

Handbuch zur Serverkonfiguration für ESXi

ESXi 4.0
vCenter Server 4.0

DE-000114-00



Die neuesten Versionen der technischen Dokumentation finden Sie auf der VMware Website unter:

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese bitte an:

docfeedback@vmware.com

© 2009 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanische und internationale Urheberrechtsgesetze sowie Gesetze zum geistigen Eigentumsrecht geschützt. Die Produkte von VMware sind durch mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware, das VMware-Logo und -Design, Virtual SMP und VMotion sind eingetragene Marken oder Marken der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

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

Inhalt

Info zu diesem Handbuch 7

1 Einführung in die ESXi-Konfiguration 9

Netzwerk

2 Einführung in Netzwerke 13

Übersicht über Netzwerkkonzepte 13

Netzwerkdienste 14

Anzeigen der Netzwerkinformationen im vSphere-Client 15

Anzeigen der Netzwerkadapterinformationen auf dem vSphere-Client 15

3 Einfache Netzwerke mit vNetwork-Standard-Switches 17

vNetwork-Standard-Switches 17

Portgruppen 18

Konfiguration von Portgruppen für virtuelle Maschinen 18

Netzwerkkonfiguration des VMkernels 19

Eigenschaften von vNetwork-Standard-Switches 22

4 Einfache Netzwerke mit verteilten vNetwork-Switches 25

Architektur von verteilten vNetwork-Switches 25

Konfigurieren eines verteilten vNetwork-Switches 26

dvPortgruppen 28

Private VLANs 30

Konfigurieren der Netzwerkadapter des verteilten vNetwork-Switches 32

Konfigurieren von Netzwerken von virtuellen Maschinen auf einem verteilten vNetwork-Switch 36

5 Erweiterte Netzwerkthemen 39

Internet Protocol Version 6 39

Netzwerkrichtlinien 40

Ändern der DNS- und Routing-Konfiguration 57

MAC-Adressen 57

TCP-Segmentierungs-Offload und Jumbo-Frames 59

NetQueue und Netzwerkleistung 61

VMDirectPath Gen I 62

6 Optimale Vorgehensweisen, Szenarien und Fehlerbehebung für Netzwerke 65

Optimale Vorgehensweisen für Netzwerke 65

Mounten von NFS-Volumes 66

Fehlerbehebung 66

Speicher

- 7 Einführung in die Speicherung 69**
 - Info zu ESXi-Speicher 69
 - Physische Speichertypen 70
 - Unterstützte Speicheradapter 71
 - Ziel- und Gerätedarstellungen 72
 - Info zu ESXi-Datenspeichern 74
 - Vergleich der Speichertypen 77
 - Anzeigen der Speicherinformationen im vSphere-Client 78

- 8 Konfigurieren von ESXi-Speicher 83**
 - Lokaler SCSI-Speicher 83
 - Fibre-Channel-Speicher 84
 - iSCSI-Speicher 84
 - Vorgänge zum Aktualisieren und erneuten Prüfen von Speichern 96
 - Erstellen eines VMFS-Datenspeichers 97
 - Network Attached Storage (NAS) 98
 - Erstellen einer Diagnosepartition 100

- 9 Speicherverwaltung 103**
 - Verwalten von Datenspeichern 103
 - Ändern von VMFS-Datenspeichereigenschaften 105
 - Verwalten von duplizierten VMFS-Datenspeichern 108
 - Verwenden von Multipathing mit ESXi 110
 - Thin-Bereitstellung 119

- 10 Raw-Gerätezuordnung 123**
 - Wissenswertes zur Raw-Gerätezuordnung 123
 - Raw-Gerätezuordnungseigenschaften 127
 - Verwalten zugeordneter LUNs 131

Sicherheit

- 11 Sicherheit für ESXi-Systeme 135**
 - Architektur und Sicherheitsfunktionen von ESXi 135
 - Sonstige Quellen und Informationen zur Sicherheit 142

- 12 Absichern einer ESXi-Konfiguration 143**
 - Absichern des Netzwerks mit Firewalls 143
 - Absichern virtueller Maschinen durch VLANs 150
 - Absichern der Ports virtueller Switches 154
 - Absichern von iSCSI-Speicher 156

- 13 Authentifizierung und Benutzerverwaltung 159**
 - Absichern von ESXi über Authentifizierung und Berechtigungen 159

Verschlüsselungs- und Sicherheitszertifikate für ESXi 167

- 14** Empfehlungen für den Schutz von Implementierungen 175
 - Sicherheitsmaßnahmen für gängige ESXi-Implementierungen 175
 - ESXi-Sperrmodus 178
 - Empfehlungen für virtuelle Maschinen 179

Hostprofile

- 15** Verwalten von Hostprofilen 189
 - Modell für die Verwendung von Hostprofilen 189
 - Zugreifen auf die Ansicht „Hostprofile“ 190
 - Erstellen eines Hostprofils 190
 - Exportieren eines Hostprofils 191
 - Importieren eines Hostprofils 192
 - Bearbeiten eines Hostprofils 192
 - Verwalten von Profilen 194
 - Prüfen der Übereinstimmung 197

Index 199

Info zu diesem Handbuch

In diesem *Handbuch zur Konfiguration für ESXi* finden Sie Informationen zur Konfiguration des Netzwerks von ESXi (z. B. zur Erstellung virtueller Switches und Ports sowie zur Einrichtung des Netzwerks für virtuelle Maschinen, VMotion und IP-Speicher). Es enthält außerdem Informationen zum Konfigurieren des Dateisystems und verschiedener Speichertypen, z. B. iSCSI, Fibre-Channel usw. Zum Schutz Ihrer ESXi-Installation enthält das Handbuch umfassende Informationen zu den in ESXi enthaltenen Sicherheitsfunktionen und Maßnahmen, die zum Schutz vor Angriffen ergriffen werden können. Ferner enthalten ist eine Liste mit technischen Unterstützungsbefehlen für ESXi und deren Entsprechung im vSphere-Client sowie eine Beschreibung des Dienstprogramms `vmkfstools`.

Diese Informationen beziehen sich auf ESXi 4.0.

Zielgruppe

Dieses Handbuch richtet sich an jeden, der ESXi installieren, aktualisieren oder verwenden muss. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit dem Betrieb virtueller Maschinen im Datacenter vertraut sind.

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.

VMware vSphere-Dokumentation

Die Dokumentation zu vSphere umfasst die kombinierte Dokumentation zu VMware vCenter Server und ESXi.

In Abbildungen verwendete Abkürzungen

In den Abbildungen, die in diesem Handbuch enthalten sind, werden die in [Tabelle 1](#) aufgeführten Abkürzungen verwendet.

Tabelle 1. Abkürzungen

Abkürzung	Beschreibung
Datenbank	vCenter Server-Datenbank
Datenspeicher	Speicher für den verwalteten Host
Festplatte#	Speicherfestplatte für den verwalteten Host
Hostn	Verwaltete vCenter Server-Hosts

Tabelle 1. Abkürzungen (Fortsetzung)

Abkürzung	Beschreibung
SAN	Storage Area Network-Datenspeicher (SAN), der von den verwalteten Hosts gemeinsam genutzt wird
Vrlg	Vorlage
Benutzer#	Benutzer mit Zugriffsberechtigungen
VC	vCenter Server
VM#	Virtuelle Maschinen auf einem verwalteten Host

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 unterstützt VMware Consulting Services Sie bei der Beurteilung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting-Diensten finden Sie auf der folgenden Webseite: <http://www.vmware.com/services>.

Einführung in die ESXi-Konfiguration

In diesem Handbuch werden die Aufgaben beschrieben, die Sie zur Konfiguration des ESXi-Hostnetzwerks, des Speichers und der Sicherheitsfunktionen durchführen müssen. Außerdem enthält es Übersichten, Empfehlungen und Grundlagenerläuterungen, die Ihnen beim Verständnis dieser Aufgaben und bei der Bereitstellung eines Hosts helfen, der Ihren Anforderungen entspricht.

Bevor Sie diese Informationen verwenden, lesen Sie *Einführung in vSphere*. Dort erhalten Sie einen Überblick über die Systemarchitektur sowie die physischen und virtuellen Geräte, aus denen sich ein vSphere-System zusammensetzt.

Diese Einführung bietet einen Überblick über den Inhalt des vorliegenden Handbuchs.

Netzwerk

Die Informationen über Netzwerke bieten Ihnen eine Einführung in physische und virtuelle Netzwerkkonzepte, eine Beschreibung der Basisaufgaben, die Sie erfüllen müssen, um die Netzwerkanschlüsse Ihres ESXi-Hosts zu konfigurieren, sowie eine Diskussion der erweiterten Netzwerkthemen und -aufgaben.

Speicher

Hier werden grundlegende Informationen zu Speichervorgängen vermittelt. Außerdem werden die grundlegenden erforderlichen Aufgaben zum Konfigurieren und Verwalten des Speichers von ESXi-Hosts beschrieben und das Einrichten von Raw-Gerätezuordnungen (RDM) erläutert.

Sicherheit

In den Informationen zur Sicherheit werden Sicherheitsmaßnahmen erläutert, die von VMware in ESXi integriert wurden. Außerdem werden Maßnahmen beschrieben, mit denen Sie den Host vor Sicherheitsrisiken schützen können. Zu diesen Maßnahmen zählen das Einrichten von Firewalls, die Ausnutzung der Sicherheitsfunktionen virtueller Switches sowie das Konfigurieren von Benutzerauthentifizierungen und -berechtigungen.

Hostprofile

In diesem Abschnitt wird die Hostprofilfunktion beschrieben und wie diese zum Verkapseln einer Hostkonfiguration in ein Hostprofil eingesetzt werden kann. In diesem Abschnitt wird ebenfalls beschrieben, wie dieses Hostprofil von einem anderen Host oder Cluster übernommen, ein Profil bearbeitet und die Übereinstimmung eines Hosts mit einem Profil überprüft werden kann.

Netzwerk

Einführung in Netzwerke

In dieser Netzeinführung werden die grundlegenden Konzepte von ESXi-Netzwerken sowie die Einrichtung und Konfiguration von Netzwerken in einer vSphere-Umgebung erläutert.

Dieses Kapitel behandelt die folgenden Themen:

- [„Übersicht über Netzwerkkonzepte“](#), auf Seite 13
- [„Netzwerkdienste“](#), auf Seite 14
- [„Anzeigen der Netzwerkinformationen im vSphere-Client“](#), auf Seite 15
- [„Anzeigen der Netzwerkadapterinformationen auf dem vSphere-Client“](#), auf Seite 15

Übersicht über Netzwerkkonzepte

Es sind bestimmte Grundlagen notwendig, um virtuelle Netzwerke vollständig zu verstehen. Wenn Sie bisher noch nicht mit ESXi gearbeitet haben, sollten Sie sich diese Konzepte ansehen.

Ein physisches Netzwerk ist ein Netzwerk aus physischen Computern, die so miteinander verbunden sind, dass sie untereinander Daten empfangen und versenden können. VMware ESXi wird auf einem physischen Computer ausgeführt.

Ein virtuelles Netzwerk ist ein Netzwerk aus virtuellen Computern (virtuellen Maschinen), die auf einem einzelnen physischen Computer ausgeführt werden. Diese sind logisch miteinander verbunden, sodass sie untereinander Daten empfangen und versenden können. Virtuelle Maschinen können an die virtuellen Netzwerke angeschlossen werden, die Sie beim Hinzufügen eines Netzwerks erstellen.

Ein physischer Ethernet-Switch verwaltet den Netzwerkdatenverkehr zwischen den Computern im physischen Netzwerk. Ein Switch verfügt über mehrere Ports. Jeder dieser Ports kann an einen einzigen Computer oder einen anderen Switch im Netzwerk angeschlossen sein. Jeder Port kann je nach Bedarf des angeschlossenen Computers so konfiguriert werden, dass er sich auf eine bestimmte Art verhält. Der Switch stellt fest, welche Hosts an welche seiner Ports angeschlossen sind, und verwendet diese Informationen, um Daten an den entsprechenden richtigen physischen Computer weiterzuleiten. Switches bilden den Kern eines physischen Netzwerks. Es können mehrere Switches zusammengeschlossen werden, um größere Netzwerke zu bilden.

Ein virtueller Switch, ein sog. vSwitch, funktioniert ähnlich wie ein physischer Ethernet-Switch. Er weiß, welche virtuellen Maschinen logisch an welche virtuellen Ports angeschlossen sind, und verwendet diese Informationen, um Daten an die entsprechende richtige virtuelle Maschine weiterzuleiten. Ein vSwitch kann über physische Ethernet-Adapter (auch Uplink-Adapter) an physische Switches angeschlossen werden, um virtuelle und physische Netzwerke zu verbinden. Diese Verbindung ähnelt der Vernetzung physischer Switches zur Bildung größerer Netzwerke. Obwohl ein vSwitch ähnlich wie ein physischer Switch funktioniert, verfügt er nicht über alle erweiterten Funktionsmerkmale eines physischen Switches.

Ein verteilter vNetwork-Switch agiert als einzelner vSwitch für alle verbundenen Hosts in einem Datacenter. Dies ermöglicht virtuellen Maschinen bei der Migration zwischen mehreren Hosts die Beibehaltung einer konsistenten Netzwerkkonfiguration.

Ein dvPort ist ein Port auf einem verteilten vNetwork-Switch, der eine Verbindung zur Servicekonsole oder zum VMkernel eines Hosts oder zum Netzwerkadapter einer virtuellen Maschine herstellt.

Eine Portgruppe legt Port-Konfigurationsoptionen, z. B. Bandbreitenbeschränkungen oder VLAN-Tagging-Richtlinien, für jeden Port in der Portgruppe fest. Netzwerkdienste werden über Portgruppen an vSwitches angeschlossen. Portgruppen definieren, wie eine Verbindung über den vSwitch an das physische Netzwerk erfolgt. Standardmäßig wird ein einzelner vSwitch mindestens einer Portgruppe zugeordnet.

Eine dvPortgruppe ist eine Portgruppe, die mit einem verteilten vNetwork-Switch verbunden ist. Sie enthält die Portkonfigurationsoptionen für jeden zur Gruppe gehörenden Port. dvPortgruppen definieren, wie über den verteilten vNetwork-Switch eine Verbindung zum Netzwerk hergestellt wird.

NIC-Gruppierung tritt auf, wenn einem vSwitch mehrere Uplink-Adapter zugewiesen werden, um eine Gruppe zu bilden. Eine Gruppe kann entweder den Datenverkehr zwischen dem physischen und dem virtuellen Netzwerk auf einige oder alle Netzwerkkarten der Gruppe aufteilen oder ein passives Failover im Falle einer Hardwarestörung oder eines Netzwerkausfalls bereitstellen.

Mit VLANs kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten. Der Standard ist 802.1Q.

Der VMkernel-TCP/IP-Netzwerkstapel unterstützt iSCSI, NFS und VMotion. Virtuelle Maschinen führen TCP/IP-Stapel ihrer eigenen Systeme aus und verbinden sich auf Ethernet-Ebene über virtuelle Switches mit dem VMkernel.

IP-Speicher bezeichnet jedwede Art von Speicher, der auf TCP/IP-Netzwerkkommunikation beruht. iSCSI kann als Datenspeicher für virtuelle Maschinen verwendet werden. NFS kann als Datenspeicher für virtuelle Maschinen oder für die direkte Einbindung von .ISO-Dateien, die dann von der virtuellen Maschine als CD-ROMs erkannt werden, verwendet werden.

TCP Segmentation Offload, TSO, ermöglicht einem TCP/IP-Stapel das Senden sehr großer Datenblöcke (bis zu 64 KB), obgleich die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der Schnittstelle kleiner ist. Der Netzwerkadapter trennt anschließend den großen Datenblock in Datenblöcke mit MTU-Größe und stellt eine angepasste Kopie der einleitenden TCP/IP-Header voran.

Über die Migration mit VMotion kann eine aktivierte virtuelle Maschine von einem ESXi-Host auf einen anderen übertragen werden, ohne dass die virtuelle Maschine heruntergefahren werden muss. Für die optionale VMotion-Funktion ist ein eigener Lizenzschlüssel notwendig.

Netzwerkdienste

Ein vNetwork stellt für den Host und die virtuellen Maschinen mehrere verschiedene Dienste zur Verfügung. Sie können zwei Typen von Netzwerkdiensten in ESXi aktivieren:

- Die Verbindung von virtuellen Maschinen zum physischen Netzwerk sowie die Verbindung untereinander.
- VMkernel-Dienste (zum Beispiel NFS, iSCSI oder VMotion) mit dem physischen Netzwerk verbinden.

Anzeigen der Netzwerkinformationen im vSphere-Client

Der vSphere-Client zeigt sowohl die allgemeinen Netzwerkinformationen als auch solche Informationen an, die spezifisch für Netzwerkadapter sind.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie auf **[Virtueller Switch]**, um das vNetwork-Standard-Switch-Netzwerk, bzw. auf **[Verteilter virtueller Switch]**, um das verteilte vNetwork-Switch-Netzwerk auf dem Host anzuzeigen.

Die Option **[Verteilter virtueller Switch]** wird nur auf den Hosts angeboten, die einem verteilten vNetwork-Switch zugewiesen sind.

Für jeden virtuellen Switch auf dem Host werden Netzwerkinformationen angezeigt.

Anzeigen der Netzwerkadapterinformationen auf dem vSphere-Client

Zu jedem physischen Netzwerkadapter auf dem Host können Sie Informationen wie beispielsweise Geschwindigkeit, Duplex und überwachte IP-Bereiche anzeigen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration (Configuration)]** und anschließend auf **[Netzwerkadapter (Network Adapters)]**.

Das Netzwerkadapterfenster zeigt die folgenden Informationen an:

Option	Beschreibung
[Gerät]	Name des Netzwerkadapters.
[Geschwindigkeit]	Tatsächliche Geschwindigkeit und Duplex des Netzwerkadapters
[Konfiguriert]	Konfigurierte Geschwindigkeit und Duplex des Netzwerkadapters
[vSwitch]	vSwitch, dem der Netzwerkadapter zugeordnet ist
[Überwachte IP-Bereiche]	IP-Adressen, auf die der Netzwerkadapter zugreifen kann
[Wake-on-LAN unterstützt]	Fähigkeit des Netzwerkadapters zur Unterstützung von Wake-on-LAN

Einfache Netzwerke mit vNetwork-Standard-Switches

3

Die folgenden Themen führen Sie durch die Installation und Konfiguration eines einfachen vNetwork-Standard-Switch-Netzwerks (vSwitch-Netzwerk) in einer vSphere-Umgebung.

Mit dem vSphere-Client können Sie eine Netzwerkanbindung herstellen. Dabei gibt es Kategorien, die die Typen von Netzwerkdiensten widerspiegeln:

- Virtuelle Maschinen
- VMkernel

Dieses Kapitel behandelt die folgenden Themen:

- [„vNetwork-Standard-Switches“](#), auf Seite 17
- [„Portgruppen“](#), auf Seite 18
- [„Konfiguration von Portgruppen für virtuelle Maschinen“](#), auf Seite 18
- [„Netzwerkkonfiguration des VMkernels“](#), auf Seite 19
- [„Eigenschaften von vNetwork-Standard-Switches“](#), auf Seite 22

vNetwork-Standard-Switches

Sie können abstrakte Netzwerkgeräte erstellen, die als Standard-vNetwork-Switches (vSwitches) bezeichnet werden. Ein vSwitch kann Datenverkehr intern zwischen virtuellen Maschinen und zwischen virtuellen Maschinen und externen Netzwerken steuern.

Mit vSwitches können Sie die Bandbreite mehrerer Netzwerkadapter kombinieren und den Datenverkehr darauf verteilen. Ein vSwitch kann auch konfiguriert werden, um ein physisches Failover von Netzwerkkarten zu gewährleisten.

Ein vSwitch ersetzt einen physischen Ethernet-Switch. Die Standardanzahl an logischen Ports für einen vSwitch ist 56. In ESXi kann ein vSwitch jedoch bis zu 1016 Ports haben. An jedem Port können Sie einen Netzwerkadapter einer virtuellen Maschine anschließen. Jeder Uplink-Adapter, der mit einem vSwitch verknüpft wurde, verwendet einen Port. Jeder logische Port auf dem vSwitch gehört zu einer Portgruppe. Jedem vSwitch kann darüber hinaus mindestens eine Portgruppe zugewiesen werden. Sie können auf einem einzelnen Host maximal 127 vSwitches einrichten.

Wenn zwei oder mehr virtuelle Maschinen an den gleichen vSwitch angeschlossen sind, wird der Netzwerkdatenverkehr zwischen diesen virtuellen Maschinen lokal gesteuert. Wenn ein Uplink-Adapter an den vSwitch angeschlossen wird, kann jede virtuelle Maschine auf das externe Netzwerk zugreifen, mit dem der Adapter verbunden ist.

Portgruppen

Portgruppen vereinen mehrere Ports unter einer gemeinsamen Konfiguration und bieten so einen stabilen Ankerpunkt für virtuelle Maschinen, die an bezeichnete Netzwerke angeschlossen sind. Sie können auf einem einzelnen Host maximal 512 Portgruppen anlegen.

Jede Portgruppe wird durch eine Netzwerkbezeichnung gekennzeichnet, die im Host eindeutig ist. Netzwerkbezeichnungen sorgen dafür, dass die Konfiguration virtueller Maschinen zwischen Hosts portierbar wird. Alle Portgruppen in einem Datacenter, die physisch mit demselben Netzwerk verbunden sind (in dem Sinne, dass sie Übertragungen von anderen empfangen können), sollten dieselbe Bezeichnung erhalten. Wenn dagegen zwei Portgruppen keine Übertragungen voneinander empfangen können, haben sie unterschiedliche Bezeichnungen.

Eine VLAN-ID, die den Datenverkehr der Portgruppe auf ein logisches Ethernet-Segment im physischen Netzwerk einschränkt, kann optional zugewiesen werden. Damit die Portgruppen, die sich auf anderen VLANs befinden, für eine Portgruppe erreichbar sind, muss die VLAN-ID auf 4095 gesetzt sein. Wenn Sie VLAN-IDs verwenden, müssen Sie die Bezeichnungen der Portgruppen und die VLAN-IDs zusammen ändern, sodass die Bezeichnungen die Konnektivität ordnungsgemäß widerspiegeln.

Konfiguration von Portgruppen für virtuelle Maschinen

Sie können eine Portgruppe einer virtuellen Maschine über den vSphere-Client hinzufügen oder ändern.

Der Assistent zum Hinzufügen von Netzwerken des vSphere-Clients führt Sie durch das Erstellen eines virtuellen Netzwerks, zu dem virtuelle Maschinen eine Verbindung herstellen können, einschließlich des Erstellens eines vSwitches und des Konfigurierens von Einstellungen für eine Netzwerkbezeichnung.

Bedenken Sie beim Einrichten von Netzwerken mit virtuellen Maschinen, ob Sie die virtuellen Maschinen des Netzwerks zwischen Hosts migrieren möchten. Falls ja, stellen Sie sicher, dass sich beide Hosts in derselben Broadcast-Domäne befinden, also im selben Schicht 2-Subnetz.

ESXi unterstützt die Migration virtueller Maschinen zwischen Hosts unterschiedlicher Broadcast-Domänen nicht, weil die migrierte virtuelle Maschine möglicherweise Systeme und Ressourcen benötigt, auf die sie im neuen Netzwerk keinen Zugriff mehr hätte. Selbst wenn Ihre Netzwerkkonfiguration als Hochverfügbarkeitsumgebung eingerichtet ist oder intelligente Switches enthält, die in der Lage sind, dem Bedarf einer virtuellen Maschine auch in verschiedenen Netzwerken zu entsprechen, könnte es sein, dass es in der ARP-Tabelle (Address Resolution Protocol) zu Verzögerungen bei der Aktualisierung und der Wiederaufnahme des Netzwerkverkehrs der virtuellen Maschine kommt.

Virtuelle Maschinen greifen über Uplink-Adapter auf physische Netzwerke zu. Ein vSwitch kann nur dann Daten in externe Netzwerke übertragen, wenn mindestens ein Netzwerkadapter an den vSwitch angeschlossen ist. Wenn zwei oder mehr Adapter an einen vSwitch angeschlossen sind, werden sie transparent gruppiert.

Hinzufügen einer Portgruppe für virtuelle Maschinen

VM-Portgruppen stellen virtuellen Maschinen das Netzwerk bereit.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie die Ansicht Virtueller Switch aus.
vSwitches werden in einer Übersicht angezeigt, die ein detailliertes Layout enthält.
- 4 Klicken Sie auf der rechten Bildschirmseite auf **[Netzwerk hinzufügen (Add Networking)]**.
- 5 Akzeptieren Sie den Standardverbindungstyp **[Virtuelle Maschinen]** und klicken Sie auf **[Weiter]**.

- 6 Wählen Sie **[Einen virtuellen Switch erstellen]** oder einen der aufgelisteten vorhandenen vSwitches und die zugewiesenen physischen Adapter aus, die für diese Portgruppe verwendet werden sollen.

Sie können einen neuen vSwitch mit oder ohne Ethernet-Adapter erstellen.

Wenn Sie einen vSwitch ohne physische Netzwerkadapter erstellen, ist der Datenverkehr auf diesem vSwitch auf diesen vSwitch beschränkt. Andere Hosts im physischen Netzwerk oder virtuelle Maschinen auf anderen vSwitches können dann keine Daten über diesen vSwitch senden oder empfangen. Sie können einen vSwitch ohne physische Netzwerkadapter erstellen, wenn eine Gruppe virtueller Maschinen untereinander, nicht jedoch mit anderen Hosts oder virtuellen Maschinen außerhalb der Gruppe kommunizieren soll.

- 7 Klicken Sie auf **[Weiter]**.

- 8 Geben Sie unter Eigenschaften der Portgruppe (Port Group Properties) eine Netzwerkbezeichnung für die zu erstellende Portgruppe ein.

Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts kennzeichnen.

- 9 (Optional) Geben Sie in das Feld **[VLAN-ID]** eine Nummer zwischen 1 und 4094 ein, wenn Sie ein VLAN verwenden. Lassen Sie das Feld leer, wenn Sie kein VLAN verwenden.

Wenn Sie 0 eingeben oder diese Option frei lassen, kann die Portgruppe nur nicht gekennzeichneten (Nicht-VLAN) Datenverkehr sehen. Wenn Sie 4095 eingeben, kann die Portgruppe jeden Datenverkehr in einem VLAN sehen, und die VLAN-Kennzeichen bleiben intakt.

- 10 Klicken Sie auf **[Weiter]**.

- 11 Überprüfen Sie die ordnungsgemäße Konfiguration des vSwitches noch einmal, und klicken Sie dann auf **[Beenden]**.

Netzwerkconfiguration des VMkernels

Eine VMkernel-Netzwerkschnittstelle wird für VMware vMotion und IP-Speicher verwendet.

In ESXi bietet die VMkernel-Netzwerkschnittstelle eine Netzwerkverbindung für den ESXi-Host und übernimmt die Verarbeitung von vMotion und dem IP-Speicher.

Die Verschiebung einer virtuellen Maschine von einem Host auf einen anderen wird Migration genannt. Mit vMotion können Sie aktivierte virtuelle Maschinen ohne Ausfallzeit migrieren. Der Protokollstapel des VMkernel muss ordnungsgemäß eingerichtet sein, damit vMotion funktioniert.

IP-Speicher bezeichnet jede Art von Speicher, die auf TCP/IP-Netzwerkkommunikation beruht. Dazu gehören iSCSI und NFS für ESXi. Da diese Speichertypen netzwerkbasierend sind, können sie die gleiche VMkernel-Schnittstelle und Portgruppe verwenden.

Die von VMkernel zur Verfügung gestellten Netzwerkdienste (iSCSI, NFS und vMotion) verwenden im VMkernel einen TCP/IP-Stapel. Dieser TCP/IP-Stapel ist vollständig vom TCP/IP-Stapel getrennt, der in der Servicekonsole verwendet wird. Jeder dieser TCP/IP-Stapel greift durch die Anbindung mindestens eines vSwitches an mindestens eine Portgruppe auf verschiedene Netzwerke zu.

TCP/IP-Stapel auf VMkernel-Ebene

Der VMware VMkernel TCP/IP-Netzwerkstack bietet für alle verwalteten Dienste vielfältige Netzwerkunterstützung.

Der VMkernel-TCP/IP-Stack verarbeitet iSCSI, NFS und vMotion folgendermaßen.

- iSCSI als Datenspeicher für virtuelle Maschinen
- iSCSI zur direkten Einbindung von .ISO-Dateien, die von virtuellen Maschinen als CD-ROMs erkannt werden

- NFS als Datenspeicher für virtuelle Maschinen
- NFS zur direkten Einbindung von ISO-Dateien, die von virtuellen Maschinen als CD-ROMs erkannt werden
- Migration mit VMotion

Wenn Sie mehrere physische Netzwerkkarten verwenden, konfigurieren Sie mithilfe der Port-Bindung mehrere Pfade für das Software-iSCSI erstellen. Weitere Informationen zur Port-Bindung finden Sie im *SAN-Konfigurationshandbuch (für iSCSI)*.

HINWEIS ESXi unterstützt über TCP/IP nur die NFS-Version 3.

Einrichten von VMkernel-Netzwerken

Erstellen Sie einen VMkernel-Netzwerkadapter zur Verwendung als eine VMotion-Schnittstelle oder eine IP-Speicherportgruppe.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie in der Ansicht „Virtueller Switch“ auf **[Netzwerk hinzufügen]**.
- 4 Wählen Sie **[VMkernel]** aus, und klicken Sie auf **[Weiter]**.
- 5 Wählen Sie den vSwitch aus, den Sie verwenden möchten, oder aktivieren Sie **[Einen virtuellen Switch erstellen]**, um einen neuen vSwitch anzulegen.
- 6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSwitch verwenden soll.

Wählen Sie für jeden vSwitch Adapter aus, sodass die virtuellen Maschinen oder sonstigen Dienste, die an diesen Adapter angeschlossen sind, auf das richtige Ethernet-Segment zugreifen können. Wenn unter Neuen virtuellen Switch erstellen (Create a new virtual switch) keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden. Sie können entweder einen neuen vSwitch ohne Netzwerkadapter erstellen oder einen Netzwerkadapter auswählen, der von einem bereits vorhandenen vSwitch verwendet wird.
- 7 Klicken Sie auf **[Weiter]**.
- 8 Wählen Sie eine Netzwerkbezeichnung und eine VLAN-ID aus oder erstellen Sie sie.

Option	Beschreibung
[Netzwerkbezeichnung]	Ein Name, der die Portgruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration von VMkernel-Diensten wie VMotion und IP-Speicher während der Konfiguration des virtuellen Adapters, der an diese Portgruppe angeschlossen wird, festlegen.
[VLAN-ID]	Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Portgruppe verwendet wird.

- 9 Aktivieren Sie **[Diese Portgruppe für VMotion verwenden]**, damit diese Portgruppe einem anderen Host melden kann, dass sie als die Netzwerkverbindung dient, an die VMotion-Datenverkehr gesendet werden soll.

Auf jedem Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn diese Eigenschaft für keine der Portgruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.

- 10 Wählen Sie aus, ob Sie diese Portgruppe für die Protokollierung der Fehlertoleranz verwenden möchten, und klicken Sie auf **[Weiter]**.

- 11 Wählen Sie **[IP-Einstellungen automatisch abrufen]** , um DHCP zum Abrufen der IP-Einstellungen zu verwenden, oder **[Die folgenden IP-Einstellungen verwenden]** , um IP-Einstellungen manuell anzugeben.

Wenn Sie sich für die manuelle Eingabe von IP-Einstellungen entscheiden, geben Sie diese Informationen an.

- a Geben Sie die IP-Adresse und die Subnetzmaske der VMkernel-Schnittstelle ein.

Diese Adresse muss sich von der IP-Adresse unterscheiden, die für die Servicekonsole festgelegt wurde.

- b Klicken Sie auf **[Bearbeiten]** , um den VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. VMotion, NAS und iSCSI, zu verwenden.

- c Auf der Registerkarte **[DNS-Konfiguration]** ist standardmäßig der Hostname eingetragen.

Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.

- d Auf der Registerkarte **[Routing]** benötigen die Servicekonsole und der VMkernel jeweils eigene Gateway-Angaben.

Ein Gateway wird zur Verbindung mit Computern benötigt, die sich nicht im selben IP-Subnetz wie die Servicekonsole oder der VMkernel befinden. Standardmäßig sind statische IP-Einstellungen eingestellt.

- e Klicken Sie auf **[OK]** und dann auf **[Weiter]** .

- 12 Wählen Sie auf einem IPv6-aktivierten Host **[Keine IPv6-Einstellungen]** , um nur IPv4-Einstellungen auf der VMkernel-Schnittstelle zu verwenden, oder **[Die folgenden IPv6-Einstellungen verwenden]** , um IPv6 für die VMkernel-Schnittstelle zu konfigurieren.

Dieser Bildschirm wird nicht angezeigt, wenn IPv6 auf dem Host deaktiviert ist.

- 13 Wenn Sie sich für die Verwendung von IPv6 für die VMkernel-Schnittstelle entscheiden, wählen Sie eine der folgenden Optionen zum Abrufen der IPv6-Adressen.

- **[IPv6-Adressen automatisch mittels DHCP erhalten]**
- **[IPv6-Adressen automatisch mittels Router-Ankündigung abrufen]**
- **[Statische IPv6-Adressen]**

- 14 Führen Sie die folgenden Schritte aus, wenn Sie sich für die Verwendung von statischen IPv6-Adressen entscheiden.

- a Klicken Sie auf **[Hinzufügen]** , um eine neue IPv6-Adresse hinzuzufügen.

- b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf **[OK]** .

- c Klicken Sie auf **[Bearbeiten]** , um das Standard-Gateway des VMkernels zu ändern.

- 15 Klicken Sie auf **[Weiter]** .

- 16 Überprüfen Sie die Informationen, klicken Sie auf **[Zurück]** , wenn Sie Einträge ändern möchten, und klicken Sie auf **[Beenden]** .

Eigenschaften von vNetwork-Standard-Switches

Die vNetwork-Standard-Switch-Einstellungen steuern Portstandardeinstellungen für den gesamten vSwitch, die durch Portgruppeneinstellungen für jeden Switch außer Kraft gesetzt werden können. Sie können vSwitch-Eigenschaften, wie beispielsweise die Uplink-Konfiguration und die Anzahl der verfügbaren Ports, bearbeiten.

Ändern der Anzahl der Ports für einen vSwitch

Ein vSwitch dient als Behälter für Portkonfigurationen, die einen gemeinsamen Satz an Netzwerkadaptern verwenden, einschließlich Sätze, die überhaupt keine Netzwerkadapter enthalten. Jeder virtuelle Switch stellt eine bestimmte Anzahl von Ports bereit, über die virtuelle Maschinen und Netzwerkdienste auf mindestens ein Netzwerk zugreifen können.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie rechts auf der Seite auf **[Eigenschaften]** für den zu bearbeitenden vSwitch.
- 4 Klicken Sie auf die Registerkarte **[Ports (Ports)]**.
- 5 Markieren Sie den vSwitch in der Liste Konfiguration, und klicken Sie auf **[Bearbeiten]**.
- 6 Klicken Sie auf die Registerkarte **[Allgemein]**.
- 7 Wählen Sie die Anzahl der Ports, die Sie verwenden möchten, in der Dropdown-Liste aus.
- 8 Klicken Sie auf **[OK]**.

Weiter

Änderungen werden erst bei Neustart des Systems wirksam.

Ändern der Geschwindigkeit eines Uplink-Adapters

Sie können die Verbindungsgeschwindigkeit und Duplex-Einstellung eines Uplink-Adapters ändern.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie einen vSwitch, und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie auf die Registerkarte **[Netzwerkadapter (Network Adapters)]**.
- 5 Um die eingestellte Geschwindigkeit (den Duplexwert) eines Netzwerkadapters zu ändern, markieren Sie den Netzwerkadapter und klicken Sie auf **[Bearbeiten (Edit)]**.
- 6 Um die Verbindungsgeschwindigkeit manuell einzustellen, wählen Sie die Geschwindigkeits- und Duplexeinstellung im dem Dropdown-Menü aus.

Die Verbindungsgeschwindigkeit muss manuell eingestellt werden, wenn die Netzwerkkarte oder ein physischer Switch die ordnungsgemäße Verbindungsgeschwindigkeit nicht erkennen. Anzeichen für falsche Geschwindigkeit und Duplex sind niedrige Bandbreite oder fehlende Konnektivität.

Der Adapter und der physische Switchport, an den der Adapter angeschlossen ist, müssen auf den gleichen Wert gesetzt werden, entweder Auto/Auto oder ND/ND (wobei ND für die Geschwindigkeit/Duplex steht), nicht jedoch Auto/ND.

- 7 Klicken Sie auf **[OK]**.

Hinzufügen von Uplink-Adaptern

Sie können einem einzelnen vSwitch mehrere Adapter zuweisen, um NIC-Gruppierung zu bewirken. Die Gruppe kann den Datenverkehr gemeinsam verarbeiten und Ausfallsicherheit gewährleisten.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie einen vSwitch, und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie auf die Registerkarte **[Netzwerkadapter (Network Adapters)]**.
- 5 Klicken Sie auf **[Hinzufügen]**. Der Assistent zum Hinzufügen eines Adapters wird aufgerufen.
- 6 Wählen Sie mindestens einen Adapter in der Liste aus, und klicken Sie auf **[Weiter]**.
- 7 (Optional) Um die Netzwerkkarten in einer anderen Kategorie neu anzuordnen, wählen Sie eine Netzwerkkarte aus und klicken Sie auf **[Nach oben verschieben]** und auf **[Nach unten verschieben]**.

Option	Beschreibung
Aktive Adapter	Vom vSwitch verwendete Adapter.
Standby-Adapter	Adapter, die aktiv werden, wenn einer oder mehrere der aktiven Adapter ausfallen.

- 8 Klicken Sie auf **[Weiter]**.
- 9 Überprüfen Sie die Informationen auf der Seite „Adapterübersicht“, klicken Sie zum Ändern von Einträgen auf **[Zurück]** und klicken Sie anschließend auf **[Beenden]**.

Die Liste der Netzwerkadapter mit den nun dem vSwitch zugewiesenen Adaptern wird erneut angezeigt.

- 10 Klicken Sie auf **[Schließen]**, um das Dialogfeld vSwitch-Eigenschaften zu schließen.

Der Abschnitt Netzwerk auf der Registerkarte **[Konfiguration]** zeigt die Netzwerkadapter in ihrer festgelegten Reihenfolge und den gewählten Kategorien.

Cisco Discovery-Protokoll

Mit dem Cisco Discovery-Protokoll (CDP) können Administratoren von ESXi den Cisco-Switchport bestimmen, mit dem ein bestimmter vSwitch verbunden ist. Wenn CDP für einen bestimmten vSwitch aktiviert ist, können Sie im vSphere-Client Eigenschaften des Cisco-Switches anzeigen (z. B. Geräte-ID, Softwareversion und Zeitlimit).

In ESXi ist CDP auf „Überwachen“ festgelegt, was bedeutet, dass ESXi Informationen zum verknüpften Cisco-Switchport erkennt und anzeigt. Informationen zum vSwitch stehen jedoch dem Administrator des Cisco-Switches nicht zur Verfügung.

Anzeigen von Cisco-Switchinformationen auf dem vSphere-Client

Wenn CDP auf **[Überwachen]** oder **[Beide]** festgelegt ist, können Sie Cisco-Switchinformationen anzeigen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie auf das Infosymbol rechts neben dem vSwitch.

Einfache Netzwerke mit verteilten vNetwork-Switches

4

Diese Themen befassen sich mit den grundlegenden Konzepten von Netzwerken mit verteilten vNetwork-Switches und mit dem Einrichten und Konfigurieren der Netzwerke in einer vSphere-Umgebung.

Dieses Kapitel behandelt die folgenden Themen:

- „Architektur von verteilten vNetwork-Switches“, auf Seite 25
- „Konfigurieren eines verteilten vNetwork-Switches“, auf Seite 26
- „dvPortgruppen“, auf Seite 28
- „Private VLANs“, auf Seite 30
- „Konfigurieren der Netzwerkadapter des verteilten vNetwork-Switches“, auf Seite 32
- „Konfigurieren von Netzwerken von virtuellen Maschinen auf einem verteilten vNetwork-Switch“, auf Seite 36

Architektur von verteilten vNetwork-Switches

Ein verteilter vNetwork-Switch dient als einzelner virtueller Switch für alle verbundenen Hosts. Dies ermöglicht virtuellen Maschinen bei der Migration zwischen mehreren Hosts die Beibehaltung einer konsistenten Netzwerkkonfiguration.

Genau wie ein vNetwork-Standard-Switch ist jeder verteilter vNetwork-Switch ein Netzwerk-Hub, der von virtuellen Maschinen genutzt werden kann. Mit einem verteilten vNetwork-Switch kann der interne Datenverkehr zwischen virtuellen Maschinen weitergeleitet werden oder es kann über eine Verbindung zu einem physischen Ethernet-Adapter, auch bekannt als „Uplink-Adapter“, eine Verknüpfung mit einem externen Netzwerk hergestellt werden.

Jedem verteilten vNetwork-Switch kann eine oder mehrere dvPortgruppen zugewiesen werden. dvPortgruppen fassen mehrere Ports unter einer gemeinsamen Konfiguration zusammen und bieten einen stabilen Ankerpunkt für virtuelle Maschinen, die eine Verbindung zu benannten Netzwerken herstellen. Jede dvPortgruppe wird durch eine Netzwerkbezeichnung gekennzeichnet, die im entsprechenden Datencenter eindeutig ist. Eine VLAN-ID, die den Datenverkehr der Portgruppe auf ein logisches Ethernet-Segment im physischen Netzwerk einschränkt, kann optional zugewiesen werden.

Neben verteilten vNetwork-Switches von VMware bietet vSphere 4 auch Unterstützung bei der Einrichtung von Drittanbieter-virtuelle-Switches. Weitere Informationen zum Konfigurieren dieser Drittanbieter-Switches finden Sie unter <http://www.cisco.com/go/1000vdocs>.

Konfigurieren eines verteilten vNetwork-Switches

Sie können einen verteilten vNetwork-Switch auf einem vCenter Server-Datencenter erstellen. Nachdem Sie einen verteilten vNetwork-Switch erstellt haben, können Sie Hosts hinzufügen, dvPortgruppen erstellen und die Eigenschaften und Richtlinien des verteilten vNetwork-Switches bearbeiten.

Erstellen eines verteilten vNetwork-Switches

Erstellen Sie einen verteilten vNetwork-Switch, um den Netzwerkverkehr für die zugeordneten Hosts im Datencenter zu bewältigen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und zeigen Sie das Datencenter in der Ansicht „Netzwerk“ an.
- 2 Wählen Sie aus dem Menü „Bestandsliste“ **[Datencenter]** > **[Verteilter vNetwork-Switch]** .
Der Assistent Verteilten vNetwork-Switch erstellen wird angezeigt.
- 3 Geben Sie einen Namen für den verteilten vNetwork-Switch in das Feld „Name“ ein.
- 4 Wählen Sie die **[Anzahl der dvUplink-Ports]** aus und klicken Sie auf **[Weiter]** .
dvUplink-Ports verbinden einen verteilten vNetwork-Switch mit physischen Netzwerkkarten auf zugehörigen ESXi-Hosts. Die Anzahl der dvUplink-Ports ist die maximale Anzahl der zulässigen physischen Verbindungen zum verteilten vNetwork-Switch pro Host.
- 5 Klicken Sie auf **[Weiter]** .
- 6 Wählen Sie zwischen **[Jetzt hinzufügen]** und **[Später hinzufügen]** .
- 7 Wenn Sie **[Jetzt hinzufügen]** möchten, wählen Sie die zu verwendenden Hosts und physischen Adapter aus, indem Sie auf das Kontrollkästchen neben dem jeweiligen Host oder Adapter klicken. Sie können bei der Erstellung von verteilten vNetwork-Switches nur physische Adapter hinzufügen, die noch nicht verwendet werden.
- 8 Klicken Sie auf **[Weiter]** .
- 9 Wählen Sie, ob Sie **[Eine Standard-Portgruppe automatisch erstellen]** möchten.
Diese Option erstellt eine Portgruppe mit früher Bindung mit 128 Ports. Lassen Sie für Systeme mit komplexen Portgruppenanforderungen die Standard-Portgruppe aus und erstellen Sie eine neue dvPortgruppe, nachdem Sie mit dem Hinzufügen des verteilten vNetwork-Switches fertig sind.
- 10 Zeigen Sie das Diagramm des verteilten vNetwork-Switches an, um die ordnungsgemäße Konfiguration zu überprüfen, und klicken Sie auf **[Beenden]** .

Weiter

Wenn Sie auswählen, Hosts später hinzuzufügen, müssen Sie dies tun, bevor Sie dem verteilten vNetwork-Switch Netzwerkadapter hinzufügen.

Netzwerkadapter können über die Hostkonfigurationsseite des vSphere-Clients oder mithilfe von Hostprofilen hinzugefügt werden.

Hinzufügen eines Hosts zu einem verteilten vNetwork-Switch

Mit dem Assistenten zum Hinzufügen eines Hosts zu einem verteilten vNetwork-Switch können Sie einen Host mit einem verteilten vNetwork-Switch verknüpfen. Sie können Hosts auch mithilfe von Hostprofilen zu einem verteilten vNetwork-Switch hinzufügen.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Verteilter Virtueller Switch] > [Host hinzufügen]**.

Der Assistent zum Hinzufügen eines Hosts zu einem verteilten vNetwork-Switch wird angezeigt.

- 3 Wählen Sie den hinzuzufügenden Host aus.
- 4 Wählen Sie unter dem ausgewählten Host die hinzuzufügenden physischen Adapter aus und klicken Sie auf **[Weiter]**.

Sie können sowohl freie physische Adapter auswählen als auch solche, die gerade verwendet werden. Wenn Sie einen Adapter auswählen, der gerade von einem Host verwendet wird, wählen Sie aus, ob die zugewiesenen virtuellen Adapter in den Verteilten vNetwork-Switches verschoben werden sollen.

HINWEIS Wenn Sie einen physischen Adapter auf einen verteilten vNetwork-Switch verschieben, ohne zugewiesene virtuelle Adapter zu verschieben, verlieren diese virtuellen Adapter die Netzwerkkonktivität.

- 5 Klicken Sie auf **[Beenden]**.

Bearbeiten der allgemeinen Einstellungen für den verteilten vNetwork-Switch

Sie können die allgemeinen Eigenschaften eines verteilten vNetwork-Switch bearbeiten, z. B. den Namen des verteilten vNetwork-Switches und die Anzahl der Uplink-Ports auf dem verteilten vNetwork-Switch.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü „Bestandsliste“ **[Verteilter virtueller Switch] > [Einstellungen bearbeiten]**.
- 3 Wählen Sie **[Allgemein]**, um die folgenden Einstellungen des verteilten vNetwork-Switches zu bearbeiten.
 - a Geben Sie den Namen für den verteilten vNetwork-Switch ein.
 - b Wählen Sie die Anzahl der Uplink-Ports aus.
 - c Klicken Sie zum Bearbeiten der Uplink-Portnamen auf **[Uplink-Portnamen bearbeiten]**, geben Sie die neuen Namen ein und klicken Sie auf **[OK]**.
 - d Geben Sie beliebige Anmerkungen für den verteilten vNetwork-Switch ein.
- 4 Klicken Sie auf **[OK]**.

Bearbeiten der erweiterten Einstellungen des verteilten vNetwork-Switches

Verwenden Sie im Dialogfeld das „Einstellungen für einen verteilten vNetwork-Switch“ zum Konfigurieren von erweiterten Einstellungen für den verteilten vNetwork-Switch, wie z. B. das Cisco Discovery-Protokoll und den Maximalwert für MTU für den verteilten vNetwork-Switch.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü „Bestandsliste“ **[Verteilter Virtueller Switch]** > **[Einstellungen bearbeiten]** .
- 3 Wählen Sie **[Erweitert]** , um die folgenden Eigenschaften des verteilten vNetwork-Switches zu bearbeiten.
 - a Geben Sie die maximale MTU-Größe ein.
 - b Aktivieren Sie das Kontrollkästchen **[Cisco Discovery-Protokoll aktivieren]** , um CDP zu aktivieren und die Operation auf **[Überwachen]** , **[Werben]** oder **[Beide]** zu setzen.
 - c Geben Sie den Namen und weitere Details für den Administrator des verteilten vNetwork-Switches im Abschnitt für Administrator-Kontaktinformationen ein.
- 4 Klicken Sie auf **[OK]** .

Anzeigen von Netzwerkkadaptersinformationen für einen verteilten vNetwork-Switch

Zeigen Sie physische Netzwerkkadapters und Uplink-Zuweisungen für einen verteilten vNetwork-Switch über die Netzwerk-Bestandslistenansicht des vSphere-Clients an.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü „Bestandsliste“ **[Verteilter Virtueller Switch]** > **[Einstellungen bearbeiten]** .
- 3 Auf der Registerkarte **[Netzwerkkadapters]** können Sie Netzwerkkadapters und Uplink-Zuweisungen für zugewiesene Hosts anzeigen.

Diese Registerkarte ist schreibgeschützt. Netzwerkkadapters von verteilten vNetwork-Switches müssen auf der Hostebene konfiguriert werden.
- 4 Klicken Sie auf **[OK]** .

dvPortgruppen

Eine dvPortgruppe legt für jeden seiner Ports auf einem verteilten vNetwork-Switch Konfigurationsoptionen fest. dvPortgruppen definieren, wie eine Verbindung zu einem Netzwerk hergestellt wird.

Hinzufügen einer dvPortgruppe

Verwenden Sie den Assistenten zum Erstellen einer dvPortgruppe, um eine dvPortgruppe zu einem verteilten vNetwork-Switch hinzuzufügen.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** die Option **[Verteilter Virtueller Switch]** > **[Neue Portgruppe]** .

- 3 Geben Sie einen Namen und die Anzahl der Ports in der dvPortgruppe ein.
- 4 Wählen Sie einen VLAN-Typ.

Option	Beschreibung
Keine	Verwenden Sie VLAN nicht.
VLAN	Geben Sie im Feld [VLAN-ID] eine Zahl zwischen 1 und 4094 ein.
VLAN-Trunking	Geben Sie einen VLAN-Trunk-Bereich ein.
Privates VLAN	Wählen Sie einen Eintrag für ein privates VLAN. Wenn Sie keine privaten VLANs erstellt haben, bleibt dieses Menü leer.

- 5 Klicken Sie auf **[Weiter]**.
- 6 Klicken Sie auf **[Beenden]**.

Bearbeiten von allgemeinen Eigenschaften von dvPortgruppen

Im Eigenschaftendialogfeld für eine dvPortgruppe können Sie allgemeine Eigenschaften der dvPortgruppe konfigurieren, wie z. B. den Namen der dvPortgruppe und den Portgruppentyp.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk]** > **[Einstellungen bearbeiten]**.
- 3 Wählen Sie **[Allgemein]**, um die folgenden Eigenschaften der dvPortgruppe zu bearbeiten:

Option	Aktion
Name	Geben Sie den Namen für die dvPortgruppe ein.
Beschreibung	Geben Sie eine kurze Beschreibung der dvPortgruppe ein.
Anzahl der Ports	Geben Sie die Anzahl der Ports in der dvPortgruppe ein.
Port-Bindung	<p>Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser dvPortgruppe verbunden sind.</p> <ul style="list-style-type: none"> ■ Wählen Sie [Statische Bindung], um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine mit der dvPortgruppe verbunden wird. ■ Wählen Sie [Dynamische Bindung], um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine zum ersten Mal eingeschaltet wird, nachdem sie mit der dvPortgruppe verbunden wurde. ■ Wählen Sie [Flüchtig], um keine Port-Bindung einzugehen.

- 4 Klicken Sie auf **[OK]**.

Bearbeiten von erweiterten Eigenschaften von dvPortgruppen

Im Eigenschaftendialogfeld für eine dvPortgruppe können Sie erweiterte Eigenschaften der dvPortgruppe konfigurieren, wie z. B. das Format des Portnamens und die Außerkraftsetzungseinstellungen.

Vorgehensweise

- 1 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk] > [Einstellungen bearbeiten]** .
- 2 Wählen Sie **[Erweitert]** , um die Eigenschaften der dvPortgruppe zu bearbeiten.
 - a Wählen Sie **[Außerkraftsetzung der Portrichtlinien zulassen]** aus, damit die Richtlinien von dvPortgruppen für einzelne Ports außer Kraft gesetzt werden können.
 - b Klicken Sie auf **[Außerkraftsetzungseinstellungen bearbeiten]** , um auszuwählen, welche Richtlinien außer Kraft gesetzt werden können.
 - c Wählen Sie aus, ob Sie das Verschieben von Live-Port zulassen möchten.
 - d Wählen Sie **[Zurücksetzen bei Verbindungstrennung konfigurieren]** , um portspezifische Konfigurationen außer Kraft zu setzen, wenn eine dvPort-Verbindung zu einer virtuellen Maschine getrennt wird.
 - e Wählen Sie **[Bindung auf Host zulässig]** , um anzugeben, dass ESXi einer virtuellen Maschine einen dvPort zuweisen kann, wenn vCenter Server nicht verfügbar ist.
 - f Wählen Sie **[Format des Portnamens]** aus, um eine Vorlage zum Zuweisen von Namen zu den dvPorts in dieser Gruppe zur Verfügung zu stellen.
- 3 Klicken Sie auf **[OK]** .

Konfigurieren von dvPort-Einstellungen

Verwenden Sie das Dialogfeld Porteinstellungen, um allgemeine dvPort-Eigenschaften zu konfigurieren, wie z. B. Portnamen und -beschreibung.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.
- 3 Klicken Sie auf **[Allgemein]** .
- 4 Ändern Sie den Namen und die Beschreibung des Ports.
- 5 Klicken Sie auf **[OK]** .

Private VLANs

Bei bestehenden VLAN-ID-Beschränkungen und um die Verschwendung von IP-Adressen zu vermeiden, werden für bestimmte Netzwerk-Setups private VLANs verwendet.

Ein privates VLAN wird durch seine primäre VLAN-ID identifiziert. Einer primären VLAN-ID können mehrere sekundäre VLAN-IDs zugeordnet sein. Primäre VLANs sind **[Promiscuous]** , sodass Ports in einem privaten VLAN mit Ports kommunizieren können, die als primäres VLAN konfiguriert sind. Ports in einem sekundären VLAN können entweder **[Isoliert]** sein und nur mit Promiscuous-Ports kommunizieren oder es handelt sich um **[Community]** -Ports, die sowohl mit Promiscuous-Ports als auch mit anderen Ports im gleichen sekundären VLAN kommunizieren.

Wenn Sie private VLANs zwischen einem ESXi-Host und dem Rest des physischen Netzwerks verwenden möchten, muss der physische Switch, der mit dem ESXi-Host verbunden ist, privates VLAN unterstützen und ordnungsgemäß mit den von ESXi verwendeten VLAN-IDs konfiguriert sein, damit das private VLAN funktioniert. Für physische Switches, die dynamisches MAC+VLAN-ID-basiertes Lernen verwenden, müssen alle entsprechenden privaten VLAN-IDs zuerst in die VLAN-Datenbank des Switches eingegeben werden.

Um dvPorts für die Verwendung von privatem VLAN zu konfigurieren, müssen Sie zunächst auf dem verteilten vNetwork-Switch, mit dem die dvPorts verbunden sind, die benötigten privaten VLANs erstellen.

Erstellen eines privaten VLANs

Sie können ein privates VLAN erstellen, das auf einem verteilten vNetwork-Switch und seinen zugeordneten dvPorts verwendet wird.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** die Option **[Verteilter vNetwork-Switch] > [Einstellungen bearbeiten]**.
- 3 Wählen Sie die Registerkarte **[Privates VLAN]** aus.
- 4 Klicken Sie unter ID des primären privaten VLANs auf **[] [ID eines privaten VLAN hier eingeben]** und geben Sie die Nummer des primären privaten VLANs ein.
- 5 Klicken Sie auf eine beliebige Stelle im Dialogfeld und wählen Sie dann das primäre private VLAN aus, das Sie gerade hinzugefügt haben.

Das von Ihnen hinzugefügte primäre private VLAN wird unter „ID des sekundären privaten VLANs“ angezeigt.

- 6 Klicken Sie für jedes neue sekundäre private VLAN unter „ID des sekundären privaten VLANs“ auf **[ID eines privaten VLAN hier eingeben]** und geben Sie die Nummer des sekundären privaten VLANs ein.
- 7 Klicken Sie auf eine beliebige Stelle im Dialogfeld, wählen Sie das gerade hinzugefügte, sekundäre private VLAN aus und wählen Sie als Port-Typ entweder **[Isoliert]** oder **[Community]** aus.
- 8 Klicken Sie auf **[OK]**.

Entfernen eines primären privaten VLANs

Entfernen Sie ungenutzte primäre private VLANs über die Netzwerk-Bestandslistenansicht des vSphere-Clients.

Voraussetzungen

Bevor Sie ein privates VLAN entfernen, stellen Sie sicher, dass keine Portgruppen für seine Verwendung konfiguriert sind.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** die Option **[Verteilter vNetwork-Switch] > [Einstellungen bearbeiten]**.
- 3 Wählen Sie die Registerkarte **[Privates VLAN]** aus.

- 4 Wählen Sie das primäre private VLAN aus, das entfernt werden soll.
- 5 Klicken Sie unter „ID des primären privaten VLANs“ auf **[Entfernen]** und klicken Sie auf **[OK]** .
Beim Entfernen eines primären privaten VLANs werden auch alle zugeordneten sekundären privaten VLANs entfernt.

Entfernen eines sekundären privaten VLANs

Entfernen Sie ungenutzte sekundäre private VLANs über die Netzwerk-Bestandslistenansicht des vSphere-Clients.

Voraussetzungen

Bevor Sie ein privates VLAN entfernen, stellen Sie sicher, dass keine Portgruppen für seine Verwendung konfiguriert sind.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** die Option **[Verteilter vNetwork-Switch] > [Einstellungen bearbeiten]** .
- 3 Wählen Sie die Registerkarte **[Privates VLAN]** aus.
- 4 Wählen Sie ein primäres privates VLAN aus, um die ihm zugewiesenen sekundären privaten VLANs anzuzeigen.
- 5 Wählen Sie das sekundäre private VLAN aus, das entfernt werden soll.
- 6 Klicken Sie unter „ID des sekundären privaten VLANs“ auf **[Entfernen]** und klicken Sie auf **[OK]** .

Konfigurieren der Netzwerkadapter des verteilten vNetwork-Switches

In der verteilten vNetwork-Switch-Ansicht „Netzwerk“ der Hostkonfigurationsseite wird die Konfiguration der dem Host zugewiesenen verteilten vNetwork-Switches angezeigt. Sie können dort die Netzwerkadapter und die Uplink-Ports für die verteilten vNetwork-Switches konfigurieren.

Verwalten physischer Adapter

Für jeden Host, der mit einem verteilten vNetwork-Switch verbunden ist, müssen Sie dem verteilten vNetwork-Switch physische Netzwerkadapter oder Uplinks zuweisen. Sie können auf jedem Host einen Uplink pro Uplink-Port auf dem verteilten vNetwork-Switch zuweisen.

Hinzufügen eines Uplinks zu einem verteilten vNetwork-Switch

Einem verteilten vNetwork-Switch müssen physische Uplinks hinzugefügt werden, damit die mit ihm verbundenen virtuellen Maschinen und virtuellen Netzwerkadapter sich mit den Netzwerken außerhalb der Hosts verbinden können, auf denen sie sich befinden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Wählen Sie die Ansicht Verteilter vNetwork-Switch aus.
- 4 Klicken Sie auf **[Physische Adapter verwalten]** .
- 5 Klicken Sie für den Uplink-Port, zu dem ein Uplink hinzugefügt werden soll, auf **[Klicken Sie, um eine Netzwerkkarte hinzuzufügen]** .

- 6 Wählen Sie den physischen Adapter aus, der hinzugefügt werden soll. Wenn Sie einen Adapter auswählen, der mit einem anderen Switch verbunden ist, wird er von diesem Switch entfernt und diesem verteilten vNetwork-Switch neu zugeordnet.
- 7 Klicken Sie auf **[OK]**.

Entfernen eines Uplinks aus einem verteilten vNetwork-Switch

Ein bereits einem verteilten vNetwork-Switch zugewiesener Uplink kann einem vSwitch oder einem anderen verteilten vNetwork-Switch nicht mehr zugewiesen werden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie die Ansicht Verteilter vNetwork-Switch aus.
- 4 Klicken Sie auf **[Physische Adapter verwalten]**.
- 5 Klicken Sie für den zu entfernenden Uplink auf **[Entfernen]**.
- 6 Klicken Sie auf **[OK]**.

Verwalten von virtuellen Netzwerkadaptern

Virtuelle Netzwerkadapter verwalten Netzwerkdienste eines Hosts über einen verteilten vNetwork-Switch.

Sie können virtuelle VMkernel-Adapter für einen ESXi-Host über einen zugewiesenen verteilten vNetwork-Switch konfigurieren, indem Sie neue virtuelle Adapter erstellen oder vorhandene virtuelle Adapter migrieren.

Erstellen eines VMkernel-Netzwerkadapters auf einem verteilten vNetwork-Switch

Erstellen Sie einen VMkernel-Netzwerkadapter zur Verwendung als eine VMotion-Schnittstelle oder eine IP-Speicherportgruppe.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie die Ansicht Verteilter vNetwork-Switch aus.
- 4 Klicken Sie auf **[Virtuelle Adapter verwalten]**.
- 5 Klicken Sie auf **[Hinzufügen]**.
- 6 Wählen Sie **[Neuer virtueller Adapter]** und klicken Sie auf **[Weiter]**.
- 7 Wählen Sie **[VMkernel]** aus, und klicken Sie auf **[Weiter]**.
- 8 Wählen Sie zum Hinzufügen dieses virtuellen Adapters unter „Netzwerkverbindung“ den verteilten vNetwork-Switch und die verknüpfte Portgruppe oder **[Eigenständiger Port]** aus.
- 9 Wählen Sie **[Diesen virtuellen Adapter für VMotion verwenden]**, damit diese Portgruppe auf einem anderen ESXi-Host für sich werben kann, als die Netzwerkverbindung, an die VMotion-Datenverkehr gesendet ist.

Auf jedem ESXi-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn diese Eigenschaft für keine der Portgruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.

- 10 Wählen Sie, ob Sie **[Diesen virtuellen Adapter für die Fehlertoleranz-Protokollierung verwenden]** möchten.

- 11 Wählen Sie, ob Sie **[Diesen virtuellen Adapter für den Verwaltungsdatenverkehr verwenden]** möchten, und klicken Sie auf **[Weiter]** .
- 12 Geben Sie unter „IP-Einstellungen“ die IP-Adresse und die Subnetzmaske an.
- 13 Klicken Sie auf **[Bearbeiten]** , um den VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. VMotion, NAS und iSCSI, zu verwenden.
- 14 Auf der Registerkarte **[DNS-Konfiguration]** ist standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen.
- 15 Auf der Registerkarte **[Routing]** benötigen die Servicekonsole und der VMkernel jeweils eigene Gateway-Angaben. Ein Gateway wird zur Verbindung mit Computern benötigt, die sich nicht im selben IP-Subnetz wie die Servicekonsole oder der VMkernel befinden.
Statische IP-Einstellungen sind voreingestellt.
- 16 Klicken Sie auf **[OK]** und dann auf **[Weiter]** .
- 17 Klicken Sie auf **[Beenden]** .

Migrieren eines vorhandenen virtuellen Adapters auf einen verteilten vNetwork-Switch

Migrieren Sie auf der Seite „Hostkonfiguration“ einen vorhandenen virtuellen Adapter von einem vNetwork-Standard-Switch zu einem verteilten vNetwork-Switch.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Wählen Sie die Ansicht Verteilter vNetwork-Switch aus.
- 4 Klicken Sie auf **[Virtuelle Adapter verwalten]** .
- 5 Klicken Sie auf **[Hinzufügen]** .
- 6 Wählen Sie **[Vorhandene virtuelle Adapter migrieren]** und klicken Sie auf **[Weiter]** .
- 7 Wählen Sie im Dropdown-Menü **[Auswahl nach]** aus, ob Sie diesen virtuellen Adapter mit einer Portgruppe oder einem eigenständigen dvPort verbinden möchten.
- 8 Wählen Sie mindestens einen zu migrierenden virtuellen Netzwerkadapter aus.
- 9 Wählen Sie für jeden ausgewählten Adapter eine Portgruppe oder einen dvPort aus dem Dropdown-Menü **[Portgruppe auswählen]** bzw. **[Port auswählen]** aus.
- 10 Klicken Sie auf **[Weiter]** .
- 11 Klicken Sie auf **[Beenden]** .

Migrieren eines virtuellen Adapters auf einen vNetwork-Standard-Switch

Verwenden Sie den Assistenten Nach virtuellem Switch migrieren, um einen vorhandenen virtuellen Adapter von einem verteilten vNetwork-Switch zu einem vNetwork-Standard-Switch zu migrieren.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
Die Seite **[Hardwarekonfiguration]** für diesen Server wird angezeigt.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Wählen Sie die Ansicht **[Verteilter vNetwork-Switch]** aus.

- 4 Klicken Sie auf **[Virtuelle Adapter verwalten]** .
- 5 Wählen Sie den zu migrierenden virtuellen Adapter aus und klicken Sie auf **[Nach virtuellem Switch migrieren]** .
Der Assistent Virtuellen Adapter migrieren wird angezeigt.
- 6 Wählen Sie den vSwitch aus, zu dem der Adapter migriert werden soll, und klicken Sie auf **[Weiter]** .
- 7 Geben Sie eine **[Netzwerkbezeichnung]** und optional eine **[VLAN-ID]** für den virtuellen Adapter ein und klicken Sie auf **[Weiter]** .
- 8 Klicken Sie auf **[Beenden]** , um den Assistenten abzuschließen und den virtuellen Adapter zu migrieren.

Bearbeiten der VMkernel-Konfiguration für einen verteilten vNetwork-Switch

Sie können die Eigenschaften eines vorhandenen VMkernel-Adapters auf einem verteilten vNetwork-Switch von dem zugewiesenen Host aus bearbeiten.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Wählen Sie die Ansicht Verteilter vNetwork-Switch aus.
- 4 Klicken Sie auf **[Virtuelle Adapter verwalten]** .
- 5 Wählen Sie den VMkernel-Adapter aus, der geändert werden soll, und klicken Sie auf **[Bearbeiten]** .
- 6 Wählen Sie zum Hinzufügen dieses virtuellen Adapters unter „Netzwerkverbindung“ den verteilten vNetwork-Switch und die verknüpfte Portgruppe oder **[Eigenständiger Port]** aus.
- 7 Wählen Sie **[Diesen virtuellen Adapter für VMotion verwenden]** , damit diese Portgruppe auf einem anderen ESXi-Host für sich werben kann, als die Netzwerkverbindung, an die VMotion-Datenverkehr gesendet ist.
Auf jedem ESXi-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn diese Eigenschaft für keine der Portgruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.
- 8 Wählen Sie, ob Sie **[Diesen virtuellen Adapter für die Fehlertoleranz-Protokollierung verwenden]** möchten.
- 9 Wählen Sie, ob Sie **[Diesen virtuellen Adapter für den Verwaltungsdatenverkehr verwenden]** möchten, und klicken Sie auf **[Weiter]** .
- 10 Geben Sie unter „IP-Einstellungen“ die IP-Adresse und Subnetzmaske an oder wählen Sie **[IP-Einstellungen automatisch abrufen]** .
- 11 Klicken Sie auf **[Bearbeiten]** , um den VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. VMotion, NAS und iSCSI, zu verwenden.
- 12 Klicken Sie auf **[OK]** .

Entfernen eines virtuellen Adapters

Im Dialogfeld „Virtuelle Adapter verwalten“ können Sie einen virtuellen Netzwerkadapter aus einem verteilten vNetwork-Switch entfernen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .

- 3 Wählen Sie die Ansicht **[Verteilter vNetwork-Switch]** aus.
- 4 Klicken Sie auf **[Virtuelle Adapter verwalten]**.
- 5 Wählen Sie den zu entfernenden virtuellen Adapter aus und klicken Sie auf **[Entfernen]**.
Ein Dialogfeld mit der Meldung „Möchten Sie <Adaptername> wirklich löschen?“ wird angezeigt.
- 6 Klicken Sie auf **[Ja]**.

Konfigurieren von Netzwerken von virtuellen Maschinen auf einem verteilten vNetwork-Switch

Virtuelle Maschinen können mit einem verteilten vNetwork-Switch entweder durch die Konfiguration einer individuellen virtuellen Netzwerkkarte oder durch die Migration von Gruppen virtueller Maschinen vom verteilten vNetwork-Switch selbst verbunden werden.

Virtuelle Maschinen werden mit verteilten vNetwork-Switches verbunden, indem die ihnen zugewiesenen virtuellen Netzwerkadapter mit dvPortgruppen verbunden werden. Dies kann entweder für eine individuelle virtuelle Maschine durch Ändern der Konfiguration des Netzwerkadapters der virtuellen Maschinen oder für eine Gruppe von virtuellen Maschinen durch ihre Migration von einem vorhandenen virtuellen Netzwerk auf einen verteilten vNetwork-Switch geschehen.

Migrieren virtueller Maschinen auf einen oder von einem verteilten vNetwork-Switch

Zusätzlich zum Verbinden einzelner virtueller Maschinen mit einem verteilten vNetwork-Switch können Sie eine Gruppe von virtuellen Maschinen zwischen einem Netzwerk von verteilten vNetwork-Switches und einem vNetwork-Standard-Switch-Netzwerk migrieren.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** die Option **[Verteilter virtueller Switch] > [Netzwerk virtueller Maschinen migrieren]**.
Der Assistent zum Migrieren von Netzwerken virtueller Maschinen wird angezeigt.
- 3 Wählen Sie im Dropdown-Menü **[Netzwerkquelle auswählen]** das virtuelle Netzwerk aus, das die Quelle für den Migrationsvorgang sein soll.
- 4 Wählen Sie im Dropdown-Menü **[Zielnetzwerk auswählen]** das virtuelle Netzwerk aus, das das Ziel der Migration sein soll.
- 5 Klicken Sie auf **[Virtuelle Maschinen anzeigen]**.
Im Feld **[Virtuelle Maschinen auswählen]** werden die virtuellen Maschinen angezeigt, die dem virtuellen Netzwerk zugewiesen sind, das als Quelle für die Migration dient.
- 6 Wählen Sie die virtuellen Maschinen aus, die in das virtuelle Zielnetzwerk migriert werden sollen, und klicken Sie auf **[OK]**.

Verbinden einer individuellen virtuellen Maschine mit einer dvPortgruppe

Verbinden Sie eine individuelle virtuelle Maschine durch Ändern ihrer Netzwerkkartenkonfiguration mit einem verteilten vNetwork-Switch.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Wählen Sie auf der Registerkarte **[Hardware]** den virtuellen Netzwerkadapter aus.
- 4 Wählen Sie im Dropdown-Menü **[Netzwerkbezeichnung]** die zu migrierende dvPortgruppe aus und klicken Sie auf **[OK]**.

Erweiterte Netzwerkthemen

Die folgenden Kapitel führen Sie durch die erweiterten Netzwerkthemen in einer ESXi-Umgebung sowie durch die Einrichtung und Änderung erweiterter Netzwerkkonfigurationsoptionen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Internet Protocol Version 6“](#), auf Seite 39
- [„Netzwerkrichtlinien“](#), auf Seite 40
- [„Ändern der DNS- und Routing-Konfiguration“](#), auf Seite 57
- [„MAC-Adressen“](#), auf Seite 57
- [„TCP-Segmentierungs-Offload und Jumbo-Frames“](#), auf Seite 59
- [„NetQueue und Netzwerkleistung“](#), auf Seite 61
- [„VMDirectPath Gen I“](#), auf Seite 62

Internet Protocol Version 6

vSphere unterstützt sowohl Internetprotokollversion 4 (IPv4) als auch Internetprotokollversion 6 (IPv6).

IPv6 wurde von der Internet Engineering Task Force als Nachfolger von IPv4 bestimmt. Die Verwendung von IPv6, sowohl als ein eigenständiges Protokoll als auch in einer gemischten Umgebung mit IPv4, nimmt schnell zu. In IPv6 können Sie vSphere-Funktionen wie NFS in einer IPv6-Umgebung verwenden.

Ein wesentlicher Unterschied zwischen IPv4 und IPv6 besteht in der Adressenlänge. IPv6 verwendet 128-Bit-Adressen statt die 32-Bit-Adressen, die IPv4 verwendet. Dies löst das Problem der Adressknappheit bei IPv4 und macht die Netzwerkadressübersetzung (NAT) überflüssig. Weitere bedeutende Unterschiede sind Link-Local-Adressen, die beim Initialisieren der Schnittstelle erscheinen, Adressen, die über eine Router-Ankündigung festgelegt werden, und die Fähigkeit, mehrere IPv6-Adressen auf einer Schnittstelle zu haben.

Zu einer IPv6-spezifischen Konfiguration in vSphere gehört das Angeben von IPv6-Adressen für alle relevanten vSphere-Netzwerkschnittstellen, entweder durch Eingabe von statischen Adressen oder durch Verwendung von DHCP. IPv6-Adressen können auch unter Verwendung der mittels Router-Ankündigung gesendeten Stateless-Autokonfiguration konfiguriert werden.

Aktivieren von IPv6-Unterstützung auf einem ESXi-Host

Sie können die IPv6-Unterstützung auf dem Host aktivieren oder deaktivieren.

Vorgehensweise

- 1 Klicken Sie in der Navigationsleiste auf den Pfeil neben der Schaltfläche **[Bestandsliste]**, und wählen Sie **[Hosts und Cluster]**.
- 2 Wählen Sie einen Host, und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Klicken Sie unter Hardware auf den Link **[Netzwerk]**.
- 4 Klicken Sie in der Ansicht „Virtueller Switch“ auf den Link **[Eigenschaften]**.
- 5 Wählen Sie **[IPv6-Unterstützung auf diesem Host aktivieren]** und klicken Sie auf **[OK]**.
- 6 Starten Sie den Host neu.

Netzwerkrichtlinien

Richtlinien, die auf vSwitch-Ebene oder auf dvPort-Gruppenebene festgelegt werden, werden für alle Portgruppen auf diesem vSwitch bzw. für alle dvPorts in der dvPort-Gruppe übernommen. Ausgenommen davon sind die Konfigurationsoptionen, die auf Portgruppen- oder dvPort-Gruppenebene außer Kraft gesetzt werden können.

Folgende Netzwerkrichtlinien können angewendet werden

- Lastausgleich und Failover
- VLAN (nur verteilter vNetwork-Switch)
- Sicherheit
- Traffic-Shaping
- Portblockierungsrichtlinien (nur verteilter vNetwork-Switch)

Richtlinie für Lastausgleich und Failover

Mit den Lastausgleichs- und Failover-Richtlinien können Sie festlegen, wie der Netzwerkdatenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt.

Sie können Ihre Lastausgleichs- und Failover-Richtlinien bearbeiten, indem Sie die folgenden Parameter konfigurieren:

- Die **[Lastausgleichsrichtlinie (Load Balancing policy)]** legt fest, wie der ausgehende Datenverkehr über die Netzwerkadapter verteilt wird, die einem vSwitch zugewiesen wurden.

HINWEIS Der eingehende Datenverkehr wird durch die Lastausgleichsrichtlinie auf dem physischen Switch gesteuert.

- Die **[Failover-Ermittlung]** steuert den Verbindungsstatus und die Signalprüfung. Beaconing wird nicht mit Gast-VLAN-Tagging unterstützt.
- Die **[Reihenfolge der Netzwerkadapter]** kann sich auf „Aktiv“ oder „Standby“ beziehen.

Bearbeiten der Failover- und Lastausgleichs-Richtlinie für einen vSwitch

Mit den Lastausgleichs- und Failover-Richtlinien können Sie festlegen, wie der Netzwerkdatenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Wählen Sie einen vSwitch, und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie im Dialogfeld vSwitch-Eigenschaften auf die Registerkarte **[Ports]**.
- 5 Zum Bearbeiten der Failover- und Lastausgleichswerte für den vSwitch wählen Sie das vSwitch-Element und klicken Sie auf **[Eigenschaften]**.
- 6 Klicken Sie auf die Registerkarte **[NIC-Gruppierung]**.

Sie können die Failover-Reihenfolge auf Portgruppenebene außer Kraft setzen. Standardmäßig werden neue Adapter für alle Richtlinien aktiviert. Neue Adapter übertragen den Datenverkehr für den vSwitch und seine Portgruppe, wenn Sie nichts anderes angeben.

- 7 Legen Sie die Einstellungen in der Gruppe „Richtlinienausnahmen“ fest.

Option	Beschreibung
Lastenausgleich	<p>Geben Sie an, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ [Anhand der Quelle der Port-ID routen] – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert. ■ [Anhand des IP-Hashs routen] – Der Uplink wird anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ [Anhand des Quell-MAC-Hashs routen] – Der Uplink wird anhand eines Hashs des Quell-Ethernets ausgewählt. ■ [Explizite Failover-Reihenfolge verwenden] – Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt. <p>HINWEIS Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Bei allen anderen Optionen muss „etherchannel“ deaktiviert sein.</p>
Netzwerk-Failover-Ermittlung	<p>Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.</p> <ul style="list-style-type: none"> ■ [Nur Verbindungsstatus] – Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP, eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ [Signalprüfung] – Sendet Signale, sucht nach Signalprüfpaketen auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können.

Option	Beschreibung
Switches benachrichtigen	<p>Wählen Sie [Ja] oder [Nein] , um Switches bei einem Failover zu benachrichtigen.</p> <p>Wenn Sie [Ja] wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen vSwitch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Meldung gesendet, um die Verweistabelle auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.</p> <p>HINWEIS Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastenausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.</p>
Failback	<p>Wählen Sie [Ja] oder [Nein] , um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf [Ja] (Standard) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf [Nein] gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.</p>
Failover-Reihenfolge	<p>Geben Sie an, wie die Verarbeitungslast für Uplinks verteilt werden soll. Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle reservieren möchten, z. B. wenn die verwendeten Uplinks ausfallen, legen Sie diesen Zustand fest, indem Sie sie in unterschiedliche Gruppen verschieben:</p> <ul style="list-style-type: none"> ■ [Aktive Uplinks] – Der Uplink wird weiter verwendet, wenn die Netzwerkkartenverbindung hergestellt und aktiv ist. ■ [Standby-Uplinks] – Dieser Uplink wird verwendet, wenn mindestens eine Verbindung des aktiven Adapters nicht verfügbar ist. ■ [Nicht verwendete Uplinks] – Dieser Uplink sollte nicht verwendet werden.

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

Bearbeiten der Failover- und Lastausgleichs-Richtlinie für eine Portgruppe

Sie können die Konfiguration der Failover- und Lastausgleichsrichtlinie für eine Portgruppe bearbeiten.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Wählen Sie eine Portgruppe aus und klicken Sie auf **[Bearbeiten]** .
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Ports]** .
- 5 Zum Bearbeiten der **[Failover- und Lastausgleichswerte]** für den vSwitch wählen Sie das vSwitch-Element und klicken Sie auf **[Eigenschaften]** .
- 6 Klicken Sie auf die Registerkarte **[NIC-Gruppierung]** .

Sie können die Failover-Reihenfolge auf Portgruppenebene außer Kraft setzen. Standardmäßig werden neue Adapter für alle Richtlinien aktiviert. Neue Adapter übertragen den Datenverkehr für den vSwitch und seine Portgruppe, wenn Sie nichts anderes angeben.

7 Legen Sie die Einstellungen in der Gruppe „Richtlinienausnahmen“ fest.

Option	Beschreibung
Lastenausgleich	<p>Geben Sie an, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ [Anhand der Quelle der Port-ID routen] – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert. ■ [Anhand des IP-Hashs routen] – Der Uplink wird anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ [Anhand des Quell-MAC-Hashs routen] – Der Uplink wird anhand eines Hashs des Quell-Ethernets ausgewählt. ■ [Explizite Failover-Reihenfolge verwenden] – Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt. <p>HINWEIS Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Bei allen anderen Optionen muss „etherchannel“ deaktiviert sein.</p>
Netzwerk-Failover-Ermittlung	<p>Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.</p> <ul style="list-style-type: none"> ■ [Nur Verbindungsstatus] – Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP, eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ [Signalprüfung] – Sendet Signale, sucht nach Signalprüfpaketen auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können.
Switches benachrichtigen	<p>Wählen Sie [Ja] oder [Nein], um Switches bei einem Failover zu benachrichtigen.</p> <p>Wenn Sie [Ja] wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen vSwitch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Meldung gesendet, um die Verweistabelle auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.</p> <p>HINWEIS Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastenausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.</p>

Option	Beschreibung
Failback	<p>Wählen Sie [Ja] oder [Nein] , um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf [Ja] (Standard) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf [Nein] gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.</p>
Failover-Reihenfolge	<p>Geben Sie an, wie die Verarbeitungslast für Uplinks verteilt werden soll. Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle reservieren möchten, z. B. wenn die verwendeten Uplinks ausfallen, legen Sie diesen Zustand fest, indem Sie sie in unterschiedliche Gruppen verschieben:</p> <ul style="list-style-type: none"> ■ [Aktive Uplinks] – Der Uplink wird weiter verwendet, wenn die Netzwerkadapterverbindung hergestellt und aktiv ist. ■ [Standby-Uplinks] – Dieser Uplink wird verwendet, wenn mindestens eine Verbindung des aktiven Adapters nicht verfügbar ist. ■ [Nicht verwendete Uplinks] – Dieser Uplink sollte nicht verwendet werden.

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

Bearbeiten der Gruppierungs- und Failover-Richtlinie für eine dvPortgruppe

Mit den Gruppierungs- und Failover-Richtlinien können Sie festlegen, wie der Netzwerkdatenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk]** > **[Einstellungen bearbeiten]** .
- 3 Wählen Sie **[Richtlinien]** .

4 Geben Sie in der Gruppe „Gruppierung und Failover“ Folgendes an.

Option	Beschreibung
Lastausgleich	<p>Geben Sie an, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ [Anhand der Quelle der Port-ID routen] – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert. ■ [Anhand des IP-Hashs routen] – Der Uplink wird anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ [Anhand des Quell-MAC-Hashs routen] – Der Uplink wird anhand eines Hashs des Quell-Ethernets ausgewählt. ■ [Explizite Failover-Reihenfolge verwenden] – Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt. <p>HINWEIS Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Bei allen anderen Optionen muss „etherchannel“ deaktiviert sein.</p>
Netzwerk-Failover-Erkennung	<p>Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.</p> <ul style="list-style-type: none"> ■ [Nur Verbindungsstatus] – Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ [Signalprüfung] – Sendet Signale, sucht nach Signalprüfpaketeten auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können. <p>HINWEIS Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.</p>
Switches benachrichtigen	<p>Wählen Sie [Ja] oder [Nein], um Switches bei einem Failover zu benachrichtigen.</p> <p>Wenn Sie [Ja] wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen vSwitch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Meldung gesendet, um die Verweistabelle auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.</p> <p>HINWEIS Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.</p>

Option	Beschreibung
Failback	<p>Wählen Sie [Ja] oder [Nein] , um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf [Ja] (Standard) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf [Nein] gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.</p>
Failover-Reihenfolge	<p>Geben Sie an, wie die Verarbeitungslast für Uplinks verteilt werden soll. Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle reservieren möchten, z. B. wenn die verwendeten Uplinks ausfallen, legen Sie diesen Zustand fest, indem Sie sie in unterschiedliche Gruppen verschieben:</p> <ul style="list-style-type: none"> ■ [Aktive Uplinks] – Der Uplink wird weiter verwendet, wenn die Netzwerkadapterverbindung hergestellt und aktiv ist. ■ [Standby-Uplinks] – Dieser Uplink wird verwendet, wenn mindestens eine Verbindung des aktiven Adapters nicht verfügbar ist. ■ [Nicht verwendete Uplinks] – Dieser Uplink sollte nicht verwendet werden. <p>HINWEIS Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.</p>

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

Bearbeiten von dvPort-Gruppierungs- und Failover-Richtlinien

Mit den Gruppierungs- und Failover-Richtlinien können Sie festlegen, wie der Netzwerkdatenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt.

Voraussetzungen

Um die Richtlinien für Gruppierung und Failover für einen einzelnen dvPort bearbeiten zu können, muss die zugehörige dvPort-Gruppe Außerkräftsetzungen von Richtlinien zulassen.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.
Das Dialogfeld **[Porteinstellungen]** wird angezeigt.
- 3 Klicken Sie auf **[Richtlinien]** , um Port-Netzwerkrichtlinien anzuzeigen und zu ändern.

4 Geben Sie in der Gruppe „Gruppierung und Failover“ Folgendes an.

Option	Beschreibung
Lastausgleich	<p>Geben Sie an, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ [Anhand der Quelle der Port-ID routen] – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert. ■ [Anhand des IP-Hashs routen] – Der Uplink wird anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ [Anhand des Quell-MAC-Hashs routen] – Der Uplink wird anhand eines Hashs des Quell-Ethernets ausgewählt. ■ [Explizite Failover-Reihenfolge verwenden] – Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt. <p>HINWEIS Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Bei allen anderen Optionen muss „etherchannel“ deaktiviert sein.</p>
Netzwerk-Failover-Erkennung	<p>Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.</p> <ul style="list-style-type: none"> ■ [Nur Verbindungsstatus] – Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ [Signalprüfung] – Sendet Signale, sucht nach Signalprüfpaketeten auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können. <p>HINWEIS Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.</p>
Switches benachrichtigen	<p>Wählen Sie [Ja] oder [Nein], um Switches bei einem Failover zu benachrichtigen.</p> <p>Wenn Sie [Ja] wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen vSwitch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Meldung gesendet, um die Verweistabelle auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.</p> <p>HINWEIS Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.</p>

Option	Beschreibung
Failback	<p>Wählen Sie [Ja] oder [Nein], um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf [Ja] (Standard) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf [Nein] gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.</p>
Failover-Reihenfolge	<p>Geben Sie an, wie die Verarbeitungslast für Uplinks verteilt werden soll. Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle reservieren möchten, z. B. wenn die verwendeten Uplinks ausfallen, legen Sie diesen Zustand fest, indem Sie sie in unterschiedliche Gruppen verschieben:</p> <ul style="list-style-type: none"> ■ [Aktive Uplinks] – Der Uplink wird weiter verwendet, wenn die Netzwerkadapterverbindung hergestellt und aktiv ist. ■ [Standby-Uplinks] – Dieser Uplink wird verwendet, wenn mindestens eine Verbindung des aktiven Adapters nicht verfügbar ist. ■ [Nicht verwendete Uplinks] – Dieser Uplink sollte nicht verwendet werden. <p>HINWEIS Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.</p>

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

VLAN-Richtlinie

Die VLAN-Richtlinie ermöglicht virtuellen Netzwerken, physischen VLANs beizutreten.

Bearbeiten der VLAN-Richtlinie für eine dvPortgruppe

Sie können die Konfiguration der VLAN-Richtlinie für eine dvPortgruppe bearbeiten.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk] > [Einstellungen bearbeiten]**.
- 3 Wählen Sie **[VLAN]**.
- 4 Wählen Sie den zu verwendenden **[VLAN-Typ]** aus.

Option	Beschreibung
Keine	Verwenden Sie VLAN nicht.
VLAN	Geben Sie im Feld [VLAN-ID] eine Zahl zwischen 1 und 4094 ein.
VLAN-Trunking	Geben Sie einen [VLAN-Trunk-Bereich] ein.
Privates VLAN	Wählen Sie ein verfügbares privates VLAN aus, das verwendet werden soll.

Bearbeiten von dvPort VLAN-Richtlinien

Eine auf der dvPort-Ebene eingestellte VLAN-Richtlinie ermöglicht es den einzelnen dvPorts, die auf der Ebene der dvPort-Gruppe eingerichtete VLAN-Richtlinie außer Kraft zu setzen.

Voraussetzungen

Um die VLAN-Richtlinien für einen einzelnen dvPort bearbeiten zu können, muss die zugehörige dvPort-Gruppe Außerkräftsetzungen von Richtlinien zulassen.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.
- 3 Klicken Sie auf **[Richtlinien]** .
- 4 Wählen Sie den zu verwendenden VLAN-Typ aus.

Option	Aktion
Keine	Verwenden Sie kein VLAN.
VLAN	Geben Sie als VLAN-ID eine Zahl zwischen 1 und 4095 ein.
VLAN-Trunking	Geben Sie einen VLAN-Trunk-Bereich ein.
Privates VLAN	Wählen Sie ein verfügbares privates VLAN aus, das verwendet werden soll.

- 5 Klicken Sie auf **[OK]** .

Sicherheitsrichtlinie

Netzwerksicherheitsrichtlinien legen fest, wie die Adapter ein- und ausgehende Frames filtern.

Schicht 2 ist die Sicherungsschicht. Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen.

Im Nicht-Promiscuous-Modus überwacht der Gastadapter nur den an seine eigene MAC-Adresse weitergeleiteten Datenverkehr. Im Promiscuous-Modus kann dieser alle Frames überwachen. Standardmäßig ist der Promiscuous-Modus für die Gastadapter deaktiviert.

Bearbeiten der Sicherheitsrichtlinie für Schicht 2 auf einem vSwitch

Sie können steuern, wie ein- und ausgehende Frames behandelt werden, indem Sie die Sicherheitsrichtlinien für Schicht 2 bearbeiten.

Vorgehensweise

- 1 Melden Sie sich beim VMware vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Klicken Sie auf **[Eigenschaften]** , um den vSwitch zu bearbeiten.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Ports]** .
- 5 Wählen Sie das vSwitch-Element, und klicken Sie auf **[Bearbeiten]** .

- 6 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Sicherheit]** .

In der Standardeinstellung ist die Option **[Promiscuous-Modus]** auf **[Ablehnen]** festgelegt. **[MAC-Adressenänderungen]** und **[Gefälschte Übertragungen]** sind auf **[Akzeptieren]** eingestellt.

Die Richtlinie gilt für alle virtuellen Adapter auf dem vSwitch, es sei denn, die Portgruppe für den virtuellen Adapter legt eine Richtlinienausnahme fest.

- 7 Im Fenster „Richtlinienausnahmen“ können Sie auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Modus	Ablehnen	Akzeptieren
Promiscuous-Modus	Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.	Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSwitch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressenänderungen	Wenn das Gastbetriebssystem die MAC-Adresse des Adapters auf einen Wert ändert, der nicht in der Konfigurationsdatei <code>.vmx</code> angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der <code>.vmx</code> -Konfigurationsdatei ändert, werden wieder alle eingehenden Frames gesendet.	Wenn sich die MAC-Adresse des Gastbetriebssystems ändert, werden Frames an die neue MAC-Adresse empfangen.
Gefälschte Übertragungen	Ausgehende Frames mit einer anderen als der im Adapter festgelegten Quell-MAC-Adresse werden verworfen.	Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 8 Klicken Sie auf **[OK]** .

Bearbeiten der Ausnahme der Sicherheitsrichtlinie für Schicht 2 für eine Portgruppe

Sie können steuern, wie ein- und ausgehende Frames behandelt werden, indem Sie die Sicherheitsrichtlinien für Schicht 2 bearbeiten.

Vorgehensweise

- 1 Melden Sie sich beim VMware vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .
- 3 Klicken Sie auf **[Eigenschaften]** , um die Portgruppe zu bearbeiten.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Ports]** .
- 5 Wählen Sie das Portgruppenelement aus und klicken Sie auf **[Bearbeiten]** .
- 6 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **[Sicherheit]** .

Standardmäßig ist für den **[Promiscuous-Modus]** die Option **[Ablehnen]** festgelegt. Für **[MAC-Adressenänderungen]** und **[Gefälschte Übertragungen]** ist **[Akzeptieren]** eingestellt.

Die Richtlinienausnahme überschreibt alle auf vSwitch-Ebene festgelegten Richtlinien.

- 7 Im Fenster „Richtlinienausnahmen“ können Sie auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Modus	Ablehnen	Akzeptieren
Promiscuous-Modus	Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.	Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSwitch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressenänderungen	Wenn das Gastbetriebssystem die MAC-Adresse des Adapters auf einen Wert ändert, der nicht in der Konfigurationsdatei <code>.vmx</code> angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der <code>.vmx</code> -Konfigurationsdatei ändert, werden wieder alle eingehenden Frames gesendet.	Wenn sich die MAC-Adresse des Gastbetriebssystems ändert, werden Frames an die neue MAC-Adresse empfangen.
Gefälschte Übertragungen	Ausgehende Frames mit einer anderen als der im Adapter festgelegten Quell-MAC-Adresse werden verworfen.	Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 8 Klicken Sie auf **[OK]**.

Bearbeiten der Sicherheitsrichtlinie für eine dvPortgruppe

Sie können steuern, wie ein- und ausgehende Frames für eine dvPort-Gruppe behandelt werden, indem Sie die Sicherheitsrichtlinien bearbeiten.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk]** > **[Einstellungen bearbeiten]**.
- 3 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **[Sicherheit]**.

Standardmäßig ist für den **[Promiscuous-Modus]** die Option **[Ablehnen]** festgelegt. Für **[MAC-Adressenänderungen]** und **[Gefälschte Übertragungen]** ist **[Akzeptieren]** eingestellt.

Die Richtlinienausnahme überschreibt alle auf vSwitch-Ebene festgelegten Richtlinien.

- 4 Im Fenster „Richtlinienausnahmen“ können Sie auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Modus	Ablehnen	Akzeptieren
Promiscuous-Modus	Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.	Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSwitch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressenänderungen	Wenn das Gastbetriebssystem die MAC-Adresse des Adapters auf einen Wert ändert, der nicht in der Konfigurationsdatei <code>.vmx</code> angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der <code>.vmx</code> -Konfigurationsdatei ändert, werden wieder alle eingehenden Frames gesendet.	Wenn sich die MAC-Adresse des Gastbetriebssystems ändert, werden Frames an die neue MAC-Adresse empfangen.
Gefälschte Übertragungen	Ausgehende Frames mit einer anderen als der im Adapter festgelegten Quell-MAC-Adresse werden verworfen.	Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 5 Klicken Sie auf **[OK]**.

Bearbeiten von dvPort-Sicherheitsrichtlinien

Sie können steuern, wie ein- und ausgehende Frames für einen dvPort behandelt werden, indem Sie die Sicherheitsrichtlinien bearbeiten.

Voraussetzungen

Um die Sicherheitsrichtlinien für einen einzelnen dvPort bearbeiten zu können, muss die zugehörige dvPort-Gruppe Außerkräftsetzungen von Richtlinien zulassen.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.
- 3 Klicken Sie auf **[Richtlinien]**.

In der Standardeinstellung ist die Option **[Promiscuous-Modus]** auf **[Ablehnen]** festgelegt. **[MAC-Adressenänderungen]** und **[Gefälschte Übertragungen]** sind auf **[Akzeptieren]** eingestellt.

- 4 Wählen Sie in der Sicherheitsgruppe aus, ob die Sicherheitsrichtlinienausnahmen abgelehnt oder angenommen werden:

Modus	Ablehnen	Akzeptieren
Promiscuous-Modus	Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.	Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSwitch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressenänderungen	Wenn das Gastbetriebssystem die MAC-Adresse des Adapters auf einen Wert ändert, der nicht in der Konfigurationsdatei <code>.vmx</code> angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der <code>.vmx</code> -Konfigurationsdatei ändert, werden wieder alle eingehenden Frames gesendet.	Wenn sich die MAC-Adresse des Gastbetriebssystems ändert, werden Frames an die neue MAC-Adresse empfangen.
Gefälschte Übertragungen	Ausgehende Frames mit einer anderen als der im Adapter festgelegten Quell-MAC-Adresse werden verworfen.	Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 5 Klicken Sie auf **[OK]**.

Traffic-Shaping-Richtlinie

Eine Traffic-Shaping-Richtlinie wird über drei Merkmale definiert: Durchschnittsbandbreite, Burstgröße und Spitzenbandbreite. Sie können für jede Portgruppe sowie jede dvPort-Gruppe und jeden dvPort eine Traffic-Shaping-Richtlinie erstellen.

ESXi steuert den ausgehenden Netzwerkverkehr auf vSwitches sowie den ein- und ausgehenden Datenverkehr auf einem verteilten vNetwork-Switch. Das Traffic-Shaping beschränkt die verfügbare Netzwerkbandbreite für einen Port, kann aber auch so konfiguriert werden, dass Datenverkehr-Bursts mit höherer Geschwindigkeit zulässig sind.

Durchschnittsbandbreite Legt die zulässige Zahl der Bit pro Sekunde fest, die einen Port im Durchschnitt durchlaufen darf, d. h. die zulässige durchschnittliche Datenlast.

Spitzenbandbreite Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.

Burstgröße Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugewiesene Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung **[Durchschnittliche Bandbreite]** angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt wurden und somit mit einer höheren Geschwindigkeit übertragen werden.

Bearbeiten der Traffic-Shaping-Richtlinie für einen vSwitch

Traffic-Shaping-Richtlinien werden verwendet, um die Bandbreite und die Burstgröße für einen vSwitch zu steuern.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie auf **[Eigenschaften]**, um den vSwitch zu bearbeiten.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Ports]**.
- 5 Wählen Sie das vSwitch-Element, und klicken Sie auf **[Bearbeiten]**.
- 6 Klicken Sie im Dialogfeld „Eigenschaften“ auf die Registerkarte **[Traffic-Shaping]**.

Bei deaktiviertem Traffic-Shaping werden die Optionen abgeblendet dargestellt. Sie können ausgewählte Traffic-Shaping-Funktionen auf Portgruppenebene außer Kraft setzen, wenn Traffic-Shaping aktiviert ist.

Diese Richtlinie wird in diesem Fall auf alle virtuellen Adapter angewendet, die an der Portgruppe angeschlossen sind, jedoch nicht auf den gesamten vSwitch.

HINWEIS Die Spitzenbandbreite darf nicht unter der angegebenen Durchschnittsbandbreite liegen.

Option	Beschreibung
Status	Wenn Sie die Richtlinienausnahmen im Feld [Status] aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, haben Dienste uneingeschränkten Zugang zum physischen Netzwerk.
Durchschnittsbandbreite	Ein Wert, der über einen bestimmten Zeitraum gemessen wird.
Spitzenbandbreite	Schränkt die Höchstbandbreite während eines Bursts ein. Diese darf nie niedriger als die durchschnittliche Bandbreite sein.
Burstgröße	Gibt an, wie groß ein Burst sein kann (in KB).

Bearbeiten der Traffic-Shaping-Richtlinie für eine Portgruppe

Traffic-Shaping-Richtlinien werden verwendet, um die Bandbreite und die Burstgröße für eine Portgruppe zu steuern.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie auf **[Eigenschaften]**, um die Portgruppe zu bearbeiten.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **[Ports]**.

- 5 Wählen Sie das Portgruppenelement aus und klicken Sie auf **[Bearbeiten]** .
- 6 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **[Traffic-Shaping]** .
Bei deaktiviertem Traffic-Shaping werden die Optionen abgeblendet dargestellt.

Option	Beschreibung
Status	Wenn Sie die Richtlinienausnahmen im Feld [Status] aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, haben Dienste uneingeschränkten Zugang zum physischen Netzwerk.
Durchschnittsbandbreite	Ein Wert, der über einen bestimmten Zeitraum gemessen wird.
Spitzenbandbreite	Schränkt die Höchstbandbreite während eines Bursts ein. Diese darf nie niedriger als die durchschnittliche Bandbreite sein.
Burstgröße	Gibt an, wie groß ein Burst sein kann (in KB).

Bearbeiten der Traffic-Shaping-Richtlinie für eine dvPortgruppe

Sowohl bei eingehendem als auch bei ausgehendem Datenverkehr ist Traffic-Shaping auf verteilten vNetwork-Switches möglich. Sie können die auf einem Port verfügbare Netzwerkbandbreite begrenzen oder auch zeitweise Datenverkehrspitzen über einen Port bei höherer Geschwindigkeit abwickeln.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk]** > **[Einstellungen bearbeiten]** .
- 3 Wählen Sie **[Traffic-Shaping]** .
- 4 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **[Traffic-Shaping]** .

Sie können sowohl eingehendes wie ausgehendes Traffic-Shaping konfigurieren. Bei deaktiviertem Traffic-Shaping werden die Optionen abgeblendet dargestellt.

HINWEIS Die Spitzenbandbreite darf nicht unter der angegebenen Durchschnittsbandbreite liegen.

Option	Beschreibung
Status	Wenn Sie die Richtlinienausnahmen im Feld [Status] aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, haben Dienste uneingeschränkten Zugang zum physischen Netzwerk.
Durchschnittsbandbreite	Ein Wert, der über einen bestimmten Zeitraum gemessen wird.
Spitzenbandbreite	Schränkt die Höchstbandbreite während eines Bursts ein. Diese darf nie niedriger als die durchschnittliche Bandbreite sein.
Burstgröße	Gibt an, wie groß ein Burst sein kann (in KB).

Bearbeiten von dvPort-Traffic-Shaping-Richtlinien

Sowohl bei eingehendem als auch bei ausgehendem Datenverkehr ist Traffic-Shaping auf verteilten vNetwork-Switches möglich. Sie können die auf einem Port verfügbare Netzwerkbandbreite begrenzen oder auch zeitweise Datenverkehrspitzen über einen Port bei höherer Geschwindigkeit abwickeln.

Eine Traffic-Shaping-Richtlinie wird über drei Merkmale definiert: Durchschnittsbandbreite, Burstgröße und Spitzenbandbreite.

Voraussetzungen

Um die Traffic-Shaping-Richtlinien für einen einzelnen dvPort bearbeiten zu können, muss die zugehörige dvPort-Gruppe Außerkräftsetzungen von Richtlinien zulassen.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.
- 3 Klicken Sie auf **[Richtlinien]** .
- 4 In der Traffic-Shaping-Gruppe können Sie sowohl eingehendes als auch ausgehendes Traffic-Shaping konfigurieren.

Bei deaktiviertem Traffic-Shaping werden die Optionen abgeblendet dargestellt.

Option	Beschreibung
Status	Wenn Sie die Richtlinienausnahmen im Feld [Status] aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, haben Dienste uneingeschränkten Zugang zum physischen Netzwerk.
Durchschnittsbandbreite	Ein Wert, der über einen bestimmten Zeitraum gemessen wird.
Spitzenbandbreite	Schränkt die Höchstbandbreite während eines Bursts ein. Diese darf nie niedriger als die durchschnittliche Bandbreite sein.
Burstgröße	Gibt an, wie groß ein Burst sein kann (in KB).

- 5 Klicken Sie auf **[OK]** .

Portblockierungsrichtlinien

Blockierungsrichtlinien für dvPorts können Sie vom Dialogfeld "Verschiedene Richtlinien" aus einrichten.

Bearbeiten der Portblockierungsrichtlinie für eine dvPort-Gruppe

Blockierungsrichtlinien für eine dvPort-Gruppe können Sie unter „Verschiedene Richtlinien“ einrichten.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie die dvPortgruppe aus.
- 2 Wählen Sie im Menü „Bestandsliste“ die Optionen **[Netzwerk]** > **[Einstellungen bearbeiten]** .
- 3 Wählen Sie **[Sonstiges]** .
- 4 Aktivieren Sie die Option **[Alle Ports blockieren]** , wenn Sie alle Ports dieser dvPort-Gruppe blockieren möchten.

Bearbeiten der dvPort-Portblockierungsrichtlinie

Im Dialogfeld für „Verschiedene Richtlinien“ können Sie Portblockierungsrichtlinien für einen dvPort konfigurieren.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und zeigen Sie den verteilten vNetwork-Switch an.
- 2 Klicken Sie mit der rechten Maustaste auf der Registerkarte **[Ports]** auf den zu ändernden Port und wählen Sie die Option **[Einstellungen bearbeiten]** aus.

- 3 Klicken Sie auf **[Richtlinien]** .
- 4 Wählen Sie in der Gruppe **[Verschiedenes]** mithilfe der Option **[Alle Ports blockieren]** aus, ob alle Ports blockiert werden sollen.
- 5 Klicken Sie auf **[OK]** .

Ändern der DNS- und Routing-Konfiguration

Von der Hostkonfigurationsseite im vSphere-Client aus können Sie die bei der Installation angegebenen DNS-Server- und Standard-Gateway-Informationen ändern.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration (Configuration)]** und anschließend auf **[DNS und Routing (DNS and Routing)]** .
- 3 Klicken Sie auf der rechten Bildschirmseite auf **[Eigenschaften (Properties)]** .
- 4 Geben Sie auf der Registerkarte **[DNS-Konfiguration]** einen Namen und eine Domäne ein.
- 5 Wählen Sie aus, ob Sie die Adresse des DNS-Servers automatisch beziehen oder eine DNS-Server-Adresse eingeben.
- 6 Geben Sie die Domänen an, in denen Hosts gesucht werden sollen.
- 7 Ändern Sie auf der Registerkarte **[Routing]** die Informationen zum Standard-Gateway nach Bedarf.
- 8 Klicken Sie auf **[OK]** .

MAC-Adressen

Für die von der Servicekonsole, dem VMkernel und den virtuellen Maschinen genutzten virtuellen Netzwerkadapter werden MAC-Adressen generiert.

In den meisten Fällen sind die generierten MAC-Adressen geeignet. In folgenden Fällen ist es jedoch ggf. notwendig, eine MAC-Adresse für einen virtuellen Netzwerkadapter festzulegen:

- Virtuelle Netzwerkadapter auf unterschiedlichen physischen Hosts verwenden das gleiche Subnetz, und ihnen wurde die gleiche MAC-Adresse zugewiesen, wodurch ein Konflikt entsteht.
- Sie möchten sicherstellen, dass ein virtueller Netzwerkadapter immer die gleiche MAC-Adresse hat.

Um die Begrenzung auf 256 virtuelle Netzwerkadapter pro physischem Computer zu umgehen und mögliche MAC-Adressenkonflikte zwischen virtuellen Maschinen zu vermeiden, können Systemadministratoren MAC-Adressen manuell zuweisen. VMware verwendet den OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) 00:50:56 für manuell generierte Adressen.

Der MAC-Adressbereich lautet 00:50:56:00:00:00–00:50:56:3F:FF:FF.

Sie können die Adressen festlegen, indem Sie der Konfigurationsdatei der virtuellen Maschine folgende Zeile hinzufügen:

```
Ethernet <Nummer> .address = 00:50:56:XX:YY:ZZ
```

wobei <Nummer> die Zahl des Ethernet-Adapters angibt, XX eine gültige Hexadezimalzahl von 00 bis 3F ist sowie YY und ZZ gültige Hexadezimalzahlen von 00 bis FF sind. Der Wert für XX darf nicht größer als 3F sein, um Konflikte mit MAC-Adressen zu vermeiden, die von VMware Workstation und VMware Server generiert werden. Der Höchstwert für eine manuell generierte MAC-Adresse lautet

```
Ethernet <Nummer> .address = 00:50:56:3F:FF:FF
```

Sie müssen außerdem folgende Option in der Konfigurationsdatei der virtuellen Maschine festlegen:

```
Ethernet <Nummer> .addressType="static"
```

Da virtuelle Maschinen von VMware ESXi keine beliebigen MAC-Adressen unterstützen, müssen Sie das oben genannte Format verwenden. Wenn Sie für Ihre nicht veränderlichen Adressen einen eindeutigen Wert für XX:YY:ZZ festlegen, dürfen keine Konflikte zwischen den automatisch zugewiesenen und den manuell zugewiesenen MAC-Adressen auftreten.

Generierung von MAC-Adressen

Jedem virtuellen Netzwerkadapter in einer virtuellen Maschine wird eine eindeutige MAC-Adresse zugewiesen. Jedem Hersteller von Netzwerkadapters wird ein eindeutiges, drei Byte großes Präfix zugewiesen, das als OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) genannt wird und das der Hersteller zur Generierung eindeutiger MAC-Adressen verwenden kann.

VMware bietet die folgenden drei OUIs:

- Generierte MAC-Adressen
- Manuell festgelegte MAC-Adressen
- Für ältere virtuelle Maschinen (wird jedoch bei ESXi nicht mehr verwendet)

Die ersten drei Byte der MAC-Adresse, die für jeden virtuellen Netzwerkadapter generiert wird, enthalten die OUI. Der Generierungsalgorithmus für MAC-Adressen erstellt drei weitere Byte. Der Algorithmus garantiert eindeutige MAC-Adressen innerhalb einer Maschine und versucht, eindeutige MAC-Adressen maschinenübergreifend zu erstellen.

Die Netzwerkadapter für jede virtuelle Maschine im gleichen Subnetz müssen eindeutige MAC-Adressen haben. Andernfalls können sie sich unvorhersehbar verhalten. Der Algorithmus beschränkt jederzeit auf allen Hosts die Anzahl laufender und angehaltener virtueller Maschinen. Er kann auch nicht alle Fälle identischer MAC-Adressen vermeiden, wenn sich virtuelle Maschinen auf unterschiedlichen physischen Computern ein Subnetz teilen.

Der VMware UUID (Universally Unique Identifier, universaler eindeutiger Bezeichner) generiert MAC-Adressen, die dann auf Konflikte geprüft werden. Die generierten MAC-Adressen bestehen aus drei Teilen: aus der VMware-OUI, der SMBIOS-UUID für den physischen ESXi-Computer und einem Hash, der auf dem Namen der Entität basiert, für die die MAC-Adresse generiert wird.

Wenn die MAC-Adresse generiert wurde, ändert sie sich nicht, solange die virtuelle Maschine nicht an einen anderen Speicherort verschoben wird, z. B. in ein anderes Verzeichnis auf dem gleichen Server. Die MAC-Adresse in der Konfigurationsdatei der virtuellen Maschine wird gespeichert. Alle MAC-Adressen, die Netzwerkadapters von ausgeführten oder angehaltenen virtuellen Maschinen auf einem bestimmten physischen Computer zugewiesen wurden, werden nachverfolgt.

Die MAC-Adresse einer ausgeschalteten virtuellen Maschine wird nicht mit MAC-Adressen ausgeführter oder angehaltener virtueller Maschinen abgeglichen. Es ist möglich, dass beim Hochfahren einer virtuellen Maschine eine andere MAC-Adresse angefordert wird. Diese Anforderung wird durch einen Konflikt mit einer virtuellen Maschine verursacht, die hochgefahren wurde, während diese virtuelle Maschine ausgeschaltet war.

Einrichten einer MAC-Adresse

Sie können den Netzwerkkarten einer deaktivierten virtuellen Maschine statische MAC-Adressen zuweisen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Wählen Sie in der Liste Hardware (Hardware) den Netzwerkadapter aus.

- 4 Wählen Sie unter MAC-Adresse (MAC Address) die Option **[Manuell (Manual)]** aus.
- 5 Geben Sie die gewünschte statische MAC-Adresse ein, und klicken Sie auf **[OK]**.

TCP-Segmentierungs-Offload und Jumbo-Frames

Jumbo-Frames müssen auf Hostebene über die Befehlszeilenschnittstelle aktiviert werden, indem die MTU-Größe für jeden vSwitch konfiguriert wird. Der TCP-Segmentierungs-Offload (TSO) wird standardmäßig auf der VMkernel-Schnittstelle aktiviert, muss aber auf der Ebene der virtuellen Maschine aktiviert werden.

Aktivieren von TSO

Um TSO auf virtueller Maschinenebene zu aktivieren, müssen Sie vorhandene virtuelle Netzwerkadapter vom Typ „vmxnet“ oder „Flexibel“ durch Netzwerkadapter vom Typ „Vmxnet (erweitert)“ ersetzen. Dadurch kann sich die MAC-Adresse des virtuellen Netzwerkadapters ändern.

TSO-Unterstützung über den Netzwerkadapter „Vmxnet (erweitert)“ steht für virtuelle Maschinen mit den folgenden Gastbetriebssystemen zur Verfügung:

- Microsoft Windows 2003 Enterprise Edition mit Service Pack 2 (32-Bit und 64-Bit)
- Red Hat Enterprise Linux 4 (64-Bit)
- Red Hat Enterprise Linux 5 (32-Bit und 64-Bit)
- SuSE Linux Enterprise Server 10 (32-Bit und 64-Bit)

Aktivieren der TSO-Unterstützung für eine virtuelle Maschine

Sie können die TSO-Unterstützung auf einer virtuellen Maschine aktivieren, indem Sie den Adapter „Vmxnet (erweitert)“ für diese virtuelle Maschine verwenden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Wählen Sie in der Liste Hardware (Hardware) den Netzwerkadapter aus.
- 4 Notieren Sie sich die Netzwerkeinstellungen und die MAC-Adresse des Netzwerkadapters.
- 5 Klicken Sie auf **[Entfernen (Remove)]**, um den Netzwerkadapter aus der virtuellen Maschine zu entfernen.
- 6 Klicken Sie auf **[Hinzufügen]**.
- 7 Wählen Sie **[Ethernet-Adapter (Ethernet Adapter)]**, und klicken Sie auf **[Weiter]**.
- 8 Wählen Sie unter Adaptertyp (Adapter Type) die Option **[Vmxnet (erweitert) (Enhanced vmxnet)]** aus.
- 9 Wählen Sie die Netzwerkeinstellungen und MAC-Adresse des alten Netzwerkadapters aus, und klicken Sie auf **[Weiter]**.
- 10 Klicken Sie auf **[Beenden]** und dann auf **[OK]**.
- 11 Wenn die virtuelle Maschine nicht auf das Upgrade von VMware Tools bei jeder Aktivierung eingestellt ist, müssen Sie VMware Tools manuell aktualisieren.

TSO ist für eine VMkernel-Schnittstelle aktiviert. Wenn TSO für eine bestimmte VMkernel-Schnittstelle deaktiviert wird, müssen Sie zur TSO-Aktivierung diese VMkernel-Schnittstelle löschen und sie mit aktiviertem TSO neu erstellen.

Aktivieren von Jumbo-Frames

Mithilfe von Jumbo-Frames kann ESXi größere Frames an das physische Netzwerk senden. Das Netzwerk muss Jumbo-Frames durchgängig unterstützen.

Jumbo-Frames bis zu 9KB (9000 Byte) werden unterstützt.

Jumbo-Frames werden für VMkernel-Netzwerkschnittstellen in ESXi nicht unterstützt.

Jumbo-Frames müssen über die Remote-Befehlszeilenschnittstelle Ihres ESXi-Hosts und für jeden vSwitch aktiviert werden, indem Sie im vSphere-Client den Netzwerkadapter „Vmxnet (erweitert)“ auswählen. Prüfen Sie vor der Aktivierung von Jumbo-Frames bei Ihrem Hardwareanbieter, ob Ihre physischen Netzwerkadapter Jumbo-Frames unterstützen.

Erstellen eines für Jumbo-Frames aktivierten vSwitches

Sie konfigurieren einen vSwitch für Jumbo-Frames, indem Sie die MTU-Größe für diesen vSwitch ändern.

Vorgehensweise

- 1 Verwenden Sie den Befehl `vicfg-vswitch -m <MTU> <vSwitch>` in der VMware vSphere CLI, um die MTU-Größe für den vSwitch festzulegen.
Dieser Befehl legt die MTU für alle Uplinks auf diesem vSwitch fest. Legen Sie als MTU-Größe die größte MTU-Größe der virtuellen Netzwerkadapter fest, die mit dem vSwitch verbunden sind.
- 2 Rufen Sie den Befehl `vicfg-vswitch -l` auf, um eine Liste der vSwitches auf dem Host anzuzeigen, und prüfen Sie, ob die Konfiguration des vSwitches ordnungsgemäß ist.

Aktivieren von Jumbo-Frames auf einem verteilten vNetwork-Switch

Sie aktivieren einen verteilten vNetwork-Switch für Jumbo-Frames, indem Sie die MTU-Größe für diesen verteilten vNetwork-Switch ändern.

Vorgehensweise

- 1 Rufen Sie im vSphere-Client die Bestandslistenansicht „Netzwerk“ auf und wählen Sie den verteilten vNetwork-Switch aus.
- 2 Wählen Sie im Menü „Bestandsliste“ **[Verteilter virtueller Switch] > [Einstellungen bearbeiten]** .
- 3 Wählen Sie auf der Registerkarte **[Eigenschaften]** die Option **[Erweitert]** aus.
- 4 Legen Sie als **[Maximalwert für MTU]** den größten MTU-Wert der virtuellen Netzwerkadapter fest, die mit dem verteilten vNetwork-Switch verbunden sind, und klicken Sie auf **[OK]** .

Aktivieren der Jumbo Frame-Unterstützung auf einer virtuellen Maschine

Für das Aktivieren der Jumbo-Frame-Unterstützung auf einer virtuellen Maschine ist ein erweiterter vmxnet-Adapter für diese virtuelle Maschine erforderlich.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]** .
- 3 Wählen Sie in der Liste Hardware (Hardware) den Netzwerkadapter aus.
- 4 Notieren Sie sich die Netzwerkeinstellungen und die MAC-Adresse des Netzwerkadapters.
- 5 Klicken Sie auf **[Entfernen (Remove)]** , um den Netzwerkadapter aus der virtuellen Maschine zu entfernen.

- 6 Klicken Sie auf **[Hinzufügen]** .
- 7 Wählen Sie **[Ethernet-Adapter (Ethernet Adapter)]** , und klicken Sie auf **[Weiter]** .
- 8 Wählen Sie unter Adaptertyp (Adapter Type) die Option **[Vmxnet (erweitert) (Enhanced vmxnet)]** aus.
- 9 Wählen Sie das Netzwerk des alten Netzwerkadapters aus, und klicken Sie auf **[Weiter]** .
- 10 Klicken Sie auf **[Beenden]** .
- 11 Wählen Sie in der Liste Hardware (Hardware) den neuen Netzwerkadapter aus.
- 12 Wählen Sie unter MAC-Adresse (MAC Address) die Option **[Manuell (Manual)]** , und geben Sie die von dem alten Netzwerkadapter verwendete MAC-Adresse an.
- 13 Klicken Sie auf **[OK]** .
- 14 Stellen Sie sicher, dass der Netzwerkadapter „Vmxnet (erweitert)“ mit einem für Jumbo Frames aktivierten vSwitch verbunden ist.
- 15 Konfigurieren Sie im Gastbetriebssystem den Netzwerkadapter, so dass Jumbo Frames unterstützt werden.
Informationen zu diesem Thema können Sie der Dokumentation Ihres Gastbetriebssystems entnehmen.
- 16 Konfigurieren Sie alle physischen Switches sowie alle physischen oder virtuellen Maschinen für die Unterstützung von Jumbo Frames, mit denen diese virtuelle Maschine eine Verbindung herstellt.

NetQueue und Netzwerkeistung

NetQueue in ESXi nutzt die Vorteile der Funktion einiger Netzwerkadapter, indem der Netzwerkdatenverkehr mit dem System über mehrere Empfangswarteschlangen bereitgestellt wird, die separat verarbeitet werden können. Dadurch kann die Verarbeitung auf mehrere CPUs verteilt werden, wodurch die Empfangsleistung des Netzwerks verbessert wird.

Aktivieren von NetQueue auf einem ESXi-Host

NetQueue ist standardmäßig aktiviert. Um NetQueue verwenden zu können, nachdem es deaktiviert wurde, muss es erneut aktiviert werden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und klicken Sie im Menü **[Software]** auf **[Erweiterte Einstellungen]** .
- 3 Wählen Sie **[VMkernel]** .
- 4 Wählen Sie **[VMkernel.Boot.netNetQueueEnable]** , und klicken Sie auf **[OK]** .
- 5 Verwenden Sie die VMware vSphere-CLI, um den Netzwerkkartentreiber für die Verwendung von NetQueue zu konfigurieren.
Weitere Informationen hierzu finden Sie im Handbuch *VMware vSphere Command-Line Interface - Installation und Referenz*.
- 6 Starten Sie den ESXi-Host neu.

Deaktivieren von NetQueue auf einem ESXi-Host

NetQueue ist standardmäßig aktiviert.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration (Configuration)]** und anschließend auf **[Erweiterte Einstellungen (Advanced Settings)]**.
- 3 Deaktivieren Sie **[VMkernel.Boot.netNetQueueEnable]**, und klicken Sie auf **[OK]**.
- 4 Verwenden Sie zum Deaktivieren von NetQueue auf dem Netzwerkkartentreiber den Befehl `vicfg-module -s "" [Modulname]`.

Verwenden Sie beispielsweise für den s2io-Netzwerkkartentreiber `vicfg-module -s "" s2io`.

Informationen zur VMware vSphere-CLI finden Sie im Handbuch *VMware vSphere-Befehlszeilenschnittstellen-Installation und Referenz*.

- 5 Starten Sie den Host neu.

VMDirectPath Gen I

Mit vSphere 4 unterstützt ESXi eine direkte PCI-Geräteverbindung für virtuelle Maschinen, die auf Intel Nehalem-Plattformen ausgeführt werden. Jede virtuelle Maschine kann mit bis zu zwei Passthrough-Geräten verbunden werden.

Die folgenden Funktionen sind nicht für virtuelle Maschinen verfügbar, die mit VMDirectPath konfiguriert sind:

- VMotion
- Hinzufügen und Entfernen von virtuellen Geräten bei laufendem Betrieb
- Anhalten und Fortsetzen
- Aufzeichnen und Wiedergabe
- Fehlertoleranz
- Hohe Verfügbarkeit
- DRS (eingeschränkte Verfügbarkeit; Die virtuelle Maschine kann Teil eines Clusters sein, kann aber nicht über Hosts hinweg migriert werden)

Konfigurieren von Passthrough-Geräten auf einem Host

Sie können Passthrough-Netzwerkgeräte auf einem Host konfigurieren.

Vorgehensweise

- 1 Wählen Sie einen Host im Bestandslistenfenster des vSphere-Clients aus.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** auf **[Erweiterte Einstellungen]**.

Die Seite Passthrough-Konfiguration wird angezeigt. Auf ihr werden alle verfügbaren Passthrough-Geräte aufgelistet. Ein grünes Symbol bedeutet, dass ein Gerät aktiviert und aktiv ist. Ein oranges Symbol bedeutet, dass sich der Status des Geräts geändert hat und der Host neu gestartet werden muss, bevor das Gerät verwendet werden kann.

- 3 Klicken Sie auf **[Bearbeiten]**.
- 4 Wählen Sie die für das Passthrough zu verwendenden Geräte aus und klicken Sie auf **[OK]**.

Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine

Sie können ein PCI-Passthrough-Gerät auf einer virtuellen Maschine konfigurieren.

Vorgehensweise

- 1 Wählen Sie eine virtuelle Maschine aus dem Bestandslistenfenster des vSphere-Clients aus.
- 2 Wählen Sie im Menü **[Bestandsliste]** den Befehl **[Virtuelle Maschine] > [Einstellungen bearbeiten]** .
- 3 Klicken Sie auf der Registerkarte **[Hardware]** auf **[Hinzufügen]** .
- 4 Wählen Sie **[PCI-Gerät]** und klicken Sie auf **[Weiter]** .
- 5 Wählen Sie das zu verwendende Passthrough-Gerät aus und klicken Sie auf **[Weiter]** .
- 6 Klicken Sie auf **[Beenden]** .

Wird einer virtuellen Maschine ein VMDirectPath-Gerät hinzugefügt, wird die Größe der Arbeitsspeicherreservierung auf die Arbeitsspeichergröße der virtuellen Maschine gesetzt.

Optimale Vorgehensweisen, Szenarien und Fehlerbehebung für Netzwerke

6

Diese Themen beschreiben optimale Vorgehensweisen und oft vorkommende Konfigurations- und Fehlerbehebungsszenarien für Netzwerke.

Dieses Kapitel behandelt die folgenden Themen:

- „Optimale Vorgehensweisen für Netzwerke“, auf Seite 65
- „Mounten von NFS-Volumes“, auf Seite 66
- „Fehlerbehebung“, auf Seite 66

Optimale Vorgehensweisen für Netzwerke

Ziehen Sie folgende optimale Vorgehensweisen für die Konfiguration Ihres Netzwerks in Betracht.

- Trennen Sie die Netzwerkdienste voneinander, um mehr Sicherheit und eine höhere Leistung zu erreichen.

Wenn eine bestimmte Gruppe virtueller Maschinen höchste Leistung bieten soll, schließen Sie sie an eine eigene physische Netzwerkkarte an. Durch diese Abtrennung kann ein Teil der Gesamtarbeitslast des Netzwerks gleichmäßiger auf mehrere CPUs verteilt werden. Die isolierten virtuellen Maschinen sind dann beispielsweise besser in der Lage, den Datenverkehr eines Webclients zu verarbeiten.

- Richten Sie die VMotion-Verbindung auf einem separaten Netzwerk ein, das eigens für VMotion vorgesehen ist. Bei der Migration mit VMotion wird der Inhalt des Arbeitsspeichers des Gastbetriebssystems über das Netzwerk übertragen. Diese Empfehlungen können entweder durch die Verwendung von VLANs zur Aufteilung eines physischen Netzwerks in Segmente oder durch die Verwendung getrennter physischer Netzwerke umgesetzt werden (die zweite Variante ist dabei zu bevorzugen).
- Vermeiden Sie bei Verwendung von Passthrough-Geräten mit einem Linux-Kernel der Version 2.6.20 oder früher den MSI- und MSI-X-Modus, da sich diese negativ auf die Leistung auswirken.
- Um Netzwerkdienste physisch zu trennen und eine bestimmte Gruppe von Netzwerkkarten einem bestimmten Netzwerkdienst zuzuweisen, erstellen Sie einen vSwitch für jeden Dienst. Wenn das nicht möglich ist, können sie auf einem vSwitch voneinander getrennt werden, indem sie Portgruppen mit unterschiedlichen VLAN-IDs zugeordnet werden. In jedem Fall sollte der Netzwerkadministrator bestätigen, dass die gewählten Netzwerke oder VLANs vom Rest der Umgebung isoliert sind, d.h. dass keine Router daran angeschlossen sind.

- Sie können Netzwerkkarten zum vSwitch hinzufügen oder davon entfernen, ohne dass die virtuellen Maschinen oder die Netzwerkdienste hinter diesem vSwitch beeinflusst werden. Wenn Sie die gesamte ausgeführte Hardware entfernen, können die virtuellen Maschinen weiter untereinander kommunizieren. Wenn Sie eine Netzwerkkarte intakt lassen, können alle virtuellen Maschinen weiterhin auf das physische Netzwerk zugreifen.
- Um die empfindlichsten virtuellen Maschinen zu schützen, installieren Sie Firewalls auf virtuellen Maschinen, die den Datenverkehr zwischen virtuellen Netzwerken mit Uplinks zu physischen Netzwerken und reinen virtuellen Netzwerken ohne Uplinks weiterleiten.

Mounten von NFS-Volumes

Die Weise, wie der ESXi auf NFS-Speicher von ISO-Images zugreift, die als virtuelle CD-ROMs für virtuelle Maschinen verwendet werden, unterscheidet sich von der Weise, wie das in ESX Server 2.x geschah.

ESXi unterstützt das VMkernel-basierte NFS-Mounting. Bei dem neuen Modell wird das NFS-Volume mit den ISO-Images über die NFS-Funktion des VMkernels gemounted. Alle so gemounteten NFS-Volumes werden im vSphere-Client als Datenspeicher angezeigt. Mit dem Konfigurations-Editor der virtuellen Maschine können Sie das Dateisystem der Servicekonsole nach ISO-Images durchsuchen, die als virtuelle CD-ROM-Laufwerke verwendet werden sollen.

Fehlerbehebung

In den folgenden Themen wird die Fehlerbehebung von oft vorkommenden Netzwerkproblemen vorgestellt, die in einer ESXi-Umgebung auftreten können.

Beheben von Problemen bei der Konfiguration physischer Switches

Bei einem Failover oder Failback kann die Verbindung zum vSwitch unterbrochen werden. Dadurch werden die MAC-Adressen, die von diesem vSwitch zugeordneten virtuellen Maschinen verwendet werden, auf einem anderen Switchport angezeigt.

Um dieses Problem zu vermeiden, setzen Sie Ihren physischen Switch auf den Portfast- oder Portfast-Trunk-Modus.

Beheben von Problemen bei der Konfiguration von Portgruppen

Das Umbenennen einer Portgruppe bei bereits mit dieser Portgruppe verbundenen virtuellen Maschinen kann zu einer ungültigen Netzwerkkonfiguration virtueller Maschinen führen, die für eine Verbindung mit dieser Portgruppe konfiguriert sind.

Die Verbindung virtueller Netzwerkadapter mit den Portgruppen erfolgt anhand des Namens, und der Name wird in der Konfiguration der virtuellen Maschine gespeichert. Das Ändern des Namens einer Portgruppe führt nicht zu einer Massenneukonfiguration aller virtuellen Maschinen, die mit dieser Portgruppe verbunden sind. Virtuelle Maschinen, die bereits eingeschaltet sind, werden weiterhin funktionieren, bis sie ausgeschaltet werden, da ihre Verbindungen zum Netzwerk bereits hergestellt sind.

Vermeiden Sie das Umbenennen bereits verwendeter Netzwerke. Nach dem Umbenennen einer Portgruppe müssen Sie jede zugeordnete virtuelle Maschine über die Servicekonsole neu konfigurieren, um den neuen Portgruppennamen entsprechend zu berücksichtigen.

Speicher

Einführung in die Speicherung

Diese Einführung beschreibt verfügbare Speicheroptionen für ESXi und erklärt, wie Sie Ihr ESXi-System konfigurieren können, damit es verschiedene Speichertypen verwenden und verwalten kann.

Dieses Kapitel behandelt die folgenden Themen:

- [„Info zu ESXi-Speicher“](#), auf Seite 69
- [„Physische Speichertypen“](#), auf Seite 70
- [„Unterstützte Speicheradapter“](#), auf Seite 71
- [„Ziel- und Gerätedarstellungen“](#), auf Seite 72
- [„Info zu ESXi-Datenspeichern“](#), auf Seite 74
- [„Vergleich der Speichertypen“](#), auf Seite 77
- [„Anzeigen der Speicherinformationen im vSphere-Client“](#), auf Seite 78

Info zu ESXi-Speicher

ESXi-Speicher ist Speicherplatz auf einer Vielzahl physischer Speichersysteme, lokal oder im Netzwerk, den ein Host zum Speichern der Festplatten von virtuellen Maschinen verwendet.

Eine virtuelle Maschine verwendet eine virtuelle Festplatte, um das Betriebssystem, die Programmdateien und andere Daten für ihren Betrieb zu speichern. Eine virtuelle Festplatte ist eine große physische Datei bzw. Zusammenstellung von Dateien, die sich so einfach wie jede andere Datei kopieren, verschieben, archivieren und sichern lässt. Zum Speichern von virtuellen Festplattendateien und zum Bearbeiten der Dateien benötigt ein Host dediziert zugewiesenen Speicherplatz.

Der Host verwendet Speicherplatz auf verschiedenen physischen Speichersystemen, einschließlich der internen und externen Geräte auf dem Host und Speicher im Netzwerk, der für die spezifischen Aufgaben des Speicherns und Schützens der Daten dediziert ist.

Der Host kann Speichergeräte, auf die er Zugriff hat, erkennen und sie als Datenspeicher formatieren. Der Datenspeicher ist ein spezieller logischer Container (ähnlich einem Dateisystem auf einem logischen Volume), in dem ESXi virtuelle Festplattendateien und andere Dateien ablegt, in denen wesentliche Komponenten einer virtuellen Maschine gekapselt werden. Die Datenspeicher werden auf verschiedenen Geräten bereitgestellt, wobei Angaben zu den einzelnen Speicherungsprodukten verborgen bleiben, und bieten ein einheitliches Modell für die Speicherungen der Dateien virtueller Maschinen.

Mit dem vSphere-Client können Sie Datenspeicher auf allen Speichergeräten einrichten, die Ihr Host erkennt. Sie können Ordner außerdem zum Erstellen logischer Gruppen von Datenspeichern für organisatorische Zwecke sowie zum Einstellen von Berechtigungen und Alarmen für die gesamte Datenspeichergruppe verwenden.

Physische Speichertypen

Die Verwaltung des ESXi-Datenspeichers beginnt mit dem Speicherplatz, den der Speicheradministrator auf verschiedenen Speichersystemen zuweist.

ESXi unterstützt folgende Typen von Speichergeräten:

Lokaler Speicher	Dateien von virtuellen Maschinen werden auf internen oder externen Speicherplatten oder Arrays gespeichert, die über eine Direktverbindung an Ihren Host angeschlossen sind.
Netzwerksspeicher	Dateien virtueller Maschinen werden auf externen gemeinsam genutzten Speichersystemen gespeichert, die sich außerhalb Ihres Hosts befinden. Der Host kommuniziert mit den vernetzten Geräten über ein Hochgeschwindigkeitsnetzwerk.

Lokaler Speicher

Lokale Speichergeräte können interne Festplatten innerhalb Ihres ESXi-Hosts oder externe Speichersysteme außerhalb Ihres Hosts sein, die direkt mit ihm verbunden sind.

Lokale Speichergeräte benötigen kein Speichernetzwerk für die Kommunikation mit Ihrem Host. Sie benötigen lediglich ein an die Speichereinheit angeschlossenes Kabel und möglicherweise einen kompatiblen HBA in Ihrem Host.

In der Regel können mehrere Hosts an ein einzelnes lokales Speichersystem angeschlossen werden. Die tatsächliche Anzahl der Hosts, die Sie anschließen, hängt vom Typ des Speichergeräts und der verwendeten Topologie ab.

Viele lokale Speichersysteme unterstützen redundante Verbindungspfade, um Fehlertoleranz zu gewährleisten.

Wenn mehrere Hosts an die lokale Speichereinheit angeschlossen sind, greifen die Hosts im nicht gemeinsamen Nutzungsmodus auf Speichergeräte zu. Der nicht gemeinsame Nutzungsmodus lässt nicht zu, dass mehrere Hosts gleichzeitig auf denselben VMFS-Datenspeicher zugreifen. Es gibt jedoch ein paar SAS-Speichersysteme, die mehreren Hosts einen gemeinsamen Zugriff erlauben. Diese Art des Zugriffs ermöglicht mehreren Hosts, auf denselben VMFS-Dateispeicher auf einer LUN zuzugreifen.

ESXi unterstützt verschiedene interne und externe lokale Speichergeräte, einschließlich SCSI-, IDE-, SATA-, USB- und SAS-Speichersystemen. Unabhängig vom gewählten Speichertyp verbirgt der Host eine physische Speicherebene vor den virtuellen Maschinen.

Beachten Sie beim Einrichten des lokalen Speichers Folgendes:

- Virtuelle Maschinen können nicht auf IDE-/ATA-Laufwerken gespeichert werden.
- Verwenden Sie lokalen internen und externen SATA-Speicher nur im nicht gemeinsamen Nutzungsmodus. SATA-Speicher unterstützt nicht die gemeinsame Nutzung derselben LUNs und deshalb nicht denselben VMFS-Dateispeicher für mehrere Hosts.
- Verschiedene SAS-Speichersysteme unterstützen den gemeinsamen Zugriff auf dieselben LUNs (und deshalb auf dieselben VMFS-Dateispeicher) für mehrere Hosts.

Netzwerkspeicher

Netzwerkspeicher bestehen aus externen Speichersystemen, die Ihr ESXi-Host zur Remotespeicherung von Dateien der virtuellen Maschinen verwendet. Der Host greift auf diese Systeme über ein Hochgeschwindigkeitsnetzwerk zu.

ESXi unterstützt folgende Netzwerkspeichertechnologien.

HINWEIS Der gleichzeitige Zugriff auf denselben Speicher über unterschiedliche Übertragungsprotokolle wie iSCSI und Fibre-Channel wird nicht unterstützt.

Fibre-Channel (FC)

Speichert Dateien virtueller Maschinen extern in einem FC-Speichernetzwerk (Storage Area Network, SAN). Ein FC-SAN ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Ihre Hosts mit Hochleistungsspeichergeräten verbindet. Das Netzwerk nutzt das Fibre-Channel-Protokoll zur Übertragung von SCSI-Datenverkehr virtueller Maschinen an FC-SAN-Geräte.

Für den Anschluss an das FC-SAN muss der Host mit Fibre-Channel-HBAs (Hostbusadaptern) und (außer Sie arbeiten mit Fibre-Channel-Direktverbindungsspeicher) mit Fibre-Channel-Switches ausgestattet sein, die die Weiterleitung der zu speichernden Daten unterstützen.

Internet-SCSI (iSCSI)

Speichert Dateien virtueller Maschinen auf Remote-iSCSI-Speichergeräten. iSCSI packt SCSI-Speicherdatenverkehr in das TCP/IP-Protokoll, sodass dieser über standardmäßige TCP/IP-Netzwerke anstatt über ein spezielles Fibre-Channel-Netzwerk übertragen werden kann. Bei einer iSCSI-Verbindung dient der Host als Initiator, der mit einem Ziel kommuniziert, das sich in externen iSCSI-Speichersystemen befindet.

ESXi unterstützt die folgenden iSCSI-Verbindungstypen:

Hardware-initiiertes iSCSI

Ihr Host stellt über einen iSCSI-HBA eines Drittanbieters eine Verbindung mit dem Speicher her.

Software-initiiertes iSCSI

Ihr Host verwendet einen auf Software basierenden iSCSI-Initiator im VMkernel für die Verbindung mit dem Speicher. Bei diesem iSCSI-Verbindungstyp benötigt der Host nur einen Standardnetzwerkadapter zum Herstellen der Netzwerkverbindung.

Network-Attached Storage (NAS)

Speichert Dateien von virtuellen Maschinen auf Remotedateiservern, auf die über ein standardmäßiges TCP/IP-Netzwerk zugegriffen wird. Der in ESXi integrierte NFS-Client verwendet das NFS-Protokoll, Version 3, (Network File System), um mit den NAS-/NFS-Servern zu kommunizieren. Für die Netzwerkverbindung benötigt der Host einen Standardnetzwerkadapter.

Unterstützte Speicheradapter

Speicheradapter bieten Konnektivität für Ihren ESXi-Host zu einer bestimmten Speichereinheit oder zu einem bestimmten Netzwerk.

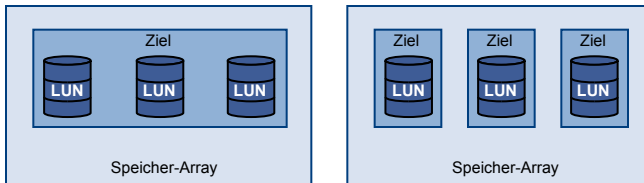
Je nachdem, welchen Speichertyp Sie verwenden, müssen Sie möglicherweise einen Speicheradapter auf Ihrem Host installieren oder aktivieren. ESXi unterstützt mit SCSI, iSCSI, RAID, Fibre-Channel und Ethernet verschiedene Adapterklassen. ESXi greift auf die Adapter direkt über Gerätetreiber im VMkernel zu.

Ziel- und Gerätedarstellungen

Im ESXi-Kontext beschreibt der Begriff „Ziel“ eine einzelne Speichereinheit, auf die der Host zugreifen kann. Die Begriffe „Gerät“ und „LUN“ beschreiben ein logisches Laufwerk, das Speicherplatz auf einem Ziel darstellt. In der Regel stehen die Begriffe „Gerät“ und „LUN“ im ESXi-Kontext für ein SCSI-Volume, das dem Host von einem Speicherziel angeboten wird und formatiert werden kann.

Verschiedene Speicheranbieter bieten ESXi-Hosts die Speichersysteme unterschiedlich an. Einige Anbieter bieten mehrere Speichergeräte bzw. LUNs auf einem einzigen Ziel, während andere Anbieter mehrere Ziele mit je einer LUN verknüpfen.

Abbildung 7-1. Ziel- und LUN-Darstellungen



In der vorliegenden Abbildung sind in jeder dieser Konfigurationen drei LUNs verfügbar. Im ersten Fall erkennt der Host ein Ziel, obwohl in diesem Ziel drei LUNs vorhanden sind, die verwendet werden können. Jede LUN steht für ein einzelnes Speicher-Volume. Im zweiten Fall werden dem Host drei unterschiedliche Ziele mit je einer LUN angezeigt.

Ziele, auf die über das Netzwerk zugegriffen wird, besitzen eindeutige Namen, die von den Speichersystemen angegeben werden. Die iSCSI-Ziele verwenden die iSCSI-Namen, während Fibre-Channel-Ziele World Wide Names (WWNs) verwenden.

HINWEIS ESXi unterstützt keinen Zugriff auf dieselbe LUN über unterschiedliche Übertragungsprotokolle wie iSCSI und Fibre-Channel.

Ein Gerät oder eine LUN wird durch den UUID-Namen identifiziert.

Grundlegendes zur Fibre-Channel-Benennung

In Fibre-Channel-SAN wird jedes Element im Netzwerk, z. B. ein Fibre-Channel-Adapter oder ein Speichergerät, durch einen World Wide Name (WWN) eindeutig identifiziert.

Der WWN ist eine 64-Bit-Adresse, die aus 16 Hexadezimalzahlen besteht und wie folgt aussehen kann:

20:00:00:e0:8b:8b:38:77 21:00:00:e0:8b:8b:38:77

Der WWN wird jedem Fibre-Channel-SAN-Element von seinem Hersteller zugewiesen.

Grundlegendes zur iSCSI-Benennung und Adressierung

In einem iSCSI-Netzwerk hat jedes iSCSI-Element, das das Netzwerk verwendet, einen eindeutigen und dauerhaften iSCSI-Namen und erhält eine Adresse für den Zugriff.

iSCSI-Name

Identifiziert ein bestimmtes iSCSI-Element, unabhängig von seinem physischen Speicherort. Der iSCSI-Name kann das IQN- oder EUI-Format verwenden.

- IQN (iSCSI-qualifizierter Name). Darf bis zu 255 Zeichen umfassen und hat das folgende Format:

`iqn.yyyy-mm.Namensvergabeestelle:eindeutiger_Name`

- `yyyy-mm` gibt Jahr und Monat an, in dem die Stelle für die Namensvergabe (Naming Authority) eingerichtet wurde.
- `Namensvergabeestelle` ist üblicherweise die Syntax des Internetdomänenname der Namensvergabeestelle in umgekehrter Reihenfolge. Zum Beispiel könnte die Namensvergabeestelle `iscsi.vmware.com` den qualifizierten iSCSI-Namen „`iqn.1998-01.com.vmware.iscsi`“ haben. Der Name gibt an, dass der Domänenname `vmware.com` im Januar 1998 registriert wurde und es sich bei „`iscsi`“ um eine Unterdomäne von `vmware.com` handelt.
- `eindeutiger_Name` steht für einen beliebigen Namen, z. B. den Namen des Hosts. Die Namensvergabeestelle muss sicherstellen, dass alle zugewiesenen Namen nach dem Doppelpunkt eindeutig sind, z. B.:
 - `iqn.1998-01.com.vmware.iscsi:Name1`
 - `iqn.1998-01.com.vmware.iscsi:Name2`
 - `iqn.1998-01.com.vmware.iscsi:Name999`
- EUI (Extended Unique Identifier). Umfasst das Präfix `eui.`, gefolgt von dem Namen aus 16 Zeichen. Zum Namen gehören 24 Bit für den Firmennamen, die von der IEEE zugewiesen wurden, und 40 Bit für einen eindeutigen Bezeichner wie z. B. die Seriennummer.

Beispiel:

`eui.0123456789ABCDEF`

iSCSI-Alias:

Ein Name, der einfach zu merken und zu verwalten ist und statt dem iSCSI-Namen verwendet wird. iSCSI-Aliase sind nicht eindeutig und sollen lediglich als benutzerfreundliche Namen dienen, die mit dem Knoten verknüpft werden.

IP-Adresse

Eine jedem iSCSI-Element zugewiesene Adresse, die Routern und Switches im Netzwerk eine Verbindung zwischen verschiedenen Elementen, z. B. dem Host und dem Speicher, ermöglicht. Dies ist mit der IP-Adresse vergleichbar, die Sie einem Computer zuweisen, um auf das Unternehmensnetzwerk oder das Internet zugreifen zu können.

Grundlegendes zur Benennung von Speichergeräten

Im vSphere-Client wird jedes Speichergerät bzw. jede LUN durch mehrere Namen identifiziert. Dazu gehören ein benutzerfreundlicher Name, eine UUID und ein Laufzeitname.

Name Ein benutzerfreundlicher Name, den der ESXi-Host einem Gerät anhand des Speichertyps und Herstellers zuweist. Sie können den Namen über den vSphere-Client ändern. Wenn Sie den Namen des Geräts auf einem Host ändern, wirkt sich die Änderung auf alle Hosts aus, die Zugriff auf dieses Gerät haben.

Bezeichner Eine einem Gerät zugewiesene UUID. Je nach dem Speichertyp werden unterschiedliche Algorithmen zum Erstellen des Bezeichners verwendet. Der Bezeichner überdauert auch Neustarts und gilt für alle Hosts, die sich das Gerät teilen.

Laufzeitname Der Name des ersten Pfads zum Gerät. Der Laufzeitname wird vom Host erstellt, ist kein zuverlässiger Bezeichner für das Gerät und ist nicht dauerhaft. Die Laufzeitname hat das folgende Format: `vmhba#:C#:T#:L#`, wobei

- „vmhba#“ der Name des Speicheradapters ist. Der Name bezieht sich auf den physischen Adapter auf dem Host, nicht auf den SCSI-Controller, den die virtuellen Maschinen verwenden.
- C# ist die Nummer des Speicherkanals.

Software-iSCSI-Initiatoren verwenden die Nummer des Speicherkanals, um mehrere Pfade zu demselben Ziel anzuzeigen.

- T# ist die Zielnummer. Die Zielnummerierung wird vom Host entschieden und kann sich ändern, wenn es eine Änderung in der Zuordnung von Zielen gibt, die für den Host sichtbar sind. Ziele, die von verschiedenen ESXi-Hosts gemeinsam genutzt werden, besitzen auf den Hosts möglicherweise nicht dieselbe Zielnummer.
- L# ist die LUN-Nummer, die die Position der LUN innerhalb des Ziels anzeigt. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).

Beispielsweise repräsentiert `vmhba1:C0:T3:L1` LUN1 auf Ziel 3, auf die über den Speicheradapter vmhba1 und den Kanal 0 zugegriffen wird.

Info zu ESXi-Datenspeichern

Datenspeicher sind besondere logische Container (analog zu Dateisystemen), bei denen Angaben zu den einzelnen Speichergeräten verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Datenspeicher können auch zum Speichern von ISO-Images, Vorlagen virtueller Maschinen und Disketten-Images genutzt werden.

Mit dem vSphere-Client greifen Sie auf verschiedene Arten von Speichergeräten zu, die der ESXi-Host erkennt, um darauf Datenspeicher bereitzustellen.

Je nach Typ des verwendeten Speichers können Datenspeichern folgende Dateisystemformate zu Grunde liegen:

Virtual Machine File System (VMFS)	Ein für das Speichern von virtuellen Maschinen optimiertes Hochleistungsdateisystem. Ihr Host kann einen VMFS-Datenspeicher auf einem beliebigen SCSI-basierten lokalen oder Netzwerkspeichergerät bereitstellen, z. B. auf Fibre-Channel- und iSCSI-SAN-Geräten. Als Alternative zur Verwendung eines VMFS-Datenspeichers kann Ihre virtuelle Maschine über eine Zuordnungsdatei (RDM) als Stellvertreter direkt auf Raw-Geräte zugreifen.
Network File System (NFS)	Dateisystem auf einem NAS-Speichergerät. ESXi unterstützt NFS Version 3 über TCP/IP. Der Host kann auf einem NFS-Server auf ein ausgewähltes NFS-Volume zugreifen, das Volume mounten und es für beliebige Speicherzwecke nutzen.

VMFS-Datenspeicher

ESXi kann SCSI-basierte Speichergeräte wie VMFS-Datenspeicher formatieren. VMFS-Datenspeicher dienen hauptsächlich als Ablagen für virtuelle Maschinen.

Sie können mehrere virtuelle Maschinen auf demselben VMFS-Volume speichern. Jede virtuelle Maschine ist in einem Satz Dateien gekapselt und belegt ein eigenes Verzeichnis. Für das Betriebssystem innerhalb der virtuellen Maschine behält VMFS die interne Dateisystemsemantik bei. Dadurch wird das ordnungsgemäße Verhalten von Anwendungen und die Datensicherheit für Anwendungen gewährleistet, die in virtuellen Maschinen ausgeführt werden.

Darüber hinaus können Sie in VMFS-Datenspeichern andere Dateien speichern, z. B. Vorlagen virtueller Maschinen und ISO-Images.

VMFS unterstützt die folgenden Datei- und Blockgrößen, sodass Sie auch die datenhungrigsten Anwendungen wie Datenbanken, ERP und CRM in virtuellen Maschinen ausführen können:

- Maximale Größe der virtuellen Festplatte: 2 TB mit einer Blockgröße von 8 MB
- Maximale Dateigröße: 2 TB mit einer Blockgröße von 8 MB
- Blockgröße: 1 MB (Standard), 2 MB, 4 MB und 8 MB

Erstellen und Vergrößern von VMFS-Datenspeichern

Sie können VMFS-Datenspeicher auf jedem SCSI-basierten Speichergerät einrichten, das der ESXi-Host erkennt. Nachdem Sie den VMFS-Datenspeicher erstellt haben, können Sie seine Eigenschaften bearbeiten.

Sie können bis zu 256 VMFS-Datenspeicher pro System verwenden, bei einer Volume-Mindestgröße von 1,2 GB.

HINWEIS Ordnen Sie jeder LUN stets nur einen VMFS-Datenspeicher zu.

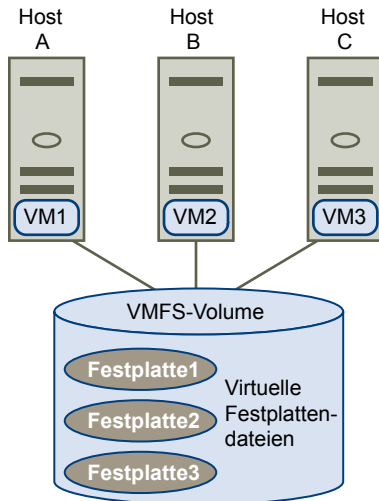
Wenn Ihr VMFS-Datenspeicher mehr Speicherplatz benötigt, können Sie das VMFS-Volume vergrößern. Sie können jedem VMFS-Datenspeicher dynamisch neue Erweiterungen hinzufügen und den Datenspeicher bis auf 64 TB vergrößern. Bei einer Erweiterung handelt es sich um eine LUN oder Partition auf einem physischen Speichergerät. Der Datenspeicher kann sich über mehrere Erweiterungen erstrecken und wird dennoch als einzelnes Volume angezeigt.

Sie haben außerdem die Möglichkeit, die vorhandene Datenspeichererweiterung zu vergrößern, wenn das Speichergerät, auf dem sich Ihr Datenspeicher befindet, über freien Speicherplatz verfügt. Sie können die Erweiterung bis auf 2 TB vergrößern.

Gemeinsames Nutzen eines VMFS-Volumes durch ESXi-Hosts

Als Clusterdateisystem ermöglicht VMFS mehreren ESXi-Hosts, parallel auf denselben VMFS-Datenspeicher zuzugreifen. Sie können bis zu 32 Hosts mit einem einzelnen VMFS-Volumen verbinden.

Abbildung 7-2. Gemeinsames Nutzen eines VMFS-Volumes durch mehrere Hosts



Um zu gewährleisten, dass nicht mehrere Server gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine festplatteninterne Sperrung.

Die gemeinsame Nutzung desselben VMFS-Volumens durch mehrere Hosts bietet folgende Vorteile:

- Sie können VMware Distributed Resource Scheduling und VMware High Availability einsetzen.
Sie können virtuelle Maschinen auf mehrere physische Server verteilen. Sie können also auf jedem Server eine Kombination virtueller Maschinen ausführen, sodass nicht alle zur selben Zeit im selben Bereich einer hohen Nachfrage unterliegen. Falls ein Server ausfällt, können Sie die virtuellen Maschinen auf einem anderen physischen Server neu starten. Im Störfall wird die festplatteninterne Sperre für die einzelnen virtuellen Maschinen aufgehoben.
- Mit vMotion können Sie virtuelle Maschinen bei laufendem Betrieb von einem physischen Server auf einen anderen migrieren.
- Mit VMware Consolidated Backup kann ein VCB-Proxy genannter Proxy-Server einen Snapshot einer virtuellen Maschine sichern, während diese eingeschaltet ist und Daten in ihren Speicher schreibt und in diesem liest.

NFS-Datenspeicher

ESXi kann auf ein ausgewähltes NFS-Volumen auf einem NAS-Server zugreifen, dieses Volumen mounten und es für Speichierzwecke nutzen. Mithilfe von NFS-Volumen können Sie virtuelle Maschinen ebenso wie mithilfe von VMFS-Datenspeichern speichern und starten.

ESXi unterstützt auf NFS-Volumen die folgenden Funktionen zur gemeinsamen Speichernutzung:

- vMotion
- VMware DRS und VMware HA
- ISO-Images, die virtuellen Maschinen als CD-ROMs angezeigt werden
- Snapshots einer virtuellen Maschine

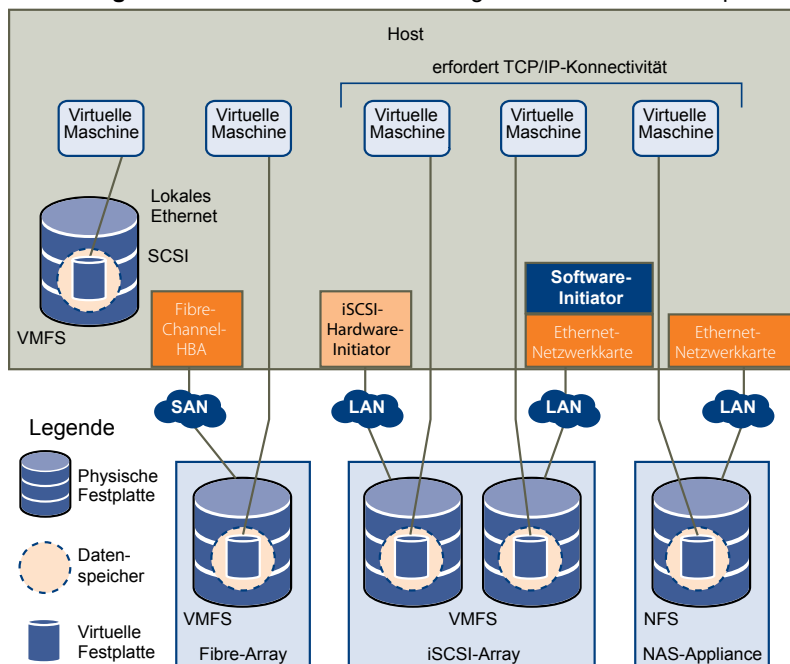
Speicherzugriff durch virtuelle Maschinen

Wenn eine virtuelle Maschine mit ihrer virtuellen Festplatte kommuniziert, die in einem Datenspeicher gespeichert sind, ruft sie SCSI-Befehle auf. Da sich die Datenspeicher auf verschiedenen Arten physischer Speicher befinden können, werden diese Befehle je nach Protokoll, das der ESXi-Host zur Anbindung an ein Speichergerät verwendet, umgewandelt.

ESXi unterstützt die Protokolle Fibre-Channel (FC), Internet-SCSI (iSCSI) und NFS. Die virtuelle Festplatte wird unabhängig vom Typ des Speichergeräts, den Ihr Host verwendet, immer als gemountetes SCSI-Gerät angezeigt. Die virtuelle Festplatte verbirgt die physische Speicherebene vor dem Betriebssystem der virtuellen Maschine. Dadurch können in der virtuellen Maschine Betriebssysteme ausgeführt werden, die nicht für bestimmte Speichersysteme, z. B. SAN, zertifiziert sind.

Abbildung 7-3 zeigt die Unterschiede zwischen den Speichertypen: Fünf virtuelle Maschinen verwenden unterschiedliche Arten von Speichern.

Abbildung 7-3. Virtuelle Maschinen mit Zugriff auf verschiedene Speichertypen



HINWEIS Diese Abbildung dient nur zur Veranschaulichung. Es handelt sich nicht um eine empfohlene Konfiguration.

Vergleich der Speichertypen

Welche vSphere-Funktionen unterstützt werden ist abhängig von der verwendeten Speichertechnologie.

Tabelle 7-1 vergleicht Netzwerkspeichertechnologien, die ESXi unterstützen.

Tabelle 7-1. Von ESXi unterstützter Netzwerkspeicher

Technologie	Protokolle	Übertragungen	Schnittstelle
Fibre-Channel	FC/SCSI	Blockzugriff für Daten/LUN	FC-HBA
iSCSI	IP/SCSI	Blockzugriff für Daten/LUN	<ul style="list-style-type: none"> ■ iSCSI-HBA (Hardware-initiiertes iSCSI) ■ Netzwerkkarte (Software-initiiertes iSCSI)
NAS	IP/NFS	Datei (kein direkter LUN-Zugriff)	Netzwerkkarte

[Tabelle 7-2](#) werden die von verschiedenen Speichertypen unterstützten vSphere-Funktionen verglichen.

Tabelle 7-2. Von Speichertypen unterstützte vSphere-Funktionen

Speichertyp	Starten von VMs	vMotion	Datenspeicher	RDM	VM-Cluster	VMware HA und DRS	VCB
Lokaler Speicher	Ja	Nein	VMFS	Nein	Nein	Nein	Ja
Fibre-Channel	Ja	Ja	VMFS	Ja	Ja	Ja	Ja
iSCSI	Ja	Ja	VMFS	Ja	Ja	Ja	Ja
NAS über NFS	Ja	Ja	NFS	Nein	Nein	Ja	Ja

Anzeigen der Speicherinformationen im vSphere-Client

Der vSphere-Client zeigt detaillierte Informationen zu Speicheradaptern und -geräten sowie allen verfügbaren Datenspeichern an.

Anzeigen von Speicheradaptern

Ihr Host verwendet Speicheradapter zum Zugreifen auf verschiedene Speichergeräte. Sie können die verfügbaren Speicheradapter anzeigen lassen und ihre Informationen überprüfen.

[Tabelle 7-3](#) listet die Informationen auf, die Sie beim Anzeigen der Details für die einzelnen Adapter erhalten. Bestimmte Adapter, z. B. iSCSI-Adapter, müssen vor dem Anzeigen ihrer Informationen konfiguriert oder aktiviert werden.

Tabelle 7-3. Informationen zu Speicheradaptern

Informationen zu Adaptern	Beschreibung
Modell	Adaptermodell.
Ziele (Fibre-Channel und SCSI)	Die Anzahl der Ziele, auf die über den Adapter zugegriffen wurde.
Verbundene Ziele (iSCSI)	Anzahl an verbundenen Zielen auf einem iSCSI-Adapter.
WWN (Fibre-Channel)	Ein in Übereinstimmung mit den Fibre-Channel-Standards erstellter World Wide Name, der den FC-Adapter eindeutig identifiziert.
iSCSI-Name (iSCSI)	Ein in Übereinstimmung mit den iSCSI-Standards erstellter eindeutiger Name, der den FC-Adapter eindeutig identifiziert.
iSCSI-Alias (iSCSI)	Ein benutzerfreundlicher Name, der anstelle des iSCSI-Namens verwendet wird.
IP-Adresse (Hardware-iSCSI)	Eine dem iSCSI-Adapter zugewiesene Adresse.
Erkennungsmethoden (iSCSI)	Erkennungsmethoden, die der iSCSI-Adapter für den Zugriff auf iSCSI-Ziele verwendet.

Tabelle 7-3. Informationen zu Speicheradaptern (Fortsetzung)

Informationen zu Adaptern	Beschreibung
Geräte	Alle Speichergeräte oder LUNs, auf die der Adapter zugreifen kann.
Pfade	Alle vom Adapter zum Zugreifen auf Speichergeräte verwendeten Pfade.

Anzeigen von Informationen zu Speicheradaptern

Sie können von Ihrem Host verwendete Speicheradapter anzeigen und ihre Informationen überprüfen.

Vorgehensweise

- 1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.
- 2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.
- 4 Wählen Sie einen Adapter in der Liste „Speicheradapter“ aus, um Details dazu anzuzeigen.
- 5 Klicken Sie zum Auflisten aller Speichergeräte, auf die der Adapter zugreifen kann, auf **[Geräte]**.
- 6 Klicken Sie zum Auflisten aller Pfade, die der Adapter verwendet, auf **[Pfade]**.

Kopieren von Speicheradapterbezeichnern in die Zwischenablage

Wenn Ihre Speicheradapter eindeutige Bezeichner verwenden, wie z. B. „iSCSI-Name“ oder „WWN“, können Sie sie direkt aus der Benutzerschnittstelle in die Zwischenablage kopieren.

Vorgehensweise

- 1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.
- 2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.
- 4 Wählen Sie den Adapter in der Liste „Speicheradapter“ aus.
- 5 Klicken Sie mit der rechten Maustaste im Fenster „Details“ auf den Wert im Feld „Name“ und wählen Sie **[Kopieren]**.

Anzeigen von Speichergeräten

Sie können alle auf dem Host verfügbaren Speichergeräte oder LUNs, einschließlich Netzwerk- und lokale Geräte, anzeigen. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden durch die Plug-Ins verfügbare Speichergeräte ebenfalls in der Liste angezeigt.

Sie können für jeden Speicheradapter eine separate Liste von Speichergeräten, die nur für diesen Adapter verfügbar sind, erstellen.

In der Regel wird Ihnen beim Überprüfen einer Liste von Speichergeräten Folgendes angezeigt.

Informationen zum Speichergerät	Beschreibung
Name	Ein benutzerfreundlicher Name, den der ESXi-Host dem Gerät anhand des Speichertyps und Herstellers zuweist. Sie können diesen Namen ändern.
Bezeichner	Eine für ein bestimmtes Gerät spezifische UUID.
Laufzeitname	Der Name des ersten Pfads zum Gerät.
LUN	Die LUN-Nummer, die die Position der LUN innerhalb des Ziels anzeigt.
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.

Informationen zum Speichergerät	Beschreibung
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet.
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten des Speichergeräts verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In.

Zu den Details für jedes Speichergerät gehören die Folgenden:

- Ein Pfad zum Speichergerät im Verzeichnis `/vmfs/devices/`.
- Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.

Anzeigen von Speichergeräten für einen Host

Sie können alle für einen Host verfügbaren Speichergeräte und LUNs anzeigen. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden durch die Plug-Ins verfügbare Speichergeräte ebenfalls in der Liste angezeigt.

Vorgehensweise

- 1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.
- 2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Klicken Sie unter „Hardware“ auf **[Speicher]**.
- 4 Klicken Sie auf **[Geräte]**.
- 5 Wählen Sie ein Gerät in der Liste aus, wenn Sie zusätzlich Details zu diesem bestimmten Gerät erfahren möchten.

Anzeigen von Speichergeräten für einen Adapter

Sie können eine Liste der Speichergeräte anzeigen, auf die ein bestimmter Speicheradapter auf dem Host zugreifen kann.

Vorgehensweise

- 1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.
- 2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.
- 4 Wählen Sie den Adapter in der Liste „Speicheradapter“ aus.
- 5 Klicken Sie auf **[Geräte]**.

Kopieren von Speichergerätebezeichnern in die Zwischenablage

Ein Speichergerätebezeichner ist eine UUID, die einem Speichergerät oder einer LUN zugewiesen ist. Je nach dem Speichertyp werden unterschiedliche Algorithmen zum Erstellen des Bezeichners verwendet, der lang und komplex sein kann. Sie können den Speichergerätebezeichner direkt aus der Benutzerschnittstelle kopieren.

Vorgehensweise

- 1 Zeigen Sie eine Liste von Speichergeräten an.
- 2 Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **[Bezeichner in die Zwischenablage kopieren]**.

Anzeigen von Datenspeichern

Sie können alle auf den Hosts verfügbaren Datenspeicher anzeigen und deren Eigenschaften analysieren.

Es gibt folgende Möglichkeiten, dem vSphere-Client Datenspeicher hinzuzufügen:

- Erstellung auf einem verfügbaren Speichergerät.
- Erkennung, sobald ein Host der Bestandsliste hinzugefügt wird. Wenn Sie der Bestandsliste einen Host hinzufügen, zeigt der vSphere-Client alle Datenspeicher an, die dem Host zur Verfügung stehen.

Wenn Ihr vSphere-Client mit einem vCenter Server-System verbunden ist, können Sie die Datenspeicherinformationen in der Ansicht „Datenspeicher“ anzeigen. In dieser Ansicht werden alle Datenspeicher in der Bestandsliste nach Datacenter sortiert angezeigt. Mithilfe dieser Ansicht können Sie Datenspeicher in Ordnerhierarchien organisieren, neue Datenspeicher erstellen, ihre Eigenschaften bearbeiten und vorhandene Datenspeicher entfernen.

Diese Ansicht zeigt umfangreiche Informationen zu Ihren Datenspeichern an. Dazu gehören die Hosts und die virtuellen Maschinen, die die Datenspeicher verwenden, Informationen zu Speicherberichten, Berechtigungen, Alarme, Aufgaben und Ereignisse, die Speichertopologie sowie die Speicherberichte selbst. Für jeden Datenspeicher werden auf der Registerkarte „Konfiguration“ in der Ansicht „Datenspeicher“ Konfigurationen zu allen mit dem Datenspeicher verbundenen Hosts aufgeführt.

HINWEIS Die Ansicht „Datenspeicher“ ist nicht verfügbar, wenn der vSphere-Client direkt mit ihrem Host verbunden ist. In diesem Fall können Sie über die Registerkarte für die hostspezifische Speicherkonfiguration Datenspeicherinformationen einsehen.

In der Regel können Sie folgende Konfigurationsinformationen für Datenspeicher anzeigen:

- Das Zielspeichergerät, auf dem sich der Datenspeicher befindet
- Das vom Datenspeicher verwendete Dateisystem
- Den Speicherort des Datenspeichers
- Die Gesamtkapazität sowie der belegte und freie Speicher
- Einzelne Erweiterungen, aus denen der Datenspeicher besteht, samt Kapazität (nur VMFS-Datenspeicher)
- Pfade, die zum Zugriff auf das Speichergerät verwendet werden (nur VMFS-Datenspeicher)

Überprüfen von Dateneigenschafteneigenschaften

Sie können alle auf den Hosts verfügbaren Datenspeicher anzeigen und deren Eigenschaften analysieren.

Vorgehensweise

- 1 Zeigen Sie den Host in der Bestandsliste an.
- 2 Wählen Sie in der Bestandsliste einen Host aus und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Klicken Sie unter „Hardware“ auf **[Speicher]**.
- 4 Klicken Sie unter „Ansicht“ auf **[Datenspeicher]**.
- 5 Wählen Sie einen Datenspeicher in der Liste aus, um Details dazu anzuzeigen.

Konfigurieren von ESXi-Speicher

Die folgenden Themen enthalten Informationen zur Konfiguration lokaler SCSI-Speichergeräte sowie zur Fibre-Channel-SAN-, iSCSI- und NFS-Speicherung.

Dieses Kapitel behandelt die folgenden Themen:

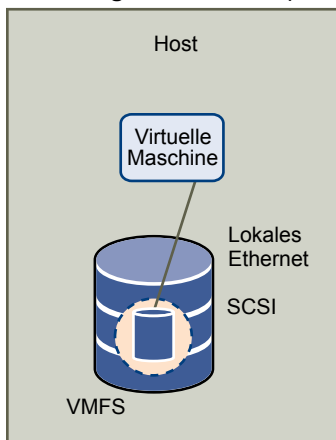
- „Lokaler SCSI-Speicher“, auf Seite 83
- „Fibre-Channel-Speicher“, auf Seite 84
- „iSCSI-Speicher“, auf Seite 84
- „Vorgänge zum Aktualisieren und erneuten Prüfen von Speichern“, auf Seite 96
- „Erstellen eines VMFS-Datenspeichers“, auf Seite 97
- „Network Attached Storage (NAS)“, auf Seite 98
- „Erstellen einer Diagnosepartition“, auf Seite 100

Lokaler SCSI-Speicher

Der lokale Speicher verwendet ein SCSI-Gerät, z. B. die Festplatte des ESXi-Hosts oder ein externes dediziertes Speichersystem, das direkt an den Host angeschlossen ist.

Abbildung 8-1 zeigt eine virtuelle Maschine, die lokalen SCSI-Speicher verwendet.

Abbildung 8-1. Lokaler Speicher



Bei diesem Beispiel einer lokalen Speichertopologie verwendet der ESXi-Host eine einzelne Verbindung, um eine Festplatte anzuschließen. Auf dieser Festplatte können Sie einen VMFS-Datenspeicher erstellen, der zur Speicherung der Festplattendateien der virtuellen Maschine verwendet wird.

Wenngleich diese Speicherkonfiguration möglich ist, wird sie nicht empfohlen. Das Verwenden einzelner Verbindungen zwischen Speicherarrays und Hosts sorgt für einzelne Ausfallstellen, die Störungen verursachen können, wenn eine Verbindung unzuverlässig wird oder ausfällt.

Um für Fehlertoleranz zu sorgen, unterstützen verschiedene direkt angeschlossene Speichersysteme redundante Verbindungspfade.

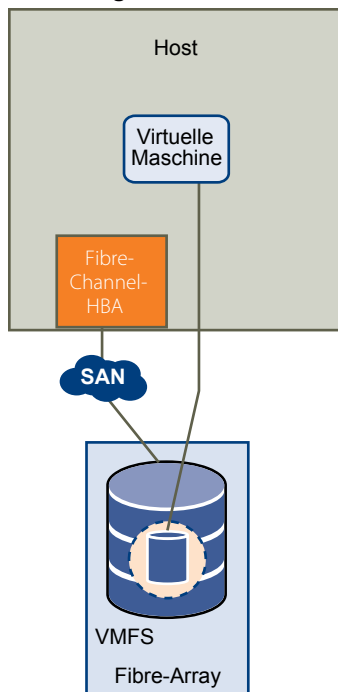
Fibre-Channel-Speicher

ESXi unterstützt Fibre-Channel-Adapter, wodurch ein Host sich mit einem SAN verbinden und Speichergeräte auf dem SAN sehen kann.

Sie müssen Fibre-Channel-Adapter (FC) installieren, bevor der Host FC-Speichergeräte anzeigen kann.

Abbildung 8-2 zeigt virtuelle Maschinen, die einen Fibre-Channel-Speicher verwenden.

Abbildung 8-2. Fibre-Channel-Speicher



Bei dieser Konfiguration ist der ESXi-Host mithilfe eines Fibre-Channel-Adapters mit einem SAN-Fabric verbunden, das aus Fibre-Channel-Switches und Speicherarrays besteht. LUNs eines Speicherarrays können vom Host verwendet werden. Sie können auf die LUNs zugreifen und einen Datenspeicher für Ihre Speicheranforderungen erstellen. Der Datenspeicher verwendet das VMFS-Format.

Nähere Informationen dazu, wie FC SAN-Fabric und -Speicher-Arrays eingerichtet werden, damit sie mit ESXi verwendet werden können, finden Sie im *SAN-Konfigurationshandbuch (für Fibre-Channel)*.

iSCSI-Speicher

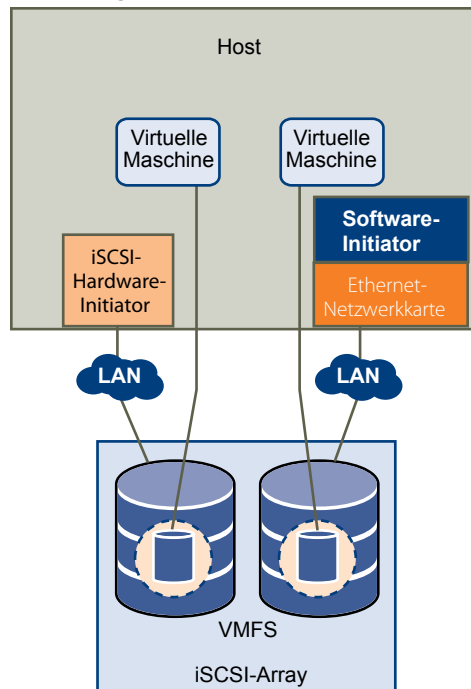
ESXi unterstützt die iSCSI-Technologie, die es Ihrem Host ermöglicht, beim Zugriff auf Remotespeicher ein IP-Netzwerk zu verwenden. Bei iSCSI werden die SCSI-Speicherbefehle, die die virtuelle Maschine an ihre virtuelle Festplatte erteilt, in TCP/IP-Pakete umgewandelt und an ein Remotegerät, oder Ziel, übertragen, auf dem die virtuelle Festplatte gespeichert ist.

Für den Zugriff auf Remoteziele verwendet der Host iSCSI-Initiatoren. Die Initiatoren übermitteln SCSI-Anforderungen und -Antworten zwischen dem Host und dem Zielspeichergerät über das IP-Netzwerk. ESXi unterstützt hardwarebasierte und softwarebasierte iSCSI-Initiatoren.

Sie müssen iSCSI-Initiatoren konfigurieren, damit der Host auf iSCSI-Speichergeräte zugreifen und diese anzeigen kann.

Abbildung 8-3 zeigt zwei virtuelle Maschinen, die verschiedene Arten von iSCSI-Initiatoren verwenden.

Abbildung 8-3. iSCSI-Speicher



Im linken Beispiel verwendet der Host einen Hardware-iSCSI-Adapter für die Verbindung zum iSCSI-Speichersystem.

Im rechten Beispiel wird der Host mit dem Software-iSCSI-Initiator konfiguriert. Unter Verwendung des Software-Initiators stellt der Host über einen vorhandenen Netzwerkkarte eine Verbindung mit einem iSCSI-Speicher her.

Die iSCSI-Speichergeräte des Speichersystems stehen dem Host nun zur Verfügung. Sie können auf die Speichergeräte zugreifen und VMFS-Datenspeicher erstellen, die Sie zur Speicherung benötigen.

Nähere Informationen dazu, wie iSCSI SAN-Fabric eingerichtet wird, damit sie mit ESXi verwendet werden kann, finden Sie im *SAN-Konfigurationshandbuch (für iSCSI)*.

Einrichten von Hardware-iSCSI-Initiatoren

Mit dem hardwarebasierten iSCSI-Speicher werden spezielle Adapter von Drittanbietern verwendet, die über TCP/IP auf iSCSI-Speicher zugreifen können. Dieser iSCSI-Initiator steuert die gesamte iSCSI- und Netzwerk-Verarbeitung und -Verwaltung für das ESXi-System.

Bevor Sie einen Datenspeicher auf einem iSCSI-Speichergerät einrichten, müssen Sie den Hardware-iSCSI-Adapter installieren und konfigurieren.

Anzeigen von Hardware-iSCSI-Initiatoren

Zeigen Sie einen iSCSI-Hardware-Initiator an, um zu überprüfen, ob er korrekt installiert und konfigurationsbereit ist.

Voraussetzungen

Bevor Sie mit der Konfiguration des Hardware-iSCSI-Initiators beginnen, überprüfen Sie, dass der iSCSI-HBA ordnungsgemäß installiert wurde und in der Liste der konfigurierbaren Initiatoren angezeigt wird. Wenn der Initiator installiert wurde, können Sie seine Eigenschaften anzeigen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.

Der Hardware-iSCSI-Initiator wird in der Liste der Speicheradapter angezeigt.

- 3 Wählen Sie den anzuzeigenden Initiator aus.
Die standardmäßigen Details für den Initiator werden angezeigt, darunter das Modell, der iSCSI-Name, iSCSI-Alias, IP-Adresse sowie Ziel- und Pfadinformationen.
- 4 Klicken Sie auf **[Eigenschaften]**.

Das Dialogfeld **[iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)]** wird angezeigt. Auf der Registerkarte **[Allgemein (General)]** werden zusätzliche Merkmale des Initiators angezeigt.

Sie können den Hardware-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Ändern des Namens und der IP-Adresse für Hardware-Initiator

Stellen Sie beim Konfigurieren der Hardware-iSCSI-Initiatoren sicher, dass ihre Namen und IP-Adressen ordnungsgemäß formatiert sind.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.
- 3 Wählen Sie den zu konfigurierenden Initiator aus und klicken Sie auf **[Eigenschaften] > [Konfigurieren]**.

- 4 Um den Standard-iSCSI-Namen für den Initiator zu ändern, geben Sie einen neuen Namen ein.

Stellen Sie sicher, dass der eingegebene Name weltweit eindeutig und ordnungsgemäß formatiert ist, anderenfalls wird der Hardware-iSCSI-Initiator möglicherweise von bestimmten Speichergeräten nicht erkannt.

- 5 (Optional) Geben Sie das iSCSI-Alias ein.

Das Alias ist ein Name, der zur Identifizierung des Hardware-iSCSI-Initiators verwendet wird.

- 6 Ändern Sie die Standard-IP-Einstellungen.

Sie müssen die Standard-IP-Einstellungen ändern, damit diese für das IP-SAN ordnungsgemäß konfiguriert sind. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Einstellung für den HBA zu erfahren.

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

Wenn Sie den iSCSI-Namen ändern, wird er für neue iSCSI-Sitzungen verwendet. In vorhandenen Sitzungen werden neue Einstellungen nicht verwendet. Sie treten erst bei erneuter Anmeldung in Kraft.

Einrichten von Software-iSCSI-Initiatoren

Bei einer softwarebasierten iSCSI-Implementierung können Sie Standardnetzwerkadapter verwenden, um das ESXi-Host mit einem Remote-iSCSI-Ziel im IP-Netzwerk zu verbinden. Der im ESXi integrierte iSCSI-Software-Initiator vereinfacht diesen Verbindungsaufbau, indem er über den Netzwerkstapel mit dem Netzwerkadapter kommuniziert.

Bevor Sie den iSCSI-Software-Initiator konfigurieren, müssen Sie die folgenden Aufgaben durchführen:

- 1 Erstellen Sie einen VMkernel-Port für physische Netzwerkadapter.
- 2 Aktivieren Sie den Software-iSCSI-Initiator.
- 3 Wenn Sie mehrere Netzwerkadapter verwenden, konfigurieren Sie mithilfe der Port-Bindung das Multipathing auf Ihrem Host.

Weitere Informationen zur Port-Bindung finden Sie im *SAN-Konfigurationshandbuch (für iSCSI)*.

- 4 Aktivieren Sie bei Bedarf Jumbo-Frames. Jumbo-Frames müssen für jeden vSwitch über die vSphere-CLI aktiviert werden. Wenn Sie einen ESX-Host verwenden, müssen Sie ebenfalls eine VMkernel-Netzwerkschnittstelle erstellen, die für Jumbo-Frames aktiviert ist.

Weitere Informationen finden Sie im Abschnitt *Netzwerk*.

Netzwerkconfiguration für Software-iSCSI-Speicher

Die Netzwerkconfiguration für Software-iSCSI umfasst die Erstellung eines iSCSI-VMkernel-Ports und dessen Zuordnung zu einer physischen Netzwerkkarte, die den iSCSI-Datenverkehr verarbeitet.

Abhängig von der Anzahl an physischen Netzwerkkarten, die Sie für den iSCSI-Datenverkehr verwenden möchten, sind unterschiedliche Netzwerk-Setups möglich:

- Wenn eine physische Netzwerkkarte vorhanden ist, erstellen Sie einen VMkernel-Port auf einem vSwitch und ordnen den Port dabei der physischen Netzwerkkarte zu. VMware empfiehlt, einen separaten Netzwerkadapter nur für iSCSI zu bestimmen. Es sind keine zusätzlichen Netzwerkconfigurationsschritte erforderlich.

Weitere Informationen zum Erstellen eines Ports finden Sie unter [„Erstellen eines VMkernel-Ports für Software-iSCSI“](#), auf Seite 87.

- Wenn Sie mehrere physische Netzwerkkarten verwenden, konfigurieren Sie mithilfe der Port-Bindung mehrere Pfade für das Software-iSCSI erstellen.

Weitere Informationen zur Port-Bindung finden Sie im *SAN-Konfigurationshandbuch (für iSCSI)*.

Erstellen eines VMkernel-Ports für Software-iSCSI

Mit diesem Verfahren können Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, mit dem physischen Netzwerkadapter verbinden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.
- 3 Klicken Sie in der Ansicht „Virtueller Switch“ auf **[Netzwerk hinzufügen]**.
- 4 Wählen Sie **[VMkernel (VMkernel)]** aus, und klicken Sie auf **[Weiter]**.

- 5 Wählen Sie **[Einen virtuellen Switch erstellen]** , um einen neuen vSwitch zu erstellen.
Falls kein Adapter unter **[Einen virtuellen Switch erstellen (Create a virtual switch)]** angezeigt wird, werden bereits alle Netzwerkadapter im System von den vorhandenen vSwitches verwendet. Sie können einen vorhandenen vSwitch für Ihren iSCSI-Datenverkehr verwenden.
- 6 Wählen Sie einen Adapter aus, den Sie für iSCSI-Datenverkehr verwenden möchten.

WICHTIG Verwenden Sie iSCSI nicht bei Adaptern mit 100 MBit/s oder weniger.

- 7 Klicken Sie auf **[Weiter]** .
- 8 Geben Sie unter **[Portgruppeneigenschaften]** eine Netzwerkbezeichnung ein. Die Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Port identifiziert, den Sie erstellen.
- 9 Klicken Sie auf **[Weiter]** .
- 10 Geben Sie die IP-Einstellungen an und klicken Sie auf **[Weiter]** .
- 11 Überprüfen Sie die Informationen und klicken Sie auf **[Beenden]** .

Weiter

Sie können jetzt Ihren Software-Initiator aktivieren.

Aktivieren des Software-iSCSI-Initiators

Aktivieren Sie Ihren Software-iSCSI-Initiator, damit er von ESXi für den Zugriff auf den iSCSI-Speicher verwendet werden kann.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]** .
- 4 Klicken Sie auf **[Konfigurieren]** .
Das Dialogfeld **[Allgemeine Eigenschaften]** zeigt den Status des Initiators, den Standardnamen und das Alias an.
- 5 Aktivieren Sie das Kontrollkästchen **[Aktiviert]** , um den Initiator zu aktivieren.
- 6 Um den Standard-iSCSI-Namen für den Initiator zu ändern, geben Sie einen neuen Namen ein.
Stellen Sie sicher, dass der eingegebene Name weltweit eindeutig und ordnungsgemäß formatiert ist, anderenfalls wird der Software-iSCSI-Initiator möglicherweise von bestimmten Speichergeräten nicht erkannt.
- 7 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Wenn Sie den iSCSI-Namen ändern, wird er für neue iSCSI-Sitzungen verwendet. In vorhandenen Sitzungen werden neue Einstellungen nicht verwendet. Sie treten erst bei erneuter Anmeldung in Kraft.

Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren

Sie müssen Zielerkennungsadressen einrichten, damit der iSCSI-Initiator erkennen kann, welche Speicherressourcen im Netzwerk zur Verfügung stehen.

Das ESXi-System unterstützt die folgenden Erkennungsmethoden:

Dynamische Erkennung Wird auch als „Send Targets“-Erkennungsmethode bezeichnet. Immer wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, übermittelt der Initiator eine Ziele senden-Anforderung an den Server. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Die Namen und IP-Adressen dieser Ziele werden auf der Registerkarte **[Statische Erkennung (Static Discovery)]** angezeigt. Wenn Sie ein von der dynamischen Erkennung hinzugefügtes statisches Ziel entfernen, kann das Ziel entweder bei einer erneuten Überprüfung, beim Zurücksetzen des HBA oder durch einen Neustart des Hosts erneut zur Liste hinzugefügt werden.

Statische Erkennung Der Initiator muss keine Erkennung durchführen. Der Initiator kennt bereits alle Ziele, mit denen er Kontakt aufnehmen möchte, und verwendet ihre IP-Adressen und Domännennamen für die Kommunikation mit ihnen.

Einrichten der dynamischen Erkennung

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, eine „Send Targets“-Anforderung an den Server übermittelt. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie im Dialogfeld **[iSCSI-Initiator-Eigenschaften]** auf die Registerkarte **[Dynamische Erkennung]**.
- 5 Um der „Send Targets“-Erkennungsmethode eine Adresse hinzuzufügen, klicken Sie auf **[Hinzufügen]**.
Das Dialogfeld **[Ziel-senden-Server hinzufügen (Add Send Targets Server)]** wird angezeigt.
- 6 Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf **[OK]**.
Nachdem der Host die „Send Targets“-Sitzung mit diesem System gestartet hat, werden in der Liste „Statische Erkennung“ alle neu erkannten Ziele angezeigt.
- 7 Sie können einen bestimmten „Send Targets“-Server löschen, indem Sie ihn auswählen und auf **[Entfernen]** klicken.
Nachdem Sie einen „Send Targets“-Server entfernt haben, wird er möglicherweise immer noch im Feld „Vererbung“ als übergeordnetes Element von statischen Zielen angezeigt. Dieser Eintrag zeigt an, wo die statischen Ziele ermittelt wurden, und wirkt sich nicht auf die Funktionsweise aus.

HINWEIS Es ist nicht möglich, die IP-Adresse, den DNS-Namen oder die Portnummer eines vorhandenen „Send Targets“-Servers zu ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie den vorhandene Server und fügen Sie einen neuen hinzu.

Einrichten der statischen Erkennung

Bei iSCSI-Initiatoren können Sie neben der dynamischen Erkennungsmethode auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie im Dialogfeld **[iSCSI-Initiator-Eigenschaften]** auf die Registerkarte **[Statische Erkennung (Static Discovery)]**.
Die Registerkarte zeigt alle dynamisch erkannten Ziele und alle bereits eingegebenen statischen Ziele an.
- 5 Um ein Ziel hinzuzufügen, klicken Sie auf **[Hinzufügen]** und geben Sie die Informationen des Ziels ein.
- 6 Sie können ein bestimmtes Ziel löschen, indem Sie das Ziel auswählen und auf **[Entfernen]** klicken.

HINWEIS Sie können die IP-Adresse, den DNS-Namen, den iSCSI-Zielnamen oder die Portnummer eines vorhandenen Ziels nicht ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

Konfigurieren von CHAP-Parametern für iSCSI-Initiatoren

Da die IP-Netzwerke, die die iSCSI-Technologie zum Verbinden mit Remotezielen verwendet, die von ihnen transportierten Daten nicht schützen, muss die Sicherheit der Verbindung gewährleistet werden. iSCSI erfordert, dass alle Geräte im Netzwerk das Challenge Handshake Authentication Protocol (CHAP) implementieren, das die Legitimität der Initiatoren verifizieren kann, die auf Ziele im Netzwerk zugreifen.

CHAP verwendet einen dreiteiligen Handshake-Algorithmus, um die Identität Ihres Hosts und, sofern zutreffend, des iSCSI-Ziels zu verifizieren, wenn der Host und das Ziel eine Verbindung herstellen. Die Verifizierung basiert auf einem vordefinierten privaten Wert, dem CHAP-Schlüssel, den der Initiator und das Ziel gemeinsam verwenden.

ESXi unterstützt die CHAP-Authentifizierung auf der Adapterebene. In diesem Fall erhalten alle Ziele vom iSCSI-Initiator denselben CHAP-Namen und -Schlüssel. Für Software-iSCSI unterstützt ESXi auch die CHAP-Authentifizierung für einzelne Ziele, was Ihnen ermöglicht, unterschiedliche Anmeldedaten für die einzelnen Ziele zu konfigurieren und so die Sicherheit zu erhöhen.

Auswählen der CHAP-Authentifizierungsmethode

ESXi unterstützt unidirektionales CHAP für Hardware- und Software-iSCSI sowie beiderseitiges CHAP für Software-iSCSI.

Bevor Sie CHAP konfigurieren, überprüfen Sie, ob CHAP im iSCSI-Speichersystem aktiviert ist und welche CHAP-Authentifizierungsmethode vom System unterstützt wird. Wenn CHAP aktiviert ist, müssen Sie es für Ihre Initiatoren aktivieren und dabei sicherstellen, dass die Anmeldedaten für die CHAP-Authentifizierung mit den Anmeldedaten im iSCSI-Speicher übereinstimmen.

ESXi unterstützt die folgenden CHAP-Authentifizierungsmethoden:

Unidirektionales CHAP	Bei der unidirektionalen CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel.
Beiderseitiges CHAP (nur Software-iSCSI)	Bei der beiderseitigen oder bidirektionalen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels.

Bei Software-iSCSI können Sie unidirektionales CHAP und beiderseitiges CHAP für die einzelnen Initiatoren oder auf der Zielebene festlegen. Hardware-iSCSI unterstützt CHAP nur auf der Initiatorebene.

Wenn Sie die CHAP-Parameter festlegen, geben Sie eine Sicherheitsstufe für CHAP an.

Tabelle 8-1. CHAP-Sicherheitsstufe

CHAP-Sicherheitsstufe	Beschreibung	Unterstützt
CHAP nicht verwenden	Der Host verwendet keine CHAP-Authentifizierung. Wählen Sie diese Option aus, um die Authentifizierung zu deaktivieren, wenn sie derzeit aktiviert ist.	Software-iSCSI Hardware-iSCSI
CHAP nur verwenden, wenn Ziel dies erfordert	Der Host bevorzugt eine Nicht-CHAP-Verbindung, er kann jedoch eine CHAP-Verbindung verwenden, wenn das Ziel dies erfordert.	Software-iSCSI
CHAP verwenden, sofern Ziel dies unterstützt	Der Host bevorzugt CHAP, er kann jedoch Nicht-CHAP-Verbindungen verwenden, wenn das Ziel CHAP nicht unterstützt.	Software-iSCSI Hardware-iSCSI
CHAP verwenden	Für den Host ist eine erfolgreiche CHAP-Authentifizierung erforderlich. Die Verbindung schlägt fehl, wenn die CHAP-Aushandlung fehlschlägt.	Software-iSCSI

Einrichten von CHAP-Anmeldedaten für einen iSCSI-Initiator

Zur Erhöhung der Sicherheit können alle Ziele so eingerichtet werden, dass sie denselben CHAP-Namen und -Schlüssel vom iSCSI-Initiator auf der Initiatorebene empfangen. Standardmäßig übernehmen alle Erkennungsadressen und statischen Ziele die CHAP-Parameter, die Sie auf der Initiatorebene einrichten.

Voraussetzungen

Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI fest, ob unidirektionales oder beiderseitiges CHAP konfiguriert werden soll. Beiderseitiges CHAP wird von Hardware-iSCSI nicht unterstützt.

- Bei unidirektionalem CHAP authentifiziert das Ziel den Initiator.
- Bei beiderseitigem CHAP authentifizieren sich das Ziel und der Initiator gegenseitig. Stellen Sie sicher, dass Sie für CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

Stellen Sie beim Konfigurieren von CHAP-Parametern sicher, dass sie mit den Parametern auf der Speicherseite übereinstimmen.

Bei Software-iSCSI darf der CHAP-Name nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen. Bei Hardware-iSCSI darf der CHAP-Name nicht mehr als 255 und der CHAP-Schlüssel nicht mehr als 100 alphanumerische Zeichen umfassen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

- 3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]** .
- 4 Klicken Sie auf der Registerkarte **[Allgemein]** auf **[CHAP]** .
- 5 Wenn Sie unidirektionales CHAP konfigurieren möchten, geben Sie unter CHAP Folgendes an.
 - a Wählen Sie eine der folgenden Optionen aus:
 - **[CHAP nur verwenden, wenn Ziel dies erfordert]** (nur Software-iSCSI)
 - **[CHAP verwenden, sofern Ziel dies unterstützt]**
 - **[CHAP verwenden]** (nur Software-iSCSI). Um beidseitiges CHAP konfigurieren zu können, müssen Sie diese Option auswählen.
 - b Geben Sie den CHAP-Namen an.

Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.

 - Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **[Initiator-Name verwenden]** .
 - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **[Initiator-Name verwenden]** und geben Sie einen Namen in das Feld **[Name]** ein.
 - c Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Stellen Sie sicher, dass Sie denselben Schlüssel verwenden, den Sie auf der Speicherseite eingeben.
- 6 Wenn Sie beidseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter [Schritt 5](#) befolgen.

Stellen Sie sicher, dass Sie als Option für unidirektionales CHAP **[CHAP verwenden]** auswählen. Geben Sie anschließend unter **[Beidseitiges CHAP]** Folgendes an:

 - a Wählen Sie die Option **[CHAP verwenden]** aus.
 - b Geben Sie den Namen für beidseitiges CHAP an.
 - c Geben Sie den Schlüssel für beidseitiges CHAP an. Stellen Sie sicher, dass Sie für unidirektionales CHAP und beidseitiges CHAP verschiedene Schlüssel verwenden.
- 7 Klicken Sie auf **[OK]** .
- 8 Prüfen Sie den Initiator erneut.

Wenn Sie die Parameter für CHAP oder beidseitiges CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Einrichten von CHAP-Anmeldedaten für ein Ziel

Für Software-iSCSI können Sie verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.

Stellen Sie beim Konfigurieren von CHAP-Parametern sicher, dass sie mit den Parametern auf der Speicherseite übereinstimmen. Bei Software-iSCSI darf der CHAP-Name nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen.

Voraussetzungen

Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI fest, ob unidirektionales oder beiderseitiges CHAP konfiguriert werden soll.

- Bei unidirektionalem CHAP authentifiziert das Ziel den Initiator.
- Bei beiderseitigem CHAP authentifizieren sich das Ziel und der Initiator gegenseitig. Stellen Sie sicher, dass Sie für CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Wählen Sie den zu konfigurierenden Software-iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]**.
- 4 Wählen Sie die Registerkarte **[Dynamische Erkennung]** oder **[Statische Erkennung]** aus.
- 5 Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **[Einstellungen] > [CHAP]**.
- 6 Wenn Sie unidirektionales CHAP konfigurieren möchten, geben Sie unter CHAP Folgendes an.
 - a Deaktivieren Sie **[Vom übergeordneten Element übernehmen]**.
 - b Wählen Sie eine der folgenden Optionen aus:
 - **[CHAP nur verwenden, wenn Ziel dies erfordert]**
 - **[CHAP verwenden, sofern Ziel dies unterstützt]**
 - **[CHAP verwenden]**. Um beiderseitiges CHAP konfigurieren zu können, müssen Sie diese Option auswählen.
 - c Geben Sie den CHAP-Namen an.
Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.
 - Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **[Initiator-Name verwenden]**.
 - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **[Initiator-Name verwenden]** und geben Sie einen Namen in das Feld **[Name]** ein.
 - d Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Stellen Sie sicher, dass Sie denselben Schlüssel verwenden, den Sie auf der Speicherseite eingeben.
- 7 Wenn Sie beiderseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter [Schritt 6](#) befolgen.
Stellen Sie sicher, dass Sie als Option für unidirektionales CHAP **[CHAP verwenden]** auswählen. Geben Sie anschließend unter **[Beiderseitiges CHAP]** Folgendes an:
 - a Deaktivieren Sie **[Vom übergeordneten Element übernehmen]**.
 - b Wählen Sie die Option **[CHAP verwenden]** aus.
 - c Geben Sie den Namen für beiderseitiges CHAP an.
 - d Geben Sie den Schlüssel für beiderseitiges CHAP an. Stellen Sie sicher, dass Sie für unidirektionales CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

- 8 Klicken Sie auf **[OK]** .
- 9 Prüfen Sie den Initiator erneut.

Wenn Sie die Parameter für CHAP oder beiderseitiges CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Deaktivieren von CHAP

Sie können CHAP deaktivieren, wenn Ihr Speichersystem dieses nicht erfordert.

Wenn Sie CHAP auf einem System deaktivieren, das die CHAP-Authentifizierung benötigt, bleiben bestehende iSCSI-Sitzungen so lange aktiv, bis Sie Ihren ESXi-Host neu starten oder das Speichersystem eine Abmeldung erzwingt. Nachdem die Sitzung beendet wurde, können Sie keine Verbindungen mehr zu Zielen herstellen, die CHAP benötigen.

Vorgehensweise

- 1 Öffnen Sie das Dialogfeld „CHAP-Anmeldedaten“.
- 2 Wählen Sie für Software-iSCSI, wenn Sie nur das beiderseitige CHAP deaktivieren möchten, unter **[Beiderseitiges CHAP]** unter **[CHAP nicht verwenden]** .
- 3 Wenn Sie das unidirektionale CHAP deaktivieren möchten, wählen Sie unter **[CHAP]** die Option **[CHAP nicht verwenden]** .

Wenn Sie das unidirektionale CHAP deaktivieren, wird für das beiderseitige CHAP, sofern dies eingerichtet ist, automatisch die Option **[CHAP nicht verwenden]** festgelegt.

- 4 Klicken Sie auf **[OK]** .

Konfigurieren zusätzlicher Parameter für iSCSI

Möglicherweise müssen Sie für Ihre iSCSI-Initiatoren zusätzliche Parameter konfigurieren. Beispielsweise erfordern einige iSCSI-Speichersysteme eine ARP-Umleitung (Address Resolution Protocol), um iSCSI-Datenverkehr dynamisch von einem Port auf einen anderen zu verschieben. In diesem Fall müssen Sie die ARP-Umleitung auf Ihrem Host aktivieren.

Sie sollten die erweiterten iSCSI-Einstellungen nur ändern, wenn Sie eng mit dem Support-Team von VMware zusammenarbeiten oder anderweitig über umfassende Informationen zu den Werten der einzelnen Einstellungen verfügen.

[Tabelle 8-2](#) sind die erweiterten iSCSI-Parameter aufgelistet, die Sie mithilfe des vSphere-Clients konfigurieren können. Darüber hinaus können Sie den vSphere CLI-Befehl `vicfg-iscsi` verwenden, um einige der erweiterten Parameter zu konfigurieren. Weitere Informationen hierzu finden Sie im Handbuch *VMware vSphere-Befehlszeilenschnittstellen-Installation und -Referenz*.

Tabelle 8-2. Zusätzliche Parameter für iSCSI-Initiatoren

Erweiterte Parameter	Beschreibung	Konfigurierbar auf
Header-Digest	Erhöht die Datenintegrität. Wenn der Parameter „Header-Digest“ aktiviert ist, berechnet das System für den Header-Teil jeder iSCSI-PDU (Protocol Data Unit) eine Prüfsumme und führt anhand des CRC32C-Algorithmus eine Verifizierung durch.	Software-iSCSI
Data Digest	Erhöht die Datenintegrität. Wenn der Parameter „Data Digest“ aktiviert ist, berechnet das System für den Data-Teil jeder PDU eine Prüfsumme und führt anhand des CRC32C-Algorithmus eine Verifizierung durch. HINWEIS Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen für Software-iSCSI aus und reduzieren damit die Auswirkungen auf die Leistung.	Software-iSCSI

Tabelle 8-2. Zusätzliche Parameter für iSCSI-Initiatoren (Fortsetzung)

Erweiterte Parameter	Beschreibung	Konfigurierbar auf
Maximal ausstehendes R2T	Legt fest, wie viele R2T-PDUs (Ready to Transfer) sich im Übergang befinden können, bevor eine bestätigte PDU empfangen wird.	Software-iSCSI
Erste Burstlänge	Legt die maximale Menge an nicht angeforderten Daten in Byte fest, die ein iSCSI-Initiator während der Ausführung eines einzelnen SCSI-Befehls an das Ziel senden kann.	Software-iSCSI
Maximale Burstlänge	Die maximale SCSI-Datenlast in einer Data-In- oder einer angeforderten Data-Out-iSCSI-Sequenz in Byte.	Software-iSCSI
Maximale Datensegmentlänge	Die maximale Datensegmentlänge in Byte, die in einer iSCSI-PDU empfangen werden kann.	Software-iSCSI
ARP-Weiterleitung	Ermöglicht Speichersystemen das dynamische Verschieben von iSCSI-Datenverkehr von einem Port auf einen anderen. ARP wird von Speichersystemen benötigt, die Array-basiertes Failover durchführen.	Hardware-iSCSI (Über die vSphere-CLI konfigurierbar)
Verzögerte Quittierung (ACK)	Ermöglicht Systemen die Verzögerung der Bestätigung empfangener Datenpakete.	Software-iSCSI

Konfigurieren erweiterter Parameter für iSCSI

Die erweiterten iSCSI-Einstellungen steuern Parameter wie „Header-Digest“, „Data Digest“, „ARP-Umleitung“, „Verzögerte Quittierung (ACK)“ usw. In der Regel müssen Sie keine Änderungen an diesen Einstellungen vornehmen, da Ihr ESXi-Host mit den zugewiesenen vordefinierten Werten funktioniert.



VORSICHT Sie sollten die erweiterten iSCSI-Einstellungen nur ändern, wenn Sie eng mit dem Support-Team von VMware zusammenarbeiten oder anderweitig über umfassende Informationen zu den Werten der einzelnen Einstellungen verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Speicheradapter]**.
- 3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie zum Konfigurieren von erweiterten Parametern auf der Initiatorebene auf der Registerkarte **[Allgemein]** auf **[Erweitert]**. Fahren Sie mit [Schritt 6](#) fort.
- 5 Konfigurieren Sie erweiterte Parameter auf der Zielebene.

Auf der Zielebene können erweiterte Parameter nur für Software-iSCSI konfiguriert werden.

 - a Wählen Sie die Registerkarte **[Dynamische Erkennung]** oder **[Statische Erkennung]** aus.
 - b Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **[Einstellungen]** > **[Erweitert]**.
- 6 Geben Sie die erforderlichen Werte für die erweiterten Parameter ein, die Sie ändern möchten, und klicken Sie zum Speichern Ihrer Änderungen auf **[OK]**.

Vorgänge zum Aktualisieren und erneuten Prüfen von Speichern

Der Aktualisierungsvorgang aktualisiert die Datenspeicherlisten und die Speicherinformationen, z. B. die Datenspeicherkapazität, die im vSphere-Client angezeigt werden. Wenn Sie Änderungen an Ihrer ESXi-Host- oder SAN-Konfiguration vornehmen, müssen Sie den Vorgang „Erneut prüfen“ durchführen.

Sie können alle Adapter auf Ihrem Host erneut prüfen. Falls die von Ihnen vorgenommenen Änderungen nur einen bestimmten Adapter betreffen, prüfen Sie nur diesen Adapter neu. Wenn Ihr vSphere-Client mit einem vCenter Server-System verbunden ist, können Sie Adapter auf allen Hosts erneut prüfen, die vom vCenter Server-System verwaltet werden.

Führen Sie eine erneute Prüfung durch, wenn Sie eine der folgenden Änderungen vorgenommen haben:

- Erstellen von neuen LUNs in einem SAN.
- Ändern Sie die Pfadmaskierung auf einem Host.
- Erneutes Verbinden eines Kabels.
- Ändern eines Hosts in einem Cluster

WICHTIG Führen Sie keine erneute Prüfung durch, wenn ein Pfad nicht verfügbar ist. Wenn ein Pfad fehlschlägt, übernimmt der andere Pfad die Aufgaben dieses Pfades, und das System ist weiterhin vollständig funktionsfähig. Wenn Sie jedoch eine erneute Prüfung durchführen, wenn ein Pfad nicht verfügbar ist, entfernt der Host den Pfad aus seiner Liste der Pfade zu dem Gerät. Der Host kann den Pfad erst wieder verwenden, wenn eine erneute Prüfung durchgeführt wird, während der Pfad aktiv ist.

Erneutes Prüfen von Speicheradaptern

Wenn Sie Änderungen an Ihrer ESXi-Host- oder SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihre Speicheradapter erneut prüfen. Sie können alle Adapter auf Ihrem Host erneut prüfen. Falls die von Ihnen vorgenommenen Änderungen nur einen bestimmten Adapter betreffen, prüfen Sie nur diesen Adapter neu.

Führen Sie die folgenden Schritte aus, wenn Sie die erneute Prüfung auf einen bestimmten Host oder einen Adapter auf dem Host beschränken möchten. Wenn Sie alle von Ihrem vCenter Server-System verwalteten Adapter auf allen Hosts erneut prüfen möchten, können Sie dies tun, indem Sie mit der rechten Maustaste auf ein Datacenter, einen Cluster oder einen Ordner klicken, in dem sich die Hosts befinden, und die Option **[Erneut auf Datenspeicher prüfen]** wählen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client einen Host und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 2 Wählen Sie im Fenster Hardware die Option **[Speicheradapter]**, und klicken Sie oberhalb des Fensters Speicheradapter auf **[Erneut prüfen]**.

Sie können auch mit der rechten Maustaste auf einzelne Adapter klicken und auf **[Erneut prüfen (Rescan)]** klicken, wenn Sie nur diesen Adapter erneut prüfen möchten.

WICHTIG Auf ESXi ist es nicht möglich, einen einzelnen Speicheradapter erneut zu prüfen. Wenn Sie eine erneute Prüfung für einen einzelnen Adapter durchführen, werden alle Adapter erneut geprüft.

- 3 Wenn neue Festplatten oder LUNs erkannt werden sollen, aktivieren Sie **[Auf neue Speichergeräte prüfen]** .

Wenn neue LUNs erkannt werden, werden sie in der Geräteliste angezeigt.

- 4 Um neue Datenspeicher zu erkennen oder einen Datenspeicher nach einer Konfigurationsänderung zu aktualisieren, wählen Sie **[Auf neue VMFS-Volumes prüfen (Scan for New VMFS Volumes)]** aus.

Wenn neue Datenspeicher oder VMFS-Datenträger erkannt werden, werden diese in der Datenspeicherliste angezeigt.

Erstellen eines VMFS-Datenspeichers

VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf jedem SCSI-basierten Speichergerät einrichten, das der Host erkennt.

Voraussetzungen

Installieren und konfigurieren Sie alle Adapter, die Ihr Speicher benötigt, bevor Sie Datenspeicher erstellen. Prüfen Sie alle Adapter erneut auf neu hinzugefügte Speicher.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration (Configuration)]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]** .
- 3 Klicken Sie auf **[Datenspeicher]** und anschließend auf **[Speicher hinzufügen]** .
- 4 Markieren Sie den Speichertyp **[Festplatte/LUN]** , und klicken Sie auf **[Weiter]** .
- 5 Wählen Sie ein Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **[Weiter]** .

HINWEIS Wählen Sie das Gerät aus, für das in der Spalte „VMFS-Bezeichnung“ kein Datenspeichernamen angezeigt wird. Wenn ein Name vorhanden ist, enthält das Gerät eine Kopie des vorhandenen VMFS-Datenspeichers.

Wenn die zu formatierende Festplatte leer ist, zeigt die Seite „Aktuelles Festplattenlayout“ automatisch den gesamten, für die Konfiguration verfügbaren Festplattenspeicher an.

- 6 Wenn die Festplatte nicht leer ist, überprüfen Sie im oberen Bereich auf der Seite „Aktuelles Festplattenlayout“ das aktuelle Festplattenlayout, und wählen Sie im unteren Bereich eine Konfigurationsoption aus.

Option	Beschreibung
Alle verfügbaren Partitionen verwenden	Reserviert die gesamte Festplatte oder LUN für einen einzelnen VMFS-Datenspeicher. Bei Auswahl dieser Option werden die momentan auf diesem Gerät gespeicherten Dateisysteme und Daten dauerhaft gelöscht.
Freien Speicherplatz verwenden	Stellt einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereit.

- 7 Klicken Sie auf **[Weiter]** .
- 8 Geben Sie auf der Seite Eigenschaften einen Datenspeichernamen ein und klicken Sie auf **[Weiter]** .
- 9 Passen Sie bei Bedarf das Dateisystem und die Größen an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

- 10 Klicken Sie auf **[Weiter]** .
- 11 Überprüfen Sie auf der Seite **[Bereit zum Abschließen (Ready to Complete)]** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **[Beenden]** .

Es wird ein Datenspeicher auf dem SCSI-basierten Gerät erstellt. Wenn Sie das vCenter Server-System zum Verwalten Ihrer Hosts verwenden, wird der neu erstellte Datenspeicher automatisch zu allen Hosts hinzugefügt.

Network Attached Storage (NAS)

ESXi unterstützt NAS über das NFS-Protokoll. Das NFS-Protokoll ermöglicht die Kommunikation zwischen einem NFS-Client und einem NFS-Server.

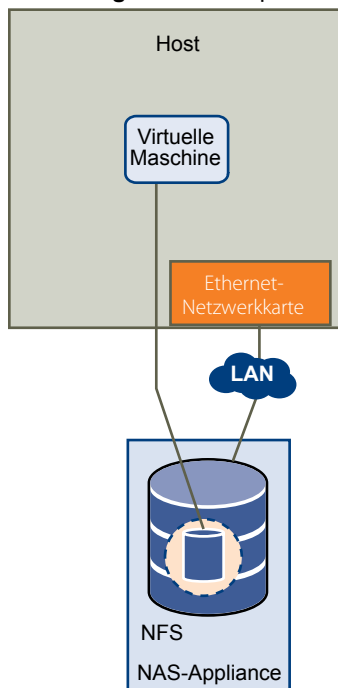
Über den in ESXi integrierten NFS-Client können Sie auf den NFS-Server zugreifen und NFS-Volumes zum Speichern verwenden. ESXi unterstützt ausschließlich NFS Version 3 über TCP.

Mit dem vSphere-Client können Sie NFS-Volumes als Datenspeicher konfigurieren. Konfigurierte NFS-Datenspeicher werden im vSphere-Client angezeigt und können genau wie VMFS-basierte Datenspeicher zur Speicherung virtueller Festplattendateien verwendet werden.

HINWEIS ESXi unterstützt nicht die Funktion für delegierte Benutzer, die den Zugriff auf NFS-Volumes mit Nicht-Root-Anmeldedaten ermöglicht.

Abbildung 8-4 zeigt eine virtuelle Maschine, die ein NFS-Volume zur Speicherung ihrer Dateien verwendet. In dieser Konfiguration stellt der Host über einen regulären Netzwerkadapter eine Verbindung zu dem NFS-Server her, auf dem die virtuellen Festplattendateien gespeichert sind.

Abbildung 8-4. NFS-Speicher



Die von Ihnen in NFS-basierten Datenspeichern erstellten virtuellen Festplatten verwenden ein Festplattenformat, das vom NFS-Server vorgegeben wird. In der Regel ist dies ein Thin-Format, das eine bedarfsgerechte Speicherplatzzuordnung erfordert. Wenn der Speicherplatz auf der virtuellen Maschine während des Schreibvorgangs auf die Festplatte nicht mehr ausreicht, erhalten Sie vom vSphere-Client eine Benachrichtigung darüber, dass zusätzlicher Speicherplatz erforderlich ist. Sie können dann aus den folgenden Optionen wählen:

- Zusätzlichen Speicherplatz auf dem Volume freimachen, damit der Schreibvorgang auf die Festplatte fortgesetzt werden kann.
- Beenden der virtuellen Maschinensitzung. Durch Beenden der Sitzung wird die virtuelle Maschine heruntergefahren.



VORSICHT Wenn Ihr Host auf die Festplattendatei einer virtuellen Maschine auf einem NFS-basierten Datenspeicher zugreift, wird im gleichen Verzeichnis, in dem sich die Festplattendatei befindet, eine .lck-XXX-Sperrdatei erstellt, um zu verhindern, dass andere Hosts auf diese virtuelle Festplattendatei zugreifen. Diese .lck-XXX-Sperrdatei darf nicht gelöscht werden, da sonst die aktive virtuelle Maschine nicht auf ihre virtuelle Festplattendatei zugreifen kann.

NFS-Datenspeicher als Repository für häufig verwendete Dateien

Neben der Verwendung von NFS-Datenspeichern als Ablageort für virtuelle Festplatten können Sie NFS auch als zentrales Repository für ISO-Images, Vorlagen für virtuelle Maschinen usw. nutzen.

Wenn Sie NFS als gemeinsam genutztes Repository verwenden möchten, erstellen Sie auf dem NFS-Server ein Verzeichnis und mounten es auf allen Hosts als Datenspeicher. Wenn Sie den Datenspeicher für ISO-Images verwenden möchten, können Sie das CD-ROM-Laufwerk der virtuellen Maschine mit einer ISO-Datei auf dem Datenspeicher verbinden und ein Gastbetriebssystem aus der ISO-Datei installieren.

Weitere Informationen zum Konfigurieren virtueller Maschinen finden Sie unter *Grundlagen der Systemverwaltung*.

HINWEIS Falls das NFS-Laufwerk, auf dem die Dateien gespeichert sind, schreibgeschützt ist, stellen Sie sicher, das das Laufwerk von dem NFS-Server als schreibgeschützte Freigabe exportiert wurde, oder konfigurieren Sie es auf dem ESXi-Host als schreibgeschützten Datenspeicher. Anderenfalls betrachtet der Host den Datenspeicher als beschreibbar und kann die Dateien möglicherweise nicht öffnen.

Erstellen eines NFS-basierten Datenspeichers

Sie können mithilfe des Assistenten zum Hinzufügen von Speicher ein NFS-Volume einbinden und dieses wie einen VMFS-Datenspeicher verwenden.

Voraussetzungen

Da NFS zum Zugriff auf die auf Remoteservern gespeicherten Daten eine Netzwerkkonnektivität benötigt, müssen Sie vor dem Konfigurieren des NFS zunächst das VMkernel-Netzwerk konfigurieren.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher]**.
- 3 Klicken Sie auf **[Datenspeicher]** und anschließend auf **[Speicher hinzufügen]**.
- 4 Wählen Sie **[Network File System (NFS)]** als Speichertyp aus, und klicken Sie auf **[Weiter]**.

- 5 Geben Sie den Server-, den Mount-Punkt-Ordner- und den Datenspeichernamen ein.

HINWEIS Wenn Sie das gleiche NFS-Volumen auf verschiedenen Hosts mounten, müssen Sie sicherstellen, dass Server- und Ordnernamen auf allen Hosts identisch sind. Wenn die Namen nicht genau übereinstimmen und Sie beispielsweise als Ordnernamen auf einem Host **share** und auf dem anderen Host **/share** verwenden, betrachten die Hosts das gleiche NFS-Volumen als zwei unterschiedliche Datenspeicher. Bei Funktionen wie vMotion kann dies zu einem Fehler führen.

- 6 (Optional) Wählen Sie **[NFS schreibgeschützt mounten]** , wenn das Laufwerk vom NFS-Server als schreibgeschützt exportiert wurde.
- 7 Klicken Sie auf **[Weiter]** .
- 8 Überprüfen Sie auf der Übersichtsseite für das Netzwerkdateisystem (NFS) die Konfigurationsoptionen, und klicken Sie auf **[Beenden]** .

Erstellen einer Diagnosepartition

Zum Ausführen des Hosts wird eine Diagnosepartition bzw. Dump-Partition benötigt, um Core-Dumps für das Debuggen und den technischen Support zu speichern. Die Diagnosepartition kann auf einer lokalen Festplatte oder einer privaten oder freigegebenen SAN-LUN erstellt werden.

Es ist jedoch nicht möglich, eine Diagnosepartition auf einer iSCSI-LUN zu speichern, auf die über einen Software-iSCSI-Initiator zugegriffen wird.

Für jeden Host ist eine Diagnosepartition mit 100 MB erforderlich. Wenn mehrere ESXi-Hosts ein gemeinsames SAN verwenden, konfigurieren Sie pro Host eine Diagnosepartition mit 100 MB.



VORSICHT Falls zwei Hosts, die eine gemeinsame Diagnosepartition verwenden, ausfallen und ein Core-Dump auf denselben Steckplatz speichern, können die Core-Dumps verloren gehen. Um Core-Dump-Daten zu erfassen, führen Sie sofort nach dem Ausfall einen Neustart eines Hosts durch und extrahieren Sie dessen Protokolldateien. Falls jedoch ein anderer Host ausfällt, bevor Sie die Diagnosedaten für den ersten Host erfasst haben, kann der zweite Host seinen Core-Dump nicht speichern.

Erstellen einer Diagnosepartition

Sie können auf dem Host eine Diagnosepartition erstellen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher]** .
- 3 Klicken Sie auf **[Datenspeicher]** und anschließend auf **[Speicher hinzufügen]** .
- 4 Wählen Sie **[Diagnose (Diagnostic)]** aus, und klicken Sie auf **[Weiter]** .

Wenn **[Diagnose]** nicht als Option angezeigt wird, ist auf dem Host bereits eine Diagnosepartition vorhanden.

Sie können die Diagnosepartition auf dem Host abfragen und durchsuchen, indem Sie den Befehl `vicfg-dumppart -l` in die vSphere-CLI eingeben.

- 5 Legen Sie den Diagnosepartitionstyp fest.

Option	Beschreibung
Privater lokaler Speicher	Erstellt die Diagnosepartition auf einer lokalen Festplatte. In dieser Partition werden ausschließlich Fehlerinformationen für Ihren Host gespeichert.
Privater SAN-Speicher	Erstellt die Diagnosepartition auf einer nicht freigegebenen SAN-LUN. In dieser Partition werden ausschließlich Fehlerinformationen für Ihren Host gespeichert.
Freigegebener SAN-Speicher	Erstellt die Diagnosepartition auf einer freigegebenen SAN-LUN. In dieser Partition, auf die mehrere Hosts zugreifen, können ggf. Fehlerinformationen für mehrere Host gespeichert werden.

- 6 Klicken Sie auf **[Weiter]** .
- 7 Wählen Sie das Gerät, das Sie für die Diagnosepartition verwenden möchten, und klicken Sie auf **[Weiter]** .
- 8 Überprüfen Sie die Konfigurationsinformationen für die Partition, und klicken Sie auf **[Beenden]** .

Speicherverwaltung

Nachdem Sie Ihre Datenspeicher erstellt haben, können Sie ihre Eigenschaften ändern, Ordner nach geschäftlichen Anforderungen zum Gruppieren von Datenspeichern anlegen oder nicht verwendete Datenspeicher löschen. Möglicherweise müssen Sie auch Multipathing für Ihren Speicher einrichten oder Datenspeicherkopien neu signieren.

Dieses Kapitel behandelt die folgenden Themen:

- [„Verwalten von Datenspeichern“](#), auf Seite 103
- [„Ändern von VMFS-Datenspeichereigenschaften“](#), auf Seite 105
- [„Verwalten von duplizierten VMFS-Datenspeichern“](#), auf Seite 108
- [„Verwenden von Multipathing mit ESXi“](#), auf Seite 110
- [„Thin-Bereitstellung“](#), auf Seite 119

Verwalten von Datenspeichern

Ein ESXi-System nutzt Datenspeicher, um alle Dateien, die seinen virtuellen Maschinen zugeordnet sind, zu speichern. Sie können nach dem Erstellen von Datenspeichern diese verwalten und dazu unterschiedliche Aufgaben ausführen.

Der Datenspeicher ist eine logische Speichereinheit, die Festplattenspeicher auf einem physischen Gerät, auf einer Festplattenpartition oder übergreifend auf mehreren physischen Geräten verwendet. Der Datenspeicher kann sich auf verschiedenen Typen physischer Geräte wie SCSI, iSCSI, Fibre-Channel-SANs oder NFS befinden.

Es gibt zwei Möglichkeiten, dem vSphere-Client Datenspeicher hinzuzufügen:

- Standardmäßige Erstellung beim ersten Booten des ESXi-Hosts. Die Software formatiert sämtliche angezeigten leeren lokalen Festplatten und Partitionen mit VMFS-Datenspeichern, damit Sie darin virtuelle Maschinen erstellen können.
- Erkennung, sobald ein Host der Bestandsliste hinzugefügt wird. Der vSphere-Client zeigt alle Datenspeicher an, die der Host erkennt.
- Erstellung auf einem verfügbaren Speichergerät mit dem Befehl **[Speicher hinzufügen]**.

Nachdem Sie die Datenspeicher erstellt haben, können Sie diese zum Speichern der Dateien virtueller Maschinen verwenden. Sie können die Datenspeicher verwalten. Dazu gehört das Umbenennen und Entfernen von Datenspeichern sowie das Erstellen von Zugriffsberechtigungen. Außerdem können Sie Datenspeicher gruppieren, um sie zu ordnen und für alle zur gleichen Zeit dieselben Berechtigungen zu erstellen.

Weitere Informationen zum Erstellen von Zugriffsberechtigungen für Datenspeicher finden Sie in der *Hilfe zum vSphere-Client*.

Umbenennen von Datenspeichern

Der Name eines vorhandenen Datenspeichers kann geändert werden.

Vorgehensweise

- 1 Zeigen Sie die Datenspeicher an.
- 2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher, den Sie umbenennen möchten, und wählen Sie **[Umbenennen]**.
- 3 Geben Sie einen neuen Datenspeichernamen ein.

Wenn Sie das vCenter Server-System zum Verwalten Ihrer Hosts verwenden, wird der neue Name auf allen Hosts angezeigt, die Zugriff auf den Datenspeicher haben.

Gruppieren von Datenspeichern

Wenn Sie Ihre Hosts über das vCenter Server-System verwalten, können Sie Datenspeicher in Ordnern gruppieren. Dies ermöglicht Ihnen das Ordnen Ihrer Datenspeicher nach Geschäftsmethoden und das gleichzeitige Zuweisen derselben Berechtigungen und Alarmer zu allen Datenspeichern in der Gruppe.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an.
- 2 Erstellen Sie die Datenspeicher bei Bedarf.
Einzelheiten dazu finden Sie in der Hilfe zum vSphere-Client.
- 3 Klicken Sie im Fenster „Bestandsliste“ auf **[Datenspeicher]**.
- 4 Wählen Sie den Datencenter aus, der die zu gruppierenden Datenspeicher enthält.
- 5 Klicken Sie im Verknüpfungsmenü auf das Symbol **[Neuer Ordner]**.
- 6 Geben Sie dem Ordner einen aussagekräftigen Namen.
- 7 Verschieben Sie die entsprechenden Datenspeicher per Drag & Drop in den Ordner.

Löschen von Datenspeichern

Sie können jede Art von VMFS-Datenspeicher löschen, einschließlich Kopien, die Sie gemountet haben, ohne sie neu zu signieren. Beim Löschen eines Datenspeichers wird er zerstört und auf keinem Host mehr angezeigt, der davor Zugriff auf ihn hatte.

Voraussetzungen

Bevor Sie einen Datenspeicher löschen, müssen Sie alle virtuellen Maschinen daraus entfernen. Stellen Sie sicher, dass kein anderer Host auf den Datenspeicher zugreift.

Vorgehensweise

- 1 Zeigen Sie die Datenspeicher an.
- 2 Klicken Sie mit der rechten Maustaste auf den zu entfernenden Datenspeicher und wählen Sie **[Löschen]**.
- 3 Bestätigen Sie, dass Sie den Datenspeicher löschen möchten.

Unmounten von Datenspeichern

Wenn Sie einen Datenspeicher unmounten, bleibt dieser intakt, er wird jedoch von den von Ihnen angegebenen Hosts nicht mehr angezeigt. Er wird weiterhin auf anderen Hosts angezeigt, auf denen er gemountet bleibt.

Sie können nur die folgenden Typen von Datenspeichern unmounten:

- NFS-Datenspeicher
- VMFS-Datenspeicherkopien, die ohne Neusignierung gemountet wurden

Vorgehensweise

- 1 Zeigen Sie die Datenspeicher an.
- 2 Klicken Sie mit der rechten Maustaste auf den entsprechenden Datenspeicher und wählen Sie **[Unmounten]**.
- 3 Wenn der Datenspeicher gemeinsam genutzt wird, geben Sie an, welche Hosts nicht mehr auf den Datenspeicher zugreifen sollen.
 - a Heben Sie ggf. die Auswahl der Hosts auf, auf denen der Datenspeicher gemountet bleiben soll. Standardmäßig sind alle Hosts ausgewählt.
 - b Klicken Sie auf **[Weiter]**.
 - c Überprüfen Sie die Liste der Hosts, von denen Sie den Datenspeicher unmounten möchten, und klicken Sie auf **[Beenden]**.
- 4 Bestätigen Sie, dass Sie den Datenspeicher unmounten möchten.

Ändern von VMFS-Datenspeichereigenschaften

Sie können einen VMFS-basierten Datenspeicher bearbeiten, nachdem Sie ihn erstellt haben. Sie können ihn beispielsweise vergrößern, wenn Sie mehr Speicherplatz benötigen. Wenn Sie über VMFS-2-Datenspeicher verfügen, können Sie sie in das VMFS-3-Format aktualisieren.

Datenspeicher im VMFS-Format werden auf SCSI-basierten Speichergeräten bereitgestellt.

Sie können keinen VMFS-Datenspeicher neu formatieren, den ein Remotehost verwendet. Falls Sie es dennoch versuchen, wird eine Warnmeldung mit dem Namen des verwendeten Datenspeichers und des Hosts, der ihn verwendet, eingeblendet. Diese Warnung wird auch im VMkernel und in **[vmkwarning]**-Protokolldateien angezeigt.

Je nachdem, ob Ihr vSphere-Client mit einem vCenter Server-System oder direkt mit einem Host verbunden ist, gibt es verschiedene Möglichkeiten, auf das Dialogfeld „Datenspeichereigenschaften“ zuzugreifen.

- Nur vCenter Server. Um auf das Dialogfeld „Datenspeichereigenschaften“ zuzugreifen, wählen Sie den Datenspeicher in der Bestandsliste aus, klicken Sie auf die Registerkarte **[Konfiguration]** und klicken Sie anschließend auf **[Eigenschaften]**.
- vCenter Server und ESX/ESXi-Host. Um auf das Dialogfeld „Datenspeichereigenschaften“ zuzugreifen, wählen Sie einen Host in der Bestandsliste aus, klicken Sie auf die Registerkarte **[Konfiguration]** und klicken Sie anschließend auf **[Speicher]**. Wählen Sie in der Ansicht „Datenspeicher“ den zu ändernden Datenspeicher aus und klicken Sie auf **[Eigenschaften]**.

Erweitern von VMFS-Datenspeichern

Wenn Sie neue virtuelle Maschinen auf einem Datenspeicher erstellen müssen oder die auf dem Datenspeicher vorhandenen virtuellen Maschinen mehr Speicherplatz benötigen, können Sie die Kapazität des VMFS-Datenspeichers dynamisch erhöhen.

Verwenden Sie eine der folgenden Methoden:

- Fügen Sie eine neue Erweiterung hinzu. Eine Erweiterung ist eine Partition auf einer LUN. Zu jedem vorhandenen VMFS-Datenspeicher können Sie eine neue Erweiterung hinzufügen. Der Datenspeicher kann bis zu 32 Erweiterungen umfassen.

HINWEIS Einem Datenspeicher auf einer SAN-LUN kann keine lokale Erweiterung hinzugefügt werden.

- Vergrößern Sie eine Erweiterung in einem vorhandenen VMFS-Datenspeicher. Nur Erweiterungen mit nachfolgendem freiem Speicherplatz sind erweiterbar. Deshalb können Sie die vorhandene Erweiterung auch vergrößern, sodass sie den verfügbaren angrenzenden Speicherplatz belegt, anstatt eine neue Erweiterung hinzuzufügen.

HINWEIS Falls eingeschaltete virtuelle Maschinen auf einen gemeinsam genutzten Datenspeicher zugreifen und dieser vollständig beschrieben ist, können Sie die Kapazität des Datenspeichers nur von dem Host aus erhöhen, mit dem die eingeschalteten virtuellen Maschinen registriert sind.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Speicher]**.
- 3 Wählen Sie in der Ansicht „Datenspeicher“ den zu erhöhenden Datenspeicher aus und klicken Sie auf **[Eigenschaften]**.
- 4 Klicken Sie auf **[Erhöhen]**.
- 5 Wählen Sie ein Gerät aus der Liste der Speichergeräte aus und klicken Sie auf **[Weiter]**.
 - Wenn Sie eine neue Erweiterung hinzufügen möchten, wählen Sie das Gerät dessen Spalte „Erweiterbar“ mit „Nein“ beschriftet ist.
 - Wenn Sie eine vorhandene Erweiterung erweitern möchten, wählen Sie das Gerät dessen Spalte „Erweiterbar“ mit „Ja“ beschriftet ist.
- 6 Wählen Sie eine Konfigurationsoption im unteren Fenster aus.

Die angezeigten Optionen variieren abhängig von dem aktuellen Festplattenlayout und Ihrer vorherigen Auswahl.

Option	Beschreibung
Freien Speicherplatz nutzen, um eine neue Erweiterung hinzuzufügen	Fügt den freien Speicherplatz auf dieser Festplatte als neues Datenspeicher-Erweiterungsgerät hinzu.
Freien Speicherplatz nutzen, um eine vorhandene Erweiterung zu erweitern	Vergrößert eine vorhandene Erweiterung auf die erforderliche Kapazität.

Option	Beschreibung
Freien Speicherplatz verwenden	Stellt eine Erweiterung im verbleibenden freien Speicherplatz auf der Festplatte bereit. Diese Option ist nur verfügbar, wenn eine Erweiterung hinzugefügt wird.
Alle verfügbaren Partitionen verwenden	Weist einem einzelnen Datenspeicher-Erweiterungsgerät die gesamte Festplatte zu. Diese Option ist nur verfügbar, wenn eine Erweiterung hinzugefügt wird und die zu formatierende Festplatte nicht leer ist. Die Festplatte wird neu formatiert und dabei werden alle darauf enthaltenen Datenspeicher und Daten gelöscht.

- 7 Geben Sie die Kapazität der Erweiterung an.
Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.
- 8 Klicken Sie auf **[Weiter]**.
- 9 Überprüfen Sie das vorgeschlagene Layout und die neue Konfiguration des Datenspeichers, und klicken Sie anschließend auf **[Beenden]**.

Weiter

Nachdem Sie eine Erweiterung in einem gemeinsam genutzten VMFS-Datenspeicher vergrößert haben, aktualisieren Sie den Datenspeicher auf jedem Host, der auf diesen Datenspeicher zugreifen kann, damit der vSphere-Client für alle Hosts die richtige Datenspeicherkapazität anzeigen kann.

Aktualisieren von Datenspeichern

ESXi umfasst VMFS Version 3 (VMFS-3). Wenn der Datenspeicher mit VMFS-2 formatiert wurde, können Sie die auf VMFS-2 gespeicherten Dateien zwar lesen, aber nicht schreiben. Um vollständigen Zugriff auf die Dateien zu gewährleisten, müssen Sie VMFS-2 auf VMFS-3 aktualisieren.

Wenn Sie ein Upgrade von VMFS-2 auf VMFS-3 durchführen, stellt der Mechanismus zur Dateisperrung von ESXi sicher, dass während der Konvertierung weder ein Remotehost noch lokale Prozesse auf den VMFS-Datenspeicher zugreifen. Ihr Host behält alle Dateien im Datenspeicher bei.

Vor der Aktualisierung werden als Vorsichtsmaßnahme folgende Schritte empfohlen:

- Akzeptieren oder verwerfen Sie alle Änderungen an virtuellen Festplatten auf dem VMFS 2-Volume, für das ein Upgrade durchgeführt werden soll.
- Sichern Sie das VMFS-2-Volume.
- Stellen Sie sicher, dass das VMFS-2-Volume nicht von aktiven virtuellen Maschinen verwendet wird.
- Stellen Sie sicher, dass kein anderer ESXi-Host auf das VMFS-2-Volume zugreift.

Der Konvertierungsvorgang von VMFS-2 in VMFS-3 ist nicht umkehrbar. Nach der Konvertierung des VMFS-basierten Datenspeichers in VMFS-3 ist eine Rückkonvertierung in VMFS-2 nicht mehr möglich.

Beim Upgrade des Dateisystems VMFS-2 darf die Dateiblockgröße 8 MB nicht übersteigen.

Vorgehensweise

- 1 Melden Sie sich beim vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Speicher]**.
- 3 Wählen Sie den Datenspeicher, der das VMFS-2-Format verwendet.
- 4 Klicken Sie auf **[Auf VMFS-3 aktualisieren]**.
- 5 Führen Sie auf allen Hosts, auf denen der Datenspeicher angezeigt wird, eine erneute Prüfung durch.

Verwalten von duplizierten VMFS-Datenspeichern

Wenn eine LUN eine Kopie eines VMFS-Datenspeichers enthält, können Sie den Datenspeicher mit der vorhandenen Signatur mounten oder eine neue Signatur zuweisen.

Jeder in einer LUN erstellte VMFS-Datenspeicher besitzt eine eindeutige UUID, die im Superblock des Dateisystems gespeichert ist. Wenn die LUN repliziert oder ein Snapshot von ihr erstellt wird, ist die dabei entstehende LUN-Kopie Byte für Byte mit der ursprünglichen LUN identisch. Wenn die ursprüngliche LUN einen VMFS-Datenspeicher mit der UUID X enthält, scheint daher die LUN-Kopie einen identischen VMFS-Datenspeicher bzw. eine VMFS-Datenspeicherkopie mit genau derselben UUID X zu enthalten.

ESXi kann ermitteln, ob eine LUN die VMFS-Datenspeicherkopie enthält, und entweder die Datenspeicherkopie mit ihrer ursprünglichen UUID mounten oder die UUID ändern, wodurch der Datenspeicher neu signiert wird.

Mounten von VMFS-Datenspeichern mit vorhandenen Signaturen

In bestimmten Fällen ist das Neusignieren einer VMFS-Datenspeicherkopie möglicherweise nicht erforderlich. Sie können eine VMFS-Datenspeicherkopie mounten, ohne ihre Signatur zu ändern.

Sie können beispielsweise synchronisierte Kopien von virtuellen Maschinen als Teil eines Notfallplans auf einer sekundären Site unterhalten und bei einem Notfall an der primären Site die Datenspeicherkopie auf den virtuellen Maschinen der sekundären Site einschalten.

WICHTIG Sie können einen VMFS-Datenspeicher nur mounten, wenn er nicht mit einem bereits gemounteten VMFS-Datenspeicher mit derselben UUID kollidiert.

Wenn Sie den VMFS-Datenspeicher mounten, lässt ESXi Lese- und Schreibvorgänge in den Datenspeicher zu, der sich auf der LUN-Kopie befindet. Die LUN-Kopie darf nicht schreibgeschützt sein. Die Datenspeicher-Mounts sind über Systemneustarts hinweg dauerhaft und gültig.

Da ESXi das Neusignieren des gemounteten Datenspeichers nicht zulässt, müssen Sie den Datenspeicher vor dem Neusignieren unmounten.

Mounten eines VMFS-Datenspeichers mit einer vorhandenen Signatur

Wenn Sie eine Kopie eines VMFS-Datenspeichers nicht neu signieren müssen, können Sie sie mounten, ohne ihre Signatur zu ändern.

Voraussetzungen

Führen Sie vor dem Mounten eines VMFS-Datenspeichers eine erneute Speicherprüfung auf Ihrem Host durch, sodass er seine Ansicht der ihm präsentierten LUNs aktualisiert.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]**.
- 3 Klicken Sie auf **[Speicher hinzufügen]**.
- 4 Markieren Sie den Speichertyp **[Festplatte/LUN (Disk/LUN)]**, und klicken Sie auf **[Weiter]**.
- 5 Wählen Sie in der Liste der LUNs die LUN aus, die einen Datenspeichernamen in der Spalte „VMFS-Bezeichnung“ enthält, und klicken Sie auf **[Weiter]**.

Der in der Spalte „VMFS-Bezeichnung“ vorhandene Name gibt an, dass die LUN eine Kopie ist, die eine Kopie eines vorhandenen VMFS-Datenspeichers enthält.

- 6 Wählen Sie unter „Optionen für das Mounten“ die Option **[Vorhandene Signatur beibehalten]** aus.
- 7 Überprüfen Sie auf der Seite **[Bereit zum Abschließen (Ready to Complete)]** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **[Beenden]**.

Weiter

Wenn Sie den gemounteten Datenspeicher zu einem späteren Zeitpunkt erneut signieren möchten, müssen Sie ihn zunächst unmounten.

Neusignieren von VMFS-Kopien

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten. Beim Neusignieren einer VMFS-Kopie weist ESXi der Kopie eine neue UUID und eine neue Bezeichnung zu und mountet die Kopie als einen vom Original unabhängigen Datenspeicher.

Die neue Bezeichnung, die dem Datenspeicher zugewiesen wird, besitzt das Standardformat `snap-<Snap-ID>-<Alte_Bezeichnung>`, wobei `<Snap-ID>` für eine Ganzzahl und `<Alte_Bezeichnung>` für die Bezeichnung des ursprünglichen Datenspeichers steht.

Beachten Sie bei der Datenspeicher-Neusignierung Folgendes:

- Die Datenspeicher-Neusignierung kann nicht rückgängig gemacht werden.
- Die LUN-Kopie, die den VMFS-Datenspeicher enthält, der neu signiert wird, wird nicht länger als LUN-Kopie behandelt.
- Ein übergreifender Datenspeicher kann nur neu signiert werden, wenn all seine Erweiterungen online sind.
- Der Neusignierungsprozess ist absturz- und fehlertolerant. Wenn der Prozess unterbrochen wird, können Sie ihn später fortsetzen.
- Sie können den neuen VMFS-Datenspeicher mounten, ohne dass das Risiko besteht, dass seine UUID mit UUIDs anderer Datenspeicher, wie z. B. einem über- oder untergeordneten Datenspeicher in einer Hierarchie von LUN-Snapshots, kollidiert.

Neusignieren einer VMFS-Datenspeicherkopie

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten.

Voraussetzungen

Wenn Sie eine gemountete Datenspeicherkopie neu signieren möchten, müssen Sie sie zunächst unmounten.

Führen Sie vor dem Neusignieren eines VMFS-Datenspeichers eine erneute Speicherprüfung auf Ihrem Host durch, sodass der Host seine Ansicht der ihm präsentierten LUNs aktualisiert und vorhandene LUN-Kopien erkennt.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]**.
- 3 Klicken Sie auf **[Speicher hinzufügen]**.
- 4 Markieren Sie den Speichertyp **[Festplatte/LUN (Disk/LUN)]**, und klicken Sie auf **[Weiter]**.

- 5 Wählen Sie in der Liste der LUNs die LUN aus, die einen Datenspeichernamen in der Spalte „VMFS-Bezeichnung“ enthält, und klicken Sie auf **[Weiter]** .

Der in der Spalte „VMFS-Bezeichnung“ vorhandene Name gibt an, dass die LUN eine Kopie ist, die eine Kopie eines vorhandenen VMFS-Datenspeichers enthält.

- 6 Wählen Sie unter „Optionen für das Mounten“ die Option **[Neue Signatur zuweisen]** aus und klicken Sie auf **[Weiter]** .
- 7 Überprüfen Sie auf der Seite **[Bereit zum Abschließen (Ready to Complete)]** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **[Beenden]** .

Weiter

Nach der erneuten Signierung sind möglicherweise die folgenden Schritte erforderlich:

- Wenn die neu signierten Datenspeicher virtuelle Maschinen enthalten, aktualisieren Sie die Referenzen auf den VMFS-Datenspeicher in den Dateien der virtuellen Maschine, darunter die Dateien mit den Erweiterungen `.vmx`, `.vmdk`, `.vmsd` und `.vmsn`.
- Registrieren Sie virtuelle Maschinen mit vCenter Server, wenn Sie sie einschalten möchten.

Verwenden von Multipathing mit ESXi

ESXi unterstützt Multipathing, um eine dauerhafte Verbindung zwischen einem ESXi-Host und seinem Speicher zu erhalten. Multipathing ist eine Technik, mit deren Hilfe Sie mehrere physische Pfade zur Übertragung von Daten zwischen dem ESXi-Host und dem externen Speichergerät verwenden können.

Beim Ausfall eines Elements im SAN-Netzwerk, z. B. eines HBAs, Switches oder Kabels, kann ESXi ein Failover auf einen anderen physischen Pfad durchführen. Neben dem Pfad-Failover bietet Multipathing Lastausgleich, wodurch E/A-Lasten zwischen mehreren Pfaden verteilt und potenzielle Engpässe reduziert oder vermieden werden.

Verwalten mehrerer Pfade

Zur Verwaltung von Speicher-Multipathing verwendet ESXi eine spezielle VMkernel-Schicht: die Architektur des im laufenden Betrieb austauschbaren Speichers (Pluggable Storage Architecture, PSA). PSA stellt ein offenes, modulares Framework dar, das die gleichzeitige Ausführung von mehreren Multipathing-Plug-Ins (MPPs) koordiniert.

Das von ESXi standardmäßig bereitgestellte VMkernel-Multipathing-Plug-In ist das NMP (VMware Native Multipathing Plugin). Das NMP ist ein erweiterbares Modul zur Verwaltung von Sub-Plug-Ins. Das NMP-Modul verwaltet zwei Sub-Plug-In-Typen: die Speicher-Array-Typ-Plug-Ins (SATPs) und die Pfadauswahl-Plug-Ins (PSPs). SATPs und PSPs können von VMware bereitgestellt und integriert oder durch einen Drittanbieter zur Verfügung gestellt werden.

Wenn mehr Multipathing-Funktionen erforderlich sind, kann ein Drittanbieter MPP zusätzlich oder als Ersatz für das Standard-NMP bereitstellen.

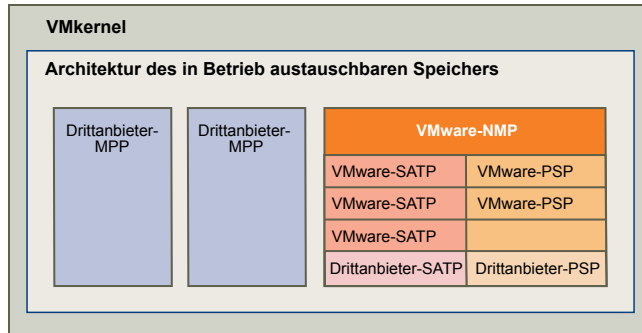
Bei der Koordination vom VMware NMP und ggf. installierter Drittanbieter-MPPs führt PSA die folgenden Aufgaben aus:

- Laden und Entladen von Multipathing-Plug-Ins.
- Verbergen von Angaben zur virtuellen Maschine vor einem bestimmten Plug-In.
- Weiterleiten von E/A-Anforderungen für ein bestimmtes logisches Gerät an das MPP, das das Gerät verwaltet.
- Verarbeiten der E/A-Warteschlangen für logische Geräte.
- Implementieren der gemeinsamen Nutzung der Bandbreite für logische Geräte durch virtuelle Maschinen.

- Verarbeiten der E/A-Warteschlangen für physische Speicher-HBAs.
- Verarbeiten der Erkennung und Entfernung physischer Pfade.
- Bereitstellen von E/A-Statistiken für logische Geräte und physische Pfade.

Wie unter [Abbildung 9-1](#) beschrieben, kann mehrere Drittanbieter-MPPs parallel zum VMware NMP ausgeführt werden. Die Drittanbieter-MPPs ersetzen das Verhalten des NMP und übernehmen die gesamte Steuerung des Pfad-Failovers und der Lastenausgleichs-Vorgänge für bestimmte angegebene Speichergeräte.

Abbildung 9-1. Architektur des im Betrieb austauschbaren Speichers



Mit den Multipathing-Modulen werden die folgenden Verfahren ausgeführt:

- Verwalten des Beanspruchens und Freigebens physischer Pfade.
- Verwalten der Erstellung, Registrierung und der Aufhebung der Registrierung von logischen Geräten.
- Zuordnen physischer Pfade zu logischen Geräten.
- Verarbeiten von E/A-Anforderungen an logische Geräte:
 - Auswahl eines optimalen physischen Pfades für die Anforderung.
 - Je nach Speichergerät Ausführen bestimmter Aktionen, die zur Verarbeitung von Pfadfehlern und Wiederholungsversuchen für E/A-Befehle notwendig sind.
- Unterstützen von Verwaltungsaufgaben, wie z. B. dem Abbrechen oder Zurücksetzen von logischen Geräten.

VMware Multipathing-Modul

Standardmäßig bietet ESXi ein erweiterbares Multipathing-Modul, das als NMP (Native Multipathing Plugin) bezeichnet wird.

Das VMware NMP unterstützt normalerweise alle in der VMware Speicher-HCL aufgeführten Speicher-Arrays und bietet einen auf dem Array-Typ basierenden Pfadauswahl-Algorithmus. Das NMP weist einem bestimmten Speichergerät oder einer bestimmten LUN mehrere physische Pfade zu. Die jeweiligen Details der Verarbeitung eines Pfad-Failovers für ein bestimmtes Speicher-Array werden an ein Speicher-Array-Typ-Plug-In (SATP) delegiert. Die jeweiligen Details zum Festlegen des physischen Pfads, der zum Ausgeben einer E/A-Anforderung an ein Speichergerät verwendet wird, werden von einem Pfadauswahl-Plug-In (Path Selection Plugin, PSP) verarbeitet. SATPs und PSPs sind Sub-Plug-Ins innerhalb des NMP-Moduls.

VMware SATPs

SATPs (Storage Array Type Plugins) werden in Verbindung mit dem VMware NMP ausgeführt und übernehmen arrayspezifische Vorgänge.

ESXi bietet ein SATP für jeden von VMware unterstützten Array-Typ. Diese SATPs beinhalten ein Aktiv/Aktiv-SATP und ein Aktiv/Passiv-SATP für nicht angegebene Speicher-Arrays und das lokale SATP für direkt angeschlossenen Speicher. Jedes SATP enthält spezielle Merkmale einer bestimmten Klasse von Speicher-Arrays und kann die arrayspezifischen Vorgänge ausführen, die zum Ermitteln des Pfadstatus und zum Aktivieren eines inaktiven Pfads erforderlich sind. Daher kann das NMP-Modul mit mehreren Speicher-Arrays arbeiten, ohne die Angaben zu den Speichergeräten zu kennen.

Nachdem das NMP ermittelt, welches SATP für ein bestimmtes Speichergerät aufgerufen werden muss, und das SATP physischen Pfaden für dieses Speichergerät zuweist, implementiert das SATP die folgenden Aufgaben:

- Überwachung des Status der einzelnen physischen Pfade.
- Melden von Änderungen des Status der einzelnen physischen Pfade.
- Ausführen von für das Speicher-Failover erforderlichen arrayspezifischen Aktionen. Beispielsweise kann es für Aktiv/Passiv-Geräte passive Pfade aktivieren.

VMware PSPs

Pfadauswahl-Plug-Ins (PSPs) werden in Verbindung mit dem VMware NMP ausgeführt und sind verantwortlich für die Auswahl eines physischen Pfads für E/A-Anforderungen.

Das VMware NMP weist auf der Grundlage des SATP, das den physischen Pfaden für das jeweilige Gerät zugeordnet ist, ein Standard-PSP für jedes logische Gerät zu. Sie können das Standard-PSP außer Kraft setzen.

Standardmäßig unterstützt VMware NMP die folgenden PSPs:

Zuletzt verwendet (MRU, Most Recently Used) Wählt den Pfad aus, den der ESXi-Host zuletzt verwendet hat, um auf ein bestimmtes Gerät zuzugreifen. Wenn dieser Pfad nicht verfügbar ist, wechselt der Host zu einem anderen Pfad und verwendet weiterhin den neuen Pfad, wenn dieser verfügbar ist.

Fest Verwendet den festgelegten bevorzugten Pfad, wenn dieser konfiguriert wurde. Anderenfalls wird der erste funktionierende Pfad verwendet, der beim Systemstart ermittelt wird. Wenn der Host den bevorzugten Pfad nicht verwenden kann, trifft er eine zufällige Auswahl für einen alternativen verfügbaren Pfad. Sobald der bevorzugte Pfad verfügbar ist, kehrt der Host zu diesem zurück.

HINWEIS Bei Aktiv/Passiv-Arrays mit einer auf **[Fest]** gesetzten Pfadrichtlinie, kann Pfad-Thrashing ein Problem darstellen.

Round Robin (RR) Verwendet einen Pfadauswahlalgorithmus, bei dem eine Rotation unter Berücksichtigung aller verfügbaren Pfade stattfindet und ein pfadübergreifender Lastenausgleich ermöglicht wird.

NMP-E/A-Ablauf von VMware

Wenn eine virtuelle Maschine eine E/A-Anforderung an ein vom NMP verwaltetes Speichergerät ausgibt, läuft der folgende Prozess ab.

- 1 Das NMP ruft das PSP auf, das diesem Speichergerät zugewiesen ist.
- 2 Das PSP wählt einen entsprechenden physischen Pfad für die zu sendende E/A.
- 3 Wenn der E/A-Vorgang erfolgreich ist, meldet das NMP dessen Abschluss.

- 4 Wenn der E/A-Vorgang einen Fehler meldet, ruft das NMP ein entsprechendes SATP auf.
- 5 Das SATP interpretiert die E/A-Fehlercodes und aktiviert ggf. inaktive Pfade.
- 6 Das PSP wird aufgerufen, um einen neuen Pfad für das Senden der E/A zu wählen.

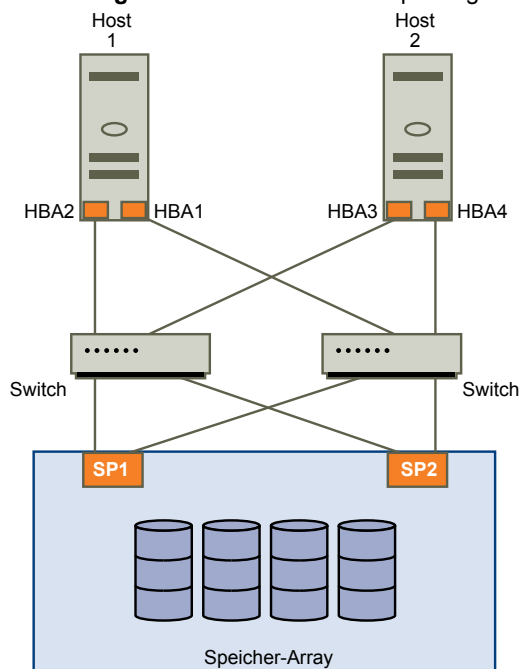
Multipathing mit lokalem Speicher und Fibre-Channel-SANs

Bei der einfachen lokalen Speichertopologie für das Multipathing können Sie mit einem ESXi-Host arbeiten, der über zwei HBAs verfügt. Der ESXi-Host wird über zwei Kabel an das lokale Speichersystem mit zwei Ports angeschlossen. Diese Konfiguration stellt die Fehlertoleranz sicher, sollte eines der Verbindungselemente zwischen dem ESXi-Host und dem lokalen Speichersystem ausfallen.

Um Pfadwechseln mit Fibre-Channel-SAN zu unterstützen, verfügt der ESXi-Host in der Regel über mindestens zwei HBAs, über die das Speicher-Array unter Verwendung eines oder mehrerer Switches erreicht werden kann. Alternativ kann die Konfiguration auch einen HBA und zwei Speicherprozessoren aufweisen, sodass der HBA einen anderen Pfad verwenden kann, um auf das Festplatten-Array zuzugreifen.

Abbildung 9-2 zeigt, dass jeder Server über mehrere Pfade mit dem Speichergerät verbunden ist. Wenn zum Beispiel HBA1 oder die Verbindung zwischen HBA1 und dem Switch ausfällt, übernimmt HBA2 und stellt eine Verbindung zwischen dem Server und dem Switch zur Verfügung. Der Prozess, in dem ein HBA für einen anderen HBA einspringt, wird als HBA-Failover bezeichnet.

Abbildung 9-2. Fibre-Channel-Multipathing



Analog dazu übernimmt SP2 bei einem Ausfall von SP1 oder der Verbindung zwischen SP1 und dem Switch und stellt eine Verbindung zwischen dem Switch und dem Speichergerät zur Verfügung. Dieser Vorgang wird SP-Failover genannt. ESXi unterstützt über die Multipathing-Funktion HBA- und SP-Failover.

Multipathing mit iSCSI-SAN

Mit iSCSI-Speicher können Sie die Multipathing-Unterstützung durch das IP-Netzwerk nutzen. Außerdem unterstützt ESXi Host-basierendes Multipathing für Hardware- und Software-iSCSI-Initiatoren.

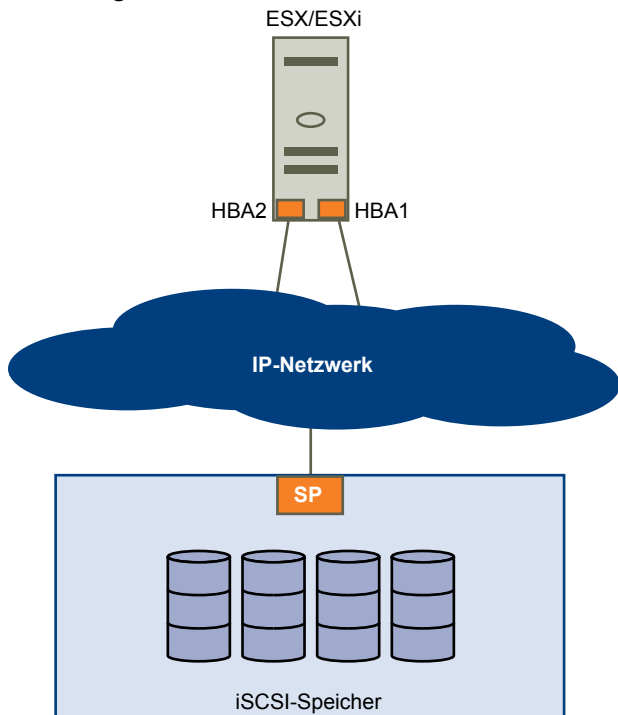
ESXi kann die im IP-Netzwerk integrierte Multipathing-Unterstützung nutzen, die dem Netzwerk das Routen ermöglicht. Über die dynamische Erkennung erhalten iSCSI-Initiatoren eine Liste mit Zieladressen, welche die Initiatoren als mehrere Pfade zu iSCSI-LUNs zu Failover-Zwecken nutzen können.

ESXi unterstützt auch Host-basierendes Multipathing.

Mit Hardware-iSCSI kann der Host über zwei oder mehr Hardware-iSCSI-Adapter verfügen und diese als unterschiedliche Pfade zum Speichersystem verwenden.

Wie [Abbildung 9-3](#) zeigt, hat der Host zwei Hardware-iSCSI-Adapter, HBA1 und HBA2, die zwei physische Pfade zum Speichersystem zur Verfügung stellen. Multipathing-Plug-Ins auf dem Host, ob VMkernel-NMP oder Drittanbieter-MPPs, haben standardmäßig Zugriff auf die Pfade und können den Status der einzelnen physischen Pfade überwachen. Wenn beispielsweise HBA1 oder die Verknüpfung zwischen HBA1 und dem Netzwerk fehlschlägt, können Multipathing-Plug-Ins den Pfad auf HBA2 wechseln.

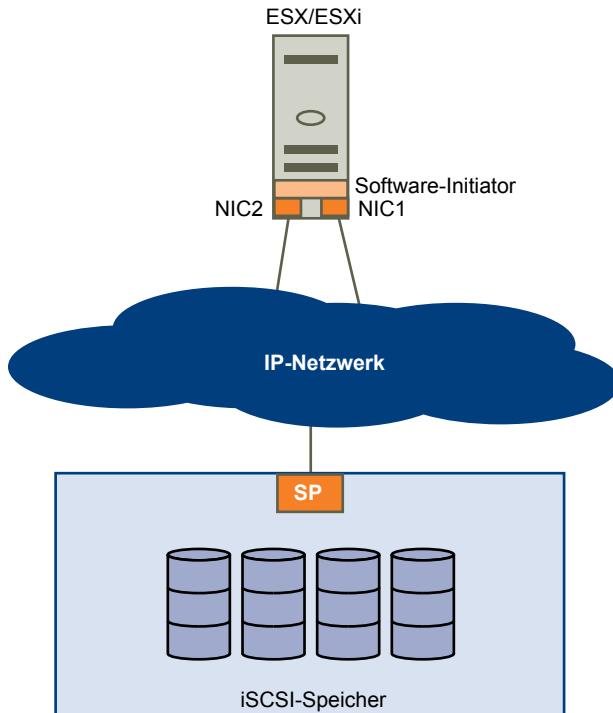
Abbildung 9-3. Hardware-iSCSI und Failover



Wie [Abbildung 9-4](#) zeigt, können Sie mit Software-iSCSI mehrere Netzwerkkarten verwenden, die Failover- und Lastausgleichsfunktionen für iSCSI-Verbindungen zwischen dem Host und Speichersystemen bieten.

Da Multipathing-Plug-Ins bei diesem Setup keinen direkten Zugriff auf die physischen Netzwerkkarten auf Ihrem Host haben, müssen Sie dazu zuerst jede einzelne physische Netzwerkkarte mit einem separaten VMkernel-Port verbinden. Danach verbinden Sie mithilfe einer Port-Bindungstechnik alle VMkernel-Ports mit dem Software-iSCSI-Initiator. Somit erhält jeder VMkernel-Port, der mit einer separaten NIC verbunden ist, einen anderen Pfad, der vom iSCSI-Speicherstapel und dessen speicherfähigen Multipathing-Plug-Ins verwendet werden kann.

Weitere Informationen zu dieser Konfiguration finden Sie im *iSCSI-SAN-Konfigurationshandbuch*.

Abbildung 9-4. Software-iSCSI und Failover

Prüfen und Beanspruchen von Pfaden

Wenn Sie Ihren ESXi-Host starten oder Ihren Speicheradapter erneut prüfen, ermittelt der Host alle physischen Pfade zu Speichergeräten, die für den Host verfügbar sind. Auf Basis von Beanspruchungsregeln, die in der Datei `/etc/vmware/esx.conf` definiert sind, ermittelt der Host, welches Multipathing-Plug-In (MPP) die Pfade zu einem bestimmten Gerät beanspruchen und die Verwaltung der Multipathing-Unterstützung für das Gerät übernehmen soll.

Standardmäßig führt der Host alle 5 Minuten eine periodische Pfadauswertung durch, wodurch alle freien Pfade durch das entsprechende MPP beansprucht werden.

Die Beanspruchungsregeln sind nummeriert. Für jeden physischen Pfad arbeitet der Host die Beanspruchungsregeln ab und beginnt dabei mit der niedrigsten Nummer. Die Attribute des physischen Pfads werden mit der Pfadspezifikation in der Beanspruchungsregel verglichen. Wenn eine Übereinstimmung gefunden wird, weist der Host das in der Beanspruchungsregel angegebene MPP zum Verwalten des physischen Pfads zu. Dies wird so lange fortgesetzt, bis alle physischen Pfade durch entsprechende MPPs beansprucht werden, bei denen es sich um Drittanbieter-Multipathing-Plug-Ins oder das systemeigene Multipathing-Plug-In (Native Multipathing Plugin, NMP) handeln kann.

Für die durch das NMP-Modul verwalteten Pfade wird ein zweiter Satz von Beanspruchungsregeln angewendet. Diese Regeln bestimmen, welches SATP zum Verwalten der Pfade aus einem bestimmten Array-Typ verwendet werden sollte, und welches PSP für die einzelnen Speichergeräte verwendet werden soll. Beispielsweise ist für ein Speichergerät aus der EMC CLARiiON CX-Speicherfamilie das Standard-SATP „VMW_SATP_CX“ und das Standard-PSP „Zuletzt verwendet“.

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen. Bei Bedarf können Sie das Standard-PSP von VMware mithilfe des vSphere-Clients ändern. Zum Ändern des Standard-SATPs müssen Sie die Beanspruchungsregeln unter Verwendung der vSphere-CLI ändern.

Detaillierte Beschreibungen der zur Verwaltung von PSAs verfügbaren Befehle finden Sie im Handbuch *VMware vSphere-Befehlszeilenschnittstellen-Installation und -Referenz*.

Anzeigen der Pfadinformationen

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der ESXi-Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen. Sie können aus den Ansichten „Datenspeicher“ und „Geräte“ auf die Pfadinformationen zugreifen. Für Datenspeicher überprüfen Sie die Pfade, die eine Verbindung zu dem Gerät herstellen, auf dem der Datenspeicher bereitgestellt wird.

Zu den Pfadinformationen gehören das zum Verwalten des Geräts zugewiesene SATP, die Pfadauswahl-Richtlinie (PSP) und eine Liste von Pfaden mit ihren physischen Merkmalen, z. B. einem Adapter und einem Ziel, die von den einzelnen Pfaden verwendet werden, und dem Status der einzelnen Pfade. Es können die folgenden Informationen zum Pfadstatus angezeigt werden:

Aktiv Pfade, die zum Senden von E/A an eine LUN verfügbar sind. Ein einzelner oder mehrere Arbeitspfade, die derzeit zur Übertragung von Daten verwendet werden, sind als „Aktiv (E/A)“ markiert.

HINWEIS Für Hosts, die ESXi 3.5 oder früher ausführen, bezeichnet der Begriff „Aktiv“ den einzigen Pfad, den der Host zum Senden von E/A an eine LUN verwendet.

Standby Der Pfad ist verfügbar und kann für E/A verwendet werden, wenn aktive Pfade fehlschlagen.

Deaktiviert Der Pfad wurde deaktiviert, sodass keine Daten übertragen werden können.

Beschädigt Die Software kann über diesen Pfad keine Verbindung mit der Festplatte herstellen.

Wenn Sie die Pfadrichtlinie **[Fest]** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Sternchen (*) in der bevorzugten Spalte gekennzeichnet.

Anzeigen von Datenspeicherpfaden

Verwenden Sie den vSphere-Client, um die Pfade zu überprüfen, die eine Verbindung zu Speichergeräten herstellen, auf denen die Datenspeicher bereitgestellt werden.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]**.
- 3 Klicken Sie unter „Ansicht“ auf **[Datenspeicher]**.
- 4 Wählen Sie in der Liste der konfigurierten Datenspeicher den Datenspeicher aus, dessen Pfade Sie anzeigen oder konfigurieren möchten.
Im Fenster „Details“ wird die Gesamtanzahl an Pfaden angezeigt, die zum Zugriff auf das Gerät verwendet werden, sowie Informationen dazu, ob Pfade beschädigt oder deaktiviert sind.
- 5 Klicken Sie auf **[Eigenschaften] > [Pfade verwalten]**, um das Dialogfeld „Pfade verwalten“ zu öffnen.
Sie können das Dialogfeld **[Pfade verwalten]** verwenden, um die Pfade zu aktivieren oder zu deaktivieren, die Multipathing-Richtlinie zu konfigurieren oder den bevorzugten Pfad anzugeben.

Anzeigen von Speichergerätepfaden

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]**.
- 3 Klicken Sie unter „Ansicht“ auf **[Geräte]**.
- 4 Klicken Sie auf **[Pfade verwalten (Manage Paths)]**, um das Dialogfeld **[Pfade verwalten (Manage Paths)]** zu öffnen.

Festlegen einer Pfadauswahl-Richtlinie

Der ESXi-Host legt für jedes Speichergerät die Pfadauswahl-Richtlinie auf Basis der in der Datei `/etc/vmware/esx.conf` definierten Beanspruchungsregeln fest.

Standardmäßig unterstützt VMware die folgenden Pfadauswahlrichtlinien: Wenn Sie die PSP eines Drittanbieters auf Ihrem Host installiert haben, wird die zugehörige Richtlinie ebenfalls in der Liste aufgeführt.

Fest (VMware)	Der Host verwendet immer den bevorzugten Pfad zur Festplatte, wenn dieser Pfad verfügbar ist. Wenn nicht über den bevorzugten Pfad auf die Festplatte zugegriffen werden kann, versucht der Host, über die anderen Pfade auf die Festplatte zuzugreifen. Die Standardrichtlinie für Aktiv/Aktiv-Speichergeräte ist fest.
Zuletzt verwendet (VMware)	Der Host verwendet so lange einen Pfad zur Festplatte, bis dieser nicht mehr verfügbar ist. Ist der Pfad nicht mehr verfügbar, wählt der Host einen alternativen Pfad aus. Der Host wird nicht auf den ursprünglichen Pfad zurückgesetzt, wenn dieser wieder verfügbar ist. Die MRU-Richtlinie beinhaltet keine Einstellung für den bevorzugten Pfad. MRU ist die Standardrichtlinie für Aktiv/Passiv-Speichergeräte und ist für solche Geräte erforderlich.
Round Robin (VMware)	Der Host verwendet einen Algorithmus zur automatischen Pfadauswahl, der alle verfügbaren Pfade durchgehend rotiert. Dadurch wird Lastenausgleich auf alle verfügbaren physischen Pfaden implementiert. Lastenausgleich ist der Vorgang zum Verteilen von E/A-Anforderungen eines Servers auf alle verfügbaren Hostpfade. Das Ziel ist die Optimierung der Leistung im Hinblick auf den Durchsatz (E/A pro Sekunde, MB pro Sekunde oder Reaktionszeiten).

Unter [Tabelle 9-1](#) wird zusammengefasst, wie sich das Verhalten des Hosts abhängig vom Array-Typ und von der Failover-Richtlinie ändert.

Tabelle 9-1. Auswirkungen der Pfadrichtlinie

Richtlinie/Controller	Aktiv/Aktiv	Aktiv/Passiv
Zuletzt verwendet	Um nach einem Pfadausfall ein Failback durchzuführen, muss der Administrator einige Schritte ausführen.	Um nach einem Pfadausfall ein Failback durchzuführen, muss der Administrator einige Schritte ausführen.
Fest	Der VMkernel wird nach Wiederherstellung der Konnektivität unter Verwendung des bevorzugten Pfades fortgesetzt.	Es wird versucht, den VMkernel unter Verwendung des bevorzugten Pfades fortzusetzen. Dies kann zu Pfad-Thrashing oder einem Ausfall führen, wenn die LUN nun zu einem anderen Speicherprozessor gehört.
Round Robin	Kein Failback.	Der nächste Pfad in der Round-Robin-Planung wird ausgewählt.

Ändern der Pfadauswahl-Richtlinie

In der Regel müssen Sie die standardmäßigen Multipathing-Einstellungen, die Ihr Host für ein bestimmtes Speichergerät verwendet, nicht ändern. Falls Sie jedoch Änderungen vornehmen möchten, können Sie im Dialogfeld „Pfade verwalten“ eine Pfadauswahl-Richtlinie ändern und den bevorzugten Pfad für die Richtlinie „Fest“ angeben.

Vorgehensweise

- 1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.
- 2 Wählen Sie eine Pfadauswahlrichtlinie aus.

Standardmäßig unterstützt VMware die folgenden Pfadauswahlrichtlinien: Wenn Sie die PSP eines Drittanbieters auf Ihrem Host installiert haben, wird die zugehörige Richtlinie ebenfalls in der Liste aufgeführt.

- [Fest (VMware)]
- [Zuletzt verwendet (VMware)]
- [Round Robin (VMware)]

- 3 Geben Sie für die Richtlinie „Fest“ den bevorzugten Pfad an, indem Sie mit der rechten Maustaste auf den Pfad klicken, den Sie als bevorzugten Pfad zuweisen möchten, und die Option **[Bevorzugt]** auswählen.
- 4 Klicken Sie auf **[OK]**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Deaktivieren von Pfaden

Pfade können zu Wartungszwecken oder aus anderen Gründen vorübergehend deaktiviert werden. Diese Aufgabe kann über den vSphere-Client ausgeführt werden.

Vorgehensweise

- 1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.
- 2 Klicken Sie im Fenster „Pfade“ mit der rechten Maustaste auf den zu deaktivierenden Pfad und wählen Sie **[Deaktivieren]**.
- 3 Klicken Sie auf **[OK]**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Sie können einen Pfad auch aus der Ansicht „Pfade“ des Adapters deaktivieren, indem Sie in der Liste mit der rechten Maustaste auf den Pfad klicken und **[Deaktivieren]** wählen.

Thin-Bereitstellung

Wenn Sie eine virtuelle Maschine erstellen, wird ein bestimmter Teil des Speicherplatzes auf einem Datenspeicher für die virtuellen Festplattendateien bereitgestellt bzw. ihnen zugeteilt.

Standardmäßig bietet ESXi eine traditionelle Methode zur Speicherbereitstellung: Sie berechnen, wie viel Speicherplatz die virtuelle Maschine jemals benötigen wird, stellen diesen Speicherplatz bereit und übergeben ihn der zugehörigen virtuellen Festplatte bei ihrer Erstellung vollständig. Eine virtuelle Festplatte, die sofort den gesamten bereitgestellten Speicherplatz belegt, wird Thick-Festplatte genannt. Das Erstellen einer virtuellen Festplatte im Thick-Format kann jedoch dazu führen, dass die Datenspeicherkapazität zu wenig genutzt wird, da große Mengen an Speicherplatz, die einzelnen virtuellen Maschinen im Voraus zugeteilt wurden, ungenutzt bleiben können.

ESXi bietet zur Vermeidung der Überreservierung und zum Einsparen von Speicherplatz die Thin-Bereitstellung, die Ihnen ermöglicht, am Anfang nur den tatsächlich benötigten Speicherplatz zu belegen und später weiteren Speicherplatz nach Bedarf hinzuzufügen. Die Funktion „Thin-Bereitstellung“ von ESXi ermöglicht Ihnen das Erstellen von virtuellen Festplatten im Thin-Format. ESXi teilt einer thin bereitgestellten virtuellen Festplatte den gesamten für aktuelle und zukünftige Aktionen erforderlichen Speicherplatz zu, übergibt am Anfang jedoch nur so viel Speicherplatz, wie die Festplatte anfänglich benötigt.

Info zu Formaten virtueller Festplatten

Wenn Sie bestimmte Vorgänge für die Verwaltung virtueller Maschinen ausführen, z. B. eine virtuelle Festplatte erstellen, eine virtuelle Maschine in eine Vorlage klonen oder eine virtuelle Maschine migrieren, können Sie ein Format für die Datei der virtuellen Festplatte festlegen.

Die folgenden Festplattenformate werden unterstützt. Sie können das Festplattenformat nicht angeben, wenn sich die Festplatte auf einem NFS-Datenspeicher befindet. Der NFS-Server bestimmt die Zuteilungsrichtlinie für die Festplatte.

Format „Thin-bereitgestellt“

Verwenden Sie dieses Format, um Speicherplatz zu sparen. Für eine Festplatte mit diesem Format stellen Sie genauso viel Datenspeicherplatz bereit, wie die Festplatte ausgehend von dem Wert erfordern würde, den Sie für die Datenträgergröße eingeben. Die Festplatte besitzt jedoch zunächst nur eine geringe Größe und verwendet nur so viel Datenspeicherplatz, wie sie tatsächlich für ihre anfänglichen Vorgänge benötigt.

HINWEIS Wenn eine virtuelle Festplatte Clusterlösungen wie z. B. die Fehlertoleranz unterstützt, können Sie für die Festplatte das Format „Thin-bereitgestellt“ nicht verwenden.

Wenn die Festplatte später mehr Speicherplatz benötigt, kann sie auf ihre maximale Kapazität anwachsen und den gesamten für sie bereitgestellten Datenspeicherplatz in Anspruch nehmen. Außerdem können Sie die Festplatte manuell in das Thick-Format konvertieren.

Thick-Format

Dies ist das Standardformat für virtuelle Festplatten. Die Festplatte im Thick-Format ändert ihre Größe nicht und belegt von Anfang an den gesamten für sie bereitgestellten Datenspeicherplatz. Das Thick-Format füllt die Blöcke im zugeteilten Speicher nicht mit Nullen auf. Eine Festplatte im Thick-Format kann nicht in Thin-Format konvertiert werden.

Erstellen von virtuellen Thin-bereitgestellten Festplatten

Wenn Sie Speicherplatz sparen müssen, können Sie eine virtuelle Festplatte im Thin-bereitgestellten Format erstellen. Die Größe der virtuellen Thin-bereitgestellten Festplatte ist zunächst gering und steigt an, sobald mehr virtueller Festplattenspeicher erforderlich ist.

Für dieses Verfahren wird vorausgesetzt, dass Sie mit dem Assistenten für neue virtuelle Maschinen eine standardmäßige oder benutzerdefinierte virtuelle Maschine erstellen.

Voraussetzungen

Sie können Thin-Festplatten nur auf Datenspeichern erstellen, die Thin-Bereitstellung unterstützen. Wenn sich die Festplatte auf einem NFS-Datenspeicher befindet, können Sie das Festplattenformat nicht angeben, da der NFS-Server die Zuteilungsrichtlinie für die Festplatte festlegt.

Vorgehensweise

- ◆ Wählen Sie im Dialogfeld „Festplatte erstellen“ die Option **[Speicherplatz nach Bedarf zuteilen und übernehmen (Thin-Bereitstellung)]**.

Es wird eine virtuelle Festplatte im Thin-Format erstellt. Wenn Sie die Option für Thin-Bereitstellung nicht auswählen, wird die virtuelle Festplatte im standardmäßigen Thick-Format erstellt.

Weiter

Wenn die virtuelle Festplatte das Thin-Format aufweist, können Sie sie später auf ihre volle Größe vergrößern.

Anzeigen von Speicherressourcen virtueller Maschinen

Sie können anzeigen, wie Speicherplatz von Datenspeichern Ihren virtuellen Maschinen zugeteilt ist.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **[Übersicht (Summary)]**.
- 3 Überprüfen Sie die Informationen zur Speicherplatzzuteilung im Abschnitt „Ressourcen“.
 - Bereitgestellter Speicher – Zeigt den für die virtuelle Maschine garantierten Speicherplatz. Wenn die virtuelle Maschine über Festplatten im Thin-bereitgestellten Format verfügt, kann möglicherweise nicht der gesamte Speicherplatz genutzt werden. Andere virtuelle Maschinen können nicht genutzten Speicherplatz in Anspruch nehmen.
 - Nicht gemeinsam genutzter Speicher - Zeigt den Datenspeicherplatz, der von der virtuellen Maschine beansprucht und nicht gemeinsam mit anderen virtuellen Maschinen genutzt wird.
 - Verwendeter Speicher – Zeigt Datenspeicherplatz, der tatsächlich von den Dateien der virtuellen Maschine, z. B. Konfigurations- und Protokolldateien, Snapshots, virtuellen Festplatten usw., beansprucht wird. Wenn die virtuelle Maschine läuft, werden im verwendeten Speicherplatz auch die Auslagerungsdateien berücksichtigt.

Festlegen des Festplattenformats für eine virtuelle Maschine

Sie können festlegen, ob Ihre virtuelle Festplatte im Thick- oder im Thin-Format vorliegen soll.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf **[Einstellungen bearbeiten]**, um das Eigenschaftendialogfeld für die virtuelle Maschine anzuzeigen.

- 3 Klicken Sie auf die Registerkarte **[Hardware]** und wählen Sie die entsprechende Festplatte aus der Hardwareliste aus.

Der Typ der virtuellen Festplatte, entweder „Thin“ oder „Thick“, wird rechts im Abschnitt „Festplattenbereitstellung“ angezeigt.

- 4 Klicken Sie auf **[OK]**.

Weiter

Wenn die virtuelle Festplatte das Format „Schnell“ aufweist, können Sie sie auf ihre volle Größe vergrößern.

Konvertieren einer virtuellen Festplatte von „Schnell“ (Thin) nach Thick

Virtuelle Festplatten, die Sie im Schnell-Format erstellt haben, können in das Thick-Format konvertiert werden.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie zum Öffnen des Dialogfelds „Datenspeicherbrowser“ auf die Registerkarte **[Übersicht]** und doppelklicken Sie unter „Ressourcen“ auf den Datenspeicher für die virtuelle Maschine.
- 3 Klicken Sie zum Auffinden der virtuellen Festplattendatei, die Sie konvertieren möchten, auf den VM-Ordner. Die Datei weist die Erweiterung `.vmdk` auf.
- 4 Klicken Sie mit der rechten Maustaste auf die virtuelle Festplattendatei und wählen Sie **[Vergrößern]**.

Die virtuelle Festplatte im Thick-Format belegt den gesamten Datenspeicherplatz, der für sie ursprünglich bereitgestellt wurde.

Handhabung von Datenspeicher-Überbuchung

Da der für Thin-Festplatten verfügbare Speicherplatz größer sein kann als der übernommene Speicherplatz, kann eine Datenspeicher-Überbuchung auftreten. Dadurch kann der gesamte für die Festplatten der virtuellen Maschine bereitgestellte Speicherplatz die tatsächliche Kapazität überschreiten.

Eine Überbuchung ist möglich, weil normalerweise nicht alle virtuellen Maschinen mit Thin-Festplatten den gesamten für sie bereitgestellten Datenspeicherplatz zur gleichen Zeit benötigen. Sie können jedoch zum Vermeiden einer Datenspeicher-Überbuchung einen Alarm einrichten, der Sie warnt, wenn der bereitgestellte Speicherplatz einen bestimmten Schwellenwert erreicht.

Weitere Informationen zu Berechtigungen finden Sie unter *Grundlagen der Systemverwaltung*.

Wenn Ihre virtuellen Maschinen mehr Speicherplatz benötigen, wird der Datenspeicherplatz in der Reihenfolge der Anforderungen zugeteilt. Wenn der Datenspeicherplatz nicht mehr ausreicht, können Sie den physischen Speicher erweitern und den Datenspeicher vergrößern.

Siehe [„Erweitern von VMFS-Datenspeichern“](#), auf Seite 106.

Raw-Gerätezuordnung

Die Raw-Gerätezuordnung bietet virtuellen Maschinen einen Mechanismus für den direkten Zugriff auf eine LUN im physischen Speichersubsystem (nur Fibre-Channel oder iSCSI).

Die folgenden Themen enthalten Informationen über RDMs und bieten Anleitungen zum Erstellen und Verwalten von RDMs.

Dieses Kapitel behandelt die folgenden Themen:

- „Wissenswertes zur Raw-Gerätezuordnung“, auf Seite 123
- „Raw-Gerätezuordnungseigenschaften“, auf Seite 127
- „Verwalten zugeordneter LUNs“, auf Seite 131

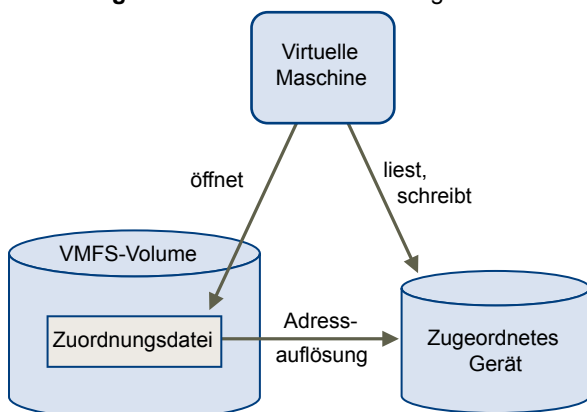
Wissenswertes zur Raw-Gerätezuordnung

Zur Raw-Gerätezuordnung gehört eine Zuordnungsdatei in einem getrennten VMFS-Volume, die als Stellvertreter für ein physisches Raw-Gerät fungiert, das direkt von einer virtuellen Maschine verwendet wird. Die RDM enthält Metadaten, mit denen Festplattenzugriffe auf das physische Gerät verwaltet und umgeleitet werden.

Die Datei bietet Ihnen einige der Vorteile des direkten Zugriffs auf ein physisches Gerät, während Sie gleichzeitig verschiedene Vorteile einer virtuellen Festplatte im VMFS nutzen können. Folglich verbindet die Datei die VMFS-Verwaltungs- und Wartungsfreundlichkeit mit einem Raw-Gerätezugriff.

Raw-Gerätezuordnungen können beispielsweise wie folgt beschrieben werden: „Zuordnen eines Raw-Geräts zu einem Datenspeicher“, „Zuordnen einer System-LUN“ oder „Zuordnen einer Festplattendatei zu einem physischen Festplatten-Volume“. All diese Zuordnungsbegriffe beziehen sich auf Raw-Gerätezuordnungen.

Abbildung 10-1. Raw-Gerätezuordnung



Obwohl VMFS für die meisten virtuellen Festplattenspeicher von VMware empfohlen wird, kann es in Einzelfällen erforderlich sein, Raw-LUNs oder logische Festplatten in einem SAN zu verwenden.

So ist es beispielsweise in folgenden Situationen erforderlich, Raw-LUNs zusammen mit zu Raw-Gerätezuordnungen zu verwenden:

- Wenn in der virtuellen Maschine ein SAN-Snapshot oder auf Ebenen basierende Anwendungen ausgeführt werden. Die Raw-Gerätezuordnung unterstützt Systeme zur Auslagerung von Datensicherungen, indem SAN-eigene Funktionen verwendet werden.
- In allen MSCS-Clusterszenarien, die sich über mehrere physische Hosts erstrecken (in Virtuell-zu-Virtuell-Clustern und in Physisch-zu-Virtuell-Clustern). In diesem Fall sollten Clusterdaten und Quorumfestplatten vorzugsweise als Raw-Gerätezuordnungen konfiguriert werden und nicht als Dateien auf einem freigegebenen VMFS.

Stellen Sie sich eine RDM als eine symbolische Verknüpfung zwischen einem VMFS-Volume und einer Raw-LUN vor. Die Zuordnung zeigt die LUNs wie Dateien auf einem VMFS-Volume an. In der Konfiguration der virtuellen Maschine wird auf die Raw-Gerätezuordnung und nicht auf die Raw-LUN verwiesen. Die Raw-Gerätezuordnung enthält einen Verweis auf die Raw-LUN.

Mithilfe von Raw-Gerätezuordnungen ist Folgendes möglich:

- Migrieren virtueller Maschinen mit VMotion über Raw-LUNs.
- Hinzufügen von Raw-LUNs zu virtuellen Maschinen mithilfe des vSphere-Clients
- Verwenden von Dateisystemfunktionen wie verteilte Dateispeicherung, Berechtigungen und Benennung

Für Raw-Gerätezuordnungen gibt es zwei Kompatibilitätsmodi:

- Mit dem Modus „Virtuelle Kompatibilität“ kann sich eine Raw-Gerätezuordnung ebenso wie eine virtuelle Festplattendatei verhalten. Dies umfasst auch die Verwendung von Snapshots.
- Im Modus „Physische Kompatibilität“ können Anwendungen, die eine hardwarenähere Steuerung benötigen, direkt auf das SCSI-Gerät zugreifen.

Vorteile von Raw-Gerätezuordnungen

Eine Raw-Gerätezuordnung bietet mehrere Vorteile, sollte aber nicht ständig verwendet werden. In der Regel sind virtuelle Festplattendateien aufgrund ihrer Verwaltungsfreundlichkeit Raw-Gerätezuordnungen vorzuziehen. Wenn Sie jedoch Raw-Geräte benötigen, müssen Sie die Raw-Gerätezuordnung verwenden.

RDM bietet verschiedene Vorteile:

Benutzerfreundliche, dauerhafte Namen

Die Raw-Gerätezuordnung ermöglicht benutzerfreundliche Namen für zugeordnete Geräte. Wenn Sie eine Raw-Gerätezuordnung verwenden, müssen Sie nicht auf das Gerät über den Gerätenamen verweisen. Sie verwenden stattdessen den Namen der Zuordnungsdatei, zum Beispiel:

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

Dynamische Namensauflösung

Die Raw-Gerätezuordnung speichert eindeutige Identifikationsdaten für jedes zugeordnete Gerät. VMFS ordnet jede RDM unabhängig von Änderungen der physischen Konfiguration des Servers aufgrund von Änderungen an der Adapterhardware, Verzeichniswechseln, Geräteverschiebungen usw. dem aktuellen SCSI-Gerät zu.

Verteilte Dateispeicherung

Die Raw-Gerätezuordnung ermöglicht die Verwendung einer verteilten VMFS-Speicherung für Raw-SCSI-Geräte. Die verteilte Speicherung für eine Raw-Gerätezuordnung ermöglicht die Verwendung einer freigegebenen Raw-LUN ohne Datenverlustrisiko, wenn zwei virtuelle Maschinen auf verschiedenen Servern versuchen, auf die gleiche LUN zuzugreifen.

Dateizugriffsberechtigungen

Die Raw-Gerätezuordnung ermöglicht Dateizugriffsberechtigungen. Die Berechtigungen für die Zuordnungsdatei werden beim Öffnen der Datei erzwungen, um das zugeordnete Volume zu schützen.

Dateisystemfunktionen

Die Raw-Gerätezuordnung ermöglicht bei der Arbeit mit einem zugeordneten Volume die Verwendung von Dienstprogrammen des Dateisystems, wobei die Zuordnungsdatei als Stellvertreter verwendet wird. Die meisten Vorgänge, die auf eine normale Datei angewendet werden können, können auf die Zuordnungsdatei angewendet werden und werden dann auf das zugeordnete Gerät umgeleitet.

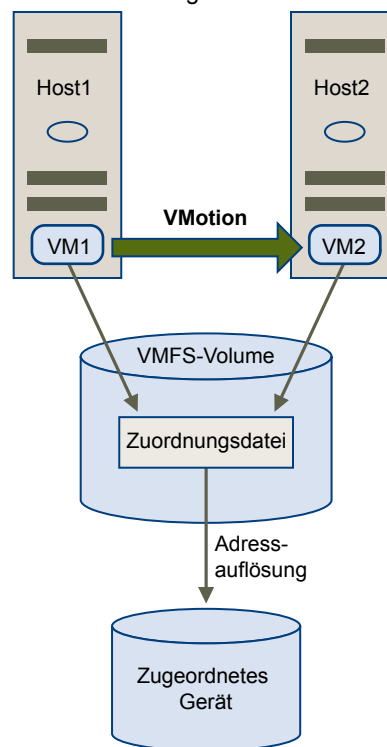
Snapshots

Die Raw-Gerätezuordnung ermöglicht die Verwendung von Snapshots virtueller Maschinen auf einem zugeordneten Volume. Snapshots stehen nicht zur Verfügung, wenn die Raw-Gerätezuordnung im Modus „Physische Kompatibilität“ verwendet wird.

vMotion

Mithilfe der Raw-Gerätezuordnung können Sie eine virtuelle Maschine mit vMotion migrieren. Die Zuordnungsdatei fungiert als Stellvertreter, sodass vCenter Server die virtuelle Maschine mit dem gleichen Mechanismus migrieren kann, der für die Migration virtueller Festplattendateien verwendet wird.

Abbildung 10-2. vMotion einer virtuellen Maschine über eine Raw-Gerätezuordnung



SAN-Management-Agenten

Die Raw-Gerätezuordnung ermöglicht die Ausführung bestimmter SAN-Management-Agenten innerhalb einer virtuellen Maschine. Außerdem kann jede Software, die Zugriff auf ein Gerät über hardware-spezifische SCSI-Befehle benötigt, in einer virtuellen Maschine ausgeführt werden. Diese Art der Software wird auch SCSI-Ziel-basierte Software genannt. Wenn Sie SAN-Verwaltungs-Agenten verwenden, müssen Sie den physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung auswählen.

N-Port-ID-Virtualisierung (NPIV)

Ermöglicht den Einsatz der NPIV-Technologie, die es einem einzelnen Fibre-Channel-HBA-Port ermöglicht, sich mit dem Fibre-Channel-Fabric anhand mehrerer WWPNs (Worldwide Port Names) zu registrieren. Dadurch kann der HBA-Port in Form mehrerer virtueller Ports angezeigt werden, die alle über eine eigene ID und einen eigenen virtuellen Portnamen verfügen. Virtuelle Maschinen können anschließend jeden dieser virtuellen Ports beanspruchen und für den gesamten zur Raw-Gerätezuordnung gehörenden Datenverkehr nutzen.

HINWEIS Sie können NPIV nur für virtuelle Maschinen mit RDM-Festplatten verwenden.

VMware kooperiert mit Anbietern von Speicherverwaltungssoftware, damit deren Software in Umgebungen wie ESXi ordnungsgemäß funktioniert. Beispiele sind:

- SAN-Verwaltungssoftware
- Software zur Verwaltung von Speicherressourcen
- Snapshot-Software
- Replikationssoftware

Diese Software verwendet für Raw-Gerätezuordnungen den Modus „Physische Kompatibilität“, damit sie direkt auf SCSI-Geräte zugreifen kann.

Verschiedene Verwaltungsprodukte werden besser zentral (nicht auf dem ESXi-Computer) ausgeführt, während andere problemlos in der Servicekonsole oder in den virtuellen Maschinen funktionieren. VMware zertifiziert diese Anwendungen nicht und stellt auch keine Kompatibilitätsmatrix zur Verfügung. Wenn Sie wissen möchten, ob eine SAN-Verwaltungsanwendung in einer ESXi-Umgebung unterstützt wird, wenden Sie sich an den Hersteller.

Einschränkungen der Raw-Gerätezuordnung

Bei der Verwendung von Raw-Gerätezuordnungen gelten bestimmte Einschränkungen.

- Nicht verfügbar für Block- und bestimmte RAID-Geräte – Die Raw-Gerätezuordnung verwendet zur Identifizierung des zugeordneten Geräts eine SCSI-Seriennummer. Da Block- und bestimmte direkt angeschlossene RAID-Geräte Seriennummern nicht exportieren, können sie nicht in Raw-Gerätezuordnungen verwendet werden.
- Nur für Volumes mit VMFS-2 und VMFS-3 – Die RDM erfordert das Format VMFS-2 oder VMFS-3. Unter ESXi ist das Dateisystem VMFS-2 schreibgeschützt. Aktualisieren Sie es auf VMFS-3, um die in VMFS-2 gespeicherten Dateien nutzen zu können.

- Keine Snapshots im physischen Kompatibilitätsmodus – Wenn Sie eine RDM im physischen Kompatibilitätsmodus verwenden, können Sie für die Festplatte keine Snapshots verwenden. Im Modus „Physische Kompatibilität“ kann die virtuelle Maschine eigene Snapshots oder Spiegelungsoperationen durchführen. Im virtuellen Modus stehen Snapshots zur Verfügung.
- Keine Partitionszuordnung – Für die Raw-Gerätezuordnung muss das zugeordnete Gerät eine vollständige LUN sein. Die Zuordnung zu einer Partition wird nicht unterstützt.

Raw-Gerätezuordnungseigenschaften

Eine Raw-Gerätezuordnung ist eine spezielle Datei auf einem VMFS-Volume, mit deren Hilfe die Metadaten für das zugeordnete Gerät verwaltet werden. Die Verwaltungssoftware erkennt die Zuordnungsdatei als normale Festplattendatei, die für normale Dateisystemoperationen zur Verfügung steht. Die virtuelle Maschine erkennt das zugeordnete Gerät aufgrund der Speichervirtualisierungsebene als virtuelles SCSI-Gerät.

Zu den wichtigsten Metadaten in der Zuordnungsdatei gehören der Speicherort (Namensauflösung) sowie der Sperrstatus des zugeordneten Geräts, Berechtigungen usw.

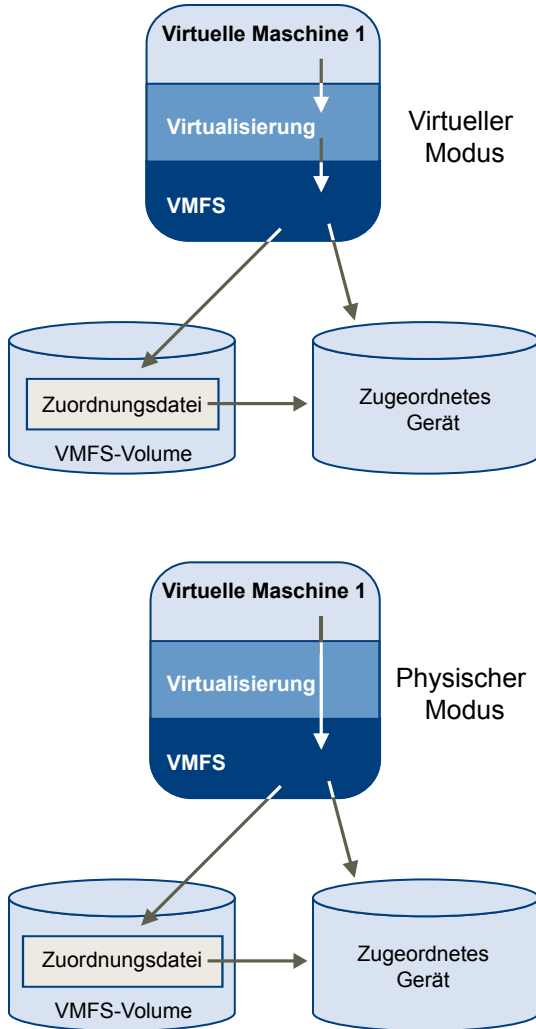
Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“ für RDM

Sie können RDMs in virtuellen oder physischen Kompatibilitätsmodi verwenden. Der virtuelle Modus legt die vollständige Virtualisierung des zugeordneten Geräts fest. Der physische Modus legt eine minimale SCSI-Virtualisierung des zugeordneten Geräts fest, wodurch eine optimale Flexibilität der SAN-Verwaltungssoftware erreicht wird.

Im virtuellen Modus erkennt das Gastbetriebssystem keinen Unterschied zwischen einem zugeordneten Gerät und einer virtuellen Festplattendatei auf einem VMFS-Volume. Die tatsächlichen Hardwaremerkmale sind verborgen. Wenn Sie eine Raw-Festplatte im virtuellen Modus verwenden, können Sie die Vorteile von VMFS wie leistungsfähige Dateisperrung zum Datenschutz und Snapshots zur Vereinfachung von Entwicklungsprozessen nutzen. Der virtuelle Modus ist auch besser zwischen Speichergeräten portierbar als der physische Modus, da er das gleiche Verhalten wie virtuelle Festplattendateien aufweist.

Im physischen Modus leitet der VMkernel alle SCSI-Befehle bis auf eine Ausnahme an das Gerät weiter: Der Befehl REPORT LUNs ist virtualisiert, damit der VMkernel die LUN für die entsprechende virtuelle Maschine isolieren kann. Ansonsten sind alle physischen Charakteristika der zu Grunde liegenden Hardware sichtbar. Der physische Modus ist für die Ausführung von SAN-Verwaltungs-Agenten oder anderer SCSI-Ziel-basierter Software in der virtuellen Maschine bestimmt. Der physische Modus ermöglicht auch zum kostengünstigen Erzielen einer hohen Verfügbarkeit die Bildung von VM-PC-Clustern.

Abbildung 10-3. Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“

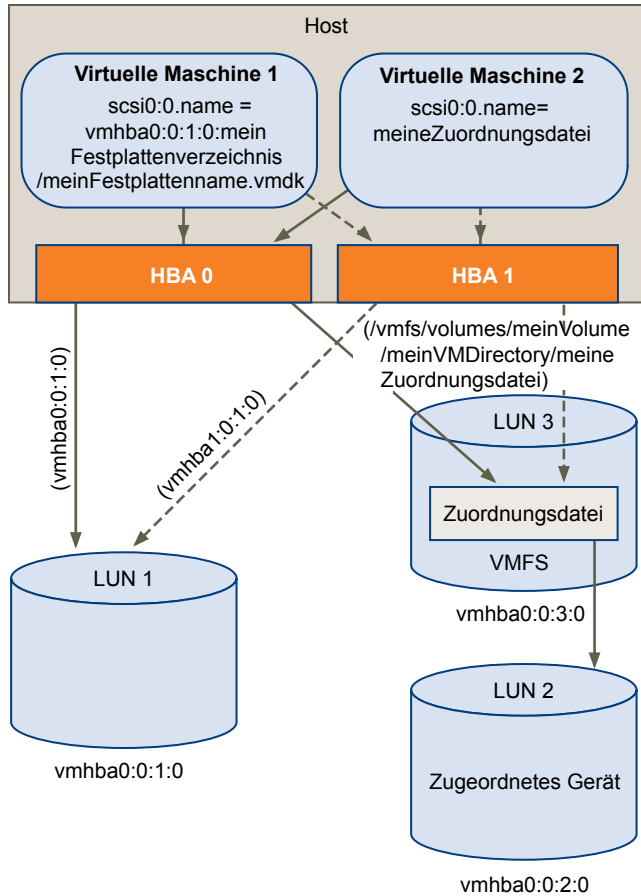


Dynamische Namensauflösung

Mit der Raw-Gerätezuordnung können Sie einem Gerät einen dauerhaften Namen geben, indem Sie auf den Namen der Zuordnungsdatei im Unterverzeichnis `/vmfs` verweisen.

Das Beispiel in [Abbildung 10-4](#) zeigt drei LUNs. Auf LUN 1 wird über den Gerätenamen zugegriffen, der von der ersten sichtbaren LUN abhängt. LUN 2 ist ein zugeordnetes Gerät, das von einer Raw-Gerätezuordnung auf LUN 3 verwaltet wird. Der Zugriff auf die Raw-Gerätezuordnung erfolgt über den festen Pfadnamen im Unterverzeichnis `/vmfs`.

Abbildung 10-4. Beispiel einer Namensauflösung

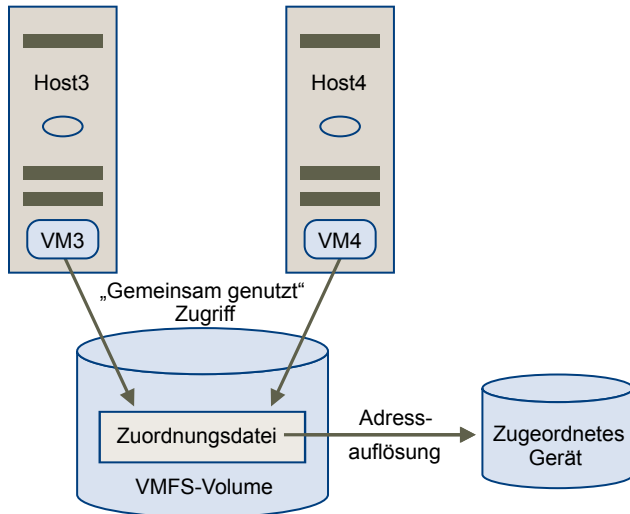


Alle zugeordneten LUNs werden durch VMFS eindeutig bezeichnet. Die Bezeichnung wird in den internen LUN-Datenstrukturen gespeichert. Alle Änderungen im SCSI-Pfad, z. B. ein Fibre-Channel-Switchfehler oder das Hinzufügen eines neuen Hostbusadapters, können den Gerätenamen ändern. Die dynamische Namensauflösung gleicht diese Änderungen durch die Anpassung der Datenstrukturen aus, wodurch die LUNs auf die neuen Gerätenamen umgeleitet werden.

Raw-Gerätezuordnung für Cluster aus virtuellen Maschinen

Die Verwendung einer Raw-Gerätezuordnung ist für Cluster mit virtuellen Maschinen erforderlich, die zur Sicherstellung von Failover auf die gleiche Raw-LUN zugreifen müssen. Die Einrichtung ist vergleichbar mit der Einrichtung eines solchen Clusters mit Zugriff auf dieselbe virtuelle Festplattendatei. Die virtuelle Festplattendatei wird dabei allerdings durch die Raw-Gerätezuordnung ersetzt.

Abbildung 10-5. Zugriff aus virtuellen Maschinen in Clustern



Vergleichen der verfügbaren Zugriffsmodi für SCSI-Geräte

Zu den Möglichkeiten, auf ein SCSI-basiertes Speichergerät zuzugreifen, gehören eine virtuelle Festplattendatei auf einem VMFS-Datenspeicher, RDM im virtuellen Modus und RDM im physischen Modus.

Um die Entscheidung zwischen den verfügbaren Zugriffsmodi für SCSI-Geräte zu erleichtern, bietet [Tabelle 10-1](#) einen Vergleich der Funktionen in den verschiedenen Modi.

Tabelle 10-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Gerätezuordnungen

ESXi-Funktionen	Virtuelle Festplatten-datei	Raw-Gerätezuordnung – Virtueller Modus	Raw-Gerätezuordnung – Physischer Modus
Weitergabe von SCSI-Befehlen	Nein	Nein	Ja Der Befehl REPORT LUNs wird nicht weitergegeben
Unterstützung von vCenter Server	Ja	Ja	Ja
Snapshots	Ja	Ja	Nein
Verteilte Sperrung	Ja	Ja	Ja
Clusterbildung	Nur systeminterne Cluster	Systeminterne und systemübergreifende Cluster	Physisch-zu-Virtuell-Clustering
SCSI-Ziel-basierte Software	Nein	Nein	Ja

VMware empfiehlt für systeminterne Cluster den Einsatz virtueller Festplattendateien. Wenn Sie systeminterne Cluster als systemübergreifende Cluster rekonfigurieren möchten, verwenden Sie für systeminterne Cluster Raw-Gerätezuordnungen.

Verwalten zugeordneter LUNs

Mithilfe des vSphere-Clients können Sie eine SAN-LUN einem Datenspeicher zuordnen und Pfade zur zugeordneten LUN verwalten.

Zu den zusätzlichen Tools zum Verwalten zugeordneter LUNs und ihrer Raw-Gerätezuordnungen gehören das Dienstprogramm `vmkfstools` sowie weitere Befehle, die mit der vSphere-CLI verwendet werden. Sie können das Dienstprogramm `vmkfstools` zum Durchführen vieler Vorgänge verwenden, die auch über den vSphere-Client verfügbar sind.

Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen

Wenn Sie eine virtuelle Maschine mit einem Direktzugriff auf eine Raw-SAN-LUN versehen, erstellen Sie eine Zuordnungsdatei (Raw-Gerätezuordnung), die sich in einem VMFS-Datenspeicher befindet und auf die LUN verweist. Wenngleich die Zuordnungsdatei dieselbe `.vmdk`-Erweiterung wie eine herkömmliche virtuelle Festplattendatei hat, enthält die Raw-Gerätezuordnungsdatei nur Zuordnungsinformationen. Die eigentlichen virtuellen Festplattendaten werden direkt in der LUN gespeichert.

Sie können die Raw-Gerätezuordnung als Ausgangsfestplatte für eine neue virtuelle Maschine erstellen oder sie einer vorhandenen virtuellen Maschine hinzufügen. Beim Erstellen der Raw-Gerätezuordnung geben Sie die zuzuordnende LUN und den Datenspeicher an, in dem die Raw-Gerätezuordnung abgelegt werden soll.

Vorgehensweise

- 1 Befolgen Sie sämtliche Anweisungen zum Erstellen einer benutzerdefinierten virtuellen Maschine.
- 2 Wählen Sie auf der Seite **[Festplatte auswählen (Select a Disk)]** die Option **[Raw-Gerätezuordnung (Raw Device Mapping)]** aus, und klicken Sie anschließend auf **[Weiter]**.
- 3 Wählen Sie in der Liste der SAN-Festplatten bzw. LUNs eine Raw-LUN aus, auf welche die virtuelle Maschine direkt zugreifen soll.
- 4 Wählen Sie einen Datenspeicher für die Raw-Gerätezuordnungsdatei aus.

Sie können die Raw-Gerätezuordnungsdatei im selben Datenspeicher ablegen, in dem sich die Konfigurationsdatei der virtuellen Maschine befindet, oder einen anderen Datenspeicher auswählen.

HINWEIS Um VMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die RDM-Dateien der virtuellen Maschinen im selben Datenspeicher befinden. Bei aktivierter NPIV ist Storage VMotion bzw. VMotion zwischen Datenspeichern nicht möglich.

- 5 Wählen Sie den Kompatibilitätsmodus aus.

Option	Beschreibung
Physisch	Ermöglicht es dem Gastbetriebssystem, auf die Hardware direkt zuzugreifen. Der physische Kompatibilitätsmodus bietet sich an, wenn Sie SAN-fähige Anwendungen in der virtuellen Maschine einsetzen. Eine virtuelle Maschine, die für einen physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung konfiguriert ist, kann jedoch weder geklont noch in eine Vorlage umgewandelt noch migriert werden, wenn für die Migration die Festplatte kopiert werden muss.
Virtuell	Ermöglicht es der RDM, sich wie eine virtuelle Festplatte zu verhalten, so dass Sie Funktionen wie Snapshots, Klonen usw. verwenden können.

- 6 Wählen Sie den Knoten des virtuellen Geräts aus.

- 7 Wenn Sie den unabhängigen Modus wählen, aktivieren Sie eine der folgenden Optionen.

Option	Beschreibung
Dauerhaft	Änderungen werden sofort wirksam und werden permanent auf die Festplatte geschrieben.
Nicht-dauerhaft	Änderungen auf der Festplatte werden beim Herunterfahren oder Wiederherstellen eines Snapshots verworfen.

- 8 Klicken Sie auf **[Weiter]** .
- 9 Überprüfen Sie auf der Seite **[Bereit zum Abschließen der neuen virtuellen Maschine (Ready to Complete New Virtual Machine)]** Ihre Angaben.
- 10 Klicken Sie auf **[Beenden]** , um die virtuelle Maschine zu erstellen.

Verwalten von Pfaden für eine zugeordnete Raw-LUN

Sie können die Pfade für zugeordnete Raw-LUNs verwalten.

Vorgehensweise

- 1 Melden Sie sich als Administrator oder als Besitzer der virtuellen Maschine an, zu der die zugeordnete Festplatte gehören soll.
- 2 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 3 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]** .
- 4 Wählen Sie auf der Registerkarte **[Hardware]** die Option **[Festplatte (Hard Disk)]** aus, und klicken Sie auf **[Pfade verwalten (Manage Paths)]** .
- 5 Im Dialogfeld **[Pfade verwalten]** können Sie Ihre Pfade aktivieren oder deaktivieren, eine Multipathing-Richtlinie festlegen und den bevorzugten Pfad angeben.

Weitere Informationen zur Verwaltung von Pfaden finden Sie unter [„Verwenden von Multipathing mit ESXi“](#), auf Seite 110.

Sicherheit

Sicherheit für ESXi-Systeme

Bei der Entwicklung von ESXi war hohe Sicherheit einer der Schwerpunkte. VMware sorgt für Sicherheit in der ESXi-Umgebung und geht das Thema Systemarchitektur vom Standpunkt der Sicherheit aus an.

Dieses Kapitel behandelt die folgenden Themen:

- „Architektur und Sicherheitsfunktionen von ESXi“, auf Seite 135
- „Sonstige Quellen und Informationen zur Sicherheit“, auf Seite 142

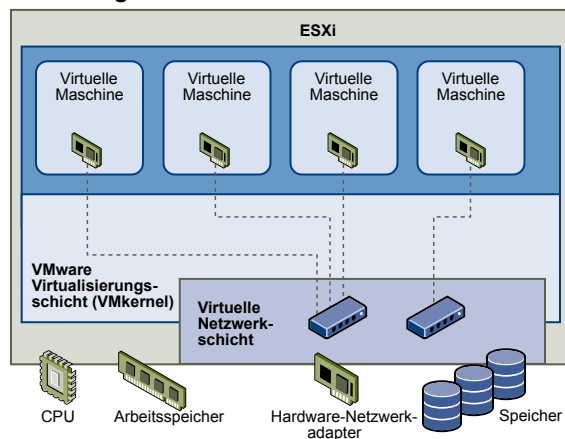
Architektur und Sicherheitsfunktionen von ESXi

Die Komponenten und die gesamte Architektur von ESXi wurden so entworfen, dass die Sicherheit des ESXi-Systems als Ganzes gewährleistet wird.

Im Hinblick auf die Sicherheit umfasst ESXi drei Hauptkomponenten: Die Virtualisierungsebene, die virtuellen Maschinen und die virtuelle Netzwerkebene.

In [Abbildung 11-1](#) finden Sie eine Übersicht über diese Komponenten.

Abbildung 11-1. ESXi-Architektur



Sicherheit und die Virtualisierungsebene

Die Virtualisierungsebene (bzw. VMkernel) ist ein Kernel, der von VMware für die Ausführung virtueller Maschinen entworfen wurde. Diese Ebene steuert die Hardware, die von den ESX-Hosts verwendet wird, und plant die Zuweisung von Hardwareressourcen an die einzelnen virtuellen Maschinen. Da VMkernel ausschließlich zur Unterstützung virtueller Maschinen verwendet wird, beschränkt sich die Schnittstelle zu VMkernel auf die API, die zur Verwaltung der virtuellen Maschinen notwendig ist.

ESXi bietet durch folgende Funktionen zusätzlichen Schutz für VMkernel:

Memory Hardening

Der ESXi-Kernel, Anwendungen im Benutzermodus und ausführbare Komponenten, z. B. Treiber und Bibliotheken, befinden sich an zufällig zugeteilten, nicht vorhersehbaren Speicheradressen. In Kombination mit dem von Mikroprozessoren bereitgestellten Schutz für nicht ausführbaren Arbeitsspeicher bietet dies Schutz gegen böswilligen Code, dem es dadurch erschwert wird, Arbeitsspeicherexploits zu verwenden, um Schwachstellen auszunutzen.

Integrität des Kernelmoduls

Digitale Signaturen überprüfen die Integrität und Echtheit von Modulen, Treibern und Anwendungen, wenn sie vom VMkernel geladen werden. Das Signieren von Modulen hilft ESXi, die Anbieter von Modulen, Treibern oder Anwendungen zu identifizieren und festzustellen, ob sie für VMware zertifiziert sind.

Trusted Platform Module (TPM)

Dieses Modul ist ein Hardwareelement, das den Startvorgang überwacht, als Vertrauensbasis für eine Plattform und zur Speicherung und zum Schutz von Kryptofieschlüsseln dient. Während des Startvorgangs überprüft ESXi den VMkernel mithilfe des TPM und protokolliert bis zum nächsten Starten die am VMkernel vorgenommenen Änderungen. Die Messwerte werden an vCenter Server weitergegeben und können mithilfe der vSphere-API von Agenten von Drittanbietern abgerufen werden.

HINWEIS Wenn TPM auf einem System vorhanden, aber im BIOS deaktiviert ist, wird möglicherweise die folgende Fehlermeldung angezeigt: Fehler beim Laden von TPM. Diese Fehlermeldung wird erwartet und kann bedenkenlos ignoriert werden.

Sicherheit und virtuelle Maschinen

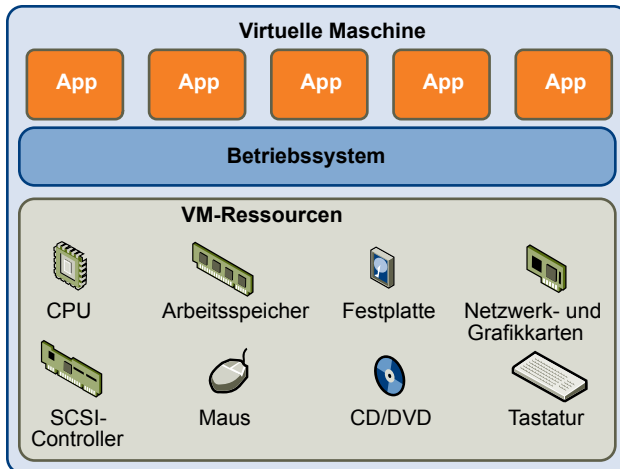
Virtuelle Maschinen sind die „Container“, in denen Anwendungen und Gastbetriebssysteme ausgeführt werden. Bedingt durch den Systemaufbau sind alle virtuellen Maschinen von VMware voneinander isoliert. Durch diese Isolierung können mehrere virtuelle Maschinen gleichzeitig und sicher auf der gleichen Hardware ausgeführt werden. Dabei werden sowohl der Hardwarezugriff als auch ununterbrochene Leistung garantiert.

Selbst ein Benutzer mit Systemadministratorrechten für das Gastbetriebssystem der virtuellen Maschine kann diese Isolierungsebene nicht überwinden und auf andere virtuelle Maschinen zugreifen, wenn er vom ESXi-Systemadministrator keine entsprechenden Rechte erhalten hat. Durch die Isolierung der virtuellen Maschinen werden bei einem Fehlschlag eines auf einer virtuellen Maschine ausgeführten Gastbetriebssystems die anderen virtuellen Maschinen auf dem gleichen Host weiterhin ausgeführt. Fehlschläge des Gastbetriebssystems hat keinen Einfluss auf Folgendes:

- Den uneingeschränkten Zugriff der Benutzer auf die anderen virtuellen Maschinen
- Den uneingeschränkten Zugriff der anderen virtuellen Maschinen auf die Ressourcen, die sie benötigen
- Die Leistung der anderen virtuellen Maschinen

Jede virtuelle Maschine ist von den anderen virtuellen Maschinen, die auf der gleichen Hardware ausgeführt werden, isoliert. Obwohl sich die virtuellen Maschinen die physischen Ressourcen wie CPU, Arbeitsspeicher und E/A-Geräte teilen, kann das Gastbetriebssystem einer einzelnen virtuellen Maschine nur die virtuellen Geräte sehen, die ihm zur Verfügung gestellt wurden (siehe [Abbildung 11-2](#)).

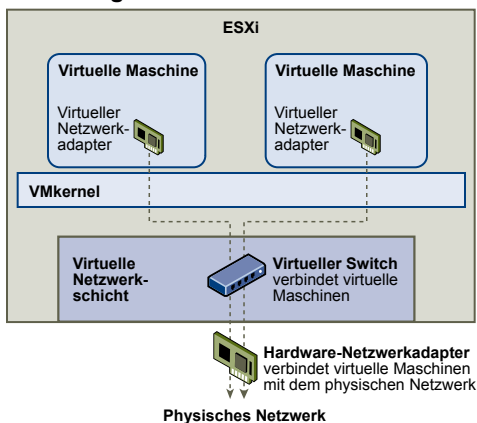
Abbildung 11-2. Isolierung virtueller Maschinen



Da VMkernel die physischen Ressourcen vermittelt und jeder Zugriff auf die physische Hardware über VMkernel erfolgt, können die virtuellen Maschinen diese Isolierungsebene nicht umgehen.

So wie ein Computer mit anderen Computern in einem Netzwerk über eine Netzwerkkarte kommuniziert, kann eine virtuelle Maschine mit anderen virtuellen Maschinen auf dem gleichen Host über einen virtuellen Switch kommunizieren. Außerdem kann die virtuelle Maschine mit einem physischen Netzwerk, einschließlich virtueller Maschinen auf anderen ESXi-Hosts, über einen physischen Netzwerkadapter kommunizieren (siehe [Abbildung 11-3](#)).

Abbildung 11-3. Virtuelle Netzwerkanbindung über virtuelle Switches



Für die Isolierung virtueller Maschinen in einem Netzwerk gelten folgende Merkmale:

- Wenn sich eine virtuelle Maschine keinen virtuellen Switch mit anderen virtuellen Maschinen teilt, ist sie von den virtuellen Netzwerken auf dem Host vollständig getrennt.
- Wenn einer virtuellen Maschine kein physischer Netzwerkadapter zugewiesen wurde, ist die virtuelle Maschine vollständig von physischen Netzwerken getrennt.
- Wenn Sie zum Schutz einer virtuellen Maschine vor dem Netzwerk die gleichen Sicherheitsmaßnahmen wie für normale Computer verwenden (Firewalls, Antiviren-Software usw.), ist die virtuelle Maschine genau so sicher, wie es ein Computer wäre.

Sie können die virtuelle Maschine außerdem durch die Einrichtung von Ressourcenreservierungen und -begrenzungen auf dem Host schützen. So können Sie zum Beispiel eine virtuelle Maschine mit den detaillierten Werkzeugen zur Ressourcensteuerung, die Ihnen in ESXi zur Verfügung stehen, so konfigurieren, dass sie immer mindestens 10 Prozent der CPU-Ressourcen des Hosts erhält, nie jedoch mehr als 20 Prozent.

Ressourcenreservierungen und -einschränkungen schützen die virtuellen Maschinen vor Leistungsabfällen, wenn eine andere virtuelle Maschine versucht, zu viele Ressourcen der gemeinsam genutzten Hardware zu verwenden. Wenn zum Beispiel eine virtuelle Maschine auf einem Host durch eine Denial-Of-Service (DoS)-Angriff außer Gefecht gesetzt wird, verhindert eine Einschränkung, dass der Angriff so viele Hardware-Ressourcen einnimmt, dass die anderen virtuellen Maschinen ebenfalls betroffen werden. Ebenso stellt eine Ressourcenreservierung für jede virtuelle Maschine sicher, dass bei hohen Ressourcenanforderungen durch den DoS-Angriff alle anderen virtuellen Maschinen immer noch über genügend Kapazitäten verfügen.

Standardmäßig schreibt ESXi eine Art der Ressourcenreservierung vor, indem ein Verteilungsalgorithmus verwendet wird, der die verfügbaren Hostressourcen zu gleichen Teilen auf die virtuellen Maschinen verteilt und gleichzeitig einen bestimmten Prozentsatz der Ressourcen für einen Einsatz durch andere Systemkomponenten bereithält. Dieses Standardverhalten bietet einen natürlichen Schutz gegen DoS- und DDoS-Angriffe. Geben Sie die spezifischen Ressourcenreservierungen und Grenzwerte individuell ein, wenn Sie das Standardverhalten auf Ihre Bedürfnisse so zuschneiden wollen, dass die Verteilung über die gesamte Konfiguration der virtuellen Maschine nicht einheitlich ist.

Sicherheit und die virtuelle Netzwerkebene

Zur virtuellen Netzwerkebene gehören virtuelle Netzwerkadapter und virtuelle Switches. ESXi verwendet die virtuelle Netzwerkebene zur Kommunikation zwischen den virtuellen Maschinen und ihren Benutzern. Außerdem verwenden Hosts die virtuelle Netzwerkebene zur Kommunikation mit iSCSI-SANs, NAS-Speicher usw.

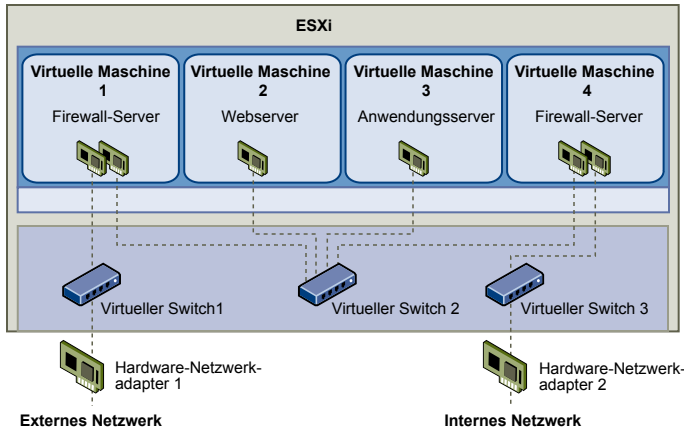
Die Methoden, die Sie zur Absicherung eines Netzwerks von virtuellen Maschinen verwenden, hängen unter anderem davon ab, welches Gastbetriebssystem installiert wurde und ob die virtuellen Maschinen in einer sicheren Umgebung betrieben werden. Virtuelle Switches bieten einen hohen Grad an Sicherheit, wenn sie in Verbindung mit anderen üblichen Sicherheitsmaßnahmen, z. B. Firewalls, verwendet werden.

ESXi unterstützt auch VLANs nach IEEE 802.1q, die zum weiteren Schutz des Netzwerkes der virtuellen Maschinen oder der Speicherkonfiguration verwendet werden können. Mit VLANs können Sie ein physisches Netzwerk in Segmente aufteilen, sodass zwei Computer im gleichen physischen Netzwerk nur dann Pakete untereinander versenden können, wenn sie sich im gleichen VLAN befinden.

Erstellen einer Netzwerk-DMZ auf einem einzelnen ESXi-Host

Ein Beispiel für die Anwendung der ESXi-Isolierung und der virtuellen Netzwerkfunktionen zur Umgebungsabsicherung ist die Einrichtung einer so genannten „entmilitarisierten Zone“ (DMZ) auf einem einzelnen Host.

[Abbildung 11-4](#) zeigt die Konfiguration.

Abbildung 11-4. Konfigurierte DMZ auf einem einzelnen ESXi-Host

In diesem Beispiel sind vier virtuelle Maschinen so konfiguriert, dass sie eine virtuelle DMZ auf dem virtuellen Switch 2 bilden.

- Die virtuelle Maschine 1 und die virtuelle Maschine 4 führen Firewalls aus und sind über virtuelle Switches an virtuelle Adapter angeschlossen. Diese beiden virtuellen Maschinen sind mehrfach vernetzt.
- Auf der virtuellen Maschine 2 wird ein Webserver ausgeführt, auf der virtuellen Maschine 3 ein Anwendungsserver. Diese beiden Maschinen sind einfach vernetzt.

Der Webserver und der Anwendungsserver befinden sich in der DMZ zwischen den zwei Firewalls. Die Verbindung zwischen diesen Elementen ist der virtuelle Switch 2, der die Firewalls mit den Servern verbindet. Dieser Switch ist nicht direkt mit Elementen außerhalb der DMZ verbunden und wird durch die beiden Firewalls vom externen Datenverkehr abgeschirmt.

Während des Betriebs der DMZ betritt externer Datenverkehr aus dem Internet die virtuelle Maschine 1 über den Hardware-Netzwerkadapter 1 (weitergeleitet vom virtuellen Switch 1) und wird von der auf dieser virtuellen Maschine installierten Firewall überprüft. Wenn die Firewall den Datenverkehr autorisiert, wird er an den virtuellen Switch in der DMZ, den virtuellen Switch 2, weitergeleitet. Da der Webserver und der Anwendungsserver ebenfalls an diesen Switch angeschlossen sind, können sie die externen Anforderungen bearbeiten.

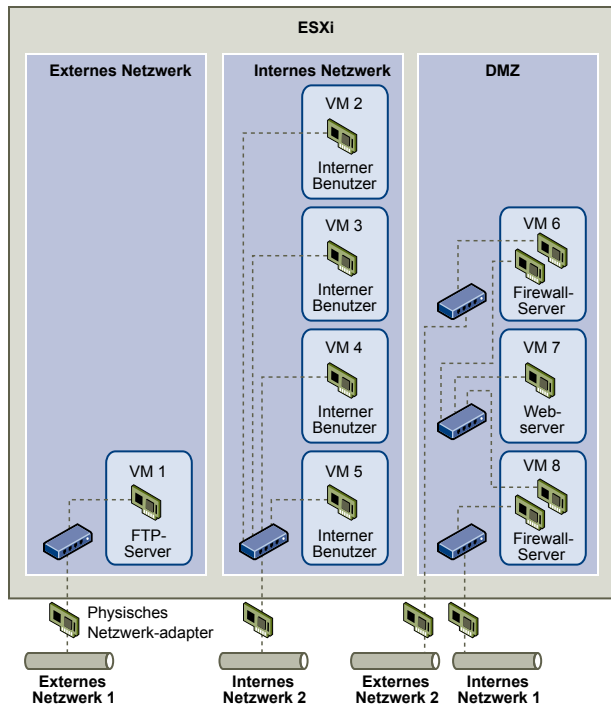
Der virtuelle Switch 2 ist auch an die virtuelle Maschine 4 angeschlossen. Auf dieser virtuellen Maschine schützt eine Firewall die DMZ vom internen Firmennetzwerk ab. Diese Firewall filtert Pakete vom Web- und Anwendungsserver. Wenn ein Paket überprüft wurde, wird es über den virtuellen Switch 3 an den Hardware-Netzwerkadapter 2 weitergeleitet. Der Hardware-Netzwerkadapter 2 ist an das interne Firmennetzwerk angeschlossen.

Bei der Implementierung einer DMZ auf einem einzelnen Host können Sie relativ einfache Firewalls verwenden. Obwohl eine virtuelle Maschine in dieser Konfiguration keine direkte Kontrolle über eine andere virtuelle Maschine ausüben oder auf ihren Arbeitsspeicher zugreifen kann, sind die virtuellen Maschinen dennoch über ein virtuelles Netzwerk verbunden. Dieses Netzwerk kann für die Verbreitung von Viren oder für andere Angriffe missbraucht werden. Die virtuellen Maschinen in der DMZ sind ebenso sicher wie getrennte physische Computer, die an dasselbe Netzwerk angeschlossen sind.

Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host

Das ESXi-System wurde so entworfen, dass Sie bestimmte Gruppen virtueller Maschinen an das interne Netzwerk anbinden können, andere an das externe Netzwerk und wiederum andere an beide Netzwerke, alles auf demselben ESXi-Host. Diese Fähigkeit basiert auf der grundlegenden Isolierung virtueller Maschinen im Zusammenspiel mit der überlegt geplanten Nutzung von Funktionen zur virtuellen Vernetzung.

Abbildung 11-5. Konfigurierte externe Netzwerke, interne Netzwerke und DMZ auf einem ESXi-Host



In [Abbildung 11-5](#) wurde ein Host vom Systemadministrator in drei eigenständige virtuelle Maschinenzonen eingeteilt: FTP-Server, interne virtuelle Maschinen und DMZ. Jede Zone erfüllt eine bestimmte Funktion.

FTP-Server

Die virtuelle Maschine 1 wurde mit FTP-Software konfiguriert und dient als Speicherbereich für Daten von und an externe Ressourcen, z. B. für von einem Dienstleister lokalisierte Formulare und Begleitmaterialien.

Diese virtuelle Maschine ist nur mit dem externen Netzwerk verbunden. Sie verfügt über einen eigenen virtuellen Switch und physischen Netzwerkadapter, die sie mit dem externen Netzwerk 1 verbinden. Dieses Netzwerk ist auf Server beschränkt, die vom Unternehmen zum Empfang von Daten aus externen Quellen verwendet werden. Das Unternehmen verwendet beispielsweise das externe Netzwerk 1, um FTP-Daten von Dienstleistern zu empfangen und den Dienstleistern FTP-Zugriff auf Daten zu gewähren, die auf extern verfügbaren Servern gespeichert sind. Zusätzlich zur Verarbeitung der Daten für die virtuelle Maschine 1 verarbeitet das externe Netzwerk 1 auch Daten für FTP-Server auf anderen ESXi-Hosts am Standort.

Da sich die virtuelle Maschine 1 keinen virtuellen Switch oder physischen Netzwerkadapter mit anderen virtuellen Maschinen auf dem Host teilt, können die anderen virtuellen Maschinen auf dem Host keine Datenpakete in das Netzwerk der virtuellen Maschine 1 übertragen oder daraus empfangen. Da-

durch werden Spionageangriffe verhindert, da dem Opfer dafür Netzwerkdaten gesendet werden müssen. Außerdem kann der Angreifer dadurch die natürliche Anfälligkeit von FTP nicht zum Zugriff auf andere virtuelle Maschinen auf dem Host nutzen.

Interne virtuelle Maschinen

Die virtuellen Maschinen 2 bis 5 sind der internen Verwendung vorbehalten. Diese virtuellen Maschinen verarbeiten und speichern vertrauliche firmeninterne Daten wie medizinische Unterlagen, juristische Dokumente und Betrugsermittlungen. Daher müssen Systemadministratoren für diese virtuellen Maschinen den höchsten Schutz gewährleisten.

Diese virtuellen Maschinen sind über ihren eigenen virtuellen Switch und physischen Netzwerkadapter an das Interne Netzwerk 2 angeschlossen. Das interne Netzwerk 2 ist der internen Nutzung durch Mitarbeiter wie Reklamationsbearbeiter, firmeninterne Anwälte und andere Sachbearbeiter vorbehalten.

Die virtuellen Maschinen 2 bis 5 können über den virtuellen Switch untereinander und über den physischen Netzwerkadapter mit internen Maschinen an anderen Stellen des internen Netzwerks 2 kommunizieren. Sie können nicht mit Computern oder virtuellen Maschinen kommunizieren, die Zugang zu den externen Netzwerken haben. Wie beim FTP-Server können diese virtuellen Maschinen keine Datenpakete an Netzwerke anderer virtueller Maschinen senden oder sie von diesen empfangen. Ebenso können die anderen virtuellen Maschinen keine Datenpakete an die virtuellen Maschinen 2 bis 5 senden oder von diesen empfangen.

DMZ

Die virtuellen Maschinen 6 bis 8 wurden als DMZ konfiguriert, die von der Marketingabteilung dazu verwendet wird, die externe Website des Unternehmens bereitzustellen.

Diese Gruppe virtueller Maschinen ist dem externen Netzwerk 2 und dem internen Netzwerk 1 zugeordnet. Das Unternehmen nutzt das externe Netzwerk 2 zur Unterstützung der Webserver, die von der Marketing- und der Finanzabteilung zur Bereitstellung der Unternehmenswebsite und anderer webbasierter Anwendungen für externe Nutzer verwendet werden. Das interne Netzwerk 1 ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung des Inhalts von der Unternehmenswebsite, zur Bereitstellung von Downloads und Diensten wie Benutzerforen verwendet.

Da diese Netzwerke vom externen Netzwerk 1 und vom internen Netzwerk 2 getrennt sind und die virtuellen Maschinen keine gemeinsamen Kontaktpunkte (Switches oder Adapter) aufweisen, besteht kein Angriffsrisiko für den FTP-Server oder die Gruppe interner virtueller Maschinen (weder als Ausgangspunkt noch als Ziel).

Wenn die Isolierung der virtuellen Maschinen genau beachtet wird, die virtuellen Switches ordnungsgemäß konfiguriert werden und die Netzwerktrennung eingehalten wird, können alle drei Zonen der virtuellen Maschinen auf dem gleichen ESXi-Host untergebracht werden, ohne dass Datenverluste oder Ressourcenmissbräuche befürchtet werden müssen.

Das Unternehmen erzwingt die Isolierung der virtuellen Maschinengruppen durch die Verwendung mehrerer interner und externer Netzwerke und die Sicherstellung, dass die virtuellen Switches und physischen Netzwerkadapter jeder Gruppe von denen anderer Gruppen vollständig getrennt sind.

Da keiner der virtuellen Switches sich über mehrere Zonen erstreckt, wird das Risiko des Durchsickerns von Daten von einer Zone in eine andere ausgeschaltet. Ein virtueller Switch kann aufbaubedingt keine Datenpakete direkt an einen anderen virtuellen Switch weitergeben. Datenpakete können nur unter folgenden Umständen von einem virtuellen Switch zu einem anderen gelangen:

- Wenn die virtuellen Switches an das gleiche physische LAN angeschlossen sind
- Wenn die virtuellen Switches an eine gemeinsame virtuelle Maschine angeschlossen sind, die dann dazu verwendet werden kann, Datenpakete zu übertragen.

In der Beispielkonfiguration wird keine dieser Bedingungen erfüllt. Wenn die Systemadministratoren sicherstellen möchten, dass es keine gemeinsamen virtuellen Switch-Pfade gibt, können sie mögliche gemeinsame Kontaktpunkte suchen, indem sie den Netzwerk-Switch-Plan im vSphere-Client überprüfen.

Zum Schutz der Hardwareressourcen der virtuellen Maschinen kann der Systemadministrator eine Reservierung und Einschränkung der Ressourcen für jede virtuelle Maschine vornehmen, um das Risiko von DoS- und DDoS-Angriffen einzudämmen. Der Systemadministrator kann den ESXi-Host und die virtuellen Maschinen außerdem durch die Installation von Softwarefirewalls im Front-End und Back-End der DMZ, durch Positionierung des ESXi-Hosts hinter einer physischen Firewall und der an das Netzwerk angeschlossenen Speicherressourcen an jeweils einen eigenen virtuellen Switch schützen.

Sonstige Quellen und Informationen zur Sicherheit

Weitere Informationen zur Sicherheit erhalten Sie auf der VMware-Website.

Tabelle 11-1 enthält eine Auflistung der Sicherheitsthemen und den Ort der dazugehörigen zusätzlichen Informationen.

Tabelle 11-1. Sicherheitsressourcen von VMware im Internet

Thema	Ressource
Sicherheitsrichtlinien von VMware, aktuelle Sicherheitswarnungen, Sicherheitsdownloads und themenspezifische Abhandlungen zu Sicherheitslücken	http://www.vmware.com/security/
Richtlinie zur Sicherheitsantwort	http://www.vmware.com/support/policies/security_response.html VMware hat es sich zur Aufgabe gemacht, Sie bei der Absicherung Ihrer virtuellen Umgebung zu unterstützen. Sicherheitslücken werden so schnell wie möglich beseitigt. Die VMware-Richtlinie zur Sicherheitsantwort dokumentiert unseren Einsatz für die Behebung möglicher Schwachstellen in unseren Produkten.
Richtlinie zur Unterstützung von Drittanbieter-Software	http://www.vmware.com/support/policies/ VMware unterstützt viele Speichersysteme und Software-Agenten wie Sicherungs-Agenten, Systemverwaltungs-Agenten usw. Ein Verzeichnis der Agenten, Werkzeuge und anderer Software, die ESXi unterstützen, finden Sie, indem Sie http://www.vmware.com/vmtn/resources/ nach ESXi-Kompatibilitätshandbüchern suchen. Die Branche bietet mehr Produkte und Konfigurationen an, als VMware testen kann. Wenn VMware ein Produkt oder eine Konfiguration nicht in einem Kompatibilitätshandbuch nennt, wird der technische Support versuchen, Ihnen bei Problemen zu helfen, kann jedoch nicht garantieren, dass das Produkt oder die Konfiguration verwendet werden kann. Testen Sie die Sicherheitsrisiken für nicht unterstützte Produkte oder Konfigurationen immer sorgfältig.
Zertifizierung von VMware Produkten	http://www.vmware.com/security/certifications/

Absichern einer ESXi-Konfiguration

Sie können mithilfe von bestimmten Maßnahmen die Umgebung für Ihre ESXi-Hosts, virtuellen Maschinen und iSCSI-SANs absichern. Beachten Sie den sicherheitsbezogenen Netzwerkkonfigurationsaufbau und die Maßnahmen, mit denen Sie die Komponenten in Ihrer Konfiguration vor Angriffen schützen können.

Dieses Kapitel behandelt die folgenden Themen:

- [„Absichern des Netzwerks mit Firewalls“](#), auf Seite 143
- [„Absichern virtueller Maschinen durch VLANs“](#), auf Seite 150
- [„Absichern der Ports virtueller Switches“](#), auf Seite 154
- [„Absichern von iSCSI-Speicher“](#), auf Seite 156

Absichern des Netzwerks mit Firewalls

Sicherheitsadministratoren verwenden Firewalls, um das Netzwerk oder ausgewählte Komponenten innerhalb des Netzwerks vor unerlaubten Zugriffen zu schützen.

Firewalls kontrollieren den Zugriff auf die Geräte in ihrem Umfeld, indem sie alle Kommunikationspfade außer denen abriegeln, die der Administrator explizit oder implizit als zulässig definiert. Diese Pfade, die der Administrator in der Firewall öffnet, werden Ports genannt und lassen Datenverkehr zwischen Geräten auf den beiden Seiten der Firewall passieren.

ESXi enthält keine Firewall, da es eine begrenzte Gruppe bekannter Dienste ausführt und das Hinzufügen weiterer Dienste nicht zulässt. Bei solchen Einschränkungen reduziert sich die Anzahl der Faktoren, die eine Firewall erforderlich machen, beträchtlich.

In ESXi ist keine Firewall integriert. Sie müssen einen Satz von Sicherheitstechnologien bereitstellen, der Ihren Anforderungen entspricht. Sie können beispielsweise eine Firewall zum Filtern des ein- und ausgehenden Datenverkehrs in einem Netzwerksegment installieren, in dem Sie ESXi installiert haben.

In der virtuellen Maschinenumgebung können Sie Ihr Layout für die Firewalls zwischen den Komponenten planen.

- Physische Maschinen, z. B. vCenter Server-Hosts und ESXi-Hosts.
- Zwischen zwei virtuellen Maschinen – beispielsweise zwischen einer virtuellen Maschine, die als externer Webserver dient, und einer virtuellen Maschine, die an das interne Firmennetzwerk angeschlossen ist.
- Zwischen einem physischen Computer und einer virtuellen Maschine, wenn Sie eine Firewall zwischen einen physischen Netzwerkadapter und eine virtuelle Maschine schalten.

Die Nutzung von Firewalls in einer ESXi-Konfiguration hängt davon ab, wie Sie das Netzwerk nutzen möchten und wie sicher die einzelnen Komponenten sein müssen. Wenn Sie zum Beispiel ein virtuelles Netzwerk erstellen, in dem jede virtuelle Maschine eine andere Benchmark-Testsuite für die gleiche Abteilung ausführt, ist das Risiko ungewollten Zugriffs von einer virtuellen Maschine auf eine andere minimal. Eine Konfiguration,

bei der Firewalls zwischen den virtuellen Maschinen vorhanden sind, ist daher nicht erforderlich. Um jedoch eine Störung der Testläufe durch einen externen Host zu verhindern, kann die Konfiguration so eingerichtet werden, dass sich eine Firewall am Eingang zum virtuellen Netzwerk befindet, um alle virtuellen Maschinen zu schützen.

Firewalls in Konfigurationen mit vCenter Server

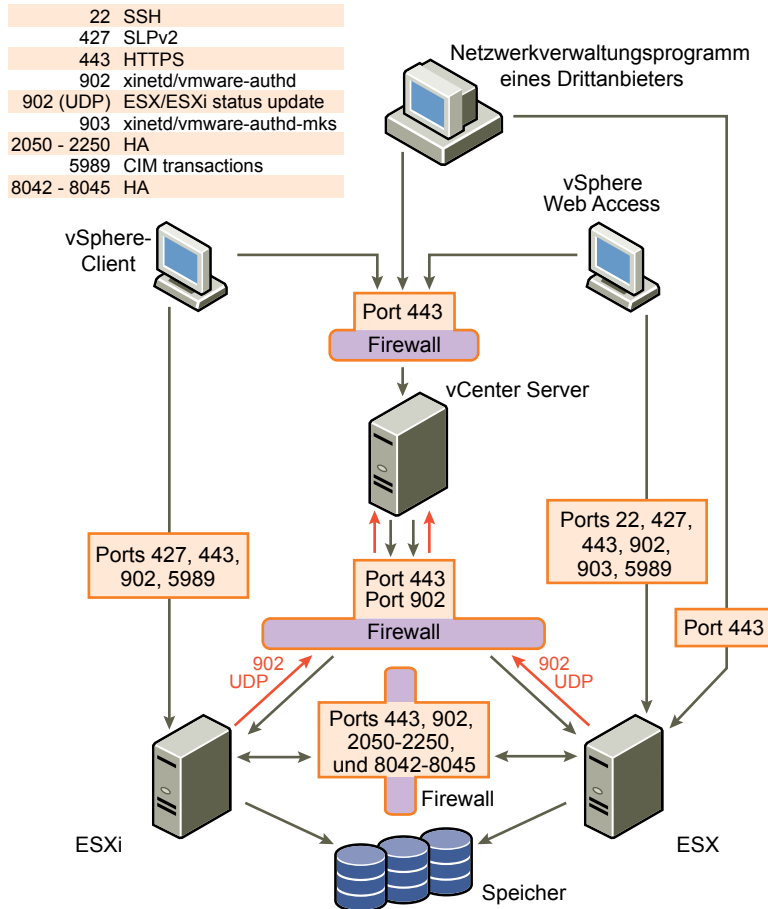
Wenn Sie über vCenter Server auf ESXi-Hosts zugreifen, schützen Sie vCenter Server normalerweise durch eine Firewall. Diese Firewall bietet einen Grundschutz für das Netzwerk.

Zwischen den Clients und vCenter Server kann sich ein Firewall befinden. Abhängig vom Netzwerkaufbau können sich aber auch sowohl der vCenter Server als auch die Clients hinter einer Firewall befinden. Wichtig ist es sicherzustellen, dass eine Firewall an den Punkten vorhanden ist, die Sie als Eingangspunkte in das System betrachten.

Wenn Sie vCenter Server verwenden, können Sie Firewalls an allen in [Abbildung 12-1](#) genannten Speicherorten installieren. Abhängig von der Konfiguration sind ggf. nicht alle in der Abbildung dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig. Zudem enthält Ihre Konfiguration möglicherweise optionale Module, z. B. VMware vCenter Update Manager, die nicht angezeigt werden. Weitere Informationen über Firewall-Setups für Produkte wie Update Manager finden Sie in der Dokumentation.

Einer umfassende Liste der TCP- und UDP-Ports, darunter die Ports für VMware VMotion™ und VMware Fault Tolerance finden Sie unter „[TCP- und UDP-Ports für den Verwaltungszugriff](#)“, auf Seite 148.

Abbildung 12-1. Beispiel für eine vSphere-Netzwerkkonfiguration und den Datenfluss



Netzwerke, die über vCenter Server konfiguriert werden, können Daten über den vSphere-Client oder Netzwerkverwaltungs-Clients von Drittanbietern erhalten, die über das SDK eine Schnittstelle zum Host einrichten. Während des normalen Betriebs wartet vCenter Server an bestimmten Ports auf Daten von verwalteten Hosts und Clients. vCenter Server geht auch davon aus, dass die verwalteten Hosts an bestimmten Ports auf Daten von vCenter Server warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass Firewall-Ports für den Datenverkehr geöffnet wurden.

Firewalls können auch an vielen anderen Zugriffspunkten im Netzwerk installiert werden. Dies hängt von der Sicherheitsebene, die für die verschiedenen Geräte benötigt wird, sowie davon ab, wie das Netzwerk genutzt werden soll. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken, die eine Analyse der Netzwerkkonfiguration ergeben hat. Die folgende Liste führt verschiedene Installationspunkte für Firewalls auf, die in ESXi-Implementierungen häufig auftreten. Viele der Installationspunkte für Firewalls in der Liste und [Abbildung 12-1](#) sind optional.

- Zwischen dem vSphere-Client oder einem Netzwerkverwaltungs-Client eines Drittanbieters und vCenter Server.
- Wenn die Benutzer über den vSphere-Client auf virtuelle Maschinen zugreifen, zwischen dem vSphere-Client und dem ESXi-Host. Diese Verbindung ist ein Zusatz zu der Verbindung zwischen dem vSphere-Client und vCenter Server und benötigt einen anderen Port.
- Zwischen vCenter Server und den ESXi-Hosts.
- Zwischen den ESXi-Hosts in Ihrem Netzwerk. Zwar ist der Datenverkehr zwischen Hosts normalerweise vertrauenswürdig, aber Sie können bei befürchteten Sicherheitsrisiken zwischen den einzelnen Computern dennoch Firewalls zwischen den Hosts installieren.

Wenn Sie Firewalls zwischen ESXi-Hosts verwenden und virtuelle Maschinen auf einen anderen Server verschieben, klonen oder VMotion verwenden möchten, müssen Sie auch Ports in allen Firewalls zwischen Quell- und Zielhost öffnen, damit Quelle und Ziel miteinander kommunizieren können.

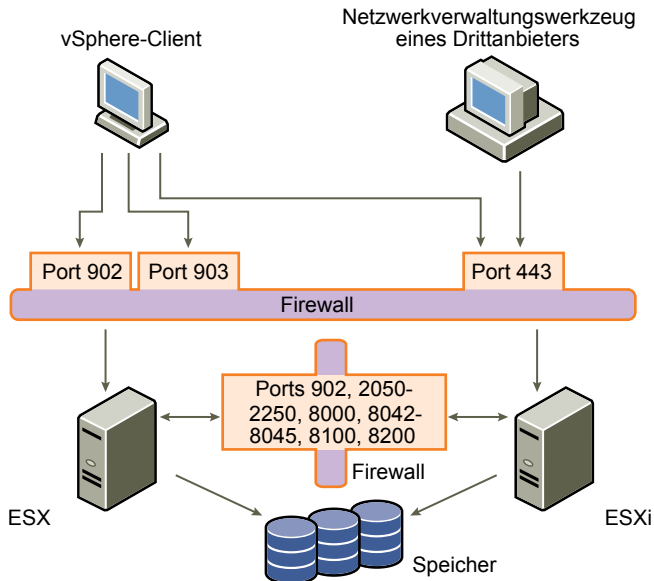
- Zwischen ESXi-Hosts und Netzwerkspeicher, z. B. NFS- oder iSCSI-Speicher. Diese Ports sind nicht VMware-spezifisch und werden anhand der Spezifikationen für das jeweilige Netzwerk konfiguriert.

Firewalls für Konfigurationen ohne vCenter Server

Wenn Sie Clients direkt an Ihr ESXi-Netzwerk anbinden anstatt über vCenter Server, gestaltet sich die Konfiguration Ihrer Firewall etwas einfacher.

Firewalls können an jeder der in [Abbildung 12-2](#) gezeigten Stellen installiert werden.

HINWEIS Abhängig von der Konfiguration sind ggf. nicht alle in der Abbildung dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig.

Abbildung 12-2. Firewall-Konfiguration für ESXi-Netzwerke, die direkt über einen Client verwaltet werden

Netzwerke ohne vCenter Server erhalten ihre Daten über die gleichen Typen von Clients wie Netzwerke mit vCenter Server: vSphere-Clients oder Netzwerkverwaltungsclients von Drittanbietern. Größtenteils sind die Anforderungen der Firewall die gleichen, aber es gibt einige markante Unterschiede.

- Wie bei Konfigurationen mit vCenter Server sollten Sie sicherstellen, dass Ihre ESXi-Ebene oder, je nach Konfiguration, Ihre Clients und die ESXi-Ebene geschützt sind. Diese Firewall bietet einen Grundschutz für das Netzwerk. Die verwendeten Firewallports sind die gleichen wie bei der Verwendung von vCenter Server.
- Die Lizenzierung gehört in dieser Konfiguration zu dem ESXi-Paket, das Sie auf allen Hosts installieren. Da die Lizenzierung über den Server abgewickelt wird, ist kein getrennter Lizenzserver erforderlich. Dadurch entfällt die Firewall zwischen dem Lizenzserver und dem ESXi-Netzwerk.

Herstellen einer Verbindung mit einem vCenter Server über eine Firewall

Der von vCenter Server zum Überwachen der von seinen Clients ausgehenden Datenübertragung verwendete Standardport ist Port 443. Wenn zwischen vCenter Server und seinen Clients eine Firewall vorhanden ist, müssen Sie eine Verbindung konfigurieren, über die vCenter Server Daten von seinen Clients empfangen kann.

Geben Sie in der Firewall Port 443 frei, damit der vCenter Server Daten von dem vSphere-Client empfangen kann. Bei weiteren Fragen zum Konfigurieren der Ports in der Firewall wenden Sie sich an Ihren Firewall-Administrator.

Wenn Sie den vSphere-Client verwenden und nicht Port 443 als Port für den Datenverkehr zwischen vSphere-Client und vCenter Server verwenden möchten, können Sie den Port über die vCenter Server-Einstellungen auf dem vSphere-Client ändern. Informationen zur Änderung dieser Einstellungen finden Sie in *Grundlagen der Systemverwaltung*.

Herstellen einer Verbindung mit der VM-Konsole über eine Firewall

Sowohl bei der Anbindung des Clients an die ESXi-Hosts über vCenter Server als auch bei der Verwendung einer direkten Verbindung mit dem Host sind bestimmte Ports für die Kommunikation zwischen Administrator bzw. Benutzer und den Konsolen für virtuelle Maschinen notwendig. Diese Ports unterstützen verschiedene Clientfunktionen, verbinden unterschiedliche Ebenen innerhalb von ESXi und verwenden verschiedene Authentifizierungsprotokolle.

Port 902

Dies ist der Port, den vCenter Server für den Empfang von Daten vom ESXi-Host als verfügbar erachtet. Der vSphere-Client nutzt diesen Port für Verbindungen der Maus-/Tastatur-/Bildschirmaktivitäten des Gastbetriebssystems auf virtuellen Maschinen. Die Benutzer interagieren über diesen Port mit dem Gastbetriebssystem und den Anwendungen der virtuellen Maschine. Port 902 ist der Port, den der vSphere-Client für verfügbar hält, wenn mit virtuellen Maschinen kommuniziert wird.

Port 902 verbindet vCenter Server mit dem Host über den VMware Authorization Daemon (`vmware-authd`). Dieser Daemon überträgt anschließend Daten an Port 902 zur Verarbeitung an die entsprechenden Empfänger. VMware unterstützt für diese Verbindung nur diesen Port.

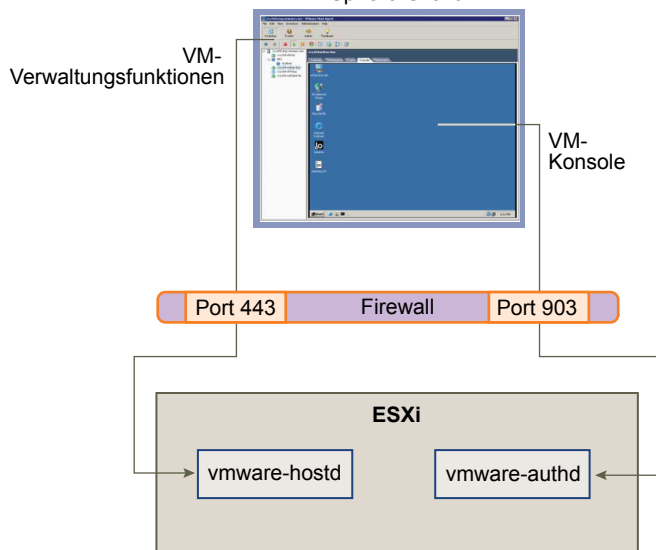
Port 443

Der vSphere-Client und die SDK verwenden diesen Port, um Daten an die von vCenter Server verwalteten Hosts zu senden. Auch der vSphere-Client und SDK verwenden diesen Port, wenn sie direkt mit dem ESXi-Host verbunden sind, um Verwaltungsfunktionen für den Server und seine virtuellen Maschinen durchzuführen. Port 443 ist der Port, den die Clients für verfügbar halten, wenn Daten an den ESXi-Host gesendet werden. VMware unterstützt für diese Verbindungen nur diesen Port.

Port 443 verbindet Clients mit dem ESXi-Host über das SDK. `vmware-hostd` überträgt anschließend Daten an Port 443 zur Verarbeitung an die entsprechenden Empfänger.

Abbildung 12-3 zeigt die Beziehungen zwischen vSphere-Client-Funktionen, Ports und ESXi-Prozessen.

Abbildung 12-3. Port-Verwendung für vSphere-Clientdatenverkehr mit ESXi



Wenn Sie zwischen dem vCenter Server-System und dem von vCenter Server verwalteten Host eine Firewall installiert haben, müssen Sie die Ports 443 und 902 in der Firewall öffnen, um Datenverkehr von vCenter Server zu den ESXi-Hosts und vom vSphere-Client direkt zu den ESXi-Hosts zuzulassen.

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewalladministrator.

Verbinden von ESXi-Hosts über Firewalls

Wenn Sie eine Firewall zwischen zwei ESXi-Hosts eingerichtet haben und Datenübertragungen zwischen den Hosts ermöglichen möchten oder mit vCenter Server Quell/Ziel-Aktivitäten wie Datenverkehr im Rahmen von VMware High Availability (HA), Migrationen, Klonen oder VMotion durchführen möchten, müssen Sie eine Verbindung konfigurieren, über die die verwalteten Hosts Daten empfangen können.

Um eine Verbindung für den Empfang von Daten zu konfigurieren, öffnen Sie folgende Ports:

- 902 (für Server-zu-Server-Migration- und Bereitstellungsdatenverkehr)
- 2050-2250 (für HA-Datenverkehr)
- 8000 (für VMotion)
- 8042–8045 (für HA-Datenverkehr)

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewall-Administrator.

Konfigurieren von Firewallports für unterstützte Dienste und Verwaltungs-Agenten

Sie müssen in Ihrer Umgebung Firewalls so konfigurieren, dass die allgemein unterstützten Dienste und installierten Verwaltungs-Agenten akzeptiert werden.

Obwohl ESXi selbst keine Firewall hat, müssen Sie in Ihrer Umgebung andere Firewalls so konfigurieren, dass Dienste und Verwaltungs-Agenten akzeptiert werden.

In einer vSphere-Umgebung sind üblicherweise die folgenden Dienste und Agenten vorhanden:

- NFS-Client (unsicherer Dienst)
- NTP-Client
- iSCSI-Software-Client
- CIM-HTTP-Server (unsicherer Dienst)
- CIM-HTTPS-Server
- Syslog-Client

HINWEIS Die aufgeführten Dienste und Agenten können sich ändern, sodass die Liste ggf. einige Dienste und Agenten nicht enthält. Zur Konfiguration und Aktivierung dieser Dienste sind gegebenenfalls weitere Aktivitäten erforderlich.

TCP- und UDP-Ports für den Verwaltungszugriff

Auf vCenter Server, ESXi-Hosts und andere Netzwerkkomponenten erfolgt der Zugriff über vorab festgelegte TCP- und UDP-Ports. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

[Tabelle 12-1](#) enthält eine Auflistung von TCP- und UDP-Ports mit dem jeweiligen Zweck und Typ.

Tabelle 12-1. TCP- und UDP-Ports

Port	Zweck	Art des Datenverkehrs
80	HTTP-Zugriff Nicht abgesicherter Standard-TCP-Webport, der normalerweise in Verbindung mit Port 443 als Front-End zum Zugriff auf ESXi-Netzwerke vom Internet aus verwendet wird. Port 80 leitet Datenverkehr auf eine HTTPS-Startseite (Port 443) um. WS-Verwaltung	Eingehendes TCP
123	NTP-Client	Ausgehendes UDP
427	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.	Ein- und ausgehendes UDP
443	HTTPS-Zugriff vCenter Server-Zugriff auf ESXi-Hosts Standard-SSL-Webport. vSphere-Clientzugriff auf vCenter Server vSphere-Client -Zugriff auf ESXi-Hosts WS-Verwaltung vCenter Server-Zugriff auf vSphere Update Manager vSphere Converter-Zugriff auf vCenter Server	Eingehendes TCP
902	Hostzugriff auf andere Hosts für Migration und Bereitstellung. Authentifizierungsverkehr für ESXi- und Remotekonsolenverkehr (xinetd/vmware-authd) vSphere-Client-Zugriff auf die Konsolen virtueller Maschinen (UDP) Statusaktualisierungsverbindung (Taktsignal) von ESXi mit dem vCenter Server	Eingehendes TCP, ausgehendes UDP
2049	Datenübertragungen von den NFS-Speichergeräten Dieser Port wird für die VMkernel-Schnittstelle verwendet.	Ein- und ausgehendes TCP
2050–2250	Datenverkehr zwischen ESXi-Hosts für VMware High Availability (HA) und EMC Autostart Manager	Ausgehendes TCP, ein- und ausgehendes UDP
3260	Transaktionen an die iSCSI-Speichergeräte. Dieser Port wird für die VMkernel-Schnittstelle verwendet.	Ausgehendes TCP
5900-5964	RFB-Protokoll, das von Verwaltungstools wie VNC verwendet wird	Ein- und ausgehendes TCP
5989	CIM-XML-Übertragungen über HTTPS	Ein- und ausgehendes TCP
8000	Anforderungen von VMotion.	Ein- und ausgehendes TCP
8042–8045	Datenverkehr zwischen ESXi-Hosts für HA und EMC Autostart Manager	Ausgehendes TCP, ein- und ausgehendes UDP
8100, 8200	Datenverkehr zwischen ESXi-Hosts für VMware-Fehlertoleranz	Ausgehendes TCP, ein- und ausgehendes UDP

Zusätzlich zu den aufgeführten TCP- und UDP-Ports können Sie andere Ports je nach Bedarf konfigurieren. Mit dem vSphere-Client können Sie Ports für installierte Verwaltungs-Agenten und unterstützte Dienste wie NFS freigeben.

Absichern virtueller Maschinen durch VLANs

Das Netzwerk gehört zu den gefährdetsten Teilen eines jeden Systems. Ihre VM-Netzwerk muss genauso wie ihr physisches Netzwerk geschützt werden. Sie können Ihr Netzwerk der virtuellen Maschinen auf verschiedene Weise absichern.

Wenn das Netzwerk virtueller Maschinen an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Computern besteht. Selbst wenn das virtuelle Maschinennetzwerk nicht an ein physisches Netzwerk angeschlossen ist, kann ein Angriff auf virtuelle Maschinen innerhalb des Netzwerks von anderen virtuellen Maschinen des Netzwerks aus erfolgen. Die Anforderungen an die Absicherung virtueller Maschinen sind oft die gleichen wie für physische Maschinen.

Virtuelle Maschinen sind voneinander isoliert. Eine virtuelle Maschine kann weder Lese- noch Schreiboperationen im Speicher der anderen virtuellen Maschine ausführen noch auf deren Daten zugreifen, ihre Anwendungen verwenden usw. Im Netzwerk kann jedoch jede virtuelle Maschine oder eine Gruppe virtueller Maschinen Ziel eines unerlaubten Zugriffs von anderen virtuellen Maschinen sein und daher weiteren Schutzes durch externe Maßnahmen bedürfen.

Sie können die Sicherheit durch unterschiedliche Maßnahmen erhöhen:

- Hinzufügen von Firewallschutz für das virtuelle Netzwerk durch Installation und Konfiguration von Softwarefirewalls auf einigen oder allen virtuellen Maschinen im Netzwerk.

Aus Effizienzgründen können Sie private Ethernet-Netzwerke virtueller Maschinen oder Virtuelle Netzwerke einrichten. Bei virtuellen Netzwerken installieren Sie eine Softwarefirewall auf einer virtuellen Maschine am Eingang des virtuellen Netzwerks. Diese dient als Schutzpufferzone zwischen dem physischen Netzwerkadapter und den übrigen virtuellen Maschinen im virtuellen Netzwerk.

Die Installation einer Softwarefirewall auf virtuellen Maschinen am Eingang eines virtuellen Netzwerks ist eine bewährte Sicherheitsmaßnahme. Da jedoch Softwarefirewalls die Leistung verlangsamen können, sollten Sie Sicherheitsbedürfnisse und Leistungsanforderungen abwägen, bevor Sie Softwarefirewalls in anderen virtuellen Maschinen im Netzwerk installieren.

- Beibehalten verschiedener Zonen aus virtuellen Maschinen innerhalb eines Hosts auf verschiedenen Netzwerksegmenten. Wenn Sie virtuelle Maschinenzonen in deren eigenen Netzwerksegmenten isolieren, minimieren Sie das Risiko eines Datenverlusts aus einer virtuellen Maschinenzone in die nächste. Die Segmentierung verhindert mehrere Gefahren. Zu diesen Gefahren gehört auch die Manipulation des Adressauflösungsprotokolls (ARP), wobei der Angreifer die ARP-Tabelle so manipuliert, dass die MAC- und IP-Adressen neu zugeordnet werden, wodurch ein Zugriff auf den Netzwerkdatenverkehr vom und zum Host möglich ist. Angreifer verwenden diese ARP-Manipulierung für Denial of Service-Angriffe (DOS), zur Übernahme des Zielsystems und zur anderweitigen Beeinträchtigung des virtuellen Netzwerks.

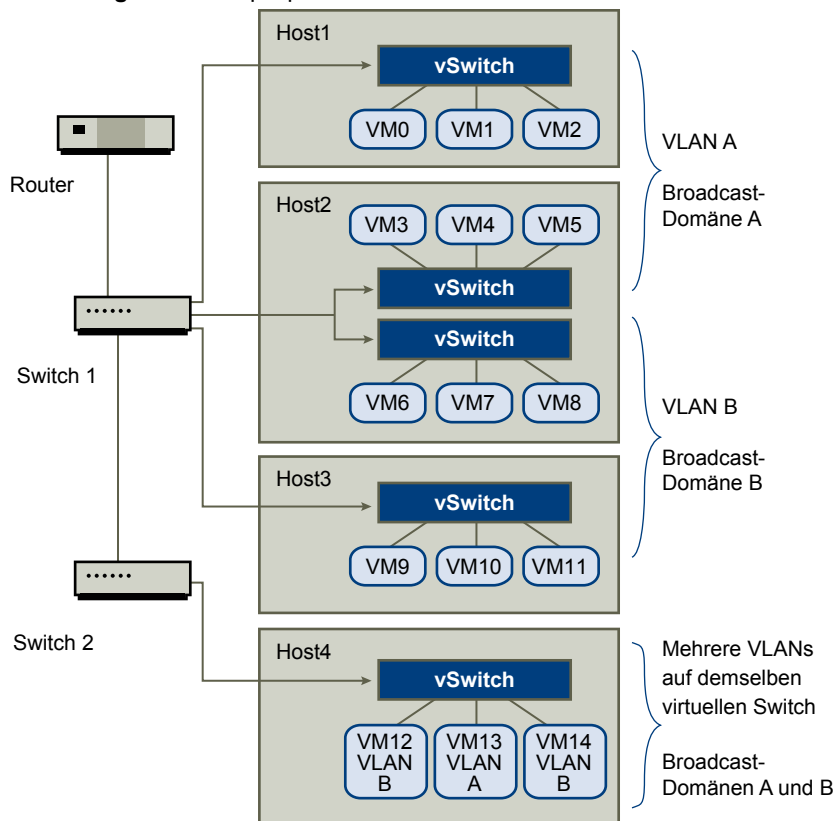
Eine sorgfältige Planung der Segmentierung senkt das Risiko von Paketübertragungen zwischen virtuellen Maschinenzonen und somit von Spionageangriffen, die voraussetzen, dass dem Opfer Netzwerkdatenverkehr zugestellt wird. So kann ein Angreifer auch keinen unsicheren Dienst in einer virtuellen Maschinenzone aktivieren, um auf andere virtuelle Maschinenzonen im Host zuzugreifen. Sie können die Segmentierung mit einer der beiden folgenden Methoden herstellen, von denen jede andere Vorteile bietet.

- Verwenden Sie getrennte physische Netzwerkadapter für Zonen virtueller Maschinen, damit die Zonen auch tatsächlich voneinander getrennt sind. Die Beibehaltung getrennter physischer Netzwerkadapter für die virtuellen Maschinenzonen stellt unter Umständen die sicherste Methode dar, und gleichzeitig ist sie am wenigsten anfällig für Konfigurationsfehler nach dem Anlegen des ersten Segments.
- Richten Sie virtuelle LANs (VLANs) zur Absicherung des Netzwerks ein. Da VLANs fast alle Sicherheitsvorteile bieten, die auch die Implementierung physisch getrennter Netzwerke aufweist, ohne dass dafür der Mehraufwand an Hardware eines physischen Netzwerks notwendig ist, stellen sie eine rentable Lösung zur Verfügung, die die Kosten für die Bereitstellung und Wartung zusätzlicher Geräte, Kabel usw. einsparen kann.

VLANs sind eine Netzwerkarchitektur nach dem IEEE-Standard und verfügen über spezifische Kennzeichnungsmethoden, durch die Datenpakete nur an die Ports weitergeleitet werden, die zum VLAN gehören. Wenn das VLAN ordnungsgemäß konfiguriert ist, ist es ein zuverlässiges Mittel zum Schutz einer Gruppe virtueller Maschinen vor zufälligem und böswilligem Eindringen.

Mit VLANs können Sie ein physisches Netzwerk so in Segmente aufteilen, dass zwei Computer oder virtuelle Maschinen im Netzwerk nur dann Pakete untereinander austauschen können, wenn sie zum gleichen VLAN gehören. So gehören zum Beispiel Buchhaltungsunterlagen und -transaktionen zu den wichtigsten vertraulichen internen Informationen eines Unternehmens. Wenn in einem Unternehmen die virtuellen Maschinen der Verkaufs-, Logistik- und Buchhaltungsmitarbeiter an das gleiche physische Netzwerk angeschlossen sind, können Sie die virtuellen Maschinen für die Buchhaltungsabteilung schützen, indem Sie VLANs wie in [Abbildung 12-4](#) einrichten.

Abbildung 12-4. Beispielplan eines VLAN



Bei dieser Konfiguration verwenden alle Mitarbeiter der Buchhaltungsabteilung virtuelle Maschinen im VLAN A, die Mitarbeiter der Vertriebsabteilung verwenden die virtuellen Maschinen im VLAN B.

Der Router leitet die Datenpakete mit Buchhaltungsdaten an die Switches weiter. Diese Pakete sind so gekennzeichnet, dass sie nur an VLAN A weitergeleitet werden dürfen. Daher sind die Daten auf die Broadcast-Domäne A beschränkt und können nur an die Broadcast-Domäne B weitergeleitet werden, wenn der Router entsprechend konfiguriert wurde.

Bei dieser VLAN-Konfiguration wird verhindert, dass Mitarbeiter des Vertriebs Datenpakete abfangen können, die für die Buchhaltungsabteilung bestimmt sind. Die Buchhaltungsabteilung kann zudem auch keine Datenpakete empfangen, die für den Vertrieb bestimmt sind. Virtuelle Maschinen, die an einen gemeinsamen virtuellen Switch angebunden sind, können sich dennoch in unterschiedlichen VLANs befinden.

Sicherheitsempfehlungen für VLANs

Wie Sie die VLANs einrichten, um Teile eines Netzwerks abzusichern, hängt von Faktoren wie dem Gastbetriebssystem und der Konfiguration der Netzwerkgeräte ab.

ESXi ist mit einer vollständigen VLAN-Implementierung nach IEEE 802.1q ausgestattet. Zwar kann VMware keine spezifischen Empfehlungen aussprechen, wie die VLANs eingerichtet werden sollten, es sollten jedoch bestimmte Faktoren berücksichtigt werden, wenn ein VLAN ein Bestandteil Ihrer Sicherheitsrichtlinien ist.

VLANs im Rahmen eines Sicherheitspakets

Mit VLANs kann effektiv gesteuert werden, wo und in welchem Umfang Daten im Netzwerk übertragen werden. Wenn ein Angreifer Zugang zum Netzwerk erlangt, wird der Angriff mit hoher Wahrscheinlichkeit nur auf das VLAN beschränkt, das als Zugangspunkt diente, wodurch das Risiko für das gesamte Netzwerk verringert wird.

VLANs bieten nur dadurch Schutz, dass sie steuern, wie Daten weitergeleitet und verarbeitet werden, nachdem sie die Switches passiert haben und sich im Netzwerk befinden. Sie können VLANs dazu nutzen, die 2. Schicht des Netzwerkmodells, die Sicherungsschicht, zu schützen. Die Einrichtung von VLANs schützt jedoch weder die Bitübertragungsschicht noch die anderen Schichten. Auch bei der Verwendung von VLANs sollten Sie zusätzlichen Schutz durch Absicherung der Hardware (Router, Hubs usw.) und Verschlüsselung der Datenübertragungen implementieren.

VLANs ersetzen Softwarefirewalls in den Konfigurationen virtueller Maschinen nicht. In den meisten Netzwerkkonfigurationen mit VLANs gibt es auch Softwarefirewalls. Wenn Sie VLANs in Ihr virtuelles Netzwerk implementieren, stellen Sie sicher, dass die installierten Firewalls SAN-fähig sind.

Ordnungsgemäßes Konfigurieren von VLANs

Eine Fehlkonfiguration der Ausstattung und Netzwerkhardware, -firmware oder -software setzt ein VLAN möglichen VLAN-Hopping-Angriffen aus.

VLAN-Hopping tritt dann auf, wenn ein Angreifer mit autorisiertem Zugriff auf ein VLAN Datenpakete erstellt, die die physischen Switches dazu bringen, die Pakete in ein anderes VLAN zu übertragen, für das der Angreifer keine Zugriffsberechtigung besitzt. Anfälligkeit für diese Art von Angriffen liegt meist dann vor, wenn ein Switch falsch für den nativen VLAN-Betrieb konfiguriert wurde, wodurch der Switch nicht gekennzeichnete Pakete empfangen und übertragen kann.

Um ein VLAN-Hopping zu verhindern, aktualisieren Sie stets Ihre Umgebung, indem Sie Updates der Hardware und Firmware sofort aufspielen. Achten Sie bei der Konfiguration Ihrer Umgebung auch stets auf die Einhaltung der Empfehlungen des Herstellers.

Virtuelle Switches von VMware unterstützen nicht das Konzept nativer VLANs. Alle Daten, die über diese Switches übertragen werden, müssen ordnungsgemäß gekennzeichnet werden. Da es jedoch im Netzwerk auch andere Switches geben kann, die für den nativen VLAN-Betrieb konfiguriert wurden, können VLANs mit virtuellen Switches dennoch anfällig für VLAN-Hopping sein.

Wenn Sie VLANs zur Netzwerksicherung verwenden möchten, deaktivieren Sie die native VLAN-Funktion für alle Switches, sofern nicht ein zwingender Grund vorliegt, dass einige VLANs im nativen Modus betrieben werden müssen. Wenn Sie ein natives VLAN verwenden müssen, beachten Sie die Konfigurationsrichtlinien des Switch-Herstellers für diese Funktion.

Schutz durch virtuelle Switches in VLANs

Die virtuellen Switches von VMware schützen gegen bestimmte Bedrohungen der VLAN-Sicherheit. Durch den Aufbau der virtuellen Switches schützen sie VLANs gegen viele Arten von Angriffen, die meist auf VLAN-Hopping basieren.

Dieser Schutz garantiert jedoch nicht, dass Ihre virtuellen Maschinen gegen andere Arten von Angriffen immun sind. So schützen virtuelle Switches zum Beispiel nicht das physische Netzwerk vor diesen Angriffen, sie schützen nur das virtuelle Netzwerk.

Virtuelle Switches und VLANs können gegen folgende Arten von Angriffen schützen:

MAC-Flooding

Diese Angriffe überschwemmen den Switch mit Datenpaketen, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet wurden. Viele Switches verwenden eine assoziative Speichertabelle (CAM-Tabelle), um die Quelladresse für jedes Datenpaket zu speichern. Wenn die Tabelle voll ist, schaltet der Switch ggf. in einen vollständig geöffneten Status um, in dem alle eingehenden Pakete auf allen Ports übertragen werden, sodass der Angreifer den gesamten Datenverkehr des Switches verfolgen kann. In diesem Fall kann es auch zu Paketlecks in andere VLANs kommen.

Zwar speichern die virtuellen Switches von VMware eine MAC-Adressentabelle, aber sie erhalten die MAC-Adressen nicht von erkennbarem Datenverkehr und sind daher gegen diese Art von Angriffen immun.

Angriffe durch 802.1q- und ISL-Kennzeichnung

Bei diesem Angriff werden die Datenblöcke durch den Switch an ein anderes VLAN weitergeleitet, indem der Switch durch einen Trick dazu gebracht wird, als Verbindungsleitung zu fungieren und den Datenverkehr an andere VLANs weiterzuleiten.

Die virtuellen Switches von VMware führen das dynamische Trunking, das für diese Art des Angriffs notwendig ist, nicht aus, und sind daher immun.

Doppelt gekapselte Angriffe

Bei dieser Art von Angriffen erstellt der Angreifer ein doppelt gekapseltes Paket, in dem sich der VLAN-Bezeichner im inneren Tag vom VLAN-Bezeichner im äußeren Tag unterscheidet. Um Rückwärtskompatibilität zu gewährleisten, entfernen native VLANs standardmäßig das äußere Tag von übertragenen Paketen. Wenn ein nativer VLAN-Switch das äußere Tag entfernt, bleibt nur das innere Tag übrig, welches das Paket zu einem anderen VLAN weiterleitet, als im jetzt fehlenden äußeren Tag angegeben war.

Die virtuellen Switches von VMware verwerfen alle doppelt eingekapselten Datenblöcke, die eine virtuelle Maschine auf einem für ein bestimmtes VLAN konfigurierten Port senden möchte. Daher sind sie immun gegen diese Art von Angriffen.

Multicast-Brute-Force-Angriffe

Bei diesen Angriffen wird eine große Anzahl von Multicast-Datenblöcken fast zeitgleich an ein bekanntes VLAN gesendet, um den Switch zu überlasten, damit er versehentlich einige Datenblöcke in andere VLANs überträgt.

Die virtuellen Switches von VMware erlauben es Datenblöcken nicht, ihren richtigen Übertragungsbereich (VLAN) zu verlassen und sind daher gegen diese Art von Angriffen immun.

Spanning-Tree-Angriffe

Diese Angriffe zielen auf das Spanning-Tree-Protokoll (STP), das zur Steuerung der Überbrückung verschiedener Teile des LANs verwendet wird. Der Angreifer sendet Pakete der Bridge Protocol Data Unit (BPDU) in dem Versuch, die Netzwerktopologie zu ändern und sich selbst als Root-Bridge einzusetzen. Als Root-Bridge kann der Angreifer dann die Inhalte übertragener Datenblöcke mitschneiden.

Die virtuellen Switches von VMware unterstützen STP nicht und sind daher gegen diese Art von Angriffen immun.

Zufallsdatenblock-Angriffe

Bei diesen Angriffen wird eine große Anzahl Pakete gesendet, bei denen die Quell- und Zieladressen gleich sind, diese jedoch Felder unterschiedlicher Länge, Art und mit verschiedenem Inhalt enthalten. Ziel des Angriffes ist es zu erzwingen, dass Pakete versehentlich in ein anderes VLAN fehlgeleitet werden.

Die virtuellen Switches von VMware sind gegen diese Art von Angriffen immun.

Da mit der Zeit immer neue Sicherheitsgefahren auftreten, kann diese Liste möglicher Angriffe nicht vollständig sein. Rufen Sie regelmäßig die VMware-Sicherheitsressourcen im Internet ab, um mehr über Sicherheit, neue Sicherheitswarnungen und die Sicherheitstaktiken von VMware zu erfahren.

Absichern der Ports virtueller Switches

Wie bei physischen Netzwerkadaptern kann ein virtueller Netzwerkadapter Datenblöcke versenden, die von einer anderen virtuellen Maschine zu stammen scheinen oder eine andere virtuelle Maschine imitieren, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind. Außerdem kann ein virtueller Netzwerkadapter, genauso wie ein physischer Netzwerkadapter, so konfiguriert werden, dass er Datenblöcke empfängt, die für andere virtuelle Maschinen bestimmt sind.

Wenn Sie einen virtuellen Switch für Ihr Netzwerk erstellen, fügen Sie Portgruppen hinzu, um für die an den Switch angeschlossenen virtuellen Maschinen und Speichersysteme Richtlinien zu konfigurieren. Virtuelle Ports werden über den vSphere-Client erstellt.

Während des Hinzufügens eines Ports oder einer Portgruppe zu einem virtuellen Switch konfiguriert der vSphere-Client ein Sicherheitsprofil für den Port. Mit diesem Sicherheitsprofil können Sie sicherstellen, dass ESXi verhindert, dass die Gastbetriebssysteme auf den virtuellen Maschinen andere Computer im Netzwerk imitieren können. Diese Sicherheitsfunktion wurde so implementiert, dass das Gastbetriebssystem, welches für die Imitation verantwortlich ist, nicht erkennt, dass diese verhindert wurde.

Das Sicherheitsprofil bestimmt, wie streng der Schutz gegen Imitierungs- oder Abfangangriffe auf virtuelle Maschinen sein soll. Damit Sie die Einstellungen des Sicherheitsprofils richtig anwenden können, benötigen Sie Grundkenntnisse darüber, wie virtuelle Netzwerkadapter Datenübertragungen steuern und wie Angriffe auf dieser Ebene vorgenommen werden.

Jedem virtuellen Netzwerkadapter wird bei seiner Erstellung eine eindeutige MAC-Adresse zugewiesen. Diese Adresse wird „Ursprünglich zugewiesene MAC-Adresse“ genannt. Obwohl die ursprüngliche MAC-Adresse von außerhalb des Gastbetriebssystems neu konfiguriert werden kann, kann sie nicht vom Gastbetriebssystem selbst geändert werden. Außerdem verfügt jeder Adapter über eine geltende MAC-Adresse, die eingehenden Netzwerkverkehr mit einer MAC-Adresse, die nicht der geltenden MAC-Adresse entspricht, herausfiltert. Das Gastbetriebssystem ist für die Einstellung der geltenden MAC-Adresse verantwortlich. In der Regel stimmen die geltende MAC-Adresse und die ursprünglich zugewiesene MAC-Adresse überein.

Beim Versand von Datenpaketen schreibt das Betriebssystem die geltende MAC-Adresse des eigenen Netzwerkadapters in das Feld mit der Quell-MAC-Adresse des Ethernet-Frames. Es schreibt auch die MAC-Adresse des Empfänger-Netzwerkadapters in das Feld mit der Ziel-MAC-Adresse. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

Bei der Erstellung stimmen die geltende und die ursprünglich zugewiesene MAC-Adresse überein. Das Betriebssystem der virtuellen Maschine kann die geltenden MAC-Adresse jedoch jederzeit auf einen anderen Wert setzen. Wenn ein Betriebssystem die geltenden MAC-Adresse ändert, empfängt der Netzwerkadapter Netzwerkdatenverkehr, der für die neue MAC-Adresse bestimmt ist. Das Betriebssystem kann jederzeit Frames mit einer imitierten Quell-MAC-Adresse senden. Daher kann ein Betriebssystem böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es einen Netzwerkadapter imitiert, der vom Empfänger-Netzwerk autorisiert wurde.

Mit den Sicherheitsprofilen für den virtuellen Switch auf den ESXi-Hosts können Sie sich gegen diese Art von Angriffen schützen, indem Sie drei Optionen einstellen: Wenn Sie eine Standardeinstellung für einen Port ändern möchten, müssen Sie das Sicherheitsprofil in den Einstellungen des virtuellen Switches im vSphere-Client ändern.

MAC-Adressenänderungen

Die Einstellung der Option **[MAC-Adressenänderungen]** beeinflusst den Datenverkehr, den eine virtuelle Maschine empfängt.

Wenn die Option auf **[Akzeptieren]** festgelegt ist, akzeptiert ESXi Anforderungen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern.

Wenn die Option auf **[Ablehnen]** festgelegt ist, lehnt ESXi Anforderungen ab, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Damit wird der Host vor MAC-Imitationen geschützt. Der Port, der von dem virtuellen Adapter zum Senden der Anforderung verwendet wird, ist deaktiviert, und der virtuelle Adapter erhält keine weiteren Frames mehr, bis er die geltende MAC-Adresse ändert, sodass sie mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Änderung der MAC-Adresse nicht angenommen wurde.

HINWEIS Der iSCSI-Initiator basiert darauf, dass er MAC-Adressänderungen von bestimmten Speichertypen erhalten kann. Wenn Sie ESXi-iSCSI verwenden und über einen iSCSI-Speicher verfügen, legen Sie die Option **[MAC-Adressänderungen]** auf **[Akzeptieren]** fest.

In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk die gleiche MAC-Adresse haben, zum Beispiel wenn Sie den Microsoft-NetzwerkLastausgleich im Unicast-Modus verwenden. Bei Verwendung des Microsoft-NetzwerkLastausgleichs im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

MAC-Adressenänderungen beeinflussen den Datenverkehr, der eine virtuelle Maschine verlässt. MAC-Adressänderungen treten ein, wenn der Absender diese vornehmen darf, selbst wenn vSwitches oder eine empfangende virtuelle Maschine keine MAC-Adressänderungen zulassen.

Gefälschte Übertragungen

Die Einstellung der Option **[Gefälschte Übertragungen]** beeinflusst den Datenverkehr, der von einer virtuellen Maschine versandt wird.

Wenn die Option auf **[Akzeptieren]** festgelegt ist, vergleicht ESXi die Quell- und die geltende MAC-Adresse nicht.

Zum Schutz gegen MAC-Imitation können Sie diese Option auf **[Ablehnen (Reject)]** einstellen. In diesem Fall vergleicht der Host die Quell-MAC-Adresse, die vom Betriebssystem übertragen wird, mit der geltenden MAC-Adresse des Adapters, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht übereinstimmen, verwirft ESXi das Paket.

Das Gastbetriebssystem erkennt nicht, dass der virtuelle Netzwerkadapter die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESXi-Host fängt alle Pakete mit imitierten Adressen vor der Übermittlung ab. Das Gastbetriebssystem geht ggf. davon aus, dass die Pakete verworfen wurden.

Betrieb im Promiscuous-Modus

Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der virtuelle Netzwerkadapter normalerweise ausführen würde, sodass das Gastbetriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt. Standardmäßig kann der virtuelle Netzwerkadapter nicht im Promiscuous-Modus betrieben werden.

Zwar kann der Promiscuous-Modus für die Nachverfolgung von Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, auch wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder Root-Benutzer in einer virtuellen Maschine rein theoretisch den Datenverkehr, der für andere Gast- oder Hostbetriebssysteme bestimmt ist, einsehen kann.

HINWEIS Unter bestimmten Umständen ist es notwendig, einen virtuellen Switch in den Promiscuous-Modus zu setzen, zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paket-Sniffer verwenden.

Absichern von iSCSI-Speicher

Der Speicher, den Sie für einen ESXi-Host konfigurieren, kann ein oder mehrere SANs (Speichernetzwerke) umfassen, die iSCSI verwenden. Wenn Sie iSCSI auf einem ESXi-Host konfigurieren, können Sie diese Sicherheitsrisiken durch verschiedene Maßnahmen minimieren.

iSCSI ist ein Instrument für den Zugriff auf SCSI-Geräte und zum Austausch von Datensätzen, indem das TCP/IP über einen Netzwerkport und nicht über einen direkten Anschluss an ein SCSI-Gerät eingesetzt wird. In iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Datensätze eingekapselt und an das Gerät oder den Benutzer, das/der die Anforderung gestellt hat, übertragen.

iSCSI-SANs ermöglichen die effiziente Verwendung bestehender Ethernet-Infrastrukturen zum Zugriff auf Speicherressourcen durch ESXi-Hosts, die diese Ressourcen dynamisch teilen können. Deshalb bieten iSCSI-SANs eine wirtschaftliche Speicherlösung für Umgebungen, die auf einem gemeinsamen Speicherpool für verschiedene Benutzer basieren. Wie in allen vernetzten Systemen sind auch iSCSI-SANs anfällig für Sicherheitsverletzungen.

HINWEIS Die Anforderungen und Vorgehensweisen für die Absicherung von iSCSI-SANs ähneln denen für Hardware-iSCSI-Adapter, die Sie für ESXi-Hosts und für iSCSI, das direkt über den ESXi-Host konfiguriert wird, verwenden.

Absichern von iSCSI-Geräten über Authentifizierung

iSCSI-Geräte können gegen ungewollten Zugriff abgesichert werden, indem der ESXi-Host, der „Initiator“, vom iSCSI-Gerät, dem „Ziel“, authentifiziert werden muss, wenn der Host versucht, auf Daten in der Ziel-LUN zuzugreifen.

Ziel der Authentifizierung ist es zu überprüfen, dass der Initiator das Recht hat, auf ein Ziel zuzugreifen. Dieses Recht wird bei der Konfiguration der Authentifizierung gewährt.

ESXi unterstützt für iSCSI weder Kerberos noch Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Außerdem unterstützt es keine IPsec-Authentifizierung und -Verschlüsselung.

Mit dem vSphere-Client können Sie bestimmen, ob die Authentifizierung derzeit verwendet wird, und das Authentifizierungsverfahren konfigurieren.

Aktivieren von Challenge-Handshake Authentication Protocol (CHAP) für iSCSI-SANs

Sie können das iSCSI-SAN so konfigurieren, dass die CHAP-Authentifizierung verwendet wird.

Bei der CHAP-Authentifizierung sendet das iSCSI-Ziel, wenn der Initiator mit ihm Kontakt aufnimmt, einen vordefinierten ID-Wert und einen Zufallswert, den Schlüssel, an den Initiator. Der Initiator erstellt einen unidirektionalen Prüfsummenwert, den er an das Ziel sendet. Die Prüfsumme enthält drei Elemente: einen vordefinierten ID-Wert, den Zufallswert, den das Ziel gesendet hat, und einen privaten Wert, den sog. CHAP-Schlüssel, den sowohl der Initiator als auch das Ziel haben. Wenn das Ziel die Prüfsumme vom Initiator erhält, erstellt es aus den gleichen Elementen seine eigene Prüfsumme und vergleicht diese mit dem Prüfsummenwert des Initiators. Wenn die Ergebnisse übereinstimmen, authentifiziert das Ziel den Initiator.

ESXi unterstützt die unidirektionale und die bidirektionale CHAP-Authentifizierung für iSCSI. Bei der unidirektionalen CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel. Bei der bidirektionalen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels.

ESXi unterstützt die CHAP-Authentifizierung auf Adapterebene, wenn nur ein Satz von Anmeldedaten für die Authentifizierung vom Host an alle Ziele gesendet werden kann. Die zielbasierte CHAP-Authentifizierung, bei der verschiedene Anmeldedaten für die Ziele konfiguriert werden können, um eine bessere Zielunterscheidung vornehmen zu können, wird ebenfalls unterstützt.

Weitere Informationen zum Arbeiten mit CHAP finden Sie unter [„Konfigurieren von CHAP-Parametern für iSCSI-Initiatoren“](#), auf Seite 90.

Deaktivieren der iSCSI-SAN-Authentifizierung

Sie können das iSCSI-SAN so konfigurieren, dass die CHAP-Authentifizierung nicht verwendet wird. Der Datenverkehr zwischen Initiator und Ziel wird dennoch rudimentär überprüft, da iSCSI-Zielgeräte normalerweise so eingerichtet sind, dass sie nur mit bestimmten Initiatoren kommunizieren.

Die Deaktivierung einer strengeren Authentifizierung kann zum Beispiel sinnvoll sein, wenn sich der iSCSI-Speicher an einem Standort befindet und ein dediziertes Netzwerk oder VLAN für alle iSCSI-Geräte erstellt wird. Die iSCSI-Konfiguration ist sicher, weil sie von ungewolltem Zugriff isoliert ist, wie dies auch in einem Fibre-Channel-SAN der Fall ist.

Deaktivieren Sie die Authentifizierung grundsätzlich nur dann, wenn Sie einen Angriff auf das iSCSI-SAN riskieren können oder Probleme beheben müssen, die durch menschliches Versagen entstanden sind.

ESXi unterstützt für iSCSI weder Kerberos noch Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Außerdem unterstützt es keine IPsec-Authentifizierung und -Verschlüsselung.

Mit dem vSphere-Client können Sie bestimmen, ob die Authentifizierung derzeit verwendet wird, und das Authentifizierungsverfahren konfigurieren.

Weitere Informationen zum Arbeiten mit CHAP finden Sie unter [„Konfigurieren von CHAP-Parametern für iSCSI-Initiatoren“](#), auf Seite 90.

Schützen eines iSCSI-SAN

Bei der Planung der iSCSI-Konfiguration sollten Sie Maßnahmen zur Verbesserung der allgemeinen Sicherheit des iSCSI-SAN ergreifen. Die iSCSI-Konfiguration ist nur so sicher wie das IP-Netzwerk. Wenn Sie also hohe Sicherheitsstandards bei der Netzwerkeinrichtung befolgen, schützen Sie auch den iSCSI-Speicher.

Nachfolgend sind einige spezifische Vorschläge zum Umsetzen hoher Sicherheitsstandards aufgeführt.

Schützen übertragener Daten

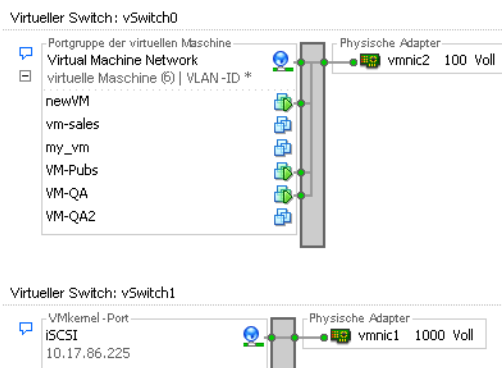
Eines der Hauptrisiken bei iSCSI-SANs ist, dass der Angreifer übertragene Speicherdaten mitschneiden kann.

Ergreifen Sie zusätzliche Maßnahmen, um zu verhindern, dass Angreifer iSCSI-Daten sehen können. Weder der Hardware-iSCSI-Adapter noch der ESXi-Host, d. h. der iSCSI-Initiator, verschlüsseln Daten, die zu und von den Zielen übertragen werden, wodurch die Daten anfälliger für Mitschneideangriffe sind.

Wenn die virtuellen Maschinen die gleichen virtuellen Switches und VLANs wie die iSCSI-Struktur verwenden, ist der iSCSI-Datenverkehr potenziell dem Missbrauch durch Angreifer der virtuellen Maschinen ausgesetzt. Um sicherzustellen, dass Angreifer die iSCSI-Übertragungen nicht überwachen können, achten Sie darauf, dass keine Ihrer virtuellen Maschinen das iSCSI-Speichernetzwerk sehen kann.

Wenn Sie einen Hardware-iSCSI-Adapter verwenden, erreichen Sie dies, indem Sie sicherstellen, dass der iSCSI-Adapter und der physische Netzwerkadapter von ESXi nicht versehentlich außerhalb des Hosts durch eine gemeinsame Verwendung des Switches oder in anderer Form verbunden sind. Wenn Sie iSCSI direkt über den ESXi-Host konfigurieren, können Sie dies erreichen, indem Sie den iSCSI-Speicher über einen anderen virtuellen Switch konfigurieren als denjenigen, der durch Ihre virtuellen Maschinen verwendet wird (siehe [Abbildung 12-5](#)).

Abbildung 12-5. iSCSI-Speicher an einem eigenen virtuellen Switch



Zusätzlich zum Schutz durch einen eigenen virtuellen Switch können Sie das iSCSI-SAN durch die Konfiguration eines eigenen VLAN für das iSCSI-SAN schützen, um Leistung und Sicherheit zu verbessern. Wenn die iSCSI-Konfiguration sich in einem eigenen VLAN befindet, wird sichergestellt, dass keine Geräte außer dem iSCSI-Adapter Einblick in Übertragungen im iSCSI-SAN haben. Auch eine Netzwerküberlastung durch andere Quellen kann den iSCSI-Datenverkehr nicht beeinträchtigen.

Sichern der iSCSI-Ports

Wenn Sie die iSCSI-Geräte ausführen, öffnet der ESXi-Host keine Ports, die Netzwerkverbindungen überwachen. Durch diese Maßnahme wird die Chance, dass ein Angreifer über ungenutzte Ports in den ESXi-Host einbrechen und Kontrolle über ihn erlangen kann, reduziert. Daher stellt der Betrieb von iSCSI kein zusätzliches Sicherheitsrisiko für den ESXi-Host dar.

Beachten Sie, dass auf jedem iSCSI-Zielgerät mindestens ein freigegebener TCP-Port für iSCSI-Verbindungen vorhanden sein muss. Wenn es Sicherheitsprobleme in der Software des iSCSI-Geräts gibt, können die Daten unabhängig von ESXi in Gefahr sein. Installieren Sie alle Sicherheitspatches des Speicherherstellers und beschränken Sie die Anzahl der an das iSCSI-Netzwerk angeschlossenen Geräte, um dieses Risiko zu verringern.

ESXi steuert die Benutzerauthentifizierung und unterstützt Benutzer- und Gruppenberechtigungen. Außerdem können Sie Verbindungen zum vSphere-Client und SDK verschlüsseln.

Dieses Kapitel behandelt die folgenden Themen:

- „Absichern von ESXi über Authentifizierung und Berechtigungen“, auf Seite 159
- „Verschlüsselungs- und Sicherheitszertifikate für ESXi“, auf Seite 167

Absichern von ESXi über Authentifizierung und Berechtigungen

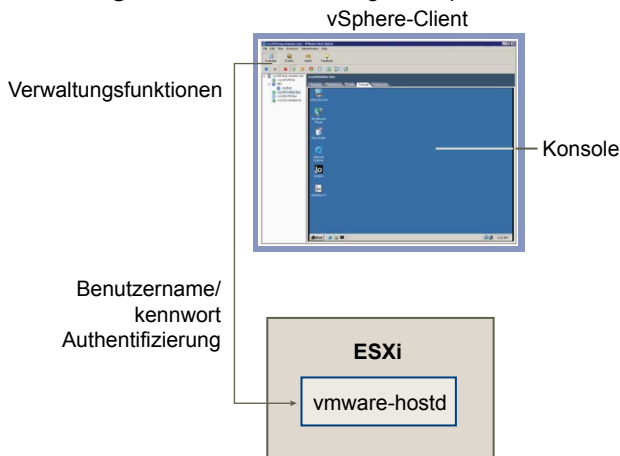
Wenn sich ein vSphere-Client- oder vCenter Server-Benutzer mit einem ESXi-Host verbindet, wird eine Verbindung mit dem Prozess „VMware Host Agent“ hergestellt. Der Prozess verwendet zur Authentifizierung Benutzernamen und Kennwörter.

ESXi authentifiziert Benutzer, die auf ESXi-Hosts zugreifen, über den vSphere-Client oder das SDK. Die Standardinstallation von ESXi verwendet für die Ausführung eine lokale Kennwortdatenbank.

Abbildung 13-1 zeigt ein einfaches Beispiel, wie ESXi Übertragungen vom vSphere-Client authentifiziert.

HINWEIS CIM-Transaktionen verwenden darüber hinaus auch die ticketbasierte Authentifizierung in Verbindung mit dem Prozess `vmware-hostd`.

Abbildung 13-1. Authentifizierung für vSphere-Clientdatenverkehr mit ESXi



ESXi-Authentifizierungstransaktionen mit Netzwerkverwaltungsclients anderer Anbieter ähneln direkten Interaktionen mit dem Prozess `vmware-hostd`.

Damit die Authentifizierung an Ihrem Standort effizient funktioniert, müssen Sie gegebenenfalls grundlegende Aufgaben wie die Einrichtung von Benutzern, Gruppen, Berechtigungen und Rollen vornehmen, die Benutzerattribute konfigurieren, eigene Zertifikate erstellen, ggf. SSL einrichten.

Informationen zu Benutzern, Gruppen, Berechtigungen und Rollen

vCenter Server und ESXi-Hosts verwenden eine Kombination aus Benutzername, Kennwort und Berechtigungen zur Authentifizierung eines Benutzers für Zugriffs- und Autorisierungsaktivitäten. Sie können den Zugriff auf Hosts, Cluster, Datenspeicher, Ressourcenpools, Netzwerkportgruppen und virtuelle Maschinen durch das Zuweisen von Berechtigungen steuern.

Der Zugriff auf einen ESXi-Host und dessen Ressourcen wird erteilt, wenn sich ein bekannter Benutzer mit entsprechenden Berechtigungen am Host mit dem richtigen Kennwort anmeldet. vCenter Server verwendet ein ähnliches Verfahren, um Benutzern Zugriff zu gewähren.

vCenter Server und ESXi-Hosts verweigern den Zugriff unter folgenden Umständen:

- Ein Benutzer, der nicht in der Benutzerliste aufgeführt wird, versucht sich anzumelden.
- Ein Benutzer gibt ein falsches Kennwort ein.
- Ein Benutzer ist zwar im Verzeichnis aufgeführt, hat aber keine Berechtigungen.
- Ein Benutzer, der sich erfolgreich angemeldet hat, versucht Vorgänge auszuführen, für die er keine Berechtigung besitzt.

Im Rahmen des ESXi-Host- und vCenter Server-Managements müssen Sie die Handhabung bestimmter Benutzer- und Berechtigungstypen planen. ESXi und vCenter Server verwenden Privilegiengruppen, sog. Rollen, um zu steuern, welche Vorgänge bestimmte Benutzer oder Gruppen ausführen dürfen. Es werden vordefinierte Rollen zur Verfügung gestellt, sie können jedoch auch neue Rolle erstellen. Sie können Benutzer leichter verwalten, wenn Sie sie Gruppen zuordnen. Wenn Sie einer Gruppe eine Rolle zuweisen, wird sie für alle Benutzer in der Gruppe übernommen.

Grundlegendes zu Benutzern

Ein Benutzer ist eine Person, die sich am ESXi-Host oder an vCenter Server anmelden darf.

ESXi Benutzer werden in zwei Kategorien unterteilt: Benutzer, die über vCenter Server auf den Host zugreifen, und Benutzer, die sich über den vSphere-Client, einen Drittanbieter-Client oder die Befehlsshell direkt auf dem Host anmelden.

Autorisierte vCenter Server-Benutzer

Autorisierte Benutzer für vCenter Server sind die Benutzer, die in der von vCenter Server referenzierten Windows-Domänenliste enthalten sind, oder lokale Windows-Benutzer auf dem vCenter Server-Host.

In vCenter Server können Sie Benutzer nicht erstellen, entfernen oder anderweitig ändern. Sie müssen die Tools zum Verwalten der Windows-Domäne verwenden. Alle Änderungen werden von vCenter Server übernommen. Auf der Benutzeroberfläche wird jedoch keine Benutzerliste zur Prüfung zur Verfügung gestellt.

Benutzer mit direktem Zugriff

Benutzer, die zum direkten Arbeiten auf einem ESXi-Host autorisiert sind, werden der internen Benutzerliste von einem Systemadministrator hinzugefügt.

Der Administrator kann zahlreiche Managementaktivitäten für diese Benutzer durchführen. Darunter fallen beispielsweise das Ändern von Kennwörtern, Gruppenmitgliedschaften und Berechtigungen sowie das Hinzufügen und Entfernen von Benutzern.

Die von vCenter Server geführte Benutzerliste ist eine andere als die Benutzerliste des Hosts. Auch wenn die Listen scheinbar gleiche Benutzer (z. B. einen Benutzer mit der Bezeichnung devuser) enthalten, müssen Sie diese Benutzer getrennt behandeln. Wenn Sie sich an vCenter Server als „devuser“ anmelden, können Sie z. B. über die Berechtigung verfügen, Dateien aus einem Datenspeicher anzusehen und zu löschen, was nicht der Fall sein muss, wenn Sie sich auf dem ESXi-Host als „devuser“ anmelden.

Überprüfen Sie vor der Erstellung von ESXi-Host-Benutzern die Benutzerliste von vCenter Server, um die Vergabe doppelter Namen zu vermeiden. Das Verzeichnis der vCenter Server-Benutzer finden Sie im Windows-Domänenverzeichnis.

Grundlegendes zu Gruppen

Eine Gruppe ist eine Zusammenstellung von Benutzern mit gemeinsamen Regeln und Berechtigungen. Wenn Sie einer Gruppe Berechtigungen zuweisen, werden diese von allen Benutzern in der Gruppe übernommen, wodurch Sie die Benutzerprofile nicht einzeln bearbeiten müssen.

Als Administrator müssen Sie entscheiden, wie die Gruppen strukturiert werden sollen, um die Sicherheits- und Verwendungsziele zu erreichen. Sie haben zum Beispiel drei Teilzeitkräfte in der Vertriebsabteilung, die an verschiedenen Tagen arbeiten und zwar auf eine bestimmte virtuelle Maschine zugreifen sollen, nicht jedoch auf die virtuellen Maschinen des Vertriebsleiters. In diesem Fall können Sie eine Gruppe mit der Bezeichnung „VertriebTeilzeit“ und drei Vertriebsmitarbeitern erstellen und dieser Gruppe die Berechtigung zuteilen, nur mit einem Objekt, der gemeinsamen virtuellen Maschine, zu interagieren. Sie können jedoch keine Vorgänge auf den virtuellen Maschinen des Vertriebsleiters durchführen.

Die Gruppenverzeichnisse in vCenter Server und auf dem ESXi-Host stammen aus den gleichen Quellen wie die entsprechenden Benutzerverzeichnisse. Wenn Sie mit vCenter Server arbeiten, wird das Gruppenverzeichnis von der Windows-Domäne abgerufen. Wenn Sie direkt an einem ESXi-Host angemeldet sind, wird die Liste der Benutzergruppen aus einer Tabelle aufgerufen, die vom Host verwaltet wird.

Grundlegendes zu Berechtigungen

Für ESXi und vCenter Server werden Berechtigungen als Zugriffsrollen definiert, die aus einem Benutzer und der dem Benutzer zugewiesenen Rolle für ein Objekt wie z. B. einer virtuellen Maschine oder einem ESXi-Host bestehen.

Die meisten vCenter Server- und ESXi-Benutzer können Objekte des Hosts nur in eingeschränktem Maß ändern. Benutzer mit der Rolle „Administrator“ haben Vollzugriff auf alle virtuellen Objekte wie Datenspeicher, Hosts, virtuelle Maschinen und Ressourcenpools. Dem Root-Benutzer ist die Rolle „Administrator“ standardmäßig zugewiesen. Wenn vCenter Server den Host verwaltet, ist vpxuser auch ein Administrator.

Die Liste der Berechtigungen ist für ESXi und vCenter Server gleich. Zum Konfigurieren der Berechtigungen wird die gleiche Methode verwendet.

Sie können über eine direkte Verbindung mit dem ESXi-Host Rollen erstellen und Berechtigungen festlegen. Da diese Aufgaben jedoch häufiger in vCenter Server durchgeführt werden, lesen Sie die Abschnitte in *Grundlagen der Systemverwaltung*, um Informationen zum Verwalten von Berechtigungen und Rollen zu erhalten.

Zuweisen von Root-Benutzerberechtigungen

Root-Benutzer können Aktivitäten nur auf dem ESXi-Host durchführen, an dem sie angemeldet sind.

Aus Sicherheitsgründen sollten Sie dem Root-Benutzer nicht die Rolle **[Administrator]** gewähren. In diesem Fall können Sie die Berechtigungen nach der Installation so ändern, dass der Root-Benutzer keine weiteren Administratorrechte hat, oder Sie löschen alle Zugriffsrechte des Root-Benutzers über den vSphere-Client, wie im Kapitel "Verwalten von Benutzern, Gruppen, Berechtigungen und Rollen" des Handbuchs *Grundlagen der Systemverwaltung* beschrieben. Wenn Sie dies tun, müssen Sie auf der Root-Ebene zunächst eine andere Genehmigung erteilen, die ein anderer Benutzer mit der Rolle des Administrators erhält.

Die Zuweisung der Administratorenrolle auf verschiedene Benutzer gewährleistet die Nachvollziehbarkeit und somit die Sicherheit. Der vSphere-Client protokolliert alle Aktionen des Administrators als Ereignisse und gibt ein Überwachungsprotokoll aus. Wenn alle Administratoren sich als Root-Benutzer anmelden, können Sie nicht wissen, welcher Administrator eine Aktion ausgeführt hat. Wenn Sie mehrere Berechtigungen auf Root-Ebene anlegen, die jeweils einem anderen Benutzer oder einer anderen Benutzergruppe zugewiesen sind, können Sie die Aktionen jedes Administrators oder jeder Administratorengruppe gut nachvollziehen.

Nachdem Sie einen alternativen Administrator-Benutzer angelegt haben, können Sie die Berechtigungen des Root-Benutzers löschen oder dessen Rolle in der Form ändern, dass seine Rechte begrenzt werden. Dann müssen Sie den neu erstellten Benutzer als Ausgangspunkt für die Hostauthentifizierung verwenden, wenn Sie den Host unter vCenter Server-Management stellen.

HINWEIS `vicfg`-Befehle führen keine Zugriffsprüfung durch. Selbst wenn Sie die Berechtigungen des Root-Benutzers einschränken, wirkt sich dies nicht auf die Befehle aus, die er über die Befehlszeilenschnittstelle ausführen kann.

Grundlegendes zu vpxuser-Berechtigungen

Die Berechtigung „vpxuser“ wird für vCenter Server beim Verwalten von Aktivitäten für den Host verwendet. Sie wird erstellt, wenn ein ESXi-Host mit vCenter Server verbunden wird.

vCenter Server hat Administratorberechtigungen auf dem Host, der die Anwendung verwaltet. So kann vCenter Server zum Beispiel virtuelle Maschinen auf Hosts verschieben und Konfigurationsänderungen vornehmen, die für die Unterstützung virtueller Maschinen notwendig sind.

Der Administrator von vCenter Server kann viele der Aufgaben des Root-Benutzers auf dem Host durchführen und Aufgaben planen, Vorlagen erstellen und nutzen usw. Der vCenter Server-Administrator kann jedoch nicht Benutzer oder Gruppen für ESXi-Hosts direkt erstellen, löschen oder bearbeiten. Diese Aufgaben können nur von einem Benutzer mit Administratorberechtigungen auf dem jeweiligen ESXi-Host durchgeführt werden.



VORSICHT Ändern Sie **[vpxuser]** und die dazugehörigen Berechtigungen nicht. Ansonsten kann es zu Problemen bei der Verwaltung des ESXi-Hosts über vCenter Server kommen.

Zuweisen von dcui-Benutzerberechtigungen

Der Benutzer **[dcui]** wird auf Hosts ausgeführt und agiert mit Administratorrechten. Der Hauptzweck dieses Benutzers ist die Konfiguration von Hosts für den Sperrmodus über die direkte Konsole.

Dieser Benutzer dient als Agent für die direkte Konsole und müssen nicht von interaktiven Benutzern geändert oder verwendet werden.



VORSICHT Ändern Sie den Benutzer „dcui“ und seine Berechtigungen unter keinen Umständen. Ansonsten kann es zu Problemen beim Arbeiten mit dem ESXi-Host auf der lokalen Benutzeroberfläche kommen.

Grundlegendes zu Rollen

vCenter Server und ESXi gewähren nur Benutzern Zugriff auf Objekte, denen Berechtigungen für das jeweilige Objekt zugewiesen wurden. Wenn Sie einem Benutzer oder einer Gruppe Berechtigungen für das Objekt zuweisen, kombinieren Sie hierzu den Benutzer oder Gruppe mit einer Rolle. Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten.

Für ESXi-Hosts gibt es drei Standardrollen. Es ist nicht möglich, die Berechtigungen für diese drei Rollen zu ändern. Jede nachfolgende Standardrolle enthält die Berechtigungen der vorhergehenden Rolle. So übernimmt beispielsweise die Rolle **[Administrator]** die Rechte der Rolle **[Nur lesen]**. Rollen, die Sie selbst anlegen, übernehmen keine Berechtigungen von den Standardrollen.

Sie können über eine direkte Verbindung mit dem ESXi-Host Rollen erstellen und Berechtigungen festlegen. Die meisten Benutzer erstellen in vCenter Server Rollen und legen dort Berechtigungen fest. Informationen zum Arbeiten mit Berechtigungen und Rollen finden Sie unter *Grundlagen der Systemverwaltung*.

Zuweisen der Rolle „Kein Zugriff“

Benutzer, denen die Rolle „Kein Zugriff“ für ein bestimmtes Objekt zugewiesen wurde, können das Objekt weder anzeigen noch ändern. Neuen Benutzern und Gruppen wird diese Rolle standardmäßig zugewiesen. Sie können die Rolle objektabhängig ändern.

Wenn einem Benutzer für ein bestimmtes Objekt die Rolle „Kein Zugriff“ zugewiesen wurde, kann er die Registerkarten im vSphere-Client für das Objekt auswählen. Es wird jedoch kein Inhalt angezeigt.

Die einzigen Benutzer, denen die Rolle „Kein Zugriff“ nicht standardmäßig zugewiesen wird, sind der Root-Benutzer und „vpxuser“. Stattdessen wird ihnen die Rolle **[Administrator]** zugewiesen. Sie können die Berechtigungen des Root-Benutzers insgesamt löschen oder seine Rolle auf **[Kein Zugriff]** festlegen, sofern Sie zunächst auf Root-Ebene eine Ersatzberechtigung mit der Rolle **[Administrator]** anlegen und diese Rolle einem anderen Benutzer zuweisen.

Zuweisen der Rolle „Nur Lesen“

Benutzer, denen die Rolle „Nur Lesen“ für ein Objekt zugewiesen wurde, können den Status des Objekts und Details zum Objekt anzeigen.

Mit dieser Rolle kann ein Benutzer die virtuelle Maschine, den Host und die Ressourcenpoolattribute anzeigen. Der Benutzer kann jedoch nicht die Remotekonsole eines Hosts anzeigen. Alle Vorgänge über die Menüs und Symbolleisten sind nicht zugelassen.

Zuweisen der Administratorrolle

Benutzer, denen die Administrator-Rolle für ein Objekt zugewiesen wurde, können sämtliche Vorgänge auf ein Objekt anwenden und diese anzeigen. Zu dieser Rolle gehören alle Berechtigungen, über die auch die Rolle **[Nur Lesen]** verfügt.

Wenn Sie auf einem ESXi-Host die Rolle des Administrators haben, können Sie einzelnen Benutzern und Gruppen auf diesem Host Berechtigungen erteilen. Wenn Sie die Rolle des Administrators in vCenter Server innehaben, können Sie allen Benutzern und Gruppen in der Windows-Domänenliste, die vCenter Server referenziert, Berechtigungen erteilen.

vCenter Server registriert alle ausgewählten Benutzer oder Gruppen der Windows-Domäne durch den Prozess der Zuweisung von Berechtigungen. Standardmäßig werden allen Benutzern, die zur lokalen Gruppe Windows-Administratoren auf dem vCenter Server gehören, die gleichen Zugriffsrechte wie Benutzern mit der Rolle Administrator zugewiesen. Benutzer, die Mitglieder der Gruppe **[Administratoren (Administrators)]** sind, können sich anmelden und verfügen dann über Vollzugriff.

Aus Sicherheitsgründen sollten Sie die Gruppe **[Windows-Administratoren]** aus der Rolle **[Administrator]** entfernen. Sie können Berechtigungen nach der Installation ändern. Sie können auch mit dem vSphere-Client Zugriffsberechtigungen der Gruppe „Windows-Administratoren“ löschen. Dazu müssen Sie auf der Root-Ebene zunächst eine andere Berechtigung einrichten, bei der einem anderen Benutzer die Rolle „Administrator“ zugewiesen ist.

Zugriff auf die Benutzerschnittstelle der direkten Konsole

Nur Benutzer mit Administratorrolle können sich an der direkten Konsole anmelden. Zum Erteilen des Zugriffs auf die direkte Konsole fügen Sie den Benutzer der lokalen Administratorgruppe hinzu.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Benutzer (Users)]** .
- 3 Klicken Sie mit der rechten Maustaste auf den Benutzer und klicken Sie zum Öffnen des Dialogfelds „Benutzer bearbeiten“ auf **[Bearbeiten]** .
- 4 Wählen Sie im Dropdown-Menü **[Gruppe]** die Option „localadmin“ und klicken Sie auf **[Hinzufügen]** .
- 5 Klicken Sie auf **[OK]** .

Arbeiten mit Benutzern und Gruppen auf ESXi-Hosts

Wenn Sie direkt über den vSphere-Client mit einem ESXi-Host verbunden sind, können Sie Benutzer und Gruppen erstellen, bearbeiten und löschen. Diese Benutzer und Gruppen werden im vSphere-Client angezeigt, wenn Sie sich am ESXi-Host anmelden. Bei Anmeldung an vCenter Server stehen sie jedoch nicht zur Verfügung.

Anzeigen, Sortieren und Exportieren einer Benutzer- und Gruppenliste

Sie können Listen mit ESXi-Benutzern und -Gruppen anzeigen, sortieren und in eine Datei im HTML-, XML-, Microsoft Excel- oder CSV-Format exportieren.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Benutzer (Users)]** oder **[Gruppen (Groups)]** .
- 3 Legen Sie die Sortierreihenfolge der Tabelle fest, und blenden Sie Spalten ein oder aus, je nachdem, welche Daten in der Exportdatei enthalten sein sollen.
 - Wenn Sie die Tabelle nach einer Spalte sortieren möchten, klicken Sie auf die entsprechende Spaltenüberschrift.
 - Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften, und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.
 - Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften, und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.
- 4 Klicken Sie mit der rechten Maustaste an eine beliebigen Stelle in der Tabelle und klicken Sie dann zum Öffnen des Dialogfelds „Speichern unter“ auf **[Liste exportieren]** .
- 5 Wählen Sie ein Verzeichnis aus, und geben Sie einen Dateinamen ein.
- 6 Wählen Sie den Dateityp aus und klicken Sie auf **[OK]** .

Hinzufügen von Benutzern zur Tabelle „Benutzer“

Wenn Sie einen Benutzer zur Tabelle „Benutzer“ hinzufügen, wird die interne Benutzerliste aktualisiert, die von ESXi verwaltet wird.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Benutzer (Users)]**.
- 3 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle der Tabelle Benutzer (Users), und klicken Sie auf **[Hinzufügen (Add)]**. Das Dialogfeld Neuen Benutzer hinzufügen (Add New User) wird angezeigt.
- 4 Geben Sie eine Anmeldung, einen Benutzernamen, eine numerische Benutzer-ID und ein Kennwort ein.
Die Angabe des Benutzernamens und der ID sind optional. Wenn Sie keine Benutzer-ID angeben, weist der vSphere-Client die nächste verfügbare Benutzer-ID zu.
- 5 Um den Benutzer einer Gruppe hinzuzufügen, wählen Sie im Dropdown-Menü **[Gruppe]** den Gruppennamen aus, und klicken Sie auf **[Hinzufügen]**.
- 6 Klicken Sie auf **[OK]**.

Ändern der Benutzereinstellungen

Sie können die Benutzer-ID, den Benutzernamen, das Kennwort und die Gruppeneinstellungen für einen Benutzer ändern. Außerdem können Sie einem Benutzer Shell-Zugriff erteilen.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Benutzer (Users)]**.
- 3 Klicken Sie mit der rechten Maustaste auf den Benutzer und klicken Sie zum Öffnen des Dialogfelds „Benutzer bearbeiten“ auf **[Bearbeiten]**.
- 4 Geben Sie zum Ändern der Benutzer-ID im Textfeld **[UID]** eine numerische Benutzer-UID ein.
Der vSphere-Client weist einem Benutzer bei seiner Erstellung die UID zu. In den meisten Fällen muss diese Zuweisung nicht geändert werden.
- 5 Geben Sie einen neuen Benutzernamen ein.
- 6 Wenn Sie das Kennwort eines Benutzers ändern möchten, aktivieren Sie das Kontrollkästchen **[Kennwort ändern (Change Password)]**, und geben Sie ein neues Kennwort ein.
Erstellen Sie ein Kennwort, das ausreichend lang und komplex genug ist, um gegen gängige Brute-Force-Angriffe zu schützen. Der Host prüft nur dann die Einhaltung der Kennwortrichtlinien, wenn Sie zu Authentifizierungszwecken zum Plug-In `pam_passwdqc.so` gewechselt sind. Die Kennwordeinstellungen im Standardauthentifizierungs-Plug-In `pam_cracklib.so` werden nicht erzwungen.
- 7 Um den Benutzer einer Gruppe hinzuzufügen, wählen Sie im Dropdown-Menü **[Gruppe]** den Gruppennamen aus, und klicken Sie auf **[Hinzufügen]**.
- 8 Wählen Sie zum Entfernen des Benutzers aus einer Gruppe den Gruppennamen im Feld **[Gruppenmitgliedschaft]** aus und klicken Sie auf **[Entfernen]**.
- 9 Klicken Sie auf **[OK]**.

Entfernen von Benutzern oder Gruppen

Sie können einen Benutzer oder eine Gruppe von dem ESXi-Host entfernen.



VORSICHT Entfernen Sie den Root-Anwender nicht.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Benutzer (Users)]** oder **[Gruppen (Groups)]**.
- 3 Klicken Sie mit der rechten Maustaste auf den zu entfernenden Benutzer bzw. die Gruppe und wählen Sie **[Entfernen]**.

Hinzufügen von Benutzern zur Tabelle „Gruppen“

Wenn Sie eine Gruppe zur ESXi-Gruppentabelle hinzufügen, wird die vom Host verwaltete, interne Gruppenliste aktualisiert.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Gruppen (Groups)]**.
- 3 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle der Tabelle Gruppen und dann auf **[Hinzufügen (Add)]**. Das Dialogfeld Neue Gruppe erstellen (Create New Group) wird angezeigt.
- 4 Geben Sie einen Gruppennamen und in das Textfeld **[Gruppen-ID]** eine numerische Gruppen-ID (GID) ein.

Die Angabe der GID ist nicht zwingend erforderlich. Wenn Sie keine GID angeben, weist der vSphere-Client die nächste verfügbare Gruppen-ID zu.
- 5 Wählen Sie die Benutzernamen aller Benutzer, die zur Gruppe gehören sollen, in der Liste aus und klicken Sie auf **[Hinzufügen]**.
- 6 Klicken Sie auf **[OK]**.

Hinzufügen zu oder Entfernen aus einer Gruppe

Sie können Benutzer einer Gruppe in der Gruppentabelle hinzufügen oder aus dieser entfernen.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am Host an.
- 2 Klicken Sie auf die Registerkarte **[Benutzer und Gruppen (Users & Groups)]** und dann auf **[Gruppen (Groups)]**.
- 3 Klicken Sie mit der rechten Maustaste auf die zu ändernde Gruppe und dann auf **[Eigenschaften]**, um das Dialogfeld „Gruppe bearbeiten“ zu öffnen.
- 4 Um den Benutzer einer Gruppe hinzuzufügen, wählen Sie im Dropdown-Menü **[Gruppe]** den Gruppennamen aus, und klicken Sie auf **[Hinzufügen]**.
- 5 Wählen Sie zum Entfernen des Benutzers aus einer Gruppe den Gruppennamen im Feld **[Gruppenmitgliedschaft]** aus und klicken Sie auf **[Entfernen]**.
- 6 Klicken Sie auf **[OK]**.

Verschlüsselungs- und Sicherheitszertifikate für ESXi

ESXi unterstützt SSL, Version 3, und TLS, Version 1, die anschließend als SSL (Secure Socket Layer) bezeichnet werden. Bei aktiviertem SSL sind die Daten vertraulich, geschützt und können nicht unbemerkt bei der Übertragung geändert werden.

Der gesamte Netzwerkdatenverkehr ist verschlüsselt, solange Sie den Web-Proxy-Dienst nicht geändert haben, damit er unverschlüsselten Datenverkehr für den Port durchlässt.

Die Hostzertifikatsüberprüfung ist standardmäßig aktiviert. Für die Verschlüsselung des Netzwerkverkehrs werden SSL-Zertifikate verwendet. ESXi verwendet jedoch automatisch generierte Zertifikate, die als Teil des Installationsprozesses erstellt und auf dem Host gespeichert werden. Zwar sind diese Zertifikate eindeutig und ermöglichen die Verwendung des Servers, sie können jedoch nicht verifiziert werden und wurden nicht von einer bekannten, vertrauenswürdigen Zertifizierungsstelle (CA) signiert. Diese Standardzertifikate sind anfällig für mögliche Man-in-the-Middle-Angriffe.

Um die Vorteile der Zertifikatsüberprüfung voll nutzen zu können, insbesondere, wenn Sie vorhaben, verschlüsselte Remoteverbindungen extern zu verwenden, installieren Sie neue Zertifikate, die von einer gültigen internen Zertifizierungsstelle (CA) signiert wurden, oder erwerben Sie ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle.

HINWEIS Bei Verwenden des selbst signierten Zertifikats erhalten Clients eine Warnmeldung zum Zertifikat. Um dieses Problem zu beheben, installieren Sie ein von einer anerkannten Zertifizierungsstelle signiertes Zertifikat. Wenn keine von einer CA signierten Zertifikate installiert sind, wird die gesamte Kommunikation zwischen vCenter Server und den vSphere-Clients mit einem selbst signierten Zertifikat verschlüsselt. Diese Zertifikate bieten nicht die für eine Produktionsumgebung möglicherweise erforderliche Authentifizierungssicherheit.

Aktivieren der Überprüfung von Zertifikaten und Host-Fingerabdrücken

Die Zertifikatüberprüfung ist standardmäßig aktiviert, um Man-in-the-Middle-Angriffe zu verhindern und sämtliche Sicherheitsfunktionen der Zertifikate zu verwenden. Sie können prüfen, ob die Zertifikatüberprüfung im vSphere-Client aktiviert ist.

HINWEIS vCenter Server-Zertifikate bleiben bei Upgrades erhalten.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Wählen Sie **[Verwaltung] > [vCenter Server-Einstellungen]**.
- 3 Klicken Sie im linken Bildschirmbereich auf **[SSL-Einstellungen]** und überprüfen Sie, dass **[Hostzertifikate prüfen]** ausgewählt ist.
- 4 Falls Hosts vorhanden sind, die eine manuelle Validierung erfordern, vergleichen Sie die für die Hosts aufgeführten Fingerabdrücke mit den Fingerabdrücken in der Hostkonsole.

Um sich den Fingerabdruck des Hosts zu beschaffen, führen Sie auf dem ESXi-Host folgenden Befehl aus:

```
openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha1 -noout
```

- 5 Stimmen die Fingerabdrücke überein, wählen Sie das Kontrollkästchen **[Überprüfen]** neben dem Host aus.
Hosts, die nicht ausgewählt sind, werden getrennt, nachdem Sie auf **[OK]** klicken.
- 6 Klicken Sie auf **[OK]**.

Generieren neuer Zertifikate für den ESXi-Host

Der ESXi-Host generiert Zertifikate, wenn das System das erste Mal gestartet wird. Unter gewissen Umständen kann es sein, dass Sie den Host zwingen müssen, neue Zertifikate zu erzeugen. Normalerweise werden neue Zertifikate nur dann erstellt, wenn der Hostname geändert oder das Zertifikat versehentlich gelöscht wird.

Vorgehensweise

- 1 Wählen Sie in der direkten Konsole **[Angepasste Einstellungen zurücksetzen]**.
- 2 Führen Sie einen Neustart des Systems durch, um die Zertifikate neu zu erstellen.

Ersetzen eines Standardzertifikats durch ein Zertifikat einer Zertifizierungsstelle

Der ESXi-Host verwendet automatisch generierte Zertifikate, die als Teil des Installationsprozesses erstellt wurden. Zwar sind diese Zertifikate eindeutig und ermöglichen die Verwendung des Servers, sie können jedoch nicht verifiziert werden und wurden nicht von einer bekannten, vertrauenswürdigen Zertifizierungsstelle (CA) signiert. Die Verwendung von selbst signierten Zertifikaten widerspricht möglicherweise der Sicherheitsrichtlinie Ihrer Organisation. Wenn Sie ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle anfordern, können Sie das Standardzertifikat ersetzen.

HINWEIS ESXi unterstützt nur X.509-Zertifikate zum Verschlüsseln von Sitzungsinformationen, die über SSL-Verbindungen zwischen Server- und Clientkomponenten gesendet werden.

Voraussetzungen

Alle Dateiübertragungen und andere Kommunikationsvorgänge erfolgen über eine sichere HTTPS-Sitzung. Der zum Authentifizieren der Sitzung verwendete Benutzer muss über die Berechtigung **Host.Config.AdvancedConfig** auf dem Host verfügen. Weitere Informationen über ESXi-Berechtigungen finden Sie unter [„Informationen zu Benutzern, Gruppen, Berechtigungen und Rollen“](#), auf Seite 160

Vorgehensweise

- 1 Verwenden Sie den `vi fs`-Befehl, um Kopien der Zertifikats- und Schlüsseldateien auf dem ESXi-Host abzulegen.

Für diesen Befehl gilt folgendes Format für Zertifikat bzw. Schlüssel:

```
vi fs --server <Hostname> --username <Benutzername> --put rui.crt /host/ssl_cert
vi fs --server <Hostname> --username <Benutzername> --put rui.key /host/ssl_key
```

- 2 Wählen Sie in der direkten Konsole den Vorgang **[Management-Agenten neu starten]** aus, damit die Einstellungen wirksam werden.

Hochladen eines Zertifikats und Schlüssels anhand von HTTPS PUT

Neben dem `vifs`-Befehl können Drittanbieteranwendungen zum Hochladen von Zertifikaten verwendet werden. Anwendungen mit Unterstützung für HTTPS PUT-Operationen können mit der HTTPS-Schnittstelle verwendet werden, die im Lieferumfang von ESXi enthalten ist. Beispielsweise können Sie SeaMonkey Composer zum Hochladen von Zertifikaten und Schlüsseln verwenden.

Vorgehensweise

- 1 Öffnen Sie die Datei in der Anwendung, die Sie für das Hochladen verwenden.
- 2 Veröffentlichen Sie die Datei an einem der folgenden Speicherorte.
 - Verwenden Sie bei Zertifikaten `https://hostname/host/ssl.crt`.
 - Verwenden Sie bei Schlüsseln `https://hostname/host/sslkey`.
- 3 Wählen Sie in der direkten Konsole den Vorgang „Verwaltungs-Agenten neu starten“, damit die Einstellungen wirksam werden.

Konfigurieren von SSL-Zeitüberschreitungen

Sie können SSL-Zeitüberschreitungen für ESXi konfigurieren.

Zeitüberschreibungsperioden können für zwei Typen von Leerlaufverbindungen festgelegt werden:

- Die Einstellung für Zeitüberschreitung beim Lesen wird für Verbindungen verwendet, die den SSL-Handshake-Prozess mit Port 443 von ESXi abgeschlossen haben.
- Die Einstellung für Handshake-Zeitüberschreitung wird für Verbindungen verwendet, die den SSL-Handshake-Prozess mit Port 443 von ESXi noch nicht beendet haben.

Beide Verbindungszeitüberschreitungen werden in Millisekunden angegeben.

Leerlaufverbindungen werden nach Ablauf der Zeitüberschreibungsperiode getrennt. Bei vollständig eingerichteten SSL-Verbindungen ist die Zeitüberschreitung auf unendlich gesetzt.

Vorgehensweise

- 1 Mit dem Befehl `vifs` erhalten Sie eine Kopie der Datei `config.xml`, die Sie bearbeiten können.

Verwenden Sie bei Linux-Systemen folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --get /host/config.xml <Verzeichnis>/config.xml
```

Verwenden Sie bei Windows-Systemen folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --get /host/config.xml <Verzeichnis>\config.xml
```

- 2 Bearbeiten Sie die Datei `config.xml` mithilfe eines Texteditors.
- 3 Geben Sie den Wert für `<readTimeoutMs>` in Millisekunden an.

Wenn Sie die Zeitüberschreitung beim Lesen beispielsweise auf 20 Sekunden festlegen, geben Sie folgenden Befehl ein.

```
<readTimeoutMs>20000</readTimeoutMs>
```

- 4 Geben Sie den Wert `<handshakeTimeoutMs>` in Millisekunden ein.

Geben Sie folgenden Befehl ein, um die Handshake-Zeitüberschreitung beispielsweise auf 20 Sekunden festzulegen.

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

- 5 Speichern Sie die Änderungen, und schließen Sie die Datei.
- 6 Verwenden Sie den Befehl `vifs`, um eine Kopie der Datei `config.xml` auf dem ESXi-Host zu speichern.
Verwenden Sie bei Linux-Systemen folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>/config.xml /host/config.xml
```


Verwenden Sie bei Windows-Systemen folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>\config.xml /host/config.xml
```
- 7 Wählen Sie in der direkten Konsole den Vorgang „Management-Agenten neu starten“ aus, damit die Einstellungen wirksam werden.

Beispiel 13-1. Konfigurationsdatei

Der folgende Abschnitt der Datei `/etc/vmware/hostd/config.xml` zeigt, an welcher Stelle die Einstellungen für die SSL-Zeitüberschreitung eingegeben werden müssen.

```
<vmacore>
  ...
  <http>
    <readTimeoutMs>20000</readTimeoutMs>
  </http>
  ...
  <ssl>
    ...
    <handshakeTimeoutMs>20000</handshakeTimeoutMs>
    ...
  </ssl>
</vmacore>
```

Ändern von ESXi-Web-Proxy-Einstellungen

Beim Ändern von Web-Proxy-Einstellungen müssen mehrere Richtlinien für Verschlüsselung und Benutzer-sicherheit berücksichtigt werden.

HINWEIS Verwenden Sie an der direkten Konsole den Vorgang „Management-Agenten neu starten“, um den Prozess `vmware-hostd` wieder zu starten, wenn Sie Änderungen an den Verzeichnissen oder den Authentifizierungsmechanismen des Hosts vorgenommen haben.

- Richten Sie Zertifikate nicht mithilfe von Kennwortsätzen ein. ESXi unterstützt keine Kennwortsätze (verschlüsselte Schlüssel). Wenn Sie einen Kennwortsatz einrichten, können ESXi-Prozesse nicht ordnungsgemäß starten.
- Sie können den Web-Proxy so konfigurieren, dass er an einer anderen Stelle als am Standardspeicherort nach Zertifikaten sucht. Dies ist hilfreich, wenn die Zertifikate zentral auf einem Computer gespeichert werden sollen, damit mehrere Hosts die Zertifikate verwenden können.



VORSICHT Wenn Zertifikate nicht lokal auf dem Host gespeichert werden, sondern z. B. auf einer NFS-Freigabe, kann der Host nicht auf diese Zertifikate zugreifen, wenn ESXi keine Netzwerkkonnektivität hat. Aus diesem Grund ist bei einem Client, der eine Verbindung zum Host herstellt, kein sicherer SSL-Handshake mit dem Host möglich.

- Zur Unterstützung von Verschlüsselung für Benutzernamen, Kennwörter und Pakete wird SSL standardmäßig für vSphere Web Services SDK-Verbindungen aktiviert. Wenn Sie diese Verbindungen so konfigurieren möchten, dass Übertragungen nicht verschlüsselt werden, deaktivieren Sie SSL für Ihre vSphere Web Services SDK-Verbindung, indem Sie die Verbindung von HTTPS auf HTTP umstellen.

Deaktivieren Sie SSL nur dann, wenn Sie eine vollständig vertrauenswürdige Umgebung für die Clients geschaffen haben, d. h. Firewalls wurden installiert und die Übertragungen zum und vom Host sind vollständig isoliert. Die Deaktivierung von SSL kann die Leistung verbessern, da der für die Verschlüsselung notwendige Verarbeitungsaufwand nicht anfällt.

- Um den Missbrauch von ESXi-Diensten zu verhindern, kann auf die meisten internen ESXi-Dienste nur über Port 443, den für HTTPS-Übertragungen verwendeten Port, zugegriffen werden. Port 443 dient als Reverse-Proxy für ESXi. Sie können eine Liste der Dienste auf dem ESXi-Host auf einer HTTP-Begrüßungsseite sehen. Sie können aber nur direkt auf die Speicheradapterdienste zugreifen, wenn Sie über die entsprechenden Berechtigungen verfügen.

Sie können diese Einstellung ändern, sodass auf bestimmte Dienste direkt über HTTP-Verbindungen zugegriffen werden kann. Nehmen diese Änderung nur vor, wenn Sie ESXi in einer vertrauenswürdigen Umgebung verwenden.

- Wenn Sie vCenter Server aktualisieren, wird das Zertifikat beibehalten.

Ändern der Sicherheitseinstellungen für einen Web-Proxy-Dienst

Sie können die Sicherheitskonfiguration ändern, sodass auf bestimmte Dienste direkt über HTTP-Verbindungen zugegriffen werden kann.

Vorgehensweise

- 1 Über den Befehl `vi fs` können Sie eine zu bearbeitende Kopie der Datei `proxy.xml` abrufen.

Verwenden Sie bei Linux-Systemen folgenden Befehl.

```
vi fs --server <Hostname> --username <Benutzername> --get /host/proxy.xml <Verzeichnis>/proxy.xml
```

Verwenden Sie bei Windows-Systemen folgenden Befehl.

```
vi fs --server <Hostname> --username <Benutzername> --get /host/proxy.xml <Verzeichnis>\proxy.xml
```



VORSICHT Falls diese Datei in eine nicht ordnungsgemäße Konfiguration geändert wird, kann das System einen nicht verwaltbaren Status aufweisen. Unter Umständen müssen Sie über die direkte Konsole die Einstellungen auf die Werkseinstellung zurücksetzen.

- 2 Bearbeiten Sie die Datei `proxy.xml` mithilfe eines Texteditors.

Der Inhalt der Datei wird standardmäßig wie folgt angezeigt.

```
<ConfigRoot>
<EndpointList>
<_length>6</_length>
<_type>vim.ProxyService.EndpointSpec[]</_type>
<e id="0">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-webserver</pipeName>
<serverNamespace></serverNamespace>
</e>
<e id="1">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-sdk</pipeName>
<serverNamespace>/sdk</serverNamespace>
</e>
<e id="2">
```

```

<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8080</port>
<serverNamespace>/ui</serverNamespace>
</e>
<e id="3">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsOnly</accessMode>
<pipeName>/var/run/vmware/proxy-vpxa</pipeName>
<serverNamespace>/vpxa</serverNamespace>
</e>
<e id="4">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-mob</pipeName>
<serverNamespace>/mob</serverNamespace>
</e>
<e id="5">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<!-- Use this mode for "secure" deployment -->
<!-- <accessMode>httpsWithRedirect</accessMode> -->
<!-- Use this mode for "insecure" deployment -->
<accessMode>httpAndHttps</accessMode>
<port>8889</port>
<serverNamespace>/wsman</serverNamespace>
</e>
</EndpointList>
</ConfigRoot>

```

3 Ändern Sie die Sicherheitseinstellungen den Anforderungen entsprechend.

Sie können beispielsweise die Einträge für Dienste ändern, die HTTPS verwenden, um den HTTP-Zugriff ergänzen.

- `<e id>` eine ID-Nummer für das XML-Tag mit der Server-ID. ID-Nummern müssen im HTTP-Bereich eindeutig sein.
- `<_type>` ist der Name des Dienstes, den Sie verschieben.
- `<accessmode>` ist die Form der Kommunikation, die der Dienst zulässt. Zu den zulässigen Werten gehören u. a.:
 - `httpOnly` – Auf den Dienst kann nur über unverschlüsselte HTTP-Verbindungen zugegriffen werden.
 - `httpsOnly` – Auf den Dienst kann nur über HTTPS-Verbindungen zugegriffen werden.
 - `httpsWithRedirect` – Auf den Dienst kann nur über HTTPS-Verbindungen zugegriffen werden. Anforderungen über HTTP werden an den entsprechenden HTTPS-URL weitergeleitet.
 - `httpAndHttps` – Auf den Dienst kann sowohl über HTTP- als auch über HTTPS-Verbindungen zugegriffen werden.
- `<port>` ist die Nummer des Ports, der dem Dienst zugewiesen wurde. Sie können dem Dienst eine andere Portnummer zuweisen.
- `<serverNamespace>` ist der Namespace des Servers, der diesen Dienst anbietet, z. B. `/sdk` oder `/mob`.

4 Speichern Sie die Änderungen, und schließen Sie die Datei.

- 5 Über den Befehl `vifs` können Sie eine Kopie der Datei `proxy.xml` wieder auf dem ESXi-Host ablegen.

Verwenden Sie bei Linux folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>/proxy.xml /host/proxy.xml
```

Verwenden Sie bei Windows folgenden Befehl.

```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>\proxy.xml /host/proxy.xml
```

- 6 Wählen Sie in der direkten Konsole den Vorgang „Management-Agenten neu starten“ aus, damit die Einstellungen wirksam werden.

Mehrere ESXi-Bereitstellungsszenarien können Ihnen helfen zu verstehen, wie Sie die Sicherheitsfunktionen in Ihrer eigenen Bereitstellung am besten verwenden. Szenarien verdeutlichen zudem grundlegende Sicherheitsempfehlungen, die Sie bei der Erstellung und Konfiguration von virtuellen Maschinen in Betracht ziehen sollten.

Dieses Kapitel behandelt die folgenden Themen:

- [„Sicherheitsmaßnahmen für gängige ESXi-Implementierungen“](#), auf Seite 175
- [„ESXi-Sperrmodus“](#), auf Seite 178
- [„Empfehlungen für virtuelle Maschinen“](#), auf Seite 179

Sicherheitsmaßnahmen für gängige ESXi-Implementierungen

Sie können Sicherheitsmaßnahmen für verschiedene Implementierungsarten vergleichen, um die Sicherheit Ihrer eigenen ESXi-Implementierung besser planen zu können.

Die Komplexität von ESXi-Implementierungen kann je nach Größe Ihres Unternehmens, der gemeinsamen Nutzung von Daten und Ressourcen durch externe Parteien und der Verwendung eines oder mehrerer Datacenter usw. variieren. Zu den folgenden Implementierungen gehören Richtlinien für den Benutzerzugriff, die gemeinsame Nutzung von Ressourcen sowie Sicherheitsstufen.

Implementierung für einen Kunden

In einer Implementierung für einen Kunden befinden sich ESXi-Hosts in einem Unternehmen und einem einzelnen Datacenter und werden auch dort verwaltet. Hostressourcen werden nicht von externen Benutzern genutzt. Die Hosts werden von einem globalen Administrator verwaltet und auf mehreren virtuellen Maschinen ausgeführt.

Die Bereitstellung für einen einzelnen Kunden lässt keine Kundenadministratoren zu und der Standortadministrator ist nur für die Verwaltung der verschiedenen virtuellen Maschinen verantwortlich. Das Unternehmen beschäftigt mehrere Systemadministratoren, die keine Konten auf dem Host haben und nicht auf ESXi-Tools wie vCenter Server oder Befehlszeilenshells für den Host zugreifen können. Diese Systemadministratoren haben über die VM-Konsole Zugriff auf die virtuellen Maschinen, sodass Sie Software installieren und andere Verwaltungsaufgaben in den virtuellen Maschinen durchführen können.

[Tabelle 14-1](#) zeigt, wie Sie die Komponenten gemeinsam nutzen und für den Host konfigurieren können.

Tabelle 14-1. Gemeinsame Komponentennutzung bei einer Implementierung für einen Kunden

Funktion	Konfiguration	Anmerkungen
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame VMFS-Nutzung?	Ja	Alle .vmdk-Dateien befinden sich in der gleichen VMFS-Partition.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 14-2 zeigt, wie die Benutzerkonten für den Host eingerichtet werden können.

Tabelle 14-2. Benutzerkonten in einer Implementierung für einen Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	0
Systemadministratoren	0
Unternehmensbenutzer	0

Tabelle 14-3 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 14-3. Benutzerzugriff in einer Implementierung für einen Kunden

Zugriffsumfang	Standortadministrator	Systemadministrator
Root-Zugriff?	Ja	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja

Eingeschränkte Implementierung für mehrere Kunden

In einer eingeschränkten Implementierung für mehrere Kunden befinden sich die ESXi-Hosts im gleichen Datacenter und werden für Anwendungen mehrerer Kunden verwendet. Der Standortadministrator verwaltet die Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen Host befinden, doch der Standortadministrator beschränkt die gemeinsame Nutzung von Ressourcen, um die Datensicherheit zu gewährleisten.

Es gibt einen Standortadministrator und mehrere Kundenadministratoren, die die virtuellen Maschinen ihrer jeweiligen Kunden verwalten. Zu dieser Bereitstellung gehören auch Systemadministratoren der Kunden, die kein ESXi-Konto haben, doch über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu installieren und andere Verwaltungsaufgaben in den virtuellen Maschinen durchzuführen.

Tabelle 14-4 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den Host konfigurieren können.

Tabelle 14-4. Gemeinsame Komponentennutzung in einer beschränkten Implementierung für mehrere Kunden

Funktion	Konfiguration	Anmerkungen
Virtuelle Maschinen im gleichen physischen Netzwerk?	Teilweise	Installieren Sie die virtuellen Maschinen jedes Kunden in einem anderen physischen Netzwerk. Alle physischen Netzwerke sind voneinander unabhängig.
Gemeinsame VMFS-Nutzung?	Nein	Jeder Kunde hat seine eigene VMFS-Partition, und die .vmdk-Dateien der virtuellen Maschinen befinden sich ausschließlich auf dieser Partition. Die Partition kann mehrere LUNs umfassen.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

[Tabelle 14-5](#) zeigt, wie die Benutzerkonten für den ESXi-Host eingerichtet werden können.

Tabelle 14-5. Benutzerkonten in einer beschränkten Implementierung für mehrere Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensbenutzer	0

[Tabelle 14-6](#) Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 14-6. Benutzerzugriff in einer beschränkten Implementierung für mehrere Kunden

Zugriffsumfang	Standortadministrator	Kundenadministrator	Systemadministrator
Root-Zugriff?	Ja	Nein	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja	Ja

Beschränkte Implementierung für mehrere Kunden

In einer unbeschränkten Implementierung für mehrere Kunden befinden sich die ESXi-Hosts im gleichen Datacenter und werden für Anwendungen mehrerer Kunden verwendet. Der Standortadministrator verwaltet die Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen Host befinden, doch es gibt weniger Beschränkungen zur gemeinsamen Nutzung von Ressourcen.

Obwohl es nur einen Standortadministrator in einer unbeschränkten Implementierung für mehrere Kunden gibt, verwalten mehrere Kundenadministratoren die virtuellen Maschinen ihrer jeweiligen Kunden. Zu dieser Bereitstellung gehören auch Systemadministratoren der Kunden, die kein ESXi-Konto haben, doch über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu laden und andere Verwaltungsaufgaben in den virtuellen Maschinen durchzuführen. Außerdem kann eine Gruppe von Unternehmensbenutzern ohne Konten die virtuellen Maschinen zur Ausführung ihrer Anwendungen verwenden.

[Tabelle 14-7](#) zeigt, wie Sie die Komponenten gemeinsam nutzen und für den Host konfigurieren können.

Tabelle 14-7. Gemeinsame Komponentennutzung in einer unbeschränkten Implementierung für mehrere Kunden

Funktion	Konfiguration	Anmerkungen
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame VMFS-Nutzung?	Ja	Die virtuellen Maschinen können VMFS-Partitionen gemeinsam nutzen, die .vmdk-Dateien der virtuellen Maschinen können sich auf einer gemeinsamen Partition befinden. Die virtuellen Maschinen verwenden keine gemeinsamen .vmdk-Dateien.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 14-8 zeigt, wie die Benutzerkonten für den Host eingerichtet werden können.

Tabelle 14-8. Benutzerkonten in einer unbeschränkten Implementierung für mehrere Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensbenutzer	0

Tabelle 14-9 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 14-9. Benutzerzugriff in einer unbeschränkten Implementierung für mehrere Kunden

Zugriffsumfang	Standortadministrator	Kundenadministrator	Systemadministrator	Unternehmensbenutzer
Root-Zugriff?	Ja	Nein	Nein	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Ja	Nein	Nein

ESXi-Sperrmodus

Um die Sicherheit von ESXi-Hosts zu verbessern, können Sie diese in den Sperrmodus versetzen. Der Sperrmodus ist nur auf ESXi-Host verfügbar, die vCenter Server hinzugefügt wurden.

Durch Aktivieren des Sperrmodus werden alle direkten Root-Zugriff auf ESXi-Maschinen deaktiviert. Sämtliche anschließenden lokalen Änderungen am Host müssen in einer vSphere-Client-Sitzung oder über einen vSphere-Befehlszeilenschnittstellen-Befehl an vCenter Server mithilfe eines vollständig editierbaren Active Directory-Kontos erfolgen. Sie können auch ein vom Host festgelegtes lokales Benutzerkonto verwenden. Standardmäßig befinden sich auf dem ESXi-System keine lokalen Benutzerkonten. Solche Konten können nur vor Aktivierung des Sperrmodus in einer vSphere-Clientsitzung direkt auf dem ESXi-System erstellt werden. Die Änderungen am Host sind auf die Berechtigungen begrenzt, die dem jeweiligen Benutzer lokal auf diesem Host zugewiesen sind.

Der Sperrmodus kann aktiviert werden, wenn Sie den Assistenten zum Hinzufügen von Hosts verwenden, um dem vCenter Server einen ESXi-Host hinzuzufügen, wobei Sie den vSphere-Client zum Verwalten eines Hosts oder die direkte Konsole verwenden.

Aktivieren des Sperrmodus über den vSphere-Client

Der Sperrmodus deaktiviert jeglichen direkten Root-Zugriff auf ESXi-Hosts. Sie können den Sperrmodus auch über die direkte Konsole aktivieren bzw. deaktivieren.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Wählen Sie den Host im Bestandslistenfenster aus.
- 3 Klicken Sie auf die Registerkarte **[Konfiguration (Configuration)]** und dann auf **[Sicherheitsprofil (Security Profile)]**.

Der vSphere-Client zeigt eine Liste der aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.

- 4 Klicken Sie neben Sperrmodus auf den Link **[Bearbeiten]**.
Das Dialogfeld **[Sperrmodus]** wird angezeigt.
- 5 Wählen Sie **[Aktivieren von Sperrmodus]**.
- 6 Klicken Sie auf **[OK]**.

Aktivieren des Sperrmodus in der direkten Konsole

Sie können den Sperrmodus in der direkten Konsole und im vSphere-Client aktivieren.

Vorgehensweise

- ◆ Umschalten der Einstellung **[Sperrmodus konfigurieren]**.

Empfehlungen für virtuelle Maschinen

Bei der Überprüfung der Sicherheit virtueller Maschinen und ihrer Verwaltung gibt es verschiedene zu berücksichtigende Sicherheitsmaßnahmen.

Installieren von Antivirensoftware.

Da auf jeder virtuellen Maschine ein Standardbetriebssystem ausgeführt wird, sollten Sie es durch die Installation von Antivirensoftware gegen Viren schützen. Je nach Verwendungszweck der virtuellen Maschine sollte ggf. auch eine Firewall installiert werden.

Planen Sie die Virenprüfungen zeitlich versetzt, insbesondere in Implementierungen mit vielen virtuellen Maschinen. Die Leistung der Systeme in Ihrer Umgebung wird entscheidend verringert, wenn alle virtuellen Maschinen gleichzeitig geprüft werden.

Softwarefirewalls und Antivirensoftware können die Virtualisierungsleistung beeinflussen. Sie können die beiden Sicherheitsmaßnahmen gegen Leistungsvorteile abwägen, insbesondere wenn Sie sich sicher sind, dass sich die virtuellen Maschinen in einer vollständig vertrauenswürdigen Umgebung befinden.

Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole

Sie können das Kopieren und Einfügen deaktivieren, um vertrauliche Daten davor zu schützen, in die Zwischenablage kopiert zu werden.

Wenn VMware Tools auf einer virtuellen Maschine ausgeführt wird, können Sie Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole ausführen. Sobald das Konsolenfenster den Eingabefokus hat, können unbefugte Benutzer und Prozesse in der virtuellen Maschine auf die Zwischenablage der Konsole der virtuellen Maschine zugreifen. Wenn ein Benutzer vor der Verwendung der Konsole vertrauliche Informationen in die Zwischenablage kopiert, macht der Benutzer der virtuellen Maschine, ggf. unwissentlich, vertrauliche Daten zugänglich. Um dies zu verhindern, können Sie Kopier- und Einfügevorgänge für das Gastbetriebssystem deaktivieren.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Wählen Sie **[Optionen] > [Erweitert] > [Allgemein]** aus und klicken Sie auf **[Konfigurationsparameter]**.
- 4 Klicken Sie auf **[Zeile hinzufügen]** und geben Sie die folgenden Werte in den Spalten „Name“ und „Wert“ ein:

Name	Wert
<code>isolation.tools.copy.disable</code>	<code>true</code>
<code>isolation.tools.paste.disable</code>	<code>true</code>
<code>isolation.tools.setGUIOptions.enable</code>	<code>false</code>

HINWEIS Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

Das Ergebnis sieht folgendermaßen aus.

Name	Feld „Wert“
<code>sched.mem.max</code>	unbegrenzt
<code>sched.swap.derivedName</code>	vmfs/volumes/e5f9f3d1-ed4d8ba/Neue virtuelle Maschine
<code>scsi0:0.redo</code>	true
<code>vmware.tools.installstate</code>	keine
<code>vmware.tools.lastInstallStatus.result</code>	unbekannt
<code>isolation.tools.copy.disable</code>	true
<code>isolation.tools.paste.disable</code>	true
<code>isolation.tools.setGUIOptions.enable</code>	false

- 5 Klicken Sie auf **[OK]**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **[OK]**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Entfernung überflüssiger Hardwaregeräte

Benutzer und Prozesse ohne Berechtigungen für die virtuelle Maschine können Hardwaregeräte wie Netzwerkadapter oder CD-ROM-Laufwerke einbinden oder trennen. Das Entfernen überflüssiger Hardwaregeräte kann somit Angriffe verhindern.

Angreifer können diese Fähigkeit auf verschiedene Arten nutzen, um die Sicherheit einer virtuellen Maschine zu gefährden. So kann zum Beispiel ein Angreifer mit Zugang zu einer virtuellen Maschine ein nicht verbundenes CD-ROM-Laufwerk einbinden und auf vertrauliche Informationen auf dem Medium zugreifen, das sich im Laufwerk befindet, oder einen Netzwerkadapter trennen, um die virtuelle Maschine vom Netzwerk zu isolieren, was zu einem Denial-Of-Service führt.

Als allgemeine Sicherheitsmaßnahme sollten Sie Befehle auf der Registerkarte **[Konfiguration]** auf dem vSphere-Client verwenden, um alle nicht benötigten oder ungenutzten Hardwaregeräte zu entfernen. Obwohl diese Maßnahme die Sicherheit der virtuellen Maschinen erhöht, aber ist sie keine gute Lösung, wenn ein ungenutztes Gerät später reaktiviert werden soll.

Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt

Wenn Sie ein Gerät nicht dauerhaft entfernen möchten, können Sie verhindern, dass ein Benutzer oder Prozess einer virtuellen Maschine das Gerät aus dem Gastbetriebssystem heraus einbindet oder trennt.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Wählen Sie die virtuelle Maschine im Bestandslistenfenster aus.
- 3 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 4 Wählen Sie **[Optionen] > [Allgemeine Optionen]** aus und notieren Sie den Pfad, der im Textfeld **[Konfigurationsdatei der virtuellen Maschine]** angezeigt wird.
- 5 Verwenden Sie den Befehl `vifs`, um eine Kopie der Konfigurationsdateien der virtuellen Maschine von dem Speicherort abzurufen, den Sie in [Schritt 4](#) notiert haben.

Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/<Datenspeicher>`, wobei es sich bei `<Datenspeicher>` um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine sich befinden. Wenn beispielsweise die Konfigurationsdatei der virtuellen Maschine, die Sie im Dialogfeld „Eigenschaften der virtuellen Maschine“ abgerufen haben, `[vol1]vm-finance/vm-finance.vmx` ist, verwenden Sie den folgenden Befehl:

```
vifs --server <Hostname> --username <Benutzername> --get /vmfs/volumes/vol1/vm-finance/vm-finance.vmx <Verzeichnis>/vm-finance.vmx
```

- 6 Fügen Sie der `.vmx`-Datei mit einem Texteditor die folgende Zeile hinzu, wobei `<Gerätename>` der Name des Geräts ist, das geschützt werden soll (z. B. `ethernet1`):

```
<Gerätename>.allowGuestConnectionControl = "false"
```

HINWEIS Standardmäßig ist Ethernet 0 so konfiguriert, dass die Trennung des Geräts nicht möglich ist. Der einzige Grund, der Sie dazu veranlassen könnte, dies zu ändern, ist dann gegeben, wenn ein vorheriger Administrator `<Gerätename>.allowGuestConnectionControl` auf `true` gesetzt hat.

- 7 Speichern Sie die Änderungen, und schließen Sie die Datei.

- 8 Legen Sie mithilfe des Befehls `vifs` die geänderte Kopie der Datei an dem Speicherort ab, den Sie in [Schritt 4](#) notiert haben.


```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>/vm-finance.vmx /vmfs/
volumes/vol1/vm-finance/vm-finance.vmx
```
- 9 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie die Option **[Ausschalten]** aus.
- 10 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie die Option **[Einschalten]** .

Beschränken von Schreibvorgängen des Gastbetriebssystems in den Hostspeicher

Die Prozesse des Gastbetriebssystems senden über VMware Tools informative Meldungen an den ESXi-Host. Wenn die Datenmenge, die als Folge dieser Meldungen auf dem Host gespeichert wird, unbegrenzt wäre, würde eine unbeschränkte Datenübertragung einem Angreifer eine Gelegenheit zum Starten eines Denial-of-Service-Angriffs (DoS) bieten.

Diese von Prozessen des Gastbetriebssystems gesendeten Informationsmeldungen, die `setinfo`-Meldungen genannt werden, enthalten normalerweise Name/Wert-Paare zu Merkmalen virtueller Maschinen oder Bezeichner, die der Host speichert, zum Beispiel `ipaddress=10.17.87.224`. Die Konfigurationsdatei mit diesen Name/Wert-Paaren ist auf eine maximale Größe von 1 MB beschränkt, womit verhindert wird, dass Angreifer einen DoS-Angriff starten können. Dazu müsste Code geschrieben werden, der VMware Tools imitiert und den Speicher des Hosts mit willkürlichen Konfigurationsdaten auffüllt, wodurch Speicherplatz belegt wird, der von den virtuellen Maschinen benötigt wird.

Wenn Sie mehr als 1 MB für die Speicherung der Name/Wert-Paare benötigen, können Sie den Wert bei Bedarf ändern. Sie können auch verhindern, dass Prozesse des Gastbetriebssystems Name/Wert-Paare in die Konfigurationsdatei schreiben.

Ändern des variablen Speicherlimits des Gastbetriebssystems

Sie können das variable Speicherlimit des Gastbetriebssystems erhöhen, wenn große Mengen von benutzerdefinierten Informationen in der Konfigurationsdatei gespeichert werden.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Wählen Sie die virtuelle Maschine im Bestandslistenfenster aus.
- 3 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]** .
- 4 Wählen Sie **[Optionen]** > **[Erweitert]** > **[Allgemein]** aus und klicken Sie auf **[Konfigurationsparameter]** .
- 5 Wenn das Attribut zur Größenbegrenzung nicht vorhanden ist, müssen Sie es hinzufügen.
 - a Klicken Sie auf **[Zeile hinzufügen]** .
 - b Geben Sie `tools.setInfo.sizeLimit` in der Spalte „Name“ ein.
 - c Geben Sie **Anzahl der Bytes** in der Spalte „Wert“ ein.

Wenn das Größenlimitattribut vorhanden ist, passen Sie es wie gewünscht an.

- 6 Klicken Sie auf **[OK]** , um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **[OK]** , um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden

Sie können Gäste daran hindern, Name/Wert-Paare in die Konfigurationsdatei zu schreiben. Dies bietet sich an, wenn Gastbetriebssysteme am Ändern von Konfigurationseinstellungen gehindert werden müssen.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Wählen Sie die virtuelle Maschine im Bestandslistenfenster aus.
- 3 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 4 Wählen Sie **[Optionen] > [Erweitert] > [Allgemein]** aus und klicken Sie auf **[Konfigurationsparameter]**.
- 5 Klicken Sie auf **[Zeile hinzufügen]** und geben Sie die folgenden Wert in den Spalten „Name“ und „Wert“ ein:
 - In der Spalte „Name“: `isolation.tools.setinfo.disable`
 - In der Spalte „Wert“: `true`
- 6 Klicken Sie auf **[OK]**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **[OK]**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Konfigurieren der Protokollierungsebenen für das Gastbetriebssystem

Virtuelle Maschinen können Informationen zur Fehlerbehebung in eine Protokolldatei der virtuellen Maschine schreiben, die auf dem VMFS-Volume gespeichert wird. Benutzer und Prozesse virtueller Maschinen können die Protokollierung entweder absichtlich oder unabsichtlich missbrauchen, sodass große Datenmengen die Protokolldatei überfluten. Mit der Zeit kann die Protokolldatei so genug Speicherplatz im Dateisystem der Servicekonsole belegen, um einen Ausfall zu verursachen.

Um dieses Problem zu verhindern, können Sie die Protokollierung für die Gastbetriebssysteme virtueller Maschinen deaktivieren. Mit diesen Einstellungen können die Gesamtgröße und die Anzahl der Protokolldateien begrenzt werden. Normalerweise wird bei jedem Neustart eines Hosts eine neue Protokolldatei erstellt, sodass die Datei relativ groß werden kann. Sie können jedoch sicherstellen, dass die Erstellung neuer Protokolldateien häufiger erfolgt, indem Sie die maximale Größe der Protokolldateien begrenzen. VMware empfiehlt das Speichern von zehn Protokolldateien mit maximal jeweils 100 KB. Diese Werte sind groß genug, um ausreichend Daten zu erfassen, die zum Beheben der meisten ggf. auftretenden Probleme erforderlich sind.

Immer wenn ein Eintrag in das Protokoll geschrieben wird, erfolgt eine Überprüfung der Protokollgröße. Ist der Grenzwert überschritten, wird der nächste Eintrag in ein neues Protokoll geschrieben. Wenn die maximale Anzahl an Protokolldateien erreicht ist, wird die älteste gelöscht. Ein Denial-of-Service-Angriff, der diese Grenzwerte umgeht, könnte versucht werden, indem ein riesiger Protokolleintrag geschrieben wird, doch jeder Protokolleintrag ist auf 4 KB begrenzt, sodass keine Protokolldatei jemals mehr als 4KB größer als der konfigurierte Grenzwert ist.

Begrenzen von Anzahl und Größe von Protokolldateien

Sie können die Anzahl und die Größe der von ESXi generierten Protokolldateien begrenzen, um zu verhindern, dass Benutzer und Prozesse von virtuellen Maschinen die Protokolldatei überfluten und damit einen Denial-of-Service verursachen können.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client bei einem vCenter Server-System an.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Wählen Sie **[Optionen] > [Allgemeine Optionen]** aus und notieren Sie den Pfad, der im Textfeld **[Konfigurationsdatei der virtuellen Maschine]** angezeigt wird.
- 4 Verwenden Sie den Befehl `vifs`, um eine Kopie der Konfigurationsdateien der virtuellen Maschine von dem Speicherort abzurufen, den Sie in [Schritt 4](#) notiert haben.

Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/<Datenspeicher>`, wobei es sich bei `<Datenspeicher>` um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine sich befinden. Wenn beispielsweise die Konfigurationsdatei der virtuellen Maschine, die Sie im Dialogfeld „Eigenschaften der virtuellen Maschine“ abgerufen haben, `[vol1]vm-finance/vm-finance.vmx` ist, verwenden Sie den folgenden Befehl:


```
vifs --server <Hostname> --username <Benutzername> --get /vmfs/volumes/vol1/vm-finance/vm-finance.vmx <Verzeichnis>/vm-finance.vmx
```
- 5 Verwenden Sie einen Texteditor, um die Protokollgröße zu begrenzen, indem Sie die `.vmx`-Datei um die folgende Zeile ergänzen, wobei `<Maximalgröße>` die Maximalgröße der Datei in Byte ist:


```
log.rotateSize=<Maximalgröße>
```


Um beispielsweise die Datei auf 100 KB zu begrenzen, geben Sie **100000** ein.
- 6 Verwenden Sie einen Texteditor, um die Anzahl der Protokolldateien zu begrenzen, indem Sie die `.vmx`-Datei um die folgende Zeile ergänzen, wobei `<Gewünschte_Anzahl_an_Dateien>` die Anzahl der Dateien ist, die auf dem Server gespeichert bleiben:


```
log.keepOld=<Anzahl_der_aufzubewahrenden_Dateien>
```


Um beispielsweise zehn Protokolldateien zu speichern und anschließend mit dem Löschen der ältesten und Erstellen neuer Dateien zu beginnen, geben Sie **10** ein.
- 7 Speichern Sie die Änderungen, und schließen Sie die Datei.
- 8 Legen Sie mithilfe des Befehls `vifs` die geänderte Kopie der Datei an dem Speicherort ab, den Sie in [Schritt 4](#) notiert haben.


```
vifs --server <Hostname> --username <Benutzername> --put <Verzeichnis>/vm-finance.vmx /vmfs/volumes/vol1/vm-finance/vm-finance.vmx
```

Deaktivieren der Protokollierung für das Gastbetriebssystem

Wenn Sie Informationen zur Fehlerbehebung nicht in eine Protokolldatei der virtuellen Maschine aufzeichnen möchten, die auf dem VMFS-Volumen gespeichert wird, können Sie die Protokollierung vollständig deaktivieren.

Wenn Sie die Protokollierung für das Gastbetriebssystem deaktivieren, sind Sie ggf. nicht in der Lage, entsprechende Protokolle für die Fehlerbehebung zu sammeln. Außerdem leistet VMware keine technische Unterstützung für virtuelle Maschinen, bei denen die Protokollierung deaktiviert wurde.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client am vCenter Server-System an und klicken Sie im Bestandslistenfenster auf die virtuelle Maschine.
- 2 Klicken Sie auf der Registerkarte **[Übersicht (Summary)]** auf **[Einstellungen bearbeiten (Edit Settings)]**.
- 3 Klicken Sie auf die Registerkarte **[Optionen]** und wählen Sie in der Optionsliste unter Erweitert die Option **[Allgemein]** aus.
- 4 Deaktivieren Sie unter „Einstellungen“ die Option **[Protokollierung aktivieren]**.
- 5 Klicken Sie auf **[OK]**, um das Eigenschaftendialogfeld der virtuellen Maschine zu schließen.

Hostprofile

Verwalten von Hostprofilen

Die Hostprofilfunktion erstellt ein Profil, das die Hostkonfiguration enthält und für deren Verwaltung hilfreich ist, insbesondere in Umgebungen, in denen ein Administrator mehrere Hosts oder Cluster in vCenter Server verwaltet.

Diese Funktion macht die hostbasierte, die manuelle oder die benutzeroberflächenbasierte Hostkonfiguration überflüssig und sorgt durch die Verwendung von Hostprofil-Richtlinien für die Konsistenz und Korrektheit der Konfiguration innerhalb des gesamten Datencenters. Diese Richtlinien halten den Entwurf einer bekannten, validierten Konfiguration des Referenzhosts fest und konfigurieren davon ausgehend das Netzwerk, den Speicher, die Sicherheit und andere Einstellungen auf mehreren Hosts oder Clustern. Sie können dann einen Host oder Cluster mit der Konfiguration eines Profils vergleichen, um Abweichungen zu erkennen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Modell für die Verwendung von Hostprofilen“](#), auf Seite 189
- [„Zugreifen auf die Ansicht „Hostprofile““](#), auf Seite 190
- [„Erstellen eines Hostprofils“](#), auf Seite 190
- [„Exportieren eines Hostprofils“](#), auf Seite 191
- [„Importieren eines Hostprofils“](#), auf Seite 192
- [„Bearbeiten eines Hostprofils“](#), auf Seite 192
- [„Verwalten von Profilen“](#), auf Seite 194
- [„Prüfen der Übereinstimmung“](#), auf Seite 197

Modell für die Verwendung von Hostprofilen

In diesem Thema werden die Arbeitsabläufe für die Verwendung von Hostprofilen beschrieben.

Es muss eine vSphere-Installation mit mindestens einem ordnungsgemäß konfigurierten Host vorhanden sein.

- 1 Richten Sie den Host, der als Referenzhost verwendet wird, ein und konfigurieren Sie ihn.
Ein Referenzhost ist der Host, aus dem das Profil erstellt wird.
- 2 Erstellen Sie mithilfe des festgelegten Referenzhosts ein Profil.
- 3 Hängen Sie einen Host oder einen Cluster an das Profil an.

- 4 Überprüfen Sie die Übereinstimmung des Hostprofils. Dadurch wird sichergestellt, dass der Host weiterhin korrekt konfiguriert ist.
- 5 Übernehmen Sie das Hostprofil des Referenzhosts für andere Hosts oder Hostcluster.

HINWEIS Die Hostprofilfunktion wird nur für VMware vSphere 4.0-Hosts unterstützt. Diese Funktion wird für VI-Hosts der Version 3.5 oder früher nicht unterstützt. Wenn vCenter Server 4.0 VI-Hosts der Version 3.5 oder früher verwaltet, kann beim Verwenden von Hostprofilen für diese Hosts Folgendes eintreten:

- Sie können kein Hostprofil erstellen, das einen VMware Infrastructure-Host der Version 3.5 oder früher als Referenzhost verwendet.
- Sie können kein Hostprofil auf VI-Hosts der Version 3.5 oder früher anwenden. Die Übereinstimmungsprüfung schlägt fehl.
- Sie können zwar ein Hostprofil an einen gemischten Cluster anhängen, der VI 3.5-Hosts oder früher enthält, die Überprüfung der Richtlinien Einhaltung für diese Hosts schlägt jedoch fehl.

Hostprofile sind als Lizenzfunktion von vSphere nur dann verfügbar, wenn die entsprechende Lizenzierung vorhanden ist. Wenn Fehler auftreten, stellen Sie sicher, dass die entsprechende vSphere-Lizenzierung für Ihren Host vorhanden ist.

Zugreifen auf die Ansicht „Hostprofile“

In der Hauptansicht für Hostprofile sind alle verfügbaren Profile aufgelistet. Administratoren können über die Hauptansicht „Hostprofile“ auch Vorgänge zu Hostprofilen ausführen und Profile konfigurieren.

Die Hauptansicht „Hostprofile“ sollte von erfahrenen Administratoren verwendet werden, die Hostprofilvorgänge durchführen sowie erweiterte Optionen und Richtlinien konfigurieren möchten. Die meisten Vorgänge, wie das Erstellen neuer Profile, das Anhängen von Elementen und das Übernehmen von Profilen, können über die Ansicht „Hosts und Cluster“ durchgeführt werden.

Vorgehensweise

- ◆ Wählen Sie **[Ansicht] > [Management] > [Hostprofile]**.

Alle vorhandenen Profile werden auf der linken Seite der Profilliste aufgelistet. Wenn ein Profil in der Profilliste ausgewählt wird, werden die Informationen zu dem Profil auf der rechten Seite angezeigt.

Erstellen eines Hostprofils

Zum Erstellen eines neuen Hostprofils verwenden Sie die Konfiguration des festgelegten Referenzhosts.

Ein Hostprofil kann von der Hauptansicht „Hostprofile“ oder dem Kontextmenü des Hosts in der Ansicht „Hosts und Cluster“ aus erstellt werden.

Erstellen eines Hostprofils über die Ansicht „Hostprofile“

Sie können über die Hauptansicht „Hostprofile“ mithilfe der Konfiguration eines bestehenden Hosts ein Hostprofil erstellen.

Voraussetzungen

Es müssen eine vSphere-Installation und mindestens ein ordnungsgemäß konfigurierter Host in der Bestandsliste vorhanden sein.

Vorgehensweise

- 1 Klicken Sie in der Hauptansicht „Hostprofile“ auf das Symbol **[Profil erstellen]** .
Der Assistent zum Erstellen von Profilen wird angezeigt.
- 2 Wählen Sie die Option zum Erstellen eines neuen Profils aus und klicken Sie auf **[Weiter]** .
- 3 Wählen Sie den zum Erstellen des Profils zu verwendenden Host aus und klicken Sie auf **[Weiter]** .
- 4 Geben Sie den Namen und eine Beschreibung für das neue Profil ein und klicken Sie dann auf **[Weiter]** .
- 5 Überprüfen Sie die zusammengefassten Informationen für das neue Profil und klicken Sie auf **[Beenden]** , um die Erstellung des Profils abzuschließen.

Das neue Profil wird in der Profilliste angezeigt.

Erstellen eines Hostprofils über den Host

Sie können in der Bestandslistenansicht „Hosts und Cluster“ über das Kontextmenü eines Hosts ein neues Hostprofil erstellen.

Voraussetzungen

Es müssen eine vSphere-Installation und mindestens ein ordnungsgemäß konfigurierter Host in der Bestandsliste vorhanden sein.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, den Sie als Referenzhost für das neue Hostprofil festlegen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **[Hostprofil] > [Profil vom Host erstellen]**
Der Assistent Profil vom Host erstellen wird geöffnet.
- 3 Geben Sie den Namen und eine Beschreibung für das neue Profil ein und klicken Sie dann auf **[Weiter]** .
- 4 Überprüfen Sie die zusammengefassten Informationen für das neue Profil und klicken Sie auf **[Beenden]** , um die Erstellung des Profils abzuschließen.

Das neue Profil wird auf der Registerkarte „Übersicht“ des Hosts angezeigt.

Exportieren eines Hostprofils

Sie können ein Profil in eine Datei exportieren, die das VMware-Profilformat (.vpf) besitzt.

Vorgehensweise

- 1 Wählen Sie auf der Hauptseite „Hostprofile“ in der Profilliste das zu exportierende Profil aus.
- 2 Wählen Sie den Speicherort aus und geben Sie den Namen der Datei ein, in die das Profil exportiert wird.
- 3 Klicken Sie auf **[Speichern (Save)]** .

Importieren eines Hostprofils

Sie können ein Profil aus einer Datei importieren, die das VMware-Profilformat (.vpf) besitzt.

Vorgehensweise

- 1 Klicken Sie auf der Hauptseite „Hostprofile“ auf das Symbol **[Profil erstellen]** .
Der Assistent zum Erstellen von Profilen wird angezeigt.
- 2 Wählen Sie die Option zum Importieren eines Profils aus und klicken Sie auf **[Weiter]** .
- 3 Geben Sie die zu importierende Datei im VMware-Profilformat an oder suchen Sie nach ihr. Klicken Sie anschließend auf **[Weiter]** .
- 4 Geben Sie den Namen und eine Beschreibung für das importierte Profil ein und klicken Sie dann auf **[Weiter]** .
- 5 Überprüfen Sie die zusammengefassten Informationen für das importierte Profil und klicken Sie auf **[Beenden]** , um den Import des Profils abzuschließen.

Das importierte Profil wird in der Profilliste angezeigt.

Bearbeiten eines Hostprofils

Sie können Hostprofil-Richtlinien anzeigen und bearbeiten, eine Richtlinie auswählen, die auf Übereinstimmung geprüft werden soll, sowie den Namen oder die Beschreibung der Richtlinie ändern.

Vorgehensweise

- 1 Wählen Sie auf der Hauptansicht „Hostprofile“ in der Profilliste das zu bearbeitende Profil aus.
- 2 Klicken Sie auf **[Hostprofil bearbeiten]** .
- 3 Ändern Sie den Namen oder die Beschreibung des Profils in den Feldern im oberen Bereich des Profileditors.
- 4 (Optional) Bearbeiten oder deaktivieren Sie die Richtlinie.
- 5 Aktivieren Sie die Übereinstimmungsprüfung für die Richtlinie.
- 6 Klicken Sie auf **[OK]** , um den Profileditor zu schließen.

Bearbeiten einer Richtlinie

Eine Richtlinie beschreibt, wie eine bestimmte Konfigurationseinstellung angewendet werden soll. Mit dem Profileditor können Sie die zu einem bestimmten Hostprofil gehörenden Richtlinien bearbeiten.

Auf der linken Seite des Profileditors können Sie das Hostprofil erweitern. Jedes Hostprofil besteht aus mehreren Unterprofilen, die nach Funktionsgruppe für die Repräsentation von Konfigurationsinstanzen festgelegt sind. Jedes Unterprofil enthält viele Richtlinien, die die für das Profil relevante Konfiguration beschreiben.

Folgende Unterprofile (sowie Beispielrichtlinien und Übereinstimmungsprüfungen) können konfiguriert werden:

Tabelle 15-1. Unterprofilkonfigurationen von Hostprofilen

Unterprofilkonfiguration	Beispielrichtlinien und Übereinstimmungsprüfungen
Arbeitsspeicherreservierung	Legen Sie die Arbeitsspeicherreservierung auf einen festen Wert fest.
Speicher	Konfigurieren Sie den NFS-Speicher.

Tabelle 15-1. Unterprofilkonfigurationen von Hostprofilen (Fortsetzung)

Unterprofilkonfiguration	Beispielrichtlinien und Übereinstimmungsprüfungen
Netzwerkbetrieb	Konfigurieren Sie Virtuellen Switch, Portgruppen, Geschwindigkeit der physischen NIC, Sicherheit und NIC-Gruppierungsrichtlinien.
Datum und Uhrzeit	Konfigurieren Sie die Zeiteinstellungen bzw. die Serverzeitzone.
Firewall	Aktivieren oder deaktivieren Sie einen Regelsatz.
Sicherheit	Fügen Sie einen Benutzer oder eine Benutzergruppe hinzu.
Dienst	Konfigurieren Sie die Einstellungen für einen Dienst.
Erweitert	Ändern Sie die erweiterten Optionen.

Vorgehensweise

- 1 Öffnen Sie den Profileditor für das Profil, das Sie bearbeiten möchten.
- 2 Erweitern Sie auf der linken Seite des Profileditors ein Unterprofil, bis Sie zu der Richtlinie gelangen, die Sie bearbeiten möchten.
- 3 Wählen Sie die Richtlinie aus.
Auf der rechten Seite des Profileditors werden die Optionen und Parameter für die Richtlinie auf der Registerkarte **[Konfigurationsinformationen]** angezeigt.
- 4 Wählen Sie im Dropdown-Menü eine Richtlinienoption aus und legen Sie ihren Parameter fest.
- 5 (Optional) Wenn Sie eine Änderung an einer Richtlinie vorgenommen haben, jedoch die Standardoption wiederherstellen möchten, klicken Sie auf **[Wiederherstellen]**. Die Option wird zurückgesetzt.

Aktivieren der Überprüfung der Richtlinieneinhaltung

Sie können festlegen, ob eine Hostprofil-Richtlinie auf Übereinstimmung geprüft werden soll.

Vorgehensweise

- 1 Öffnen Sie den Profileditor für ein Profil und navigieren Sie zu der Richtlinie, die Sie für die Übereinstimmungsprüfung aktivieren möchten.
- 2 Wählen Sie auf der rechten Seite des Profileditors die Registerkarte **[Übereinstimmungsinformationen]**.
- 3 Aktivieren Sie das Kontrollkästchen für die Richtlinie.

HINWEIS Wenn Sie das Kontrollkästchen deaktivieren, damit diese Richtlinie nicht auf Übereinstimmung geprüft wird, werden die anderen Richtlinien, die für die Übereinstimmungsprüfung aktiviert sind, dennoch überprüft.

Verwalten von Profilen

Nachdem Sie ein Hostprofil erstellt haben, können Sie es verwalten, indem Sie es an einen bestimmten Host oder Cluster anhängen und es anschließend für den Host oder Cluster übernehmen.

Anhängen von Elementen

Hosts, die konfiguriert werden müssen, werden einem Profil zugewiesen. Profile können auch einem Cluster zugewiesen werden. Zur Übereinstimmung müssen alle Hosts innerhalb eines zugewiesenen Clusters dem Profil gemäß konfiguriert werden.

Sie können einen Host oder Cluster wie folgt an ein Profil anhängen:

- Hauptansicht „Hostprofile“
- Über das Kontextmenü eines Hosts
- Über das Kontextmenü eines Clusters
- Registerkarte „Profil-Übereinstimmung“ des Clusters

Anhängen von Elementen über die Ansicht „Hostprofile“

Bevor Sie das Profil für ein Element (einen Host oder Hostcluster) übernehmen können, müssen Sie das Element an das Profil anhängen.

Sie können über die Hauptansicht „Hostprofile“ einen Host oder Cluster an ein Profil anhängen.

Vorgehensweise

- 1 Wählen Sie in der Hauptansicht „Hostprofile“ in der Profilliste das Profil aus, zu dem Sie den Anhang hinzufügen möchten.
- 2 Klicken Sie auf das Symbol **[Host/Cluster anhängen]**.
- 3 Wählen Sie den Host oder Cluster in der erweiterten Liste aus und klicken Sie auf **[Anhängen]**.
Der Host bzw. Cluster wird zur Liste der angehängten Einheiten hinzugefügt.
- 4 (Optional) Klicken Sie auf **[Trennen]**, um einen Anhang von einem Host oder Cluster zu entfernen.
- 5 Klicken Sie auf **[OK]**, um das Dialogfeld zu schließen.

Anhängen von Elementen über den Host

Bevor Sie das Profil auf den Host anwenden können, müssen Sie das Element an das Profil anhängen.

Sie können in der Bestandslistenansicht „Hosts und Cluster“ über das Kontextmenü eines Hosts ein Profil an den Host anhängen.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, dem Sie ein Profil anhängen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **[Hostprofil] > [Profil verwalten]**.

HINWEIS Wenn Ihre Bestandsliste keine Hostprofile enthält, wird ein Dialogfeld mit der Frage angezeigt, ob Sie den Host erstellen und ihn an dieses Profil anhängen möchten.

- 3 Wählen Sie im Dialogfeld Angehängtes Profil ändern das Profil aus, das Sie an den Host anhängen möchten, und klicken Sie auf **[OK]**.

Das Hostprofil wird auf der Registerkarte **[Übersicht]** des Hosts aktualisiert.

Übernehmen von Profilen

Um einen Host in den im Profil angegebenen Zustand zu versetzen, sollten Sie das Profil auf den Host anwenden.

Sie können ein Profil für einen Host wie folgt übernehmen:

- Hauptansicht „Hostprofile“
- Über das Kontextmenü eines Hosts
- Registerkarte „Profil-Übereinstimmung“ des Clusters

Anwenden eines Profils über die Ansicht „Hostprofile“

Sie können über die Hauptansicht „Hostprofile“ ein Profil auf einen Host anwenden.

Voraussetzungen

Der Host muss sich im Wartungsmodus befinden, bevor ein Profil auf ihn angewendet wird.

Vorgehensweise

- 1 Wählen Sie in der Hauptansicht „Hostprofile“ das Profil aus, das Sie auf den Host anwenden möchten.
- 2 Wählen Sie die Registerkarte **[Hosts und Cluster]** aus.

Die Liste der angehängten Hosts wird unter „Elementname“ angezeigt.

- 3 Klicken Sie auf **[Profil übernehmen]**.

Im Profileditor werden Sie möglicherweise aufgefordert, die für das Übernehmen des Profils erforderlichen Parameter einzugeben.

- 4 Geben Sie die Parameter ein und klicken Sie auf **[Weiter]**.
- 5 Fahren Sie fort, bis alle erforderlichen Parameter eingegeben sind.
- 6 Klicken Sie auf **[Beenden]**.

Der Übereinstimmungsstatus wird aktualisiert.

Anwenden eines Profils über den Host

Sie können ein Profil auf einen Host über dessen Kontextmenü anwenden.

Voraussetzungen

Der Host muss sich im Wartungsmodus befinden, bevor es anhand eines Profils konfiguriert werden kann.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, auf den Sie ein Profil anwenden möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **[Hostprofil] > [Profil übernehmen]**.
- 3 Geben Sie im Profileditor die Parameter ein und klicken Sie auf **[Weiter]**.
- 4 Fahren Sie fort, bis alle erforderlichen Parameter eingegeben sind.
- 5 Klicken Sie auf **[Beenden]**.

Der Übereinstimmungsstatus wird aktualisiert.

Ändern von Referenzhost

Zum Erstellen des Hostprofils wird die Konfiguration des Referenzhosts verwendet.

Sie können diese Aufgabe über die Hauptansicht „Hostprofile“ ausführen.

Voraussetzungen

Das Hostprofil muss bereits vorhanden sein.

Vorgehensweise

- 1 Sie können diese Aufgabe über die Hauptansicht „Hostprofile“ oder über den Host ausführen.
 - ◆ Klicken Sie in der Hauptansicht „Hostprofile“ mit der rechten Maustaste auf das Profil, für das Sie den Referenzhost ändern möchten, und wählen Sie **[Referenzhost ändern]**.
 - ◆ Klicken Sie in der Ansicht „Hosts und Cluster“ mit der rechten Maustaste auf den Host, für den Referenzen aktualisiert werden sollen, und wählen Sie **[Profile verwalten]**.

Das Dialogfeld zum Trennen oder Ändern von Hostprofilen wird angezeigt.

- 2 Geben Sie an, ob Sie das Profil vom Host oder Cluster trennen oder den Referenzhost des Profils ändern möchten.
 - ◆ Klicken Sie auf **[Trennen]**, um die Verbindung zwischen Host und Profil zu entfernen.
 - ◆ Klicken Sie auf **[Ändern]**, um den Referenzhost des Profils zu aktualisieren.

Anschließend wird das Dialogfeld Referenzhost ändern angezeigt. Der gegenwärtig vom Profil referenzierte Host wird als **[Referenzhost]** angezeigt.

- 3 Erweitern Sie die Bestandsliste und wählen Sie den Host aus, dem Sie das Profil anhängen möchten.
- 4 Klicken Sie auf **[Aktualisieren]**.

Der **[Referenzhost]** wird aktualisiert.

- 5 Klicken Sie auf **[OK]**.

Auf der Registerkarte „Übersicht“ für das Hostprofil wird der aktualisierte Referenzhost aufgelistet.

Verwalten von Profilen über einen Cluster

Sie können über das Kontextmenü des Clusters Profile erstellen, Profile anhängen oder Referenzhosts aktualisieren.

Vorgehensweise

- ◆ Klicken Sie in der Ansicht „Hosts und Cluster“ mit der rechten Maustaste auf einen Cluster und wählen Sie **[Hostprofil] > [Profil verwalten]** . Je nach Hostprofil-Setup kann Folgendes eintreten:

Profilstatus	Ergebnis
Der Cluster ist keinem Hostprofil angehängt und in Ihrer Bestandsliste wird kein Profil aufgeführt.	<ul style="list-style-type: none"> a Es wird ein Dialogfeld geöffnet, in dem Sie wählen können, ob Sie ein Profil erstellen und dieses dem Cluster anhängen möchten. b Wenn Sie [Ja] wählen, wird der Assistent zum Erstellen von Profilen geöffnet.
Der Cluster ist keinem Hostprofil angehängt und in Ihrer Bestandsliste wird mindestens ein Profil aufgeführt.	<ul style="list-style-type: none"> a Das Dialogfeld Profil anhängen wird geöffnet. b Wählen Sie das Profil aus, das Sie dem Cluster anhängen möchten, und klicken Sie auf [OK] .
Der Cluster wurde bereits einem Hostprofil angehängt.	Klicken Sie im Dialogfeld auf [Trennen] , um das Profil vom Cluster zu trennen, oder auf [Ändern] , um dem Cluster ein anderes Profil anzuhängen.

Prüfen der Übereinstimmung

Beim Prüfen der Übereinstimmung wird sichergestellt, dass der Host oder Cluster weiterhin korrekt konfiguriert ist.

Nachdem ein Host oder Cluster mit dem Profil des Referenzhost konfiguriert wurde, kann beispielsweise eine manuelle Änderungen zu einer fehlerhaften Konfiguration führen. Durch regelmäßiges Prüfen der Übereinstimmung wird sichergestellt, dass der Host oder Cluster weiterhin korrekt konfiguriert ist.

Prüfen der Übereinstimmung über die Ansicht „Hostprofile“

Sie können über die Hauptansicht „Hostprofile“ die Übereinstimmung eines Hosts oder Clusters mit einem Profil prüfen.

Vorgehensweise

- 1 Wählen Sie in der Liste „Hostprofile“ das zu prüfende Profil aus.
- 2 Wählen Sie auf der Registerkarte **[Hosts und Cluster]** den Host oder Cluster in der Liste unter „Elementname“ aus.
- 3 Klicken Sie auf **[Jetzt auf Übereinstimmung prüfen]** .

Der Übereinstimmungsstatus wird als „Übereinstimmung“, „Unbekannt“ oder „Nicht übereinstimmend“ aktualisiert.

Wenn der Übereinstimmungsstatus „Nicht übereinstimmend“ lautet, können Sie den Host dem Profil zuweisen.

Prüfen der Host-Übereinstimmung

Nachdem ein Profil an einen Host angehängt wurde, führen Sie zum Überprüfen der Konfiguration eine Übereinstimmungsprüfung durch.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, für den Sie die Übereinstimmungsprüfung durchführen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **[Hostprofil] > [Übereinstimmung prüfen]**.

Der Übereinstimmungsstatus des Hosts wird auf der Registerkarte **[Zusammenfassung]** angezeigt.

Wenn der Host nicht übereinstimmt, müssen Sie das Profil auf den Host anwenden.

Prüfen der Clusterübereinstimmung

Ein Cluster kann auf Übereinstimmung mit einem Hostprofil oder mit bestimmten Clusteranforderungen und -einstellungen geprüft werden.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Cluster aus, für den Sie die Übereinstimmungsprüfung durchführen möchten.
- 2 Klicken Sie auf der Registerkarte „Profil-Übereinstimmung“ auf **[Jetzt auf Übereinstimmung prüfen]**, um die Übereinstimmung des Clusters mit dem angehängten Hostprofil und ggf. den Clusteranforderungen zu prüfen.
 - Der Cluster wird auf Übereinstimmung mit bestimmten Einstellungen für Hosts im Cluster geprüft, z. B. DRS, HA und DPM. So kann beispielsweise geprüft werden, ob VMotion aktiviert ist. Der Übereinstimmungsstatus für die Clusteranforderungen wird aktualisiert. Die Prüfung wird auch durchgeführt, wenn dem Cluster kein Hostprofil angehängt ist.
 - Wenn dem Cluster ein Hostprofil angehängt ist, wird der Cluster auf Übereinstimmung mit dem Hostprofil geprüft. Der Übereinstimmungsstatus für das Hostprofil wird aktualisiert.
- 3 (Optional) Klicken Sie neben den Clusteranforderungen auf **[Beschreibung]**, um eine Liste der Clusteranforderungen anzuzeigen.
- 4 (Optional) Klicken Sie neben den Hostprofilen auf **[Beschreibung]**, um eine Liste der Übereinstimmungsprüfungen der Hostprofile anzuzeigen.
- 5 (Optional) Klicken Sie auf **[Ändern]**, um das Hostprofil zu ändern, das dem Cluster angehängt ist.
- 6 (Optional) Klicken Sie auf **[Entfernen]**, um das Hostprofil zu trennen, das dem Cluster angehängt ist.

Wenn der Cluster nicht übereinstimmt, muss das Profil auf jeden Host im Cluster separat angewendet werden.

Index

Symbole

* neben dem Pfad 116

A

Adapter, virtuell 34
Administrator, Rolle 162, 163
Aktiv/Aktiv-Festplatten-Arrays 117
Aktiv/Passiv-Festplatten-Arrays 117
Aktive Adapter 23
Aktive Uplinks 41, 44, 46
Aktualisieren 96
Aktueller Multipathing-Status 116
Ändern von Gruppen auf ESX-Hosts 166
Ändern von Host-Proxy-Diensten 171
Angriffe
 802.1q- und ISL-Kennzeichnung 153
 Doppelt eingekapselt 153
 MAC-Flooding 153
 Multicast-Brute-Force 153
 Spanning-Tree 153
 Zufallsdatenblock 153
Angriffe durch 802.1q- und ISL-Kennzeichnung 153
Antivirensoftware, installieren 179
Architektur des im Betrieb austauschbaren Speichers 110
Ausfallstelle 83
Ausschneiden und Einfügen, Deaktivieren für Gastbetriebssysteme 180
Außerkräftsetzungseinstellungen, dvPortgruppen 30
Authentifizierung
 Benutzer 159, 160
 Gruppen 161
 iSCSI-Speicher 156
 vSphere-Client an ESXi 159
Authentifizierungs-Daemon 159

B

Bandbreite
 Durchschnitt 54
 Spitze 54
Beanspruchen von Pfaden 115
Beanspruchungsregeln 115
Beiderseitiges CHAP 90

Benutzer

 Ändern auf Hosts 165
 Anzeigen der Benutzerliste 164
 Authentifizierung 160
 Berechtigungen und Rollen 160
 Direktzugriff 160
 Entfernen von Benutzern aus Gruppen 166
 Entfernen von Hosts 166
 Exportieren einer Benutzerliste 164
 Grundlegende Informationen 164
 Hinzufügen von Benutzern zu Gruppen 166
 in Windows-Domäne 160
 Sicherheit 160
 vCenter Server 160
 Zu Hosts hinzufügen 165
Benutzerberechtigungen
 dcui 162
 vpxuser 162
Benutzerrollen
 Administrator 163
 Kein Zugriff 163
 Nur Lesen 163
Berechtigungen
 Benutzer 161, 162
 Root-Benutzer 161
 Übersicht 161
 und Rechte 161
 vCenter Server-Administrator 161
 vpxuser 161
Bevorzugter Pfad 116
Bindung auf Host, dvPortgruppen 30
Blockgeräte 126
Blockierte Ports, dvPorts 56
Burstgröße 54, 55

C

CDP 23
CHAP
 Beiderseitig 90
 deaktivieren 94
 Für Erkennungsziele 92
 Für iSCSI-Initiatoren 91
 Für statische Ziele 92
 Unidirektional 90
CHAP-Authentifizierung 90, 157

CHAP-Authentifizierungsmethoden **90**

CIM und Firewallports **148**

Cisco Discovery-Protokoll **23, 28**

Cisco-Switches **23**

D

Dateisysteme, aktualisieren **107**

Datenspeicher

Aktualisieren **96**

Anzeigen **81**

anzeigen im vSphere-Client **78**

Datenspeicher-Überbuchung **121**

erstellen auf SCSI-Festplatte **97**

gruppieren **104**

Hinzufügen von Erweiterungen **106**

Kapazität, erhöhen **106**

konfigurieren auf NFS-Volumes **99**

mounten **108**

NFS **74**

Pfade **116**

Überprüfen von Eigenschaften **81**

umbenennen **104**

Unmounten **105**

verwalten **103**

Verwalten von Duplizierten **108**

VMFS **74**

Datenspeicherkopien, mounten **108**

dcui **162**

deaktivieren

Protokollierung für Gastbetriebssysteme **183**

SSL für vSphere SDK **170**

Deaktivieren

Ausschneiden und Einfügen für virtuelle Maschinen **180**

iSCSI-SAN-Authentifizierung **157**

Protokollierung für Gastbetriebssysteme **184**

Variable Informationsgröße **182**

Deaktivieren von Pfaden **118**

delegierter Benutzer **98**

Diagnosepartition, konfigurieren **100**

Direkte Konsole, zugreifen **163**

Direktzugriff **160**

DMZ **140**

DNS **57**

Doppelt eingekapselte Angriffe **153**

Drittanbieter-Switch **25**

Durchschnittsbandbreite **55**

dvPort-Gruppe, Lastenausgleich **44**

dvPortgruppen

Anzahl der Ports **29**

Außerkraftsetzungseinstellungen **30**

Beschreibung **29**

Bindung auf Host **30**

Failback **44**

Failover-Reihenfolge **44**

Format des Portnamens **30**

Gruppierungs- und Failover-Richtlinien **44**

hinzufügen **28**

Live-Port verschieben **30**

Name **29**

Netzwerk-Failover-Ermittlung **44**

Portblockierung **56**

Portgruppentyp **29**

Switches benachrichtigen **44**

Traffic-Shaping-Richtlinien **55**

virtuelle Maschinen **37**

Zurücksetzen bei Verbindungstrennung konfigurieren **30**

dvPorts

Blockierte Ports **56**

Eigenschaften **30**

Failback **46**

Failover-Reihenfolge **46**

Gruppierungs- und Failover-Richtlinien **46**

Lastausgleich **46**

Netzwerk-Failover-Erkennung **46**

Portrichtlinien **56**

Switches benachrichtigen **46**

Traffic-Shaping-Richtlinien **55**

VLAN-Richtlinien **49**

DVS

Cisco Discovery-Protokoll **28**

Hinzufügen eines VMkernel-Netzwerkadapters **33**

IP-Adresse **28**

Kontaktinformationen des Administrators **28**

Maximale Anzahl an Ports **28**

Maximalwert für MTU **28**

dvUplink **26**

dynamische Erkennung, konfigurieren **89**

Dynamische Erkennungsadressen **89**

E

Egress-Traffic-Shaping **55**

Eigenschaften, dvPorts **30**

Einzelne Ausfallstelle **83**

Entfernen von Benutzern aus Gruppen **166**

Erkennung

Adresse **89**

Dynamisch **89**

statisch **90**

Erneut prüfen

LUN-Erstellung **96**

Pfadmaskierung **96**

wenn Pfad nicht verfügbar ist **96**

Ersetzen, Standardzertifikate **168**

Erstellen von Hostprofilen **190**

Erweiterungen
 Hinzufügen zu Datenspeicher **106**
 Vergrößern **106**

Exportieren
 Hostbenutzer **164**
 Hostgruppen **164**

F

Failback **41, 44, 46**

Failover **40, 110**

Failover-Pfade, Status **116**

Failover-Reihenfolge **41, 44, 46**

Failover-Richtlinien
 dvPortgruppen **44**
 dvPorts **46**
 vSwitch **41**

Fest, Pfadrichtlinie **112, 117**

Festplatten, Format **120, 121**

Festplatten-Arrays
 aktiv/aktiv **117**
 aktiv/passiv **117**

Festplattenformate
 NFS **98**
 Thick-Provisioned **119**
 Thin-bereitgestellt **119**

Fibre-Channel **71**

Fibre-Channel-SANs, WWNs **72**

Fibre-Channel-Speicher, Übersicht **84**

Fingerabdrücke, Hosts **167**

Firewallports
 Herstellen einer Verbindung mit der Konsole für virtuelle Maschinen **147**
 Host zu Host **148**
 Konfiguration mit vCenter Server **144**
 Konfiguration ohne vCenter Server **145**
 Mit vCenter Server verbinden **146**
 Öffnen mit dem vSphere-Client **148**
 SDK und Konsole für virtuellen Maschinen **147**
 Übersicht **143**
 unterstützte Dienste **148**
 Verschlüsselung **167**
 Verwaltung **148**
 vSphere-Client und Konsole für virtuelle Maschinen **147**
 vSphere-Client und vCenter Server **144**
 vSphere-Clientdirektverbindung **145**

Format des Portnamens, dvPortgruppen **30**

FTP und Firewallports **148**

G

Gastbetriebssysteme
 Begrenzen der variablen Informationsgröße **182**
 Deaktivieren der Protokollierung **183, 184**
 Deaktivieren von Kopier- und Einfügevorgängen **180**
 Protokollierungsebenen **183**
 Sicherheitsempfehlungen **179**

Gefälschte Übertragungen **51, 52, 154, 155**

Generieren von Zertifikaten **168**

Gerätetrennung, Verhindern **181**

Gruppen
 Ändern auf Hosts **166**
 Anzeigen der Gruppenliste **164**
 Authentifizierung **161**
 Berechtigungen und Rollen **160**
 Entfernen von Hosts **166**
 Exportieren einer Gruppenliste **164**
 Grundlegende Informationen **164**
 Hinzufügen von Benutzern **166**
 Zu Hosts hinzufügen **166**

Gruppierungsrichtlinien
 dvPortgruppen **44**
 dvPorts **46**
 vSwitch **41**

H

Hardware-iSCSI, und Failover **113**

Hardware-iSCSI-Initiator, Ändern des iSCSI-Namens **86**

Hardware-iSCSI-Initiatoren
 anzeigen **86**
 Einrichten von Benennungsparametern **86**
 Einrichten von Erkennungsadressen **89**
 installieren **86**
 konfigurieren **85**

Hardwaregeräte, entfernen **181**

hinzufügen
 dvPortgruppen **28**
 NFS-Speicher **99**

Hinzufügen eines VMkernel-Netzwerkkadapters **20**

Hinzufügen von Benutzern zu Gruppen **166**

Host-Netzwerk, anzeigen **15**

Host-zu-Host-Firewallports **148**

Hostprofil, Elemente anhängen **194**

Hostprofil erstellen **190, 191**

Hostprofile
 bearbeiten **192**
 Elemente über den Host anhängen **194**
 Elemente über die Ansicht „Hostprofile“ anhängen **194**
 exportieren **191**

- Importieren **192**
 - Neues Profil erstellen **190**
 - Neues Profil über den Host erstellen **191**
 - Neues Profil über die Ansicht „Hostprofile“ erstellen **190**
 - Profile übernehmen **195**
 - Profile verwalten **194**
 - Richtlinien bearbeiten **192**
 - Übereinstimmung prüfen **197, 198**
 - Übereinstimmungsprüfung für Richtlinien aktivieren **193**
 - Verwendungsmodell **189**
 - zugreifen **190**
 - Hosts
 - Arbeitsspeicher **182**
 - Fingerabdrücke **167**
 - Hinzufügen von Benutzern **165**
 - Hinzufügen von Gruppen **166**
 - Hinzufügen zu einem verteilten vNetwork-Switch **27**
 - Implementierungen und Sicherheit **175**
 - HTTPS PUT, Hochladen von Zertifikaten und Schlüsseln **169**
- I**
- IDE **70**
 - Implementierungen für Sicherheit
 - Eingeschränkt für mehrere Kunden **176**
 - Unbeschränkt für mehrere Kunden **175, 177**
 - Ingress-Traffic-Shaping **55**
 - Internetprotokoll **40**
 - IP-Adresse **28**
 - IP-Adressen **73**
 - IP-Speicherportgruppen, erstellen **20, 33**
 - IPv4 **39**
 - IPv6 **39, 40**
 - iSCSI
 - Authentifizierung **156**
 - Ports schützen **157**
 - QLogic-iSCSI-Adapter **156**
 - Schützen übertragener Daten **157**
 - Sicherheit **156**
 - Softwareclient und Firewallports **148**
 - iSCSI-Aliasnamen **73**
 - iSCSI-HBA, Alias **86**
 - iSCSI-Initiatoren
 - CHAP konfigurieren **91**
 - Einrichten von CHAP-Parametern **90**
 - Erweiterte Parameter **94**
 - Hardware **85**
 - Konfigurieren erweiterter Parameter **95**
 - iSCSI-Namen **73**
 - iSCSI-Netzwerk, Erstellen eines VMkernel-Ports **87**
 - iSCSI-SAN-Authentifizierung, deaktivieren **157**
 - iSCSI-Speicher
 - hardwareinitiiert **84**
 - Initiatoren **84**
 - softwareinitiiert **84**
 - Isolierung
 - virtuelle Maschinen **136**
 - virtuelle Netzwerkebene **138**
 - Virtuelle Switches **138**
 - VLANs **138**
- J**
- Jumbo-Frames
 - Aktivieren **60**
 - virtuelle Maschinen **59, 60**
- K**
- Kein Zugriff, Rolle **162, 163**
 - Kompatibilitätsmodi
 - physisch **127**
 - virtuell **127**
 - konfigurieren
 - dynamische Erkennung **89**
 - RDM **131**
 - SCSI-Speicher **97**
 - statische Erkennung **90**
 - Kontaktinformationen des Administrators **28**
- L**
- Lastausgleich **40, 46**
 - Lastenausgleich **41, 44**
 - Live-Port verschieben, dvPortgruppen **30**
 - localadmin **163**
 - lokaler SCSI-Speicher, Übersicht **83**
 - LUNs
 - Änderungen vornehmen und erneut prüfen **96**
 - Erstellen und erneutes Prüfen **96**
 - Festlegen einer Multipathing-Richtlinie **117**
 - Maskierungsänderungen und erneutes Prüfen **96**
 - Multipathing-Richtlinie **117**
- M**
- MAC-Adresse
 - Generieren **58**
 - konfigurieren **57**
 - MAC-Adressen **51, 52**
 - MAC-Adressenänderungen **154, 155**
 - MAC-Flooding **153**
 - Maximale Anzahl an Ports **28**
 - Maximalwert für MTU **28**
 - Metadaten, RDMs **127**

Mounten von VMFS-Datenspeichern **108**
 MPPs, , *siehe* Multipathing-Plug-Ins
 MTU **60**
 Multicast-Brute-Force-Angriffe **153**
 Multipathing
 aktive Pfade **116**
 Anzeigen des aktuellen Status **116**
 beschädigte Pfade **116**
 deaktivierte Pfade **116**
 Standby-Pfade **116**
 Multipathing-Plug-Ins, Beanspruchen von Pfaden **115**
 Multipathing-Richtlinie **117**
 Multipathing-Status **116**

N

NAS, mounten **66**
 NAT **39**
 Native Multipathing Plugin **110, 111**
 NetQueue, Deaktivieren **62**
 Netzwerk-Failover-Erkennung **46**
 Netzwerk-Failover-Ermittlung **41, 44**
 Netzwerkadapter, anzeigen **15, 28**
 Netzwerkadressübersetzung **39**
 Netzwerkbetrieb, Sicherheitsrichtlinien **51, 52**
 Netzwerke, Sicherheit **150**
 Netzwerkkarte, hinzufügen **32**
 NFS, Firewallports **148**
 NFS-Datenspeicher, Unmounten **105**
 NFS-Speicher
 hinzufügen **99**
 Überblick **98**
 NIC-Gruppierung, Definition **13**
 NIS und Firewallports **148**
 NMP, Beanspruchen von Pfaden **115**
 Nur lesen, Rolle **162, 163**

O

Optimale Vorgehensweisen für Netzwerke **65**

P

Partitionszuordnungen **126**
 Passive Festplatten-Arrays **117**
 Passthrough-Gerät, Hinzufügen zu einer virtuellen Maschine **63**
 Pfad-Failover, Hostbasiert **113**
 Pfadausfall **113**
 Pfadausfall, erneutes Prüfen **96**
 Pfadauswahl-Plug-Ins **112**
 Pfade
 bevorzugt **116**
 deaktivieren **118**
 Pfadrichtlinien
 Ändern des Standardeinstellungen **118**

Fest **112, 117**
 Round Robin **112, 117**
 Zuletzt verwendet **112, 117**

Pfadverwaltung **110**
 Physische Adapter, entfernen **33**
 Physische Switches, Fehlerbehebung **66**
 Port-Bindung **87, 113**
 Portblockierung, dvPortgruppen **56**
 Portgruppe
 Definition **13**
 verwenden **18**
 Portgruppen
 Schicht 2-Sicherheit **50**
 Traffic-Shaping **54**
 Portgruppen mit früher Bindung **29**
 Portgruppen mit später Bindung **29**
 Portkonfiguration **22**
 Ports virtueller Switches, Sicherheit **154**
 Privates VLAN
 entfernen **31, 32**
 erstellen **31**
 Primär **31**
 Sekundär **32**
 Promiscuous-Modus **51, 52, 154, 156**
 Protokolldateien
 Begrenzen der Anzahl **184**
 Begrenzen der Größe **184**
 Protokollierung, Deaktivieren für Gastbetriebssysteme **183, 184**
 Protokollierungsebenen, Gastbetriebssysteme **183**
 Proxy-Dienste
 ändern **171**
 Verschlüsselung **167**
 PSA, , *siehe* Pluggable Storage Architecture
 PSPs, , *siehe* Pfadauswahl-Plug-Ins

R

RAID-Geräte **126**
 Raw-Gerätezuordnung, Gerätezuordnungen **123**
 RDM
 Dynamische Namensauflösung **128**
 erstellen **131**
 mit Cluster **130**
 physischer Kompatibilitätsmodus **127**
 Übersicht **123**
 und virtuelle Festplattendateien **130**
 virtueller Kompatibilitätsmodus **127**
 Vorteile **124**
 RDMs
 Und Snapshots **126**
 Und VMFS-Formate **126**
 Rechte und Berechtigungen **161**

Ressourceneinschränkungen und -garantien, Sicherheit **136**

Richtlinie zur Unterstützung von Drittanbieter-Software **142**

Rollen

Administrator **162**

Kein Zugriff **162**

Nur Lesen **162**

Sicherheit **162**

Standard **162**

und Berechtigungen **162**

Root-Anmeldung, Berechtigungen **161**

Round Robin, Pfadrichtlinie **112, 117**

Routing **57**

S

SAS **70**

SATA **70**

Schicht 2-Sicherheit **49**

Schlüssel, hochladen **169**

SDK, Firewallports und Konsole für virtuelle Maschinen **147**

setinfo **182**

Sicherheit

Architektur **135**

Berechtigungen **161**

DMZ auf einem einzelnen Host **138, 140**

Empfehlungen für virtuelle Maschinen **179**

Funktionen **135**

iSCSI-Speicher **156**

Ports virtueller Switches **154**

Ressourcengarantien und -einschränkungen **136**

Übersicht **135**

Virtualisierungsebene **136**

virtuelle Maschinen **136**

Virtuelle Maschinen mit VLANs **150**

virtuelle Netzwerkebene **138**

VLAN-Hopping **152**

VMkernel **136**

vmware-hostd **159**

VMware-Richtlinie **142**

Zertifizierung **142**

Sicherheitsempfehlungen **178**

Sicherheitsrichtlinien, dvPorts **51, 52**

SMB und Firewallports **148**

SNMP und Firewallports **148**

Software-iSCSI

Diagnosepartition **100**

Netzwerk **87**

und Failover **113**

Software-iSCSI-Initiatoren aktivieren **88**

Einrichten von Erkennungsadressen **89**
konfigurieren **87**

Spanning-Tree-Angriffe **153**

Speicher

absichern mit VLANs und virtuellen Switches **152**

Adapter **71**

anzeigen im vSphere-Client **78**

Bereitgestellt **120**

Bereitstellung **119**

Fibre-Channel **84**

iSCSI **84**

lokal **70**

lokaler SCSI- **83**

Netzwerk **71**

NFS **98**

Nicht freigegeben **120**

SAN **84**

Typen **70**

Übersicht **69**

Verwendet von virtuellen Maschinen **120**

Zugriff für virtuelle Maschinen **77**

Speicheradapter

anzeigen **79**

anzeigen im vSphere-Client **78**

Fibre-Channel **84**

Kopieren von Namen **79**

Speichergeräte

anzeigen **79**

Anzeigen für einen Adapter **80**

Anzeigen für einen Host **80**

Bezeichner **74**

Laufzeitnamen **74**

Namen **74**

Pfade **117**

Speicherplatz **119**

Sperrmodus, aktivieren **179**

Spitzenbandbreite **54, 55**

SSH, Firewallports **148**

SSL

Aktivieren und Deaktivieren **167**

Verschlüsselung und Zertifikate **167**

Zeitüberschreitungen **169**

Standardzertifikate, Ersetzen durch Zertifikate einer Zertifizierungsstelle **168**

Standby-Adapter **23**

Standby-Uplinks **41, 44, 46**

statische Erkennung, konfigurieren **90**

Statische Erkennungsadressen **89**

Sternchen neben dem Pfad **116**

SATPs **112**

Storage Array Type Plugins **112**

- Switch, vNetwork **34**
- Switches benachrichtigen **41, 44, 46**
- T**
- TCP-Ports **148**
- Thin-Festplatten, erstellen **120**
- Traffic-Shaping
 - Portgruppen **54**
 - vSwitch **54**
- Traffic-Shaping bei ausgehendem Datenverkehr **55**
- Traffic-Shaping bei eingehendem Datenverkehr **55**
- Traffic-Shaping-Richtlinien
 - dvPortgruppen **55**
 - dvPorts **55**
- U**
- UDP-Ports **148**
- Unidirektionales CHAP **90**
- Uplink, entfernen **33**
- Uplink-Adapter
 - Duplex **22**
 - Geschwindigkeit **22**
 - hinzufügen **23**
- Uplink-Zuweisungen **28**
- USB **70**
- V**
- Variable Informationsgröße für Gastbetriebssystem
 - Begrenzen **182**
 - Deaktivieren **182**
- vCenter Server
 - Berechtigungen **161**
 - Firewallports **144**
 - Verbinden über Firewall **146**
- vCenter Server-Benutzer **160**
- Verschlüsselung
 - Aktivieren und Deaktivieren von SSL **167**
 - Für Benutzernamen, Kennwörter und Pakete **167**
 - Zertifikate **167**
- Verteilte vNetwork-Switches
 - Cisco Discovery-Protokoll **28**
 - Hinzufügen eines VMkernel-Netzwerkadapters **33**
 - Hinzufügen von Hosts **27**
 - IP-Adresse **28**
 - Kontaktinformationen des Administrators **28**
 - Maximale Anzahl an Ports **28**
 - Maximalwert für MTU **28**
 - Sonstige Richtlinien **56**
 - Virtuelle Maschinen darauf oder davon migrieren **36**
- Verteilter vNetwork-Switch
 - Drittanbieter **25**
 - Hinzufügen einer Netzwerkkarte **32**
 - Hinzufügen eines Hosts **27**
 - Neu **26**
 - VMkernel-Adapter **35**
- Verwaltungszugriff, TCP- und UDP-Ports **148**
- Virtualisierungsebene, Sicherheit **136**
- Virtuelle Festplatten, Formate **119**
- Virtuelle Maschine, Netzwerke **14, 18**
- virtuelle Maschinen
 - Auf oder von einem verteilten vNetwork-Switch migrieren **36**
 - Begrenzen der variablen Informationsgröße **182**
 - Deaktivieren der Protokollierung **183, 184**
 - Deaktivieren von Kopier- und Einfügevorgängen **180**
 - Isolierung **138, 140**
 - Netzwerkbetrieb **37**
 - Ressourcenreservierung und -einschränkungen **136**
 - Sicherheit **136**
 - Sicherheitsempfehlungen **179**
 - Verhindern der Gerätetrengung **181**
- Virtuelle Netzwerkadapter, entfernen **35**
- Virtuelle Netzwerkebene und Sicherheit **138**
- Virtuelle Switches
 - Angriffe durch 802.1q- und ISL-Kennzeichnung **153**
 - Doppelt eingekapselte Angriffe **153**
 - Gefälschte Übertragungen **154**
 - Implementierungsszenarien **175**
 - MAC-Adressenänderungen **154**
 - MAC-Flooding **153**
 - Multicast-Brute-Force-Angriffe **153**
 - Promiscuous-Modus **154**
 - Sicherheit **153**
 - Spanning-Tree-Angriffe **153**
 - und iSCSI **157**
 - Zufallsdatenblock-Angriffe **153**
- Virtueller Adapter, VMkernel **35**
- virtueller Switch, Sicherheit **152**
- virtuelles Netzwerk, Sicherheit **150**
- VLAN
 - Definition **13**
 - Privat **31**
- VLAN-ID **28**
- VLAN-Richtlinien
 - dvPort-Gruppe **48**
 - dvPorts **49**

- VLAN-Sicherheit **152**
 - VLAN-Trunking **28, 48, 49**
 - VLAN-Typ **49**
 - VLANs
 - Implementierungsszenarien **175**
 - Schicht 2-Sicherheit **152**
 - Sicherheit **150, 152**
 - Sicherheitskonfigurierung **152**
 - und iSCSI **157**
 - VLAN-Hopping **152**
 - VMFS
 - gemeinsam nutzen **175**
 - Volume-Neusignierung **108**
 - VMFS-Datenspeicher
 - Ändern von Eigenschaften **105**
 - Ändern von Signaturen **109**
 - erstellen **75**
 - gemeinsam nutzen **76**
 - Hinzufügen von Erweiterungen **106**
 - Kapazität, erhöhen **106**
 - konfigurieren **97**
 - löschen **104**
 - Neusignierung von Kopien **109**
 - Unmounten **105**
 - VMFS-Volume-Neusignierung **108**
 - VMkernel
 - Definition **13**
 - konfigurieren **19**
 - Sicherheit **136**
 - VMkernel-Adapter **35**
 - VMkernel-Netzwerk **14**
 - VMkernel-Netzwerkadapter, hinzufügen **20, 33**
 - VMotion
 - absichern mit VLANs und virtuellen Switches **152**
 - Definition **13**
 - Netzwerkkonfiguration **19**
 - VMotion-Schnittstellen, erstellen **20, 33**
 - VMware NMP
 - E/A-Fluss **112**
 - Siehe auch* Native Multipathing Plugin
 - vmware-hostd **159**
 - Vmxnet (erweitert) **59, 60**
 - vNetwork-Standard-Switch
 - anzeigen **15**
 - Portkonfiguration **22**
 - Schicht 2-Sicherheit **49**
 - Traffic-Shaping **54**
 - Volume-Neusignierung **108, 109**
 - vpxuser **162**
 - vSphere-Client
 - Firewallports für Direktverbindung **145**
 - Firewallports mit vCenter Server **144**
 - Herstellen einer Verbindung mit der Konsole für virtuelle Maschinen über Firewallports **147**
 - vSwitch
 - anzeigen **15**
 - Definition **13**
 - Failback **41**
 - Failover-Reihenfolge **41**
 - Gruppierungs- und Failover-Richtlinien **41**
 - Lastenausgleich **41**
 - Netzwerk-Failover-Ermittlung **41**
 - Portkonfiguration **22**
 - Schicht 2-Sicherheit **49**
 - Switches benachrichtigen **41**
 - Traffic-Shaping **54**
 - verwenden **17**
- ## W
- WWNs **72**
- ## Z
- Zeitüberschreitungen, SSL **169**
 - Zertifikate
 - Deaktivieren von SSL für vSphere SDK **170**
 - Erstellen neuer Zertifikate **168**
 - hochladen **169**
 - Schlüsseldatei **167**
 - Speicherort **167**
 - SSL **167**
 - Standard **167**
 - Überprüfen **167**
 - vCenter Server **167**
 - Zertifikatsdatei **167**
 - Zertifikate einer Zertifizierungsstelle **168**
 - Zertifizierung, Sicherheit **142**
 - Ziele **72**
 - Zufallsdatenblock-Angriffe **153**
 - Zugriff auf Speicher **77**
 - Zuletzt verwendet, Pfadrichtlinie **112, 117**
 - Zurücksetzen bei Verbindungstrennung konfigurieren, dvPortgruppen **30**