vShield Data Security

Führen Sie auf jedem Host Ihres Datencenters ein Upgrade von vShield Data Security durch. Es wird empfohlen, dass Sie vor dem Upgrade von vShield Data Security ein Upgrade von vShield Endpoint durchführen.

### 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 Data Security 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]** .

# Beheben von Installationsproblemen 7

In diesem Abschnitt werden Installationsprobleme beschrieben.

Dieses Kapitel behandelt die folgenden Themen:


- „Installation von vShield App schlägt fehl“, auf Seite 51
- „Installation von vShield Data Security schlägt fehl“, auf Seite 52


## Installation von vShield App schlägt fehl

Das Installieren der vShield App führt zu einem Fehler.

### Problem

Aufgrund einer früheren unvollständigen Installation oder von Problemen bei der Deinstallation einer vorherigen Version schlägt die Installation von vShield App möglicherweise fehl.

### Lösung

1 Beginnen Sie mit einer automatischen Deinstallation von vShield App. Weitere Informationen hierzu finden Sie unter Kapitel 5, „Deinstallieren von vShield-Komponenten“, auf Seite 37.

2 Vergewissern Sie sich, dass die erforderlichen Module im ESX-Host geladen sind, indem Sie sich bei einem SSH-Client anmelden und den folgenden Befehl eingeben:

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

dvfilter 2 72

vmkapiv1_0_0_0_dvfilter_shim0 8
```

3 Falls die erforderlichen Module nicht geladen sind, geben Sie die folgenden Befehle ein, um sie zu laden.

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

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

4 Melden Sie sich bei der vShield Manager CLI als Administrator an und setzen Sie die Webschnittstelle zurück, indem Sie den folgenden Befehl eingeben:

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

5 Starten Sie nach Beendigung des Befehls **`no web-manager`** die Webservices neu, indem Sie den folgenden Befehl eingeben:

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

Wenn Sie zuvor in der Benutzeroberfläche von vShield Manager angemeldet waren, melden Sie sich wieder an, nachdem die Webservices neu gestartet wurden.

6 (Optional) Starten Sie den ESX-Host neu, falls bei der Installation von vShield App die folgende Fehlermeldung angezeigt wurde:

```
vShield App installation encountered error while installing vib
```

7 Löschen Sie den „vmservice-vswitch“, der während des Installationsvorgangs erstellt wurde, indem Sie die nachfolgenden Schritte durchführen.

   a Melden Sie sich beim vSphere-Client an.

   b Wählen Sie den ESX-Host in der Bestandslistenstruktur aus.

   c Klicken Sie auf die Registerkarte **[Konfiguration]** .

   d Klicken Sie im Bereich „Software“ auf **[Networking]** .

   e Klicken Sie im Bereich **[Standard Switch:vmservice-vswitch]** auf **[Remove]** .

8 Löschen Sie die Eigenschaft **[Net.DVFilterBindIpAddress]** für den Host, indem Sie die folgenden Schritte durchführen:

   a Wählen Sie im vSphere-Client den ESX-Host aus der Bestandslistenstruktur aus.

   b Klicken Sie auf die Registerkarte **[Konfiguration]** .

   c Klicken Sie im Bereich „Software“ auf **[Advanced Settings]**

   d Klicken Sie im Dialogfeld „Advanced Settings“ auf **[Net]** .

   e Vergewissern Sie sich, dass das Feld „Net. **[DVFilterBindIpAddress]** “ leer ist.

9 Installieren Sie vShield App erneut. Siehe „Installieren von vShield App“, auf Seite 26.

# Installation von vShield Data Security schlägt fehl

### Problem

Bei der vShield Data Security-Installation erhalte ich einen Fehler während der Installation der virtuellen Dienstmaschine sowie eine Fehlermeldung auf dem vSphere-Client.

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

.

### Ursache

Das DNS-Setup für vShield Manager ist möglicherweise nicht mit dem DNS-Setup für den Host in vCenter Server konsistent.

### Lösung

Ändern Sie das vShield Manager DNS-Setup, damit es mit dem Hostsetup übereinstimmt.

# Index


**A**

Aktualisieren
- vShield App **47**
- vShield Manager **41**
- vShield Manager auf Version 5.5 **46**

Ändern des GUI-Kennworts **22**

Anmelden bei der GUI **20**

Aufheben der Registrierung einer vShield Endpoint-SVM **38**

**B**

Bereitstellung
- Cluster **11**
- Umkreisnetzwerk (DMZ) **10**

Bereitstellungsszenarien **10**

**C**

CLI, Optimierung der Sicherheit **16**

Clientanforderungen **13**

Cluster-Schutz **11**

**D**

Daten, Planen von Sicherungen **23**

Deinstallieren
- vShield App **37**
- vShield Data Security **38**
- vShield Edge **38**
- vShield Endpoint-Modul **38**

**E**

Erwägungen zur Bereitstellung
- vShield **14**
- vShield App **16**
- vShield Edge **17**

Evaluieren von vShield-Komponenten **25**

**G**

GUI, anmelden bei **20**

**I**

Installation
- Lizenzen **26**
- vShield Endpoint:-Thin-Agent **34**
- vShield Manager **19**

Installieren
- vShield App **26**
- vShield Data Security **35**
- vShield Edge **28, 29**
- vShield Endpoint **34**

Isolieren von Netzwerken **11**

**K**

Kennwort ändern **22**

Kommunikation zwischen Komponenten **15**

**L**

Lizenzierung
- Evaluierungsmodus **25**
- Installation **26**

**O**

Optimierung der Sicherheit
- CLI **16**
- REST **16**
- vShield Manager GUI **16**

**P**

Planen von Sicherungen **23**

**R**

REST **16**

**S**

Schutz eines Clusters **11**

Schutz virtueller Maschinen **14**

Sicherungen, planen **23**

Standard-Gateway, Konfigurieren der IP-Adresse **32**

Statusfrei **27**

Synchronisierung mit vCenter **21**

Systemanforderungen **13**

**T**

Thin-Agent-Installation **34**

**U**

Umkreisnetzwerk (DMZ) **10**

upgrade, vShield Edge **47**

Upgrade von Endpoint, 5.0 auf höhere Version **48**

Uplink-Schnittstelle hinzufügen **31**

Uplink-Schnittstelle, hinzufügen **31**

## V

vCenter, vom vShield Manager aus synchronisieren **21**
vMotion **14**
Vorbereiten virtueller Maschinen für den Schutz **14**
vShield
  Bereitstellungsszenarien **10**
  Evaluieren von Komponenten **25**
  Komponenten, Kommunikation **15**
  Optimierung der Sicherheit **16**
  vShield App **8**
  vShield Edge **8**
  vShield Endpoint **9**
  vShield Manager **7**
vShield App
  Deinstallieren **37**
  Gängige Bereitstellungen **12**
  Grundlegendes **8**
  Installieren **26**
  Lizenzierung **26**
vShield Data Security, Installieren **35**
vShield Edge
  Deinstallieren **38**
  Gängige Bereitstellungen **11**
  Grundlegende Informationen **8**
  Installation **29**
  Installieren **28**
  Isolieren von Netzwerken **11**
  Lizenzierung **26**
vShield Edge, Benennen **29**
vShield Endpoint
  Aufheben der Registrierung einer SVM **38**
  Deinstallieren **38**
  Grundlegendes **9**
  Installationsschritte **34**
  Installieren **34**
  Lizenzierung **26**
  Thin-Agent-Installation **34**
vShield Manager
  Ändern des GUI-Kennworts **22**
  bei der GUI anmelden **20**
  Grundlegende Informationen **7**
  Installation **19**
  Planen einer Sicherung **23**
  Synchronisierung mit vCenter **21**
  Verfügbarkeit **15**
vShield Manager GUI **16**
vShield Manager Upgrade, version 5.5 **46**
vShield Zones, vShield Manager **7**