

# vSphere-Speicher

Update 1

Geändert am 19. April 2022

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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

<https://docs.vmware.com/de/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Global, Inc.**  
Zweigniederlassung Deutschland  
Willy-Brandt-Platz 2  
81829 München  
Germany  
Tel.: +49 (0) 89 3706 17 000  
Fax: +49 (0) 89 3706 17 333  
[www.vmware.com/de](http://www.vmware.com/de)

Copyright © 2009-2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

Grundlegende Informationen zum vSphere-Speicher 13

Aktualisierte Informationen 14

## 1 Einführung in die Speicherung 15

Speichervirtualisierung 15

Physische Speichertypen 16

Lokaler Speicher 16

Netzwerkspeicher 17

Ziel- und Gerätedarstellungen 21

Eigenschaften des Speichergeräts 22

Anzeigen von Speichergeräten für einen Host 23

Anzeigen von Speichergeräten für einen Adapter 24

Unterstützte Speicheradapter 24

Eigenschaften des Speicheradapters 24

Anzeigen von Informationen zu Speicheradaptern 25

Merkmale von Datenspeichern 25

Anzeigen von Informationen zu Datenspeichern 27

Listen von Datenspeichern für ein Infrastrukturobjekt 28

Speicherzugriff durch virtuelle Maschinen 29

Vergleich der Speichertypen 30

## 2 Übersicht über die Verwendung von ESXi in einem SAN 32

Anwendungsbeispiele für ESXi und SAN 33

Besonderheiten bei der Verwendung von SAN-Speicher mit ESXi 34

ESXi-Hosts und mehrere Speicher-Arrays 34

Entscheidungen zur Verwendung von LUNs 35

Verwenden eines Vorhersagemodells zur richtigen LUN-Wahl 36

Verwenden des adaptiven Modells zur richtigen LUN-Wahl 36

Auswählen von Speicherorten für virtuelle Maschinen 37

Mehrschichtige Anwendungen 38

Array-basierte Lösung (Drittanbieter) 38

Dateibasierte Lösung (VMFS) 39

Verwaltungsanwendungen von Drittanbietern 39

Überlegungen zu SAN-Speichersicherungen 40

Verwenden von Drittanbieter-Sicherungspaketen 41

## 3 Verwenden von ESXi mit Fibre-Channel-SAN 42

Fibre-Channel-SAN-Konzepte	42
Ports in Fibre-Channel-SAN	43
Typen von Fibre-Channel-Speicher-Arrays	43
Verwenden von Zoning mit Fibre-Channel-SANs	44
Zugriff auf Daten in einem Fibre-Channel-SAN durch virtuelle Maschinen	45
<b>4 Konfigurieren des Fibre-Channel-Speichers</b>	<b>46</b>
Anforderungen des Fibre-Channel-SAN von ESXi	46
Einschränkungen des Fibre-Channel-SAN von ESXi	47
Festlegen der LUN-Zuordnungen	47
Festlegen von Fibre-Channel-HBAs	48
Installations- und Konfigurationsschritte	48
N-Port-ID-Virtualisierung	49
Funktionsweise des NPIV-basierten LUN-Zugriffs	49
Anforderungen für die Verwendung von NPIV	50
NPIV-Funktionen und -Einschränkungen	50
Zuweisen von WWNs zu virtuellen Maschinen	51
Ändern von WWN-Zuweisungen	52
<b>5 Konfigurieren von Fibre-Channel über Ethernet</b>	<b>53</b>
Adapter für Fibre-Channel über Ethernet	53
Konfigurationsrichtlinien für Software-FCoE	54
Einrichten des Netzwerks für Software-FCoE	55
Hinzufügen von Software-FCoE-Adaptern	56
<b>6 Starten von ESXi von einem Fibre-Channel-SAN</b>	<b>57</b>
Vorteile beim Starten über ein SAN	57
Anforderungen und Überlegungen beim Starten von Fibre-Channel-SAN	58
Vorbereiten für das Starten über ein SAN	58
Konfigurieren von SAN-Komponenten und des Speichersystems	59
Konfigurieren eines Speicheradapters für das Starten über ein SAN	60
Einrichten des Systems zum Starten vom Installationsmedium	60
Konfigurieren des Emulex HBAs für das Starten über ein SAN	61
Aktivieren der BIOS-Einstellung zur Startauswahl	61
Aktivieren des BIOS	61
Konfigurieren des QLogic-HBAs für das Starten über ein SAN	62
<b>7 Starten von ESXi mit Software FCoE</b>	<b>64</b>
Anforderungen und Überlegungen für das Starten mit Software FCoE	64
Best Practices für Software FCoE Boot	65
Einrichten des Startens mit Software FCoE	65

Konfigurieren der Parameter für das Starten mit Software FCoE	66
Installieren und Starten von ESXi von Software FCoE LUN	66
Durchführen der Fehlerbehebung für die Installation und Starten von Software-FCoE	67
<b>8 Best Practices für Fibre-Channel-Speicher</b>	<b>69</b>
Vermeiden von Fibre-Channel-SAN-Problemen	69
Deaktivieren der automatischen Hostregistrierung	70
Optimieren der Fibre-Channel-SAN-Speicherleistung	71
Speicher-Array-Leistung	71
Serverleistung mit Fibre-Channel	71
<b>9 Verwenden von ESXi mit iSCSI-SAN</b>	<b>73</b>
iSCSI-SAN-Konzepte	73
Ports im iSCSI-SAN	74
iSCSI-Benennungskonventionen	74
iSCSI-Initiatoren	75
Herstellen von iSCSI-Verbindungen	76
iSCSI-Speichersystemtypen	77
Erkennung, Authentifizierung und Zugriffssteuerung	78
Fehlerkorrektur	79
Zugriff auf Daten in einem iSCSI-SAN durch virtuelle Maschinen	80
<b>10 Konfigurieren von iSCSI-Adaptern und -Speichern</b>	<b>81</b>
Anforderungen an ESXi-iSCSI-SAN	82
Einschränkungen bei ESXi-iSCSI-SAN	82
Festlegen der LUN-Zuordnungen für iSCSI	83
Netzwerkkonfiguration und Authentifizierung	83
Einrichten von unabhängigen Hardware-iSCSI-Adaptern	84
Anzeigen abhängiger Hardware-iSCSI-Adapter	85
Ändern der allgemeinen Eigenschaften für iSCSI-Adapter	85
Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI	86
Einrichten der dynamischen oder statischen Erkennung für iSCSI	87
Informationen zu abhängigen Hardware-iSCSI-Adaptern	88
Überlegungen zu abhängigen Hardware-iSCSI-Adaptern	89
Konfigurieren von abhängigen Hardware-iSCSI-Adaptern	89
Informationen zum Software-iSCSI-Adapter	98
Konfigurieren des Software-iSCSI-Adapters	98
Software-iSCSI-Adapter deaktivieren	106
Ändern der allgemeinen Eigenschaften für iSCSI-Adapter	107
Einrichten des iSCSI-Netzwerks	108
Richtlinien für die Verwendung der iSCSI-Port-Bindung in ESXi	111

Erstellen von Netzwerkverbindungen für iSCSI	111
Verwalten des iSCSI-Netzwerks	116
Fehler im iSCSI-Netzwerk beheben	117
Verwenden von Jumbo-Frames mit iSCSI	118
Aktivieren von Jumbo-Frames für Software-iSCSI und abhängige Hardware-iSCSI	118
Aktivieren von Jumbo-Frames für unabhängige Hardware-iSCSI	119
Konfigurieren von Erkennungsadressen für iSCSI-Adapter	119
Einrichten der dynamischen oder statischen Erkennung für iSCSI	120
Entfernen dynamischer oder statischer iSCSI-Ziele	121
Konfigurieren von CHAP-Parametern für iSCSI-Adapter	121
Auswählen der CHAP-Authentifizierungsmethode	122
Einrichten von CHAP für iSCSI-Adapter	123
Einrichten von CHAP für Ziele	124
Deaktivieren von CHAP	126
Konfigurieren erweiterter Parameter für iSCSI	126
Konfigurieren erweiterter Parameter für iSCSI	128
iSCSI-Sitzungsverwaltung	129
Überprüfen von iSCSI-Sitzungen	129
Hinzufügen von iSCSI-Sitzungen	130
Entfernen von iSCSI-Sitzungen	131

## **11 Starten von einem iSCSI-SAN 132**

Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN	132
Vorbereiten des iSCSI-SAN	133
Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN	134
Konfigurieren der iSCSI-Starteinstellungen	135
iBFT-iSCSI-Start - Überblick	136
iBFT-iSCSI-Start - Überlegungen	137
Konfigurieren des Startens von iBFT über ein SAN	137
Best Practices für Netzwerke	140
Ändern von iBFT-iSCSI-Starteinstellungen	140
iBFT-iSCSI-Start - Fehlerbehebung	141

## **12 Best Practices für iSCSI-Speicher 143**

Vermeiden von iSCSI-SAN-Problemen	143
Optimieren der iSCSI-SAN-Speicherleistung	144
Speichersystemleistung	144
Serverleistung mit iSCSI	145
Netzwerkleistung	146
Überprüfen von Ethernet-Switch-Statistiken	149

## 13 Verwalten von Speichergeräten 150

- Eigenschaften des Speichergeräts 150
  - Anzeigen von Speichergeräten für einen Host 151
  - Anzeigen von Speichergeräten für einen Adapter 152
- Grundlegendes zur Benennung von Speichergeräten 152
  - Umbenennen von Speichergeräten 154
- Vorgänge zum Aktualisieren und zur erneuten Prüfung von Speichern 154
  - Durchführen einer erneuten Speicherprüfung 155
  - Durchführen einer erneuten Adapterprüfung 156
  - Ändern der Anzahl gescannter Speichergeräte 156
- Identifizieren von Problemen hinsichtlich der Gerätekonnektivität 157
  - Erkennen von PDL-Bedingungen 157
  - Durchführen des geplanten Entfernens von Speichergeräten 159
  - Wiederherstellen nach PDL-Bedingungen 160
  - Handhabung vorübergehender APD-Bedingungen 161
  - Überprüfen des Verbindungsstatus eines Speichergeräts 163
  - Gerätekonnektivitätsprobleme und Hochverfügbarkeit 164
- Aktivieren oder Deaktivieren der Locator-LED auf Speichergeräten 164

## 14 Arbeiten mit Flash-Geräten 165

- Verwenden von Flash-Geräten mit vSphere 165
  - Identifizieren von vFlash-Festplatten 166
- Markieren der Speichergeräte 167
  - Markieren der Speichergeräte als Flash-Gerät 167
  - Markieren der Speichergeräte als lokal 168
- Überwachen von Flash-Geräten 168
- Best Practices für Flash-Geräte 169
  - Geschätzte Lebensdauer von Flash-Geräten 169
- Informationen zu vFlash-Ressourcen 170
  - Überlegungen zu vFlash-Ressourcen 171
  - Einrichten der vFlash-Ressource 171
  - Entfernen der vFlash-Ressource 172
  - Erweiterte Einstellungen für virtuellen Flash 172
- Konfigurieren des Hostauslagerungs-Caches 173
  - Konfigurieren des Host-Caches mit VMFS-Datenspeicher 174
  - Konfigurieren des Hostauslagerungs-Cache mit der vFlash-Ressource 174

## 15 Informationen zu VMware vSphere Flash Read Cache 176

- DRS-Unterstützung für Flash-Lesecache 177
- vSphere High Availability-Unterstützung für Flash-Lesecache 177
- Konfigurieren des Flash-Lesecaches für eine virtuelle Maschine 178

Migrieren von virtuellen Maschinen mit Flash Read Cache 179

## 16 Arbeiten mit Datenspeichern 181

- Grundlegende Informationen VMFS-Datenspeicher 182
  - Eigenschaften von VMFS5-Datenspeichern 183
  - VMFS-Datenspeicher und Speicherfestplattenformate 184
  - VMFS-Datenspeicher als Repositorys 184
  - Gemeinsames Nutzen eines VMFS-Datenspeichers durch mehrere Hosts 185
  - Updates von VMFS-Metadaten 186
  - VMFS-Sperrmechanismen 186
- Grundlegende Informationen zu NFS-Datenspeichern 191
  - Richtlinien und Anforderungen für NFS-Speicher 192
  - NFS-Protokolle und ESXi 194
  - Firewall-Konfigurationen für NFS-Speicher 196
  - Geroutete Schicht 3-Verbindungen für Zugriff auf NFS-Speicher verwenden 198
  - Einrichten der NFS-Speicherumgebung 199
  - Verwenden von Kerberos-Anmeldedaten für NFS 4.1 199
- Erstellen von Datenspeichern 202
  - Erstellen eines VMFS-Datenspeichers 203
  - Erstellen eines NFS-Datenspeichers 204
  - Erstellen eines virtuellen Datenspeichers 205
- Verwalten von duplizierten VMFS-Datenspeichern 206
  - Beibehalten der vorhandenen Datenspeichersignatur 206
  - Neusignieren einer VMFS-Datenspeicherkopie 207
- Upgrade von VMFS-Datenspeichern 208
  - Upgrade eines Datenspeichers auf VMFS5 209
- Erhöhen der VMFS-Datenspeicherkapazität 210
  - Erhöhen der VMFS-Datenspeicherkapazität 210
- Verwaltungsvorgänge für Datenspeicher 212
  - Ändern des Datenspeichernamens 212
  - Unmounten von Datenspeichern 213
  - Mounten von Datenspeichern 214
  - Entfernen von VMFS-Datenspeichern 215
  - Verwenden des Datenspeicherbrowsers 215
  - Ausschalten von Speicherfiltern 220
- Dynamische Festplattenspiegelung einrichten 222
- Erfassen von Diagnoseinformationen für ESXi-Hosts auf einem Speichergerät 223
  - Einrichten einer Gerätepartition als Core-Dump-Speicherort 223
  - Einrichten einer Datei als Core-Dump-Speicherort 225
- Überprüfen der Metadatenkonsistenz mit VOMA 228
- Konfigurieren des Cachespeichers für VMFS-Zeigerblöcke 230



Festlegen von erweiterten Hostattributen	231
Abrufen von Informationen für den Cachespeicher für VMFS-Zeigerblöcke	231

## 17 Grundlegendes zu Multipathing und Failover 233

Failover mit Fibre-Channel	234
Hostbasiertes Failover mit iSCSI	234
Array-basiertes Failover mit iSCSI	236
Pfad-Failover und virtuelle Maschinen	237
Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen	238
Verwalten mehrerer Pfade	238
VMware Multipathing-Modul	240
VMware SATPs	241
VMware PSPs	241
NMP-E/A-Ablauf von VMware	242
Prüfen und Beanspruchen von Pfaden	243
Anzeigen der Pfadinformationen	243
Anzeigen von Datenspeicherpfaden	244
Anzeigen von Speichergerätepfaden	245
Festlegen einer Pfadauswahl-Richtlinie	245
Ändern der Pfadauswahl-Richtlinie	246
Deaktivieren von Speicherpfaden	246
Verwalten von Speicherpfaden und Multipathing-Plug-Ins	247
Überlegungen zu Multipathing	247
Auflisten von Multipathing-Beanspruchungsregeln für den Host	248
Anzeigen von Multipathing-Modulen	250
Anzeigen von SATPs für den Host	250
Anzeigen von NMP-Speichergeräten	251
Hinzufügen von Multipathing-Beanspruchungsregeln	251
Löschen von Multipathing-Beanspruchungsregeln	254
Maskieren von Pfaden	255
Aufheben der Maskierung von Pfaden	256
Definieren von NMP SATP-Regeln	257
Planungswarteschlangen für VM-E/A	259
Bearbeiten der Pro-Datei-E/A-Planung	259
Verwenden von esxcli-Befehlen zur Aktivierung bzw. Deaktivierung der E/A-Planung nach Datei	260

## 18 Raw-Gerätezuordnung 262

Wissenswertes zur Raw-Gerätezuordnung	262
Vorteile von Raw-Gerätezuordnungen	264
RDM-Überlegungen und -Einschränkungen	266
Raw-Gerätezuordnungseigenschaften	267

Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“ für RDM	267
Dynamische Namensauflösung	267
Raw-Gerätezuordnung für Cluster aus virtuellen Maschinen	268
Vergleichen der verfügbaren Zugriffsmodi für SCSI-Geräte	268
Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen	269
Verwalten von Pfaden in zugeordneten LUNs	271

## 19 Arbeiten mit virtuellen Volumes 272

Konzepte zu Virtual Volumes	273
Virtuelle Volumes	274
Virtuelle Volumes und Speicheranbieter	275
Speichercontainer	276
Protokollendpunkte	276
Virtuelle Datenspeicher	277
Virtuelle Volumes und VM-Speicherrichtlinien	278
Richtlinien bei der Verwendung von virtuellen Volumes	278
Virtuelle Volumes und Speicherprotokolle	279
Architektur von Virtual Volumes	279
Virtuelle Volumes und VMware Certificate Authority	281
Schritte vor der Aktivierung virtueller Volumes	282
Synchronisieren der vSphere Storage-Umgebung mit einem NTP-Server	283
Konfigurieren virtueller Volumes	283
Registrieren von Speicheranbietern für virtuelle Volumes	284
Erstellen eines virtuellen Datenspeichers	285
Prüfen und Verwalten von Protokoll-Endpoints	285
Ändern der Pfadauswahlrichtlinie für einen Protokoll-Endpoint	286
Bereitstellen von virtuellen Maschinen auf virtuellen Datenspeichern	287
Definieren einer VM-Speicherrichtlinie für Virtual Volumes	287
Zuweisen der Speicherrichtlinie für virtuelle Volumes zu virtuellen Maschinen	288
Ändern der Standardspeicherrichtlinie für einen virtuellen Datenspeicher	289

## 20 VM-Speicherrichtlinien 291

Upgrade von Legacy Storage Profiles	291
Grundlegende Informationen zu VM-Speicherrichtlinien	292
Speicherrichtlinien und Regeln	293
Informationen zu datenspeicherspezifischen und gemeinsamen Regelsätzen	295
Arbeiten mit VM-Speicherrichtlinien	296
Erstellen und Verwalten von VM-Speicherrichtlinien	297
Zuweisen von Tags zu Datenspeichern	297
Definieren einer Speicherrichtlinie für eine virtuelle Maschine	298
Löschen einer VM-Speicherrichtlinie	302

Bearbeiten oder Klonen einer VM-Speicherrichtlinie	302
Speicherrichtlinien und virtuelle Maschinen	303
Standardspeicherrichtlinien	303
Zuweisen von Speicherrichtlinien zu virtuellen Maschinen	305
Ändern der Speicherrichtlinienzuteilung für VM-Dateien und -Festplatten	307
Überwachen der Speicherübereinstimmung für virtuelle Maschinen	307
Prüfen der Übereinstimmung für eine VM-Speicherrichtlinie	309
Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine	310
Erneutes Anwenden der VM-Speicherrichtlinien	310
<b>21 Filtern der E/A einer virtuellen Maschine</b>	<b>312</b>
Grundlegendes zu E/A-Filtern	312
E/A-Filtertypen	313
E/A-Filterkomponenten	313
Speicheranbieter für VAIO-Filter	315
Verwenden von Flash-Speichergeräten mit Cache-E/A-Filtern	315
Bereitstellen und Konfigurieren von E/A-Filtern in der vSphere-Umgebung	316
Installieren von E/A-Filtern in einem Cluster	317
Anzeigen der Speicheranbieter von E/A-Filtern	318
Prüfen von E/A-Filterfunktionen	318
Konfigurieren der vFlash-Ressource für die Zwischenspeicherung von E/A-Filtern	319
Aktivieren von E/A-Filter-Datendiensten auf virtuellen Festplatten	319
Verwalten von E/A-Filtern	323
Deinstallieren von E/A-Filtern in einem Cluster	323
Aktualisieren von E/A-Filtern in einem Cluster	324
Richtlinien und empfohlene Vorgehensweisen für E/A-Filter	324
Migrieren von virtuellen Maschinen mit E/A-Filtern	325
<b>22 VMkernel und Speicher</b>	<b>326</b>
Speicher-APIs	327
<b>23 Speicherhardware-Beschleunigung</b>	<b>329</b>
Vorteile der Hardwarebeschleunigung	329
Anforderungen der Hardwarebeschleunigung	330
Status der Hardwarebeschleunigungs-Unterstützung	330
Hardwarebeschleunigung für Blockspeichergeräte	330
Deaktivieren der Hardwarebeschleunigung für Blockspeichergeräte	331
Verwalten der Hardwarebeschleunigung auf Blockspeichergeräten	332
Hardwarebeschleunigung auf NAS-Geräten	338
Installieren des NAS-Plug-Ins	339
Deinstallieren von NAS-Plug-Ins	339

Update von NAS-Plug-Ins	340
Verifizieren des Status der Hardwarebeschleunigung für NAS	341
Überlegungen bei der Hardwarebeschleunigung	341
<b>24 Bereitstellung im Format „Thick“ bzw. „Thin“ beim Speicher</b>	<b>343</b>
Datenspeicher-Überbuchung	343
Thin Provisioning virtueller Festplatten	343
Grundlegendes zu Bereitstellungsrichtlinien für virtuelle Festplatten	344
Erstellen von virtuellen Thin-bereitgestellten Festplatten	345
Anzeigen von Speicherressourcen virtueller Maschinen	346
Festlegen des Festplattenformats für eine virtuelle Maschine	347
Vergrößern virtueller Thin-Festplatten	347
Handhabung von Datenspeicher-Überbuchung	348
Array-Thin Provisioning und VMFS-Datenspeicher	348
Überwachen der Speicherplatznutzung	349
Identifizieren von Thin-bereitgestellten Speichergeräten	350
Zurückgewinnen von angesammeltem Speicherplatz	351
<b>25 Verwenden von Speicheranbietern</b>	<b>353</b>
Speicheranbieter und Darstellung von Speicherdaten	354
Anforderungen und Überlegungen hinsichtlich Speicheranbietern	354
Speicherstatusberichte	355
Registrieren von Speicheranbietern	356
Absichern der Kommunikation mit Speicheranbietern	356
Anzeigen von Speicheranbieterinformationen	357
Aufheben der Registrierung von Speicheranbietern	358
Aktualisieren von Speicheranbietern	358
<b>26 Verwenden von „vmkfstools“</b>	<b>359</b>
vmkfstools-Befehlssyntax	359
vmkfstools-Optionen	360
Unteroption -v	361
Dateisystemoptionen	361
Optionen für virtuelle Festplatten	364
Speichergerätoptionen	371

# Grundlegende Informationen zum vSphere-Speicher

Die Dokumentation zu *vSphere-Speicher* beschreibt die Speicheroptionen für VMware® ESXi und erläutert, wie das ESXi-System konfiguriert wird, damit es verschiedene Speichertypen verwenden und verwalten kann. Zudem befasst sich die Dokumentation zu *vSphere Storage* explizit mit den Fibre Channel® - und iSCSI-SANs (Storage Area Networks) als Speicheroptionen und behandelt die Besonderheiten der Verwendung von ESXi in Fibre Channel- und iSCSI-Umgebungen.

## Zielgruppe

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen, den Vorgängen von Datencentern und SAN-Speicherkonzepten vertraut sind.

# Aktualisierte Informationen

*vSphere-Speicher* wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *vSphere-Speicher*.

Revision	Beschreibung
19. APR. 2022	Nebenversionen.
15. August 2020	Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip in unserer Kunden-, Partner- und internen Community zu fördern, ersetzen einen Teil der Terminologie in unseren Inhalten. Wir haben diesen Leitfaden aktualisiert, um Instanzen einer nicht inklusiven Sprache zu entfernen.
27. Juni 2019	Nebenversionen.
27. NOV 2018	Nebenversionen.
12. JUL 2018	Nebenversionen.
18. APR 2018	Nebenversionen.
20. MRZ 2018	Nebenversionen.
14. FEB 2018	Nebenversionen.
DE-001799-07	<a href="#">Kopieren von Datenspeicherordnern oder -dateien</a> enthält jetzt die Aussage, dass der Datenspeicherbrowser das Kopieren von VM-Dateien zwischen vCenter Server-Systemen nicht unterstützt.
DE-001799-06	<a href="#">Verwenden des Datenspeicherbrowsers</a> wurde mit weiteren Details aktualisiert.
DE-001799-05	<ul style="list-style-type: none"><li>■ <a href="#">Richtlinien und empfohlene Vorgehensweisen für E/A-Filter</a> wurde aktualisiert und enthält jetzt Angaben zu E/A-Filtern und Snapshot-Strukturen.</li><li>■ <a href="#">Speicherfilterung</a> wurde aktualisiert, um den Wert für „Filter für dieselben Hosts und Transporte“ zu korrigieren. Der korrigierte Wert lautet <code>config.vpxd.filter.sameHostsAndTransportsFilter</code>.</li></ul>
DE-001799-04	<a href="#">Geschätzte Lebensdauer von Flash-Geräten</a> wurde mit zusätzlichen Details aktualisiert.
DE-001799-03	<a href="#">Migrieren von virtuellen Maschinen mit Flash Read Cache</a> wurde korrigiert, sodass der Abschnitt jetzt mit den im vSphere Web Client verfügbaren Optionen übereinstimmt.
DE-001799-02	Unter <a href="#">Abrufen von Informationen für den Cachespeicher für VMFS-Zeigerblöcke</a> wird jetzt auch der Befehl <code>esxcli storage vmfs pbcache</code> behandelt.
DE-001799-01	Nebenversionen.
DE-001799-00	Erstversion.

# Einführung in die Speicherung

# 1

Diese Einführung beschreibt die Speichermöglichkeiten in vSphere und erklärt, wie Sie Ihren Host konfigurieren müssen, damit er verschiedene Speichertypen verwenden und verwalten kann.

Dieses Kapitel enthält die folgenden Themen:

- [Speichervirtualisierung](#)
- [Physische Speichertypen](#)
- [Ziel- und Gerätedarstellungen](#)
- [Eigenschaften des Speichergeräts](#)
- [Unterstützte Speicheradapter](#)
- [Merkmale von Datenspeichern](#)
- [Speicherzugriff durch virtuelle Maschinen](#)
- [Vergleich der Speichertypen](#)

## Speichervirtualisierung

Die vSphere-Speichervirtualisierung unterstützt Funktionen wie beispielsweise virtuelle Maschinen, Virtual SAN, virtuelle Volumes, richtlinienbasierte Speicherverwaltung usw.

ESXi bietet eine Speichervirtualisierung auf Hostebene, die die physische Speicherebene von virtuellen Maschinen logisch abstrahiert. Eine virtuelle Maschine in ESXi 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. Sie können virtuelle Maschinen mit mehreren virtuellen Festplatten konfigurieren.

Für den Zugriff auf virtuelle Festplatten verwendet eine virtuelle Maschine virtuelle SCSI-Controller. Zu diesen virtuellen Controllern gehören BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS und VMware Paravirtual. Diese Controller sind die einzigen SCSI-Controllertypen, die eine virtuelle Maschine anzeigen und auf die sie zugreifen kann.

Jede virtuelle Festplatte befindet sich in einem Datenspeicher, der auf physischem Speicher bereitgestellt wird. Jede virtuelle Festplatte wird vom Standpunkt der virtuellen Maschine aus so angezeigt, als wäre ein SCSI-Laufwerk mit einem SCSI-Controller verbunden. Ob auf den tatsächlichen physischen Speicher über parallele Speicher- oder Netzwerkadapter auf dem Host zugegriffen wird, wird normalerweise auf dem Gastbetriebssystem und den Anwendungen, die auf der virtuellen Maschine ausgeführt werden, angezeigt.

Zusätzlich zu virtuellen Festplatten bietet vSphere einen Mechanismus, der als Raw Device Mapping (RDM) bezeichnet wird. RDM ist nützlich, wenn ein Gastbetriebssystem in einer virtuellen Maschine direkten Zugriff auf ein Speichergerät anfordert. Informationen zu RDMs finden Sie unter [Kapitel 18 Raw-Gerätezuordnung](#).

Weitere Speichervirtualisierungsfunktionen von vSphere sind Virtual SAN, virtueller Flash, virtuelle Volumes und richtlinienbasierte Speicherverwaltung. Weitere Informationen zu Virtual SAN finden Sie unter *Verwalten von VMware Virtual SAN*.

## Physische Speichertypen

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

ESXi unterstützt folgende Speichertypen:

### Lokaler Speicher

Speichert die Dateien virtueller Maschinen auf internen oder direkt verbundenen externen Speicherfestplatten.

### Netzwerkspeicher

Speichert die Dateien virtueller Maschinen auf externen Speicherfestplatten oder Arrays, die über eine Direktverbindung oder ein Hochgeschwindigkeitsnetzwerk an Ihren Host angeschlossen sind.

## Lokaler Speicher

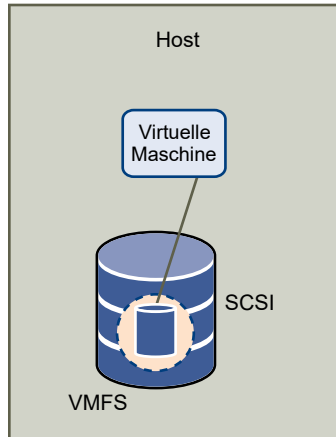
Lokale Speichergeräte können interne Festplatten innerhalb Ihres ESXi-Hosts oder externe Speichersysteme sein, die sich außerhalb des Hosts befinden und über Protokolle wie SAS oder SATA direkt mit ihm verbunden sind.

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

In der folgenden Abbildung wird eine virtuelle Maschine angezeigt, die lokalen SCSI-Speicher verwendet.



Abbildung 1-1. Lokaler Speicher



Bei diesem Beispiel einer lokalen Speichertopologie verwendet der Host eine einzelne Verbindung zu einer Speicherfestplatte. 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 Speicher-Arrays und Hosts sorgt für einzelne Ausfallstellen, die Störungen verursachen können, wenn eine Verbindung unzuverlässig wird oder ausfällt. Da die meisten lokalen Speichergeräte jedoch keine Unterstützung für mehrere Verbindungen bieten, können Sie für den Zugriff auf den lokalen Speicher nicht mehrere Pfade verwenden.

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

---

**Hinweis** Virtuelle Maschinen können nicht auf IDE-/ATA- oder USB-Laufwerken gespeichert werden.

---

Lokaler Speicher unterstützt die gemeinsame Nutzung auf mehreren Hosts nicht. Nur ein Host hat Zugriff auf einen Datenspeicher auf einem lokalen Speichergerät. Infolgedessen können Sie zwar lokalen Speicher verwenden, um virtuelle Maschinen zu erstellen, werden aber daran gehindert, VMware-Funktionen zu verwenden, die gemeinsam genutzten Speicher erfordern, z. B. HA und vMotion.

Wenn Sie jedoch einen Cluster von Hosts verwenden, die nur über lokale Speichergeräte verfügen, können Sie Virtual SAN implementieren. Virtual SAN wandelt lokale Speicherressourcen in gemeinsam genutzten softwaredefinierten Speicher um und ermöglicht Ihnen die Verwendung der Funktionen, die gemeinsam genutzten Speicher voraussetzen. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware Virtual SAN*.

## Netzwerkspeicher

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

Netzwerksspeichergeräte werden gemeinsam genutzt. Auf Datenspeicher auf Netzwerksspeichergeräten können mehrere Hosts gleichzeitig zugreifen. ESXi unterstützt mehrere Netzwerksspeichertechnologien.

Zusätzlich zu dem in diesem Thema behandelten traditionellen Netzwerksspeicher unterstützt VMware virtualisierten gemeinsam genutzten Speicher, wie beispielsweise Virtual SAN. Virtual SAN wandelt die internen Speicherressourcen Ihrer ESXi-Hosts in gemeinsam genutzten Speicher, der Funktionen wie High Availability und vMotion für virtuelle Maschinen bereitstellt. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware Virtual SAN*.

---

**Hinweis** Dieselbe LUN kann einem ESXi-Host oder mehreren Hosts nicht von verschiedenen Speicherprotokollen präsentiert werden. Um auf die LUN zuzugreifen, müssen Hosts immer ein einziges Protokoll, z. B. entweder nur Fibre-Channel oder nur iSCSI verwenden.

---

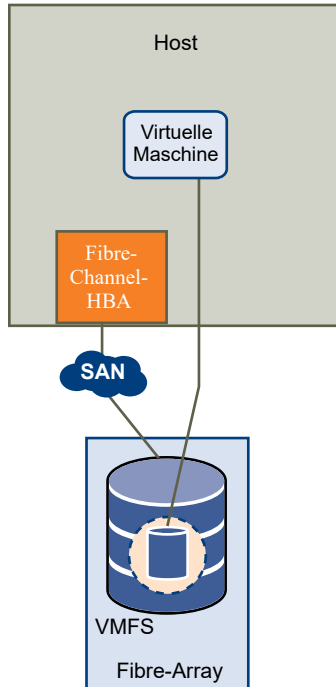
## Fibre-Channel (FC)

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) ausgestattet sein. Sofern Sie nicht mit Fibre-Channel-Direktverbindungsspeicher arbeiten, benötigen Sie Fibre-Channel-Switches für die Weiterleitung der zu speichernden Daten. Wenn der Host FCoE-Adapter (Fibre Channel-over-Ethernet-Adapter) enthält, können Sie mithilfe eines Ethernet-Netzwerks eine Verbindung zu Ihren gemeinsam genutzten Fibre-Channel-Geräten herstellen.

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

Abbildung 1-2. Fibre-Channel-Speicher



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

Weitere Informationen über das Einrichten des Fibre-Channel-SANs finden Sie unter [Kapitel 3 Verwenden von ESXi mit Fibre-Channel-SAN](#).

## 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-iSCSI

Der Host stellt eine Verbindung mit dem Speicher über einen Drittanbieter-Adapter her, der zur Auslagerung der iSCSI- und Netzwerkverarbeitung geeignet ist. Hardwareadapter können sowohl abhängig als auch unabhängig sein.

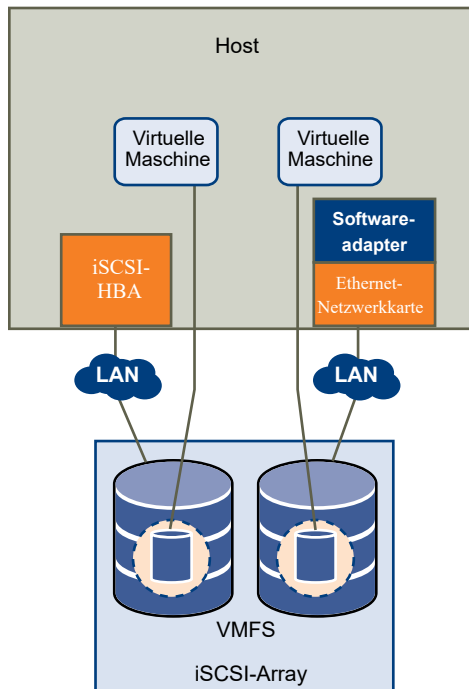
### Software-iSCSI

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.

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

iSCSI-Speicher stellt verschiedene Typen von iSCSI-Initiatoren dar.

**Abbildung 1-3. iSCSI-Speicher**



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

Im rechten Beispiel verwendet der Host zum Verbinden mit dem iSCSI-Speicher einen Software-iSCSI-Adapter und eine Ethernet-Netzwerkkarte.

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.

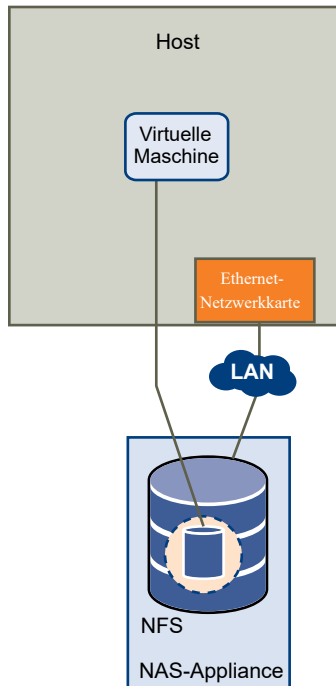
Weitere Informationen über das Einrichten des iSCSI-SANs finden Sie unter [Kapitel 9 Verwenden von ESXi mit iSCSI-SAN](#).

## 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 (Network File System)-Protokoll, Version 3 oder 4.1, um mit den NAS-/NFS-Servern zu kommunizieren. Für die Netzwerkverbindung benötigt der Host einen Standardnetzwerkadapter.

NFS-Speicher 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 1-4. NFS-Speicher



Weitere Informationen über das Einrichten eines NFS-Speichers finden Sie unter [Grundlegende Informationen zu NFS-Datenspeichern](#).

## Gemeinsam genutztes Serial Attached SCSI (SAS)

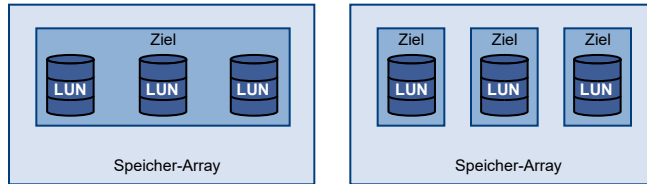
Speichert virtuelle Maschinen auf direkt angeschlossenen SAS-Speichersystemen, die gemeinsamen Zugriff auf mehrere Hosts bieten. Diese Art des Zugriffs ermöglicht mehreren Hosts, auf denselben VMFS-Dateispeicher auf eine LUN zuzugreifen.

## 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 Speicher-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 1-5. 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. Wenn eine LUN von mehreren Hosts gemeinsam verwendet wird, muss sie für alle Hosts mit der gleichen UUID bereitgestellt werden.

## Eigenschaften des Speichergeräts

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 die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

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

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

Tabelle 1-1. Informationen zum Speichergerät

Informationen zum Speichergerät	Beschreibung
Name	Auch als Anzeigenamen bezeichnet. Es ist ein 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.
Betriebszustand	Gibt an, ob das Gerät gemountet bzw. nicht gemountet ist. Weitere Informationen finden Sie unter <a href="#">Speichergeräte trennen</a> .
LUN	Logical Unit Number (LUN) innerhalb des SCSI-Ziels. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.

Tabelle 1-1. Informationen zum Speichergerät (Fortsetzung)

Informationen zum Speichergerät	Beschreibung
Laufwerkstyp	Gibt an, ob das Gerät ein Flash-Laufwerk oder ein reguläres HDD-Laufwerk ist. Weitere Informationen zur Verwendung von Flash-Laufwerken finden Sie unter <a href="#">Kapitel 14 Arbeiten mit Flash-Geräten</a> .
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet. Das Protokoll hängt vom Typ des verwendeten Speichers ab. Siehe <a href="#">Physische Speichertypen</a> .
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten der Pfade zum Speichergerät verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In. Weitere Informationen finden Sie unter <a href="#">Verwalten mehrerer Pfade</a> .
Hardwarebeschleunigung	Informationen dazu, ob das Speichergerät den Host bei Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen finden Sie unter <a href="#">Kapitel 23 Speicherhardware-Beschleunigung</a> .
Speicherort	Ein Pfad zum Speichergerät im Verzeichnis <code>/vmfs/devices/</code> .
Partitionsformat	Ein Partitionsschema, das vom Speichergerät verwendet wird. Es kann sich hierbei um einen Master Boot Record (MBR) oder eine GUID-Partitionstabelle (GPT) handeln. Die GPT-Geräte unterstützen Datenspeicher größer als 2 TB. Weitere Informationen finden Sie unter <a href="#">VMFS-Datenspeicher und Speicherfestplattenformate</a> .
Partitionen	Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.
Multipathing-Richtlinien (VMFS-Datenspeicher)	Pfadauswahlrichtlinie und Speicher-Array-Typ-Richtlinie, die der Host für die Pfade zum Speicher verwendet. Weitere Informationen finden Sie unter <a href="#">Kapitel 17 Grundlegendes zu Multipathing und Failover</a> .
Pfade (VMFS-Datenspeicher)	Pfade, die zum Zugriff auf den Speicher verwendet werden, und ihr Status.

## Anzeigen von Speichergeräten für einen Host

Zeigen Sie alle für einen Host verfügbaren Speichergeräte an. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

In der Ansicht „Speichergeräte“ können Sie die Speichergeräte des Hosts anzeigen, ihre Informationen analysieren und ihre Eigenschaften ändern.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

Alle für den Host verfügbaren Speichergeräte werden unter „Speichergeräte“ aufgeführt.

- 4 Wählen Sie ein Gerät in der Liste aus, um Details zu diesem Gerät anzuzeigen.
- 5 Auf den Registerkarten unter „Gerätedetails“ können Sie auf zusätzliche Informationen zugreifen und Eigenschaften für das ausgewählte Gerät ändern.

Registerkarte	Beschreibung
Eigenschaften	Anzeigen von Geräteeigenschaften und -merkmalen. Anzeigen und Ändern von Multipathing-Richtlinien für das Gerät.
Pfade	Anzeigen der für das Gerät verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads.

## Anzeigen von Speichergeräten für einen Adapter

Zeigen Sie eine Liste der Speichergeräte an, auf die über einen bestimmten Speicheradapter auf dem Host zugegriffen werden kann.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf „Speicheradapter“.  
Alle auf dem Host installierten Speicheradapter werden unter „Speicheradapter“ aufgeführt.
- 4 Wählen Sie den Adapter in der Liste aus und klicken Sie auf die Registerkarte **Geräte**.  
Die Speichergeräte, auf die der Host über den Adapter zugreifen kann, werden angezeigt.

## Unterstützte Speicheradapter

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

ESXi unterstützt verschiedene Adapterklassen, darunter SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE) und Ethernet. ESXi greift auf die Adapter direkt über Gerätetreiber im VMkernel zu.

Je nachdem, welchen Speichertyp Sie verwenden, müssen Sie möglicherweise einen Speicheradapter auf Ihrem Host aktivieren und konfigurieren.

Weitere Informationen zur Einrichtung von Software-FCoE-Adaptoren finden Sie unter [Kapitel 5 Konfigurieren von Fibre-Channel über Ethernet](#).

Weitere Informationen über das Konfigurieren verschiedener iSCSI-Adaptertypen finden Sie unter [Kapitel 10 Konfigurieren von iSCSI-Adaptern und -Speichern](#).

## Eigenschaften des Speicheradapters

Ihr Host verwendet Speicheradapter zum Zugreifen auf verschiedene Speichergeräte. Sie können Details zu den verfügbaren Speicheradaptern anzeigen und die Informationen überprüfen.



Sie müssen bestimmte Adapter aktivieren, beispielsweise Software-iSCSI oder FCoE, bevor Sie deren Informationen anzeigen können.

**Tabelle 1-2. Informationen zu Speicheradaptern**

Adapterinformationen	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 (unabhängige Hardware-iSCSI)	Eine dem iSCSI-HBA zugewiesene Adresse.
Geräte	Alle Speichergeräte oder LUNs, auf die der Adapter zugreifen kann.
Pfade	Alle vom Adapter zum Zugreifen auf Speichergeräte verwendeten Pfade.
Eigenschaften	Link, der angibt, dass für den Adapter eine zusätzliche Konfiguration erforderlich ist. Bei iSCSI- und FCoE-Adaptern wird dieser Link angezeigt.

## Anzeigen von Informationen zu Speicheradaptern

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

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter**.
- 4 Wählen Sie einen Adapter in der Liste aus, um Details dazu anzuzeigen.

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

Es gibt folgende Möglichkeiten, Datenspeicher zu vCenter Server hinzuzufügen:

- Mit dem Assistenten für neue Datenspeicher können Sie VMFS5-, NFS-3-, NFS-4.1- oder virtuelle Datenspeicher erstellen. Ein Virtual SAN-Datenspeicher wird automatisch erstellt, wenn Sie Virtual SAN aktivieren.
- Wenn Sie einen Host zum vCenter Server hinzufügen, werden alle Datenspeicher auf dem Host zum vCenter Server hinzugefügt.

In der folgenden Tabelle werden die Datenspeicherdetails aufgeführt, die Ihnen beim Prüfen von Datenspeichern im vSphere Web Client angezeigt werden. Bestimmte Eigenschaften sind möglicherweise nicht für alle Typen von Datenspeichern verfügbar oder anwendbar.

**Tabelle 1-3. Informationen zu Datenspeichern**

Informationen zu Datenspeichern	Anwendbarer Datenspeichertyp	Beschreibung
Name	VMFS NFS Virtual SAN VVOL	Bearbeitbarer Name, den Sie einem Datenspeicher zuweisen können. Weitere Informationen zum Umbenennen eines Datenspeichers finden Sie unter <a href="#">Ändern des Datenspeichernamens</a> .
Dateisystemtyp	VMFS NFS Virtual SAN VVOL	Das vom Datenspeicher verwendete Dateisystem. Weitere Informationen über VMFS- und NFS-Datenspeicher und deren Verwaltung finden Sie unter <a href="#">Kapitel 16 Arbeiten mit Datenspeichern</a> .  Informationen zu Datenspeichern für Virtual SAN erhalten Sie in der Dokumentation zu <i>Verwalten von VMware Virtual SAN</i> .  Informationen zu virtuellen Volumes finden Sie in <a href="#">Kapitel 19 Arbeiten mit virtuellen Volumes</a> .
Geräte-Backing	VMFS NFS Virtual SAN	Weitere Informationen zum zugrunde liegenden Speicher, z. B. einem Speichergerät, auf dem der Datenspeicher bereitgestellt wird (VMFS), Server und Ordner (NFS) oder Festplattengruppen (Virtual SAN).
Protokollendpunkte	VVOL	Informationen zu den entsprechenden Protokollendpunkten. Siehe <a href="#">Protokollendpunkte</a> .
Erweiterungen	VMFS	Einzelne Erweiterungen, aus denen der Datenspeicher besteht, samt Kapazität.
Laufwerkstyp	VMFS	Typ des zugrunde liegenden Speichergeräts: Flash-Laufwerk oder herkömmliche HDD-Festplatte. Weitere Informationen finden Sie unter <a href="#">Kapitel 14 Arbeiten mit Flash-Geräten</a> .
Kapazität	VMFS NFS Virtual SAN VVOL	Umfasst die Gesamtkapazität, bereitgestellten Speicherplatz und freien Speicherplatz.

Tabelle 1-3. Informationen zu Datenspeichern (Fortsetzung)

Informationen zu Datenspeichern	Anwendbarer Datenspeichertyp	Beschreibung
Mount-Punkt	VMFS NFS Virtual SAN VVOL	Ein Pfad zum Datenspeicher im Verzeichnis <code>/vmfs/volumes/</code> des Hosts
Funktionssätze	VMFS <b>Hinweis</b> Ein VMFS-Datenspeicher mit mehreren Erweiterungen übernimmt die Funktionalität von nur einer seiner Erweiterungen. NFS Virtual SAN	Informationen zu den Speicherdatendiensten, die vom zugrunde liegenden Speicherelement zur Verfügung gestellt werden. Sie können sie nicht ändern.
Storage I/O Control	VMFS NFS	Informationen darüber, ob die clusterweite Speicher-E/A-Priorisierung aktiviert ist. Informationen finden Sie in der Dokumentation <i>Handbuch zur vSphere-Ressourcenverwaltung</i> .
Hardwarebeschleunigung	VMFS NFS Virtual SAN VVOL	Informationen darüber, ob das zugrunde liegende Speicherelement die Hardwarebeschleunigung unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen finden Sie unter <a href="#">Kapitel 23 Speicherhardware-Beschleunigung</a> . <b>Hinweis</b> NFS 4.1 bietet keine Unterstützung für Hardwarebeschleunigung.
Tags	VMFS NFS Virtual SAN VVOL	Datenspeicherfunktionen, die Sie definieren und in Form von Tags Datenspeichern zuordnen. Weitere Informationen hierzu finden Sie unter <a href="#">Speicherrichtlinien und Regeln</a> .
Konnektivität mit Hosts	VMFS NFS VVOL	Hosts, auf denen der Datenspeicher gemountet wird.
Multipathing	VMFS VVOL	Pfadauswahlrichtlinie, die der Host zum Zugriff auf den Speicher verwendet. Weitere Informationen finden Sie unter <a href="#">Kapitel 17 Grundlegendes zu Multipathing und Failover</a> .






## Anzeigen von Informationen zu Datenspeichern

Greifen Sie mit dem vSphere Web Client-Navigator auf die Datenspeicheransicht zu. In der Datenspeicheransicht, die Sie über den Navigator anzeigen, können Sie alle Datenspeicher auflisten, die in der vSphere-Infrastruktur verfügbar sind, die Informationen analysieren und die Eigenschaften ändern. Sie können auch die Ansicht verwenden, um Datenspeicher zu erstellen.

Um Datenspeicher für ein bestimmtes übergeordnetes Objekt aufzulisten, beispielsweise ein Datacenter, einen Cluster oder einen Host, siehe [Listen von Datenspeichern für ein Infrastrukturobjekt](#).

## Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.  
Datenspeicher, die in der Bestandsliste verfügbar sind, werden im mittleren Datenspeicherbereich angezeigt.
- 2 Verwenden Sie die Symbole, um einen Datenspeicher zu erstellen oder grundlegende Aufgaben für einen ausgewählten Datenspeicher auszuführen.

Symbol	Beschreibung
	Erstellen eines Datenspeichers.
	Erhöhen der Datenspeicherkapazität.
	Mounten eines Datenspeichers auf bestimmten Hosts.
	Entfernen eines Datenspeichers.
	Unmounten eines Datenspeichers aus bestimmten Hosts.

- 3 Um spezielle Datenspeicherdetails anzuzeigen, klicken Sie auf einen ausgewählten Datenspeicher.
- 4 Verwenden Sie Registerkarten, um auf zusätzliche Informationen zuzugreifen und Datenspeichereigenschaften zu ändern.






Registerkarte	Beschreibung
<b>Erste Schritte</b>	Anzeigen einführender Informationen und Zugriff auf grundlegende Aktionen.
<b>Übersicht</b>	Zeigen Sie Statistiken und die Konfiguration für den ausgewählten Datenspeicher an.
<b>Überwachen</b>	Anzeigen von Alarmen, Leistungsdaten, Ressourcenzuteilung, Ereignissen und anderen Statusinformationen für den Datenspeicher.
<b>Verwalten</b>	Anzeigen und Ändern von Datenspeichereigenschaften, Alarmdefinitionen, Tags und Berechtigungen. Verwenden Sie diese Registerkarte, um auf Speichergeräte zuzugreifen, die die Datenbank absichert, und um Mehrfachpfad-Details für die Datenspeichergeräte anzuzeigen.
<b>Verwandte Objekte</b>	Anzeigen von Objekten, die mit dem Datenspeicher verbunden sind. Die Objekte umfassen virtuelle Maschinen, die auf dem Datenspeicher und den Hosts untergebracht sind, auf denen der Datenspeicher gemountet ist.

## Listen von Datenspeichern für ein Infrastrukturobjekt

Zeigen Sie die Datenspeicher für ein spezifisches übergeordnetes Objekt an, beispielsweise ein Datacenter, ein Cluster oder einen Host.

## Verfahren

- 1 Verwenden Sie den vSphere Web Client-Objektnavigator, um zu einem Objekt zu navigieren, das ein gültiges übergeordnetes Objekt eines Datenspeichers ist, beispielsweise ein Datacenter, ein Cluster oder ein Host.
- 2 Klicken Sie auf der Registerkarte **Verwandte Objekte** und klicken Sie auf **Datenspeicher**.  
Wenn Datenspeicher für dieses Objekt konfiguriert sind, werden sie im mittleren Bereich „Datenspeicher“ angezeigt.
- 3 Verwenden Sie die Symbole, um einen Datenspeicher zu erstellen oder grundlegende Aufgaben für einen ausgewählten Datenspeicher auszuführen.

Symbol	Beschreibung
	Erstellen eines Datenspeichers.
	Erhöhen der Datenspeicherkapazität.
	Mounten eines Datenspeichers auf bestimmten Hosts.
	Entfernen eines Datenspeichers.
	Unmounten eines Datenspeichers aus bestimmten Hosts.

- 4 Verwenden Sie Registerkarten, um auf zusätzliche Informationen zuzugreifen und Datenspeichereigenschaften zu ändern.

Registerkarte	Beschreibung
<b>Erste Schritte</b>	Anzeigen einführender Informationen und Zugriff auf grundlegende Aktionen.
<b>Übersicht</b>	Zeigen Sie Statistiken und die Konfiguration für den ausgewählten Datenspeicher an.
<b>Überwachen</b>	Anzeigen von Alarmen, Leistungsdaten, Ressourcenzuteilung, Ereignissen und anderen Statusinformationen für den Datenspeicher.
<b>Verwalten</b>	Anzeigen und Ändern von Datenspeichereigenschaften, Alarmdefinitionen, Tags und Berechtigungen. Verwenden Sie diese Registerkarte, um auf Speichergeräte zuzugreifen, die die Datenbank absichert, und um Mehrfachpfad-Details für die Datenspeichergeräte anzuzeigen.
<b>Verwandte Objekte</b>	Anzeigen von Objekten, die mit dem Datenspeicher verbunden sind. Die Objekte umfassen virtuelle Maschinen, die auf dem Datenspeicher und den Hosts untergebracht sind, auf denen der Datenspeicher gemountet ist.

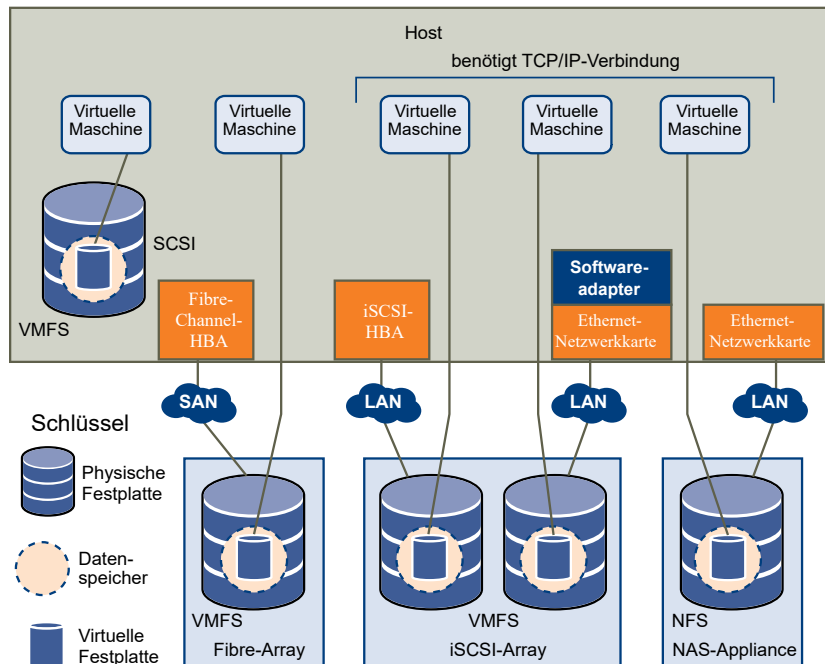
## Speicherzugriff durch virtuelle Maschinen

Wenn eine virtuelle Maschine mit ihrer virtuellen Festplatte kommuniziert, die in einem Datenspeicher gespeichert ist, 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), Fibre Channel over Ethernet (FCoE) 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.

Die folgende Abbildung zeigt die Unterschiede zwischen den Speichertypen: Fünf virtuelle Maschinen verwenden unterschiedliche Arten von Speichern.

**Abbildung 1-6. 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.

In der folgenden Tabelle werden die Netzwerkspeichertechnologien verglichen, die ESXi unterstützt.

Tabelle 1-4. Von ESXi unterstützter Netzwerkspeicher

Technologie	Protokolle	Übertragungen	Schnittstelle
Fibre-Channel	FC/SCSI	Blockzugriff für Daten/LUN	FC-HBA
Fibre-Channel über Ethernet	FCoE/SCSI	Blockzugriff für Daten/LUN	<ul style="list-style-type: none"> <li>■ Converged Network Adapter (Hardware-FCoE)</li> <li>■ Netzwerkkarte mit FCoE-Unterstützung (Software-FCoE)</li> </ul>
iSCSI	IP/SCSI	Blockzugriff für Daten/LUN	<ul style="list-style-type: none"> <li>■ iSCSI-HBA oder iSCSI-fähige Netzwerkkarte (Hardware-iSCSI)</li> <li>■ Netzwerkadapter (Software-iSCSI)</li> </ul>
NAS	IP/NFS	Datei (kein direkter LUN-Zugriff)	Netzwerkadapter

In der folgenden Tabelle werden die von verschiedenen Speichertypen unterstützten vSphere-Funktionen verglichen.

Tabelle 1-5. Von Speichertypen unterstützte vSphere-Funktionen

Speichertyp	Starten von VMs	vMotion	Datenspeicher	RDM	VM-Cluster	vSphere HA und DRS	Storage APIs - Data Protection
Lokaler Speicher	Ja	Nein	VMFS	Nein	Ja	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 3 und NFS 4.1	Nein	Nein	Ja	Ja

**Hinweis** Der lokale Speicher unterstützt einen Cluster von virtuellen Maschinen auf einem einzelnen Host (auch als „systeminterner Cluster“ bekannt). Eine gemeinsam genutzte virtuelle Festplatte ist erforderlich. Weitere Informationen zu dieser Konfiguration finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

# Übersicht über die Verwendung von ESXi in einem SAN

## 2

Die Verwendung von ESXi in einem SAN erhöht die Flexibilität, Effizienz und Zuverlässigkeit. Bei der Verwendung von ESXi mit einem SAN werden eine zentrale Verwaltung sowie Failover- und Lastausgleichstechnologien ebenfalls unterstützt.

Im Folgenden werden die Vorteile der Verwendung von ESXi mit einem SAN zusammengefasst:

- Sie haben die Möglichkeit, Daten sicher zu speichern und mehrere Pfade zu Ihrem Speicher zu konfigurieren, um solch eine Fehlerquelle auszuschließen.
- Die Fehlerresistenz wird durch die Verwendung eines SAN mit ESXi-Systemen auf die Server erweitert. Wenn Sie einen SAN-Speicher einsetzen, können alle Anwendungen nach einem Ausfall des ursprünglichen Hosts umgehend auf einem anderen Host neu gestartet werden.
- Mit VMware VMotion können Sie während des laufenden Systembetriebs Migrationen virtueller Maschinen durchführen.
- Verwenden Sie VMware High Availability (HA) zusammen mit einem SAN, um die virtuellen Maschinen mit ihrem zuletzt bekannten Status auf einem anderen Server neu zu starten, falls ihr Host ausfällt.
- Verwenden Sie VMware Fault Tolerance (FT), um geschützte virtuelle Maschinen auf zwei unterschiedlichen Hosts zu replizieren. Die virtuellen Maschinen werden weiterhin unterbrechungsfrei auf dem sekundären Host ausgeführt, falls der primäre Host ausfällt.
- Verwenden Sie VMware DRS (Distributed Resource Scheduler), um virtuelle Maschinen für den Lastausgleich von einem Host auf einen anderen Host zu migrieren. Da sich der Speicher in einem freigegebenen SAN-Array befindet, werden Anwendungen ohne Unterbrechung weiter ausgeführt.
- Wenn Sie VMware DRS-Cluster verwenden, versetzen Sie einen ESXi-Host in den Wartungsmodus, damit das System alle laufenden virtuellen Maschinen auf andere ESXi-Hosts migriert. Anschließend können Sie auf dem ursprünglichen Host Upgrades oder andere Wartungsvorgänge durchführen.



Die Portabilität und Kapselung von virtuellen VMware-Maschinen ergänzt die Eigenschaften des Speichers hinsichtlich der gemeinsamen Nutzung. Wenn sich virtuelle Maschinen in einem SAN-basierten Speicher befinden, können Sie eine virtuelle Maschine auf einem Server herunterfahren und diese auf einem anderen Server starten oder diese auf einem Server anhalten und den Betrieb auf einem anderen Server im selben Netzwerk wieder aufnehmen – und das in nur wenigen Minuten. Auf diese Weise können Sie Rechenressourcen migrieren und gleichzeitig einen konsistenten gemeinsamen Zugriff aufrechterhalten.

Dieses Kapitel enthält die folgenden Themen:

- [Anwendungsbeispiele für ESXi und SAN](#)
- [Besonderheiten bei der Verwendung von SAN-Speicher mit ESXi](#)
- [ESXi-Hosts und mehrere Speicher-Arrays](#)
- [Entscheidungen zur Verwendung von LUNs](#)
- [Auswählen von Speicherorten für virtuelle Maschinen](#)
- [Mehrschichtige Anwendungen](#)
- [Verwaltungsanwendungen von Drittanbietern](#)
- [Überlegungen zu SAN-Speichersicherungen](#)

## Anwendungsbeispiele für ESXi und SAN

Wenn mit einem SAN verwendet, kann ESXi von mehreren vSphere-Funktionen profitieren, wie z. B. Storage vMotion, DRS (Distributed Resource Scheduler), HA (High Availability) usw.

Die Verwendung von ESXi in Verbindung mit einem SAN ist für die folgenden Aufgaben hilfreich:

### Speicherkonsolidierung und Vereinfachung des Speicherlayouts

Wenn Sie mit mehreren Hosts arbeiten und auf jedem Host mehrere virtuelle Maschinen ausgeführt werden, reicht der Speicher des Hosts nicht mehr aus und es wird externer Speicher benötigt. Wählen Sie ein SAN für die externe Datenspeicherung, um eine einfachere Systemarchitektur und gleichzeitig andere Vorteile bereitzustellen.

### Wartung ohne Ausfallzeiten

Verwenden Sie bei der Wartung von ESXi-Hosts oder -Infrastrukturen vMotion für die Migration virtueller Maschinen auf einen anderen Host. Falls im SAN ein gemeinsamer Speicher vorhanden ist, kann die Wartung für Benutzer virtueller Maschinen ohne Unterbrechungen durchgeführt werden. Die aktiven Prozesse der virtuellen Maschine werden während einer Migration weiterhin ausgeführt.

### Lastenausgleich

Sie können einen Host zu einem DRS-Cluster hinzufügen. Die Hostressourcen werden dann Teil der Clusterressourcen. Die Verteilung und Verwendung von CPU- und Arbeitsspeicherressourcen für alle Hosts und virtuelle Maschinen im Cluster werden

kontinuierlich überwacht. DRS vergleicht diese Metriken mit denen einer idealen Ressourcennutzung. Die ideale Ressourcennutzung berücksichtigt die Attribute der Ressourcenpools und der virtuellen Maschinen des Clusters, des aktuellen Bedarfs sowie des Ziels des Ungleichgewichts. DRS migriert daraufhin die virtuellen Maschinen entsprechend (oder schlägt ihre Migration vor).

### Notfallwiederherstellung

Sie können VMware High Availability zum Konfigurieren von mehreren ESXi-Hosts als Cluster verwenden, um eine schnelle Wiederherstellung nach Ausfällen und kosteneffektive hohe Verfügbarkeit für Anwendungen zu bieten, die in virtuellen Maschinen ausgeführt werden.

### Vereinfachte Array-Migrationen und Speicher-Upgrades

Wenn Sie neue Speichersysteme oder -Arrays erwerben, verwenden Sie Storage vMotion, um eine automatisierte Migration der Festplattendateien virtueller Maschinen vom vorhandenen Speicher zum neuen Speicherziel ohne Unterbrechungen für die Benutzer virtueller Maschinen durchzuführen.

## Besonderheiten bei der Verwendung von SAN-Speicher mit ESXi

Die Verwendung eines SANs in Verbindung mit einem ESXi-Host unterscheidet sich von der herkömmlichen SAN-Verwendung in vielerlei Hinsicht.

Beachten Sie bei der Verwendung von SAN-Speicher mit ESXi folgende Punkte:

- Sie können SAN-Verwaltungstools nicht verwenden, um direkt auf Betriebssysteme von virtuellen Maschinen zuzugreifen, die den Speicher verwenden. Mit herkömmlichen Tools können Sie ausschließlich das VMware ESXi-Betriebssystem überwachen. Über den vSphere Web Client können Sie virtuelle Maschinen überwachen.
- Der für die SAN-Verwaltungstools sichtbare HBA gehört zum ESXi-System und nicht zum Teil der virtuellen Maschine.
- Das ESXi-System führt in der Regel für Sie ein Multipathing durch.

## ESXi-Hosts und mehrere Speicher-Arrays

Ein ESXi-Host kann auf Speichergeräte aus mehreren Speicher-Arrays zugreifen, auch auf Speicher von verschiedenen Anbietern.

Wenn Sie mehrere Arrays von verschiedenen Anbietern verwenden, gilt Folgendes:

- Wenn Ihr Host das gleiche Speicher-Array-Typ-Plug-In (SATP) für mehrere Arrays verwendet, seien Sie vorsichtig, wenn Sie die standardmäßige Pfadauswahlrichtlinie (PSP) für diesen SATP ändern müssen. Die Änderung wird auf sämtlichen Arrays wirksam. Weitere Information über SATP und PSP finden Sie unter [Kapitel 17 Grundlegendes zu Multipathing und Failover](#).

- Einige Speicher-Arrays empfehlen spezifische Warteschlangentiefen und andere Einstellungen. In der Regel werden diese Einstellungen global auf ESXi-Hostebene konfiguriert. Eine Änderung für ein Array beeinflusst andere Arrays, die LUN für den Host präsentieren. Weitere Informationen zur Warteschlangentiefe finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1267>.
- Verwenden Sie das Einzel-Initiator-Einzel-Ziel-Zoning, wenn Sie ESXi-Hosts in Fibre-Channel-Arrays einteilen. Bei dieser Art der Konfiguration beeinflussen Hersteller-spezifische Ereignisse, die in einem Array auftreten, nicht die anderen Arrays. Weitere Informationen zum Zoning finden Sie unter [Verwenden von Zoning mit Fibre-Channel-SANs](#).

## Entscheidungen zur Verwendung von LUNs

Bevor Sie LUNs mit einem VMFS-Datenspeicher formatieren, müssen Sie zunächst festlegen, wie Sie den Speicher für Ihre ESXi-Systeme einrichten möchten.

Bei der Wahl der richtigen Größe und Anzahl der zu verwendenden LUNs sollten Sie folgende Aspekte berücksichtigen:

- Jede LUN sollte über das richtige RAID-Level und die richtigen Speichermerkmale für die Anwendungen verfügen, die in virtuellen Maschinen ausgeführt werden, die die LUN verwenden.
- Jede LUN darf nur einen einzigen VMFS-Datenspeicher enthalten.
- Wenn mehrere virtuelle Maschinen auf dieselbe VMFS zugreifen, lassen sich mithilfe von Festplattenfreigaben Prioritäten für virtuelle Maschinen festlegen.

Die folgenden Gründe sprechen für weniger und dafür größere LUNs:

- Mehr Flexibilität beim Erstellen virtueller Maschinen, ohne beim Speicheradministrator mehr Speicherplatz anfordern zu müssen.
- Mehr Flexibilität bei der Größenänderung virtueller Festplatten, dem Erstellen von Snapshots usw.
- Weniger zu verwaltende VMFS-Datenspeicher.

Die folgenden Gründe sprechen für mehr und dafür kleinere LUNs:

- Weniger falsch genutzter Speicherplatz.
- Unterschiedliche Anwendungen könnten unterschiedliche RAID-Merkmale erfordern.
- Mehr Flexibilität, da die Multipathing-Richtlinie und gemeinsam genutzte Festplattenfreigaben pro LUN festgelegt werden.
- Für den Einsatz von Microsoft Clusterdienst muss jede Clusterfestplattenressource in ihrer eigenen LUN eingerichtet sein.
- Bessere Leistung aufgrund weniger Konflikte auf den einzelnen Volumes.

Wenn für eine virtuelle Maschine keine Speicherbeschreibung vorliegt, gibt es häufig keine einfache Methode zum Bestimmen der Anzahl und Größe der bereitzustellenden LUNs. Sie können experimentieren, indem Sie entweder ein Vorhersagemodell oder ein adaptives Modell verwenden.

## Verwenden eines Vorhersagemodells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESXi-Systeme einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden und welche Größe diese besitzen sollen. Sie können experimentieren, indem Sie das Vorhersagemodell verwenden.

### Verfahren

- 1 Stellen Sie mehrere LUNs mit unterschiedlichen Speichereigenschaften bereit.
- 2 Erstellen Sie einen VMFS-Datenspeicher in jeder LUN und benennen Sie jedes Volume entsprechend seinen Eigenschaften.
- 3 Erstellen Sie virtuelle Festplatten, um Kapazität für die Daten der Anwendungen virtueller Maschinen in den VMFS-Datenspeichern zu schaffen, die auf LUNs mit dem entsprechenden RAID-Level für die Anwendungsanforderungen erstellt wurden.
- 4 Sie verwenden Festplattenfreigaben, um virtuelle Maschinen mit hoher Priorität von denen mit niedriger Priorität zu unterscheiden.

---

**Hinweis** Festplattenfreigaben sind nur innerhalb eines bestimmten Hosts entscheidend. Die den virtuellen Maschinen auf einem Host zugeordneten Freigaben haben keine Auswirkungen auf virtuelle Maschinen auf anderen Hosts.

---

- 5 Sie führen die Anwendungen aus, um zu ermitteln, ob die Leistung der virtuellen Maschine zufriedenstellend ist.

## Verwenden des adaptiven Modells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESXi-Hosts einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden und welche Größe sie besitzen sollen. Sie können experimentieren, indem Sie das adaptive Modell verwenden.

### Verfahren

- 1 Stellen Sie eine große LUN (RAID 1+0 oder RAID 5) mit aktiviertem Schreibcache bereit.
- 2 Erstellen Sie in dieser LUN ein VMFS.
- 3 Erstellen Sie vier oder fünf virtuelle Festplatten im VMFS.
- 4 Sie führen die Anwendungen aus, um zu ermitteln, ob die Festplattenleistung ausreichend ist.

## Ergebnisse

Wenn die Leistung ausreicht, können Sie zusätzliche virtuelle Festplatten im VMFS einrichten. Reicht die Leistung nicht aus, haben Sie die Möglichkeit, eine neue, große LUN zu erstellen (eventuell mit einer anderen RAID-Ebene) und den Vorgang zu wiederholen. Verwenden Sie die Migrationsfunktion, damit keine Daten virtueller Maschinen bei der Neuerstellung der LUN verloren gehen.

## Auswählen von Speicherorten für virtuelle Maschinen

Bei der Leistungsoptimierung der virtuellen Maschinen ist der Speicherort ein wichtiger Faktor. Es muss stets zwischen kostenintensivem Speicher, der eine optimale Leistung und hohe Verfügbarkeit bietet, und kostengünstigem Speicher mit niedrigerer Leistung abgewogen werden.

Die Speichereinteilung in verschiedene Qualitätsstufen ist von zahlreichen Faktoren abhängig:

- Hoch. Bietet hohe Leistung und Verfügbarkeit. Bietet unter Umständen auch integrierte Snapshots, um Sicherungen und PiT-Wiederherstellungen (Point-in-Time) zu vereinfachen. Unterstützt Replizierungen, vollständige Speicherprozessorredundanz und SAS-Laufwerke. Verwendet teure Spindeln.
- Mittel. Bietet durchschnittliche Leistung, niedrigere Verfügbarkeit, geringe Speicherprozessorredundanz und SCSI- bzw. SAS-Laufwerke. Bietet möglicherweise Snapshots. Verwendet Spindeln mit durchschnittlichen Kosten.
- Niedrig. Bietet niedrige Leistung, geringe interne Speicherredundanz. Verwendet kostengünstige SCSI-Laufwerke oder SATA (serielle kostengünstige Spindeln).

Nicht alle Anwendungen müssen auf dem Speicher mit der höchsten Leistung und Verfügbarkeit ausgeführt werden – zumindest nicht während ihres gesamten Lebenszyklus.

---

**Hinweis** Wenn Sie einige der von hochwertigen Speichern bereitgestellten Funktionen, z. B. Snapshots, benötigen, die Kosten aber gering halten möchten, können Sie die gewünschten Funktionen eventuell über den Einsatz von Software erreichen. Beispielsweise können Sie Snapshots auch mit einer Software erstellen.

---

Bevor Sie entscheiden, wo Sie eine virtuelle Maschine platzieren möchten, sollten Sie sich die folgenden Fragen stellen:

- Wie wichtig ist die virtuelle Maschine?
- Welche Leistungs- und Verfügbarkeitsanforderungen gelten für sie?
- Welche PiT-Wiederherstellungsanforderungen gelten für sie?
- Welche Sicherungsanforderungen gelten für sie?
- Welche Wiederherstellungsanforderungen gelten für sie?

Die Einstufung einer virtuellen Maschine kann während ihres Lebenszyklus wechseln, z. B. wenn Prioritäten oder Technologien geändert wurden, die eine höhere oder niedrigere Einstufung zur Folge haben. Die Wichtigkeit ist relativ und kann sich aus verschiedenen Gründen ändern, z. B. bei Änderungen im Unternehmen, betriebswirtschaftlichen Abläufen, gesetzlichen Anforderungen oder Erstellung eines Notfallplans.

## Mehrschichtige Anwendungen

SAN-Administratoren verwenden üblicherweise spezialisierte Array-basierte Software für Sicherung, Notfallwiederherstellung, Data-Mining, Diagnose und Konfigurationstests.

Speicheranbieter stellen typischerweise zwei Arten von erweiterten Diensten für ihre LUNs bereit: Snapshot-Erstellung und Replikation.

- Bei der Snapshot-Erstellung wird durch effiziente Kopien von LUNs mit gemeinsamen Datenblöcken Speicherplatz geschaffen. Im Allgemeinen wird die Snapshot-Erstellung für schnelle Sicherungen, Anwendungstests, Diagnose oder Data-Mining lokal auf denselben Speichersystemen verwendet wie die primäre LUN.
- Bei der Replikation werden vollständige Kopien von LUNs erstellt. Replikationen werden üblicherweise auf separaten Speichersystemen oder sogar an separaten Standorten gespeichert, um ein System bei größeren Ausfällen zu schützen, durch die ein Array oder Standort vollständig zerstört wird.

Wenn Sie ein ESXi-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich Array-basierte Tools oder hostbasierte Tools für Ihre individuelle Situation besser eignen.

## Array-basierte Lösung (Drittanbieter)

Wenn Sie ein ESXi-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich Array-basierte Tools für Ihre individuelle Situation besser eignen.

Wenn Sie eine Array-basierte Lösung in Betracht ziehen, berücksichtigen Sie Folgendes:

- Array-basierte Lösungen bieten meist umfangreichere Statistiken. Da Daten bei RDMs immer über denselben Pfad übermittelt werden, ist die Leistungsverwaltung vereinfacht.
- Die Sicherheit ist für den Speicheradministrator bei Verwendung von RDM und einer Array-basierten Lösung transparenter, da virtuelle Maschinen mit RDMs eher mit physischen Maschinen vergleichbar sind.
- Bei Einsatz einer Array-basierten Lösung werden RDMs im physischen Kompatibilitätsmodus häufig zum Speichern von virtuellen Maschinen verwendet. Wenn keine Raw-Gerätezuordnungen (RDMs) verwendet werden sollen, erfahren Sie in der Dokumentation des Speicheranbieters, ob Vorgänge auf LUNs mit VMFS-Volumes unterstützt werden. Lesen Sie bei Verwendung von Array-Vorgängen auf VMFS-LUNs ferner den Abschnitt zur Neusignierung sorgfältig.

## Dateibasierte Lösung (VMFS)

Wenn Sie ein ESXi-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich dateibasierte Tools für Ihre individuelle Situation besser eignen.

Wenn Sie den Einsatz einer dateibasierten Lösung erwägen, welche die VMware Tools und VMFS anstelle der Array-Tools verwendet, beachten Sie die folgenden Punkte:

- Die Verwendung der VMware Tools mit VMFS bietet eine bessere Bereitstellung. Es wird eine große LUN zugeteilt, und mehrere `.vmdk`-Dateien können in dieser LUN platziert werden. Bei einer RDM ist für jede virtuelle Maschine eine neue LUN erforderlich.
- Eine Funktion zur Snapshot-Erstellung ist auf Ihrem ESXi-Host ohne zusätzliche Kosten enthalten.
- Die Verwendung von VMFS ist einfacher für ESXi-Administratoren.
- ESXi-Administratoren, die eine dateibasierte Lösung einsetzen, sind vom SAN-Administrator unabhängiger.

## Verwaltungsanwendungen von Drittanbietern

Sie können Verwaltungssoftware von Drittanbietern in Verbindung mit Ihrem ESXi-Host verwenden.

Häufig ist im Lieferumfang der SAN-Hardware eine Speicherverwaltungssoftware enthalten. Hierbei handelt es sich in der Regel um eine Webanwendung, die mit einem beliebigen Webbrowser ausgeführt werden kann, der mit dem Netzwerk verbunden ist. In anderen Fällen wird die Software typischerweise auf dem Speichersystem oder einem Einzelsystem ausgeführt, der unabhängig von den Servern betrieben wird, die das SAN zum Speichern nutzen.

Verwenden Sie diese Verwaltungssoftware von Drittanbietern für die folgenden Aufgaben:

- Speicher-Array-Verwaltung, einschließlich LUN-Erstellung, Cacheverwaltung des Arrays, LUN-Zuordnung und LUN-Sicherheit.
- Einrichtung von Replikations-, Prüfpunkt-, Snapshot- bzw. Spiegelungsfunktionen.

Wenn Sie die SAN-Verwaltungssoftware auf einer virtuellen Maschine verwenden, können Sie die Vorteile der Ausführung einer virtuellen Maschine nutzen, einschließlich Failover mit vMotion, Failover mit vSphere HA. Aufgrund der zusätzlichen Indirektionsebene ist das SAN jedoch für die Verwaltungssoftware möglicherweise nicht sichtbar. In diesem Fall können Sie eine RDM verwenden.

---

**Hinweis** Die erfolgreiche Ausführung der Verwaltungssoftware durch eine virtuelle Maschine hängt letztlich von dem betreffenden Speichersystem ab.

---

## Überlegungen zu SAN-Speichersicherungen

Das Vorhandensein einer guten Sicherungsstrategie ist einer der wichtigsten Aspekte der SAN-Verwaltung. In der SAN-Umgebung haben Sicherungen zwei Ziele. Das erste Ziel ist die Archivierung von Onlinedaten als Offlinemedien. Dieser Vorgang wird gemäß eines festgelegten Zeitplans regelmäßig für alle Onlinedaten wiederholt. Das zweite Ziel ist der Zugriff auf Offlinedaten zu Wiederherstellungszwecken. Für die Datenbankwiederherstellung müssen z. B. häufig archivierte Protokolldateien abgerufen werden, die gegenwärtig nicht online sind.

Die Planung von Sicherungen hängt von verschiedenen Faktoren ab:

- Ermittlung von kritischen Anwendungen, die häufigere Sicherungszyklen innerhalb eines bestimmten Zeitraums erfordern.
- Ziele für Wiederherstellungspunkte und -zeiten. Überlegen Sie, wie präzise Ihr Wiederherstellungspunkt sein muss und wie lange Sie darauf warten können.
- Die mit den Daten verknüpfte Änderungsrate (Rate of Change, RoC). Wenn Sie beispielsweise die synchrone bzw. asynchrone Replikation verwenden, beeinflusst die RoC die erforderliche Bandbreite zwischen den primären und den sekundären Speichergeräten.
- Auswirkungen insgesamt auf die SAN-Umgebung, Speicherleistung (während der Sicherung) und andere Anwendungen.
- Ermittlung von Spitzenzeiten für den Datenverkehr im SAN (Sicherungen, die während dieser Spitzenzeiten geplant werden, können die Anwendungen und den Sicherungsprozess verlangsamen).
- Zeit für das Planen aller Sicherungen im Datacenter.
- Zeit für das Sichern einer einzelnen Anwendung.
- Ressourcenverfügbarkeit für die Datenarchivierung; üblicherweise Zugriff auf Offlinedaten (Band).

Planen Sie für jede Anwendung ein Wiederherstellungszeitziel (Recovery Time Objective, RTO), wenn Sie die Sicherungsstrategie entwerfen. Das heißt, berücksichtigen Sie die Zeit und Ressourcen, die zum Durchführen einer Sicherung benötigt werden. Wenn eine geplante Sicherung beispielsweise eine so große Datenmenge speichert, dass die Wiederherstellung sehr lange dauert, überprüfen Sie die geplante Sicherung. Führen Sie die Sicherung häufiger durch, um die gespeicherte Datenmenge pro Sicherungsvorgang und die Wiederherstellungszeit zu reduzieren.

Wenn eine Anwendung innerhalb eines bestimmten Zeitraums wiederhergestellt werden muss, muss der Sicherungsvorgang einen Zeitplan und eine spezielle Datenverarbeitung bieten, um diese Anforderung zu erfüllen. Eine schnelle Wiederherstellung kann die Verwendung von Wiederherstellungs-Volumes in einem Onlinespeicher erfordern, um die Notwendigkeit des Zugriffs auf langsame Offlinemedien für fehlende Datenkomponenten zu minimieren oder zu eliminieren.



## Verwenden von Drittanbieter-Sicherungspaketen

Sie können in Ihren virtuellen Maschinen Sicherungslösungen von Drittanbietern zum Schutz des Systems, der Anwendung und der Benutzerdaten verwenden.

VMware bietet in Verbindung mit Drittanbieterprodukten „Storage APIs - Data Protection“. Bei Verwendung von APIs kann Drittanbietersoftware Sicherungen durchführen, ohne dass ESXi-Hosts mit der Verarbeitung der Sicherungsaufgaben belastet werden.

Die Drittanbieterprodukte, die „Storage APIs - Data Protection“ verwenden, können die folgenden Sicherungsaufgaben durchführen:

- Vollständige, differenzielle und inkrementelle Image-Sicherung und Wiederherstellen virtueller Maschinen.
- Sicherung virtueller Maschinen, die unterstützte Windows- und Linux-Betriebssysteme verwenden, auf Dateiebene.
- Sicherstellen der Datenkonsistenz durch Verwendung von Microsoft Volume Shadow Copy Service (VSS) für virtuelle Maschinen, die unterstützte Microsoft Windows-Betriebssysteme ausführen.

Da „Storage APIs - Data Protection“ die Snapshot-Funktionen von VMFS nutzt, treten bei Sicherungen, die Sie durchführen können, keine Ausfallzeiten bei virtuellen Maschinen auf. Diese Sicherungen wirken sich nicht störend aus, können jederzeit durchgeführt werden und benötigen keine erweiterten Sicherungsfenster.

Weitere Informationen zu „Storage APIs - Data Protection“ und zur Integration mit Sicherungsprodukten finden Sie auf der VMware-Website oder wenden Sie sich an den Anbieter Ihrer Sicherungslösung.

# Verwenden von ESXi mit Fibre-Channel-SAN

# 3

Bei der Einrichtung von ESXi-Hosts für die Verwendung von FC-SAN-Speicher-Arrays sollten Sie bestimmte Überlegungen anstellen. In diesem Abschnitt finden Sie Informationen zur Verwendung von ESXi mit einem FC-SAN-Array.

Dieses Kapitel enthält die folgenden Themen:

- [Fibre-Channel-SAN-Konzepte](#)
- [Verwenden von Zoning mit Fibre-Channel-SANs](#)
- [Zugriff auf Daten in einem Fibre-Channel-SAN durch virtuelle Maschinen](#)

## Fibre-Channel-SAN-Konzepte

Wenn Sie ein ESXi-Administrator sind, der Hosts zusammen mit SANs einsetzen möchte, müssen Sie über Anwendungserfahrungen mit SAN-Konzepten verfügen. Weitere Informationen zur SAN-Technologie finden Sie in Printmedien oder dem Internet. Rufen Sie diese Quellen regelmäßig ab, um sich über Neuerungen in dieser Branche zu informieren.

Falls Sie sich mit der SAN-Technologie noch nicht auskennen, sollten Sie sich mit den Grundbegriffen vertraut machen.

Ein SAN (Storage Area Network) ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Computersysteme oder Hostserver mit Hochleistungsspeicher-Subsystemen verbindet. Zu den SAN-Komponenten zählen Hostbusadapter (HBAs) in den Hostservern, Switches, die Speicherdatenverkehr weiterleiten, Verkabelung, Speicherprozessoren (SP) und Festplattenspeicher-Arrays.

Eine SAN-Topologie mit mindestens einem Switch im Netzwerk stellt ein SAN-Fabric dar.

Für den Datentransfer von Hostservern auf gemeinsamen Speicher wird vom SAN das Fibre-Channel-Protokoll verwendet, das SCSI-Befehle in Fibre-Channel-Frames bündelt.

Um den Serverzugriff auf Speicher-Arrays einzuschränken, die diesem Server nicht zugeteilt sind, wird im SAN das Zoning verwendet. Normalerweise werden Zonen für jede Servergruppe erstellt, die auf eine gemeinsam genutzte Gruppe von Speichergeräten und LUNs zugreift. Über Zonen wird festgelegt, welche HBAs mit welchen Speicherprozessoren verbunden werden können. Geräte außerhalb einer Zone sind für Geräte in einer Zone nicht sichtbar.

Das Zoning ist mit der LUN-Maskierung vergleichbar, die häufig zur Verwaltung von Berechtigungen verwendet wird. LUN-Maskierung ist ein Prozess, über den eine LUN für einige Hosts bereitgestellt wird – für andere Hosts jedoch nicht.

Bei der Datenübertragung zwischen dem Hostserver und dem Speicher nutzt das SAN eine Technik, die als Multipathing bezeichnet wird. Multipathing bietet die Möglichkeit, mehr als einen physischen Pfad vom ESXi-Host zu einer LUN in einem Speichersystem bereitzustellen.

In der Regel besteht ein einzelner Pfad von einem Host zu einer LUN aus einem HBA, Switch-Ports, Verbindungskabeln und dem Speicher-Controller-Port. Falls eine Komponente des Pfads ausfällt, wählt der Host für E/A-Vorgänge einen anderen verfügbaren Pfad. Der Prozess der Erkennung eines ausgefallenen Pfads und des Wechsels auf einen anderen Pfad wird als Pfad-Failover bezeichnet.

## Ports in Fibre-Channel-SAN

Im Kontext dieses Dokuments versteht man unter einem Port die Verbindung von einem Gerät im SAN. Jeder Knoten im SAN, wie z. B. ein Host, ein Speichergerät oder eine Fabric-Komponente, verfügt über mindestens einen Port, über den er mit dem SAN verbunden ist. Ports werden auf mehrere Arten ermittelt.

### WWPN (World Wide Port Name)

Ein globaler eindeutiger Bezeichner für einen Port, der den Zugriff bestimmter Anwendungen auf den Port ermöglicht. Die FC-Switches erkennen den WWPN eines Geräts oder Hosts und weisen dem Gerät eine Portadresse zu.

### Port\_ID (oder Portadresse)

In einem SAN verfügt jeder Port über eine eindeutige Port-ID, die als FC-Adresse für den Port dient. Diese eindeutige ID ermöglicht die Weiterleitung von Daten über das SAN zu diesem Port. Die Zuweisung der Port-ID durch die FC-Switches erfolgt beim Anmelden des Geräts am Fabric. Die Port-ID gilt nur solange das Gerät angemeldet ist.

Bei der N-Port-ID-Virtualisierung (NPIV) kann sich ein einzelner FC-HBA-Port (N-Port) mit dem Fabric über mehrere WWPNs verbinden. Auf diese Weise kann ein N-Port mehrere Fabric-Adressen beanspruchen, von denen jede als ein eindeutiges Element angezeigt wird. Im Kontext eines von ESXi-Hosts verwendeten SANs ermöglichen diese eindeutigen Bezeichner, einzelnen virtuellen Maschinen bei deren Konfiguration WWNs zuzuweisen.

## Typen von Fibre-Channel-Speicher-Arrays

ESXi unterstützt verschiedene Speichersysteme und Arrays.

Zu den Speichertypen, die Ihr Host unterstützt, gehören Aktiv-Aktiv, Aktiv-Passiv und ALUA-konform.

### Aktiv-Aktiv-Speichersystem

Ermöglicht den gleichzeitigen Zugriff auf die LUNs über alle Speicherports, die ohne wesentlichen Leistungsabfall verfügbar sind. Alle Pfade sind jederzeit aktiv (es sei denn, ein Pfad fällt aus).

### **Aktiv-Passiv-Speichersystem**

Ein System, in dem ein Speicherprozessor aktiv den Zugriff auf eine vorhandene LUN ermöglicht. Die anderen Prozessoren fungieren als Sicherung für die LUN und können den Zugriff auf andere LUN-E/A-Vorgänge aktiv bereitstellen. E/A-Daten können ausschließlich an einen aktiven Port gesendet werden. Falls der Zugriff über den aktiven Speicherport fehlschlägt, kann einer der passiven Speicherprozessoren durch die Server, die auf ihn zugreifen, aktiviert werden.

### **Asymmetrisches Speichersystem**

Unterstützt Asymmetric Logical Unit Access (ALUA). ALUA-konforme Speichersysteme bieten verschiedene Zugriffsebenen für einzelne Ports. ALUA ermöglicht es Hosts, den Status von Zielpoints festzustellen und Pfade zu priorisieren. Der Host verwendet einige der aktiven Pfade als primäre Pfade, andere als sekundäre Pfade.

## **Verwenden von Zoning mit Fibre-Channel-SANs**

Das Zoning ermöglicht die Zugriffssteuerung in der SAN-Topologie. Über Zonen wird festgelegt, welche HBAs mit welchen Zielen verbunden werden können. Wenn Sie bei der SAN-Konfiguration Zoning verwenden, sind Geräte außerhalb einer Zone für Geräte in einer Zone nicht sichtbar.

Zoning wirkt sich folgendermaßen aus:

- Verringert die Anzahl an Zielen und LUNs, die einem Host angegeben werden.
- Steuert und isoliert Pfade in einem Fabric.
- Kann verhindern, dass andere Systeme als das ESXi-System auf ein bestimmtes Speichersystem zugreifen und möglicherweise VMFS-Daten löschen.
- Kann zum Trennen verschiedener Umgebungen verwendet werden, z. B. zum Trennen einer Testumgebung von einer Produktionsumgebung.

Verwenden Sie für ESXi-Hosts ein Zoning mit einem einzelnen Initiator oder ein Zoning mit einem einzelnen Initiator und einem einzelnen Ziel. Letzteres ist eine bevorzugte Vorgehensweise für das Zoning. Die Verwendung des restriktiveren Zonings verhindert Probleme und falsche Konfigurationen, die im SAN auftreten können.

Ausführliche Anweisungen und die besten Vorgehensweisen für das Zoning erhalten Sie beim Speicher-Array- oder Switch-Anbieter.

## Zugriff auf Daten in einem Fibre-Channel-SAN durch virtuelle Maschinen

ESXi speichert Festplattendateien einer virtuellen Maschine in einem VMFS-Datenspeicher, der sich auf einem SAN-Speichergerät befindet. Sobald Gastbetriebssysteme der virtuellen Maschine SCSI-Befehle an die virtuellen Festplatten senden, übersetzt die SCSI-Virtualisierungsebene diese Befehle in VMFS-Dateivorgänge.

Wenn eine virtuelle Maschine mit seinen auf einem SAN gespeicherten virtuellen Festplatten interagiert, finden die folgenden Prozesse statt:

- 1 Wenn das Gastbetriebssystem in einer virtuellen Maschine zum Lesen oder Schreiben auf eine SCSI-Festplatte zugreifen muss, sendet dieses SCSI-Befehle an die virtuelle Festplatte.
- 2 Gerätetreiber im Betriebssystem der virtuellen Maschine kommunizieren mit den virtuellen SCSI-Controllern.
- 3 Der virtuelle SCSI-Controller leitet den Befehl an den VMkernel weiter.
- 4 Der VMkernel führt die folgenden Aufgaben aus.
  - a speichert die Datei im VMFS-Volume, das der Gastbetriebssystem-Festplatte der virtuellen Maschine entspricht.
  - b ordnet die Anforderungen für die Blöcke auf der virtuellen Festplatte den Blöcken auf dem entsprechenden physischen Gerät zu.
  - c Sendet die geänderte E/A-Anforderung vom Gerätetreiber im VMkernel an den physischen HBA.
- 5 Der physische HBA führt die folgenden Aufgaben aus.
  - a Bündelt die E/A-Anforderungen gemäß den Regeln des FC-Protokolls in Pakete.
  - b übermittelt die Anforderung an das SAN.
- 6 Abhängig von dem Port, den der HBA für die Verbindung zum Fabric verwendet, empfängt einer der SAN-Switches die Anforderung und leitet sie an das Speichergerät weiter, auf das der Host zugreifen möchte.

# Konfigurieren des Fibre-Channel-Speichers

# 4

Wenn Sie ESXi-Systeme mit SAN-Speicher verwenden, müssen bestimmte Hardware- und Systemanforderungen eingehalten werden.

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen des Fibre-Channel-SAN von ESXi](#)
- [Installations- und Konfigurationsschritte](#)
- [N-Port-ID-Virtualisierung](#)

## Anforderungen des Fibre-Channel-SAN von ESXi

Um die Konfiguration des SAN und die Einrichtung des ESXi-Systems für die Verwendung eines SAN-Speichers vorzubereiten, sollten Sie die Anforderungen und Empfehlungen lesen.

- Stellen Sie sicher, dass die SAN-Speicherhardware- und Firmware-Kombinationen in Verbindung mit ESXi-Systemen unterstützt werden. Eine aktuelle Liste finden Sie unter *VMware-Kompatibilitätshandbuch*.
- Konfigurieren Sie Ihr System, sodass nur ein VMFS-Volume pro LUN vorhanden ist.
- Wenn Sie keine Server ohne Festplatte verwenden, dürfen Sie keine Diagnosepartition auf einer SAN-LUN einrichten.

Sollten Sie jedoch Server ohne Festplatte verwenden, die über ein SAN gestartet werden, ist eine gemeinsame Diagnosepartition angebracht.

- Verwenden Sie RDMS für den Zugriff auf Raw-Festplatten. Weitere Informationen hierzu finden Sie unter [Kapitel 18 Raw-Gerätezuordnung](#).
- Damit das Multipathing ordnungsgemäß funktioniert, muss jede LUN allen ESXi-Hosts dieselbe LUN-ID-Nummer anzeigen.
- Stellen Sie sicher, dass für das Speichergerät eine ausreichend große Warteschlange angegeben ist. Die Warteschlangentiefe für den physischen HBA können Sie während der Systeminstallation festlegen. Weitere Informationen über das Ändern der Warteschlangentiefe für HBAs und virtuelle Maschinen finden Sie unter *vSphere-Fehlerbehebung*.

- Erhöhen Sie den Wert des SCSI-Parameters `TimeoutValue` auf 60 für virtuelle Maschinen, auf denen Microsoft Windows ausgeführt wird, damit Windows aus Pfad-Failover resultierende E/A-Verzögerungen besser toleriert. Weitere Informationen hierzu finden Sie unter [Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen](#).

## Einschränkungen des Fibre-Channel-SAN von ESXi

Für die Verwendung von ESXi in einem SAN gelten gewisse Einschränkungen.

- ESXi unterstützt keine über FC verbundenen Bandlaufwerke.
- Sie können keine Multipathing-Software für virtuelle Maschinen verwenden, um einen E/A-Lastenausgleich für eine einzelne physische LUN durchzuführen. Wenn jedoch Ihre virtuelle Microsoft Windows-Maschine dynamische Datenträger verwendet, gilt diese Einschränkung nicht. Weitere Informationen über das Konfigurieren dynamischer Datenträger finden Sie unter [Dynamische Festplattenspiegelung einrichten](#).

## Festlegen der LUN-Zuordnungen

Dieses Thema bietet einige grundlegende Informationen zum Zuweisen von LUNs bei Ausführung des ESXi in Verbindung mit einem SAN.

Beachten Sie beim Festlegen von LUN-Zuordnungen die folgenden Punkte:

### Bereitstellen von Speicher

Damit das ESXi-System die LUNs beim Start erkennt, müssen alle LUNs für die entsprechenden HBAs bereitgestellt werden, bevor das SAN mit dem ESXi-System verbunden wird.

VMware empfiehlt die gleichzeitige Bereitstellung aller LUNs für alle ESXi-HBAs. HBA-Failover funktioniert nur, wenn für alle HBAs dieselben LUNs sichtbar sind.

Stellen Sie für LUNs, die von mehreren Hosts gemeinsam genutzt werden, sicher, dass die LUN-IDs über alle Hosts hinweg konsistent sind. Beispielsweise sollte LUN 5 Host 1, Host 2 und Host 3 als LUN 5 zugeordnet werden.

### vMotion und VMware DRS

Wenn Sie vCenter Server und vMotion oder DRS verwenden, sollten Sie sicherstellen, dass die LUNs für die virtuellen Maschinen allen ESXi-Hosts bereitgestellt werden. Dies bietet die höchste Flexibilität beim Verschieben virtueller Maschinen.

### Aktiv/Aktiv- im Vergleich zu Aktiv/Passiv-Arrays

Bei der Verwendung von vMotion oder DRS mit einem SAN-Speichergerät vom Typ „Aktiv/Passiv“ sollten Sie sicherstellen, dass alle ESXi-Systeme über einheitliche Pfade zu allen Speicherprozessoren verfügen. Anderenfalls kann es bei vMotion-Migrationen zu einem Pfad-Thrashing kommen.

Für Aktiv/Passiv-Speicher-Arrays, die in der Speicher-/SAN-Kompatibilität nicht aufgelistet sind, werden keine Speicherport-Failover von VMware unterstützt. In solchen Fällen, müssen Sie den Server am aktiven Port des Speicher-Arrays anschließen. Durch diese Konfiguration wird sichergestellt, dass die LUNs dem ESXi-Host angezeigt werden.

## Festlegen von Fibre-Channel-HBAs

In der Regel funktionieren FC-HBAs, die Sie auf Ihrem ESXi-Host verwenden, mit den Standardkonfigurationseinstellungen ordnungsgemäß.

Sie sollten die von Ihrem Speicher-Array-Anbieter bereitgestellten Konfigurationsrichtlinien befolgen. Beachten Sie beim Einrichten von Fibre-Channel-HBA die folgenden Aspekte.

- Verwenden Sie in einem einzelnen Host keine FC-HBAs von verschiedenen Anbietern. Zwar wird der Einsatz verschiedener Modelle desselben HBAs unterstützt, auf eine einzelne LUN kann jedoch nur von HBAs desselben Typs zugegriffen werden.
- Stellen Sie sicher, dass die Firmware-Ebenen aller HBAs einheitlich sind.
- Legen Sie den Zeitüberschreitungswert für das Erkennen eines Failovers fest. Um eine optimale Leistung zu erzielen, ändern Sie den Standardwert nicht.
- ESXi unterstützt End-to-End-Konnektivität für Fibre Channel (16 GB).

## Installations- und Konfigurationsschritte

Dieses Kapitel bietet eine Übersicht über Installations- und Konfigurationsschritte zur Einrichtung Ihrer SAN-Umgebung für die Kompatibilität mit ESXi.

Führen Sie zur Konfiguration Ihrer ESXi SAN-Umgebung die folgenden Schritte aus.

- 1 Entwerfen Sie Ihr SAN, falls noch nicht konfiguriert. Die meisten SANs erfordern für die Kompatibilität mit ESXi nur geringe Änderungen.
- 2 Stellen Sie sicher, dass alle SAN-Komponenten die Anforderungen erfüllen.
- 3 Nehmen Sie die erforderlichen Änderungen am Speicher-Array vor.

Für die Konfiguration eines SAN zur Verwendung mit VMware ESXi bieten die meisten Anbieter spezifische Dokumentationen.

- 4 Richten Sie die HBAs für die Hosts ein, die mit dem SAN verbunden sind.
- 5 Installieren Sie ESXi auf den Hosts.
- 6 Erstellen Sie virtuelle Maschinen und installieren Sie Gastbetriebssysteme.
- 7 (Optional) Konfigurieren Sie das System für vSphere HA-Failover oder für die Verwendung von Microsoft Cluster-Diensten.
- 8 Aktualisieren oder ändern Sie ggf. die Umgebung.



## N-Port-ID-Virtualisierung

N-Port-ID-Virtualisierung (NPIV) ist ein ANSI T11-Standard, der beschreibt, wie ein einzelner Fibre-Channel-HBA-Port mit dem Fabric über mehrere WWPNS (Worldwide Port Names) verbunden werden kann. Auf diese Weise kann ein Fabric-gebundener N-Port mehrere Fabric-Adressen beanspruchen. Jede Adresse zeigt eine eindeutige Entität auf dem Fibre-Channel-Fabric.

### Funktionsweise des NPIV-basierten LUN-Zugriffs

NPIV bietet die Möglichkeit, dass ein einziger FC-HBA-Port mehrere eindeutige WWNs mit dem Fabric registriert, von denen jeder einer einzelnen virtuellen Maschine zugewiesen werden kann.

SAN-Objekte wie Switches, HBAs, Speichergeräte oder virtuelle Maschinen können WWN-Bezeichnern (World Wide Name) zugewiesen werden. WWNs dienen als eindeutige Bezeichner solcher Objekte im Fibre-Channel-Fabric. Verfügen virtuelle Maschinen über WWN-Zuweisungen, verwenden sie diese für den gesamten RDM-Verkehr, sodass die damit verknüpften LUNs von RDMs auf der virtuellen Maschine für die entsprechenden WWNs nicht maskiert sein dürfen. Sind für virtuelle Maschinen keine WWN-Zuweisungen vorhanden, erfolgt der Zugriff auf Speicher-LUNs über die WWNs der physischen HBAs des Hosts. Durch die Verwendung von NPIV kann ein SAN-Administrator jedoch den Speicherzugriff für jede virtuelle Maschinen überwachen und weiterleiten. Die entsprechende Funktionsweise wird im folgenden Abschnitt beschrieben.

Wenn einer virtuellen Maschine ein WWN zugewiesen ist, wird die Konfigurationsdatei der virtuellen Maschine (.vmx) aktualisiert, sodass sie ein WWN-Paar (bestehend aus World Wide Port Name (WWPN) und World Wide Node Name (WWNN)) enthält. Da diese virtuelle Maschine eingeschaltet ist, instanziiert der VMkernel einen virtuellen Port (VPORT) auf dem physischen HBA, der für den Zugriff auf die LUN verwendet wird. Beim VPORT handelt es sich um einen virtuellen HBA, der dem FC-Fabric als physischer HBA angezeigt wird. Demnach verfügt er über einen eigenen eindeutigen Bezeichner – dem WWN-Paar, das der virtuellen Maschine zugewiesen wurde. Für die virtuelle Maschine ist jeder VPORT spezifisch. Sobald die virtuelle Maschine ausgeschaltet ist, wird der VPORT auf dem Host gelöscht und dem FC-Fabric nicht mehr angezeigt. Wenn eine virtuelle Maschine von einem Host zu einem anderen migriert wird, wird der VPORT auf dem ersten Host geschlossen und auf dem Zielhost geöffnet.

Wenn NPIV aktiviert ist, werden zur Erstellungszeit WWN-Paare (WWPN & WWNN) für jede virtuelle Maschine angegeben. Wenn eine virtuelle Maschine, die NPIV verwendet, eingeschaltet wird, verwendet sie jede dieser WWN-Paare nacheinander, um einen Zugriffspfad auf den Speicher zu ermitteln. Die Anzahl an instanziierten VPORTs entspricht der Anzahl an im Host vorhandenen physischen HBAs. Auf jedem physischen HBA, zu dem ein physischer Pfad gefunden wird, wird ein VPORT erstellt. Jeder physische Pfad wird verwendet, um den virtuellen Pfad zu ermitteln, der für den Zugriff auf die LUN verwendet werden soll. Beachten Sie, dass in diesem Ermittlungsprozess HBAs, die NPIV nicht erkennen, übersprungen werden, weil darauf keine VPORTs instanziiert werden können.

## Anforderungen für die Verwendung von NPIV

Wenn Sie NPIV auf Ihren virtuellen Maschinen aktivieren möchten, sollten Sie bestimmte Anforderungen berücksichtigen.

Es bestehen die folgenden Anforderungen:

- NPIV wird nur für virtuelle Maschinen mit Raw-Gerätezuordnungsfestplatten unterstützt. Virtuelle Maschinen mit herkömmlichen virtuellen Festplatten verwenden die WWNs der physischen HBAs des Hosts.
- Die HBAs auf Ihrem Host müssen NPIV unterstützen.  
Hinweise finden Ihr unter *VMware-Kompatibilitätshandbuch* und in der Dokumentation des Anbieters.
  - Verwenden Sie HBAs des gleichen Typs, entweder ausschließlich QLogic oder ausschließlich Emulex. VMware unterstützt den Zugriff von heterogenen HBAs auf dieselben LUNs auf demselben Host nicht.
  - Wenn ein Host mehrere physische HBAs als Speicherpfade verwendet, teilen Sie alle physischen Pfade auf die virtuelle Maschine in Zonen auf. Dies ist erforderlich, damit das Multipathing selbst dann unterstützt wird, wenn nur ein Pfad aktiv ist.
  - Stellen Sie sicher, dass die physischen HBAs auf dem Host auf alle LUNs zugreifen können, auf die von NPIV-aktivierten virtuellen Maschinen zugegriffen wird, die auf dem Host ausgeführt werden.
- Die Switches in der Fabric müssen NPIV erkennen können.
- Stellen Sie bei der Konfiguration einer LUN für den NPIV-Zugriff auf Speicherebene sicher, dass die NPIV-LUN-Nummer und die NPIV-Ziel-ID mit der physischen LUN und der Ziel-ID übereinstimmen.

## NPIV-Funktionen und -Einschränkungen

Erfahren Sie mehr über die spezifischen Funktionen und Einschränkungen der Verwendung von NPIV mit ESXi.

ESXi mit NPIV unterstützt die folgenden Elemente:

- NPIV unterstützt vMotion. Wenn Sie vMotion zum Migrieren einer virtuellen Maschine verwenden, wird der zugewiesene WWN beibehalten.  
Wenn Sie eine NPIV-aktivierte virtuelle Maschine auf einen Host migrieren, der NPIV nicht unterstützt, verwendet VMkernel wieder einen physischen HBA zum Weiterleiten des E/A.
- Wenn Ihre FC-SAN-Umgebung die gleichzeitige E/A auf den Festplatten eines Aktiv-Aktiv-Arrays unterstützt, wird die gleichzeitige E/A auf zwei verschiedenen NPIV-Ports ebenfalls unterstützt.

Für die Verwendung von ESXi mit NPIV gelten folgende Einschränkungen:

- Weil die NPIV-Technologie eine Erweiterung des FC-Protokolls ist, benötigt sie einen FC-Switch und funktioniert nicht auf den direkt angehängten FC-Festplatten.
- Wenn eine virtuelle Maschine oder Vorlage mit einer WWN-Zuweisung geklont wird, behält der Klon den WWN nicht bei.
- NPIV unterstützt nicht Storage vMotion.
- Wenn während der Laufzeit virtueller Maschinen die NPIV-Fähigkeit eines FC-Switches deaktiviert und anschließend erneut aktiviert wird, kann ein FC-Link fehlschlagen und die Ein-/Ausgabe gestoppt werden.

## Zuweisen von WWNs zu virtuellen Maschinen

Weisen Sie der virtuellen Maschine mit einer RDM-Festplatte die WWN-Einstellungen zu.

Sie können bis zu 16 WWN-Paare erstellen, die jeweils den ersten 16 physischen FC-HBAs auf dem Host zugeordnet werden können.

### Voraussetzungen

Erstellen Sie eine virtuelle Maschine mit einer RDM-Festplatte. Weitere Informationen hierzu finden Sie unter [Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen](#).

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 3 Klicken Sie auf **VM-Optionen**.
- 4 Klicken Sie auf das Dreieck „Fibre-Channel-NPIV“, um die NPIV-Optionen zu erweitern.
- 5 Deaktivieren Sie das Kontrollkästchen **NPIV für diese virtuelle Maschine vorübergehend deaktivieren**.
- 6 Wählen Sie **Neue WWNs generieren**.
- 7 Geben Sie die Anzahl der WWNNs und WWPNS an.

Mindestens zwei WWPNS werden benötigt, um Failover mit NPIV zu unterstützen. In der Regel wird nur ein WWNN für jede virtuelle Maschine erstellt.

### Ergebnisse

Der Host erstellt WWN-Zuweisungen für die virtuelle Maschine.

### Nächste Schritte

Registrieren Sie den neu erstellten WWNs in der Fabric, sodass sich die virtuelle Maschine beim Switch anmelden kann, und weisen Sie den WWNs Speicher-LUNs zu.

## Ändern von WWN-Zuweisungen

Für eine virtuelle Maschine mit einer RDM können Sie WWN-Zuweisungen ändern.

In der Regel müssen Sie die vorhandenen WWN-Zuweisungen auf Ihrer virtuellen Maschine nicht ändern. Unter bestimmten Umständen, wenn beispielsweise manuell zugewiesene WWNs Konflikte auf dem SAN verursachen, müssen Sie möglicherweise WWNs ändern oder entfernen.

### Voraussetzungen

Stellen Sie hierzu sicher, dass die virtuelle Maschine ausgeschaltet ist, bevor Sie die vorhandenen WWNs bearbeiten.

Stellen Sie vor Beginn sicher, dass der SAN-Administrator die Speicher-LUN-ACL bereitgestellt hat, damit der ESXi-Host der virtuellen Maschine darauf zugreifen kann.

### Verfahren

- 1 Öffnen Sie das Eigenschaftendialogfeld der virtuellen Maschine, indem Sie auf den Link **Einstellungen bearbeiten** für die ausgewählte virtuelle Maschine klicken.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **Fibre-Channel-NPIV**.  
Das Dialogfeld Eigenschaften der virtuellen Maschinen wird geöffnet.
- 3 Bearbeiten Sie die WWN-Zuweisungen, indem Sie eine der folgenden Optionen auswählen:

Option	Beschreibung
<b>NPIV für diese virtuelle Maschine vorübergehend deaktivieren</b>	Deaktivieren Sie die WWN-Zuweisungen für die virtuelle Maschine.
<b>Unverändert lassen</b>	Die vorhandenen WWN-Zuweisungen werden beibehalten. Im Abschnitt mit den schreibgeschützten WWN-Zuweisungen in diesem Dialogfenster werden die Knoten- und die Portwerte aller vorhandenen WWN-Zuweisungen angezeigt.
<b>Neue WWNs generieren</b>	Neue WWNs werden generiert und der virtuellen Maschine zugewiesen, wobei vorhandene WWNs überschrieben werden (dies betrifft nicht die HBA-WWNs).
<b>WWN-Zuweisungen entfernen</b>	Die der virtuellen Maschine zugewiesenen WWNs werden entfernt und es werden die HBA-WWNs für den Zugriff auf die Speicher-LUNs verwendet. Diese Option ist nicht verfügbar, wenn Sie eine neue virtuelle Maschine erstellen.

- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

# Konfigurieren von Fibre-Channel über Ethernet

# 5

Mithilfe des Fibre Channel over Ethernet-(FCoE-)Protokolls kann ein ESXi-Host auf den Fibre-Channel-Speicher zugreifen.

Das FCoE-Protokoll kapselt Fibre-Channel-Frames in Ethernet-Frames ein. Deshalb benötigt Ihr Host keine speziellen Fibre-Channel-Links zum Herstellen einer Verbindung mit dem Fibre-Channel-Speicher, kann aber 10 Gbit Lossless Ethernet zum Zustellen des Fibre-Channel-Datenverkehrs verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Adapter für Fibre-Channel über Ethernet](#)
- [Konfigurationsrichtlinien für Software-FCoE](#)
- [Einrichten des Netzwerks für Software-FCoE](#)
- [Hinzufügen von Software-FCoE-Adaptern](#)

## Adapter für Fibre-Channel über Ethernet

Um Fibre-Channel über Ethernet (FCoE) zu verwenden, müssen Sie FCoE-Adapter auf dem Host installieren.

Die von VMware unterstützten Adapter lassen sich in der Regel in zwei Kategorien einteilen: Hardware-FCoE-Adapter und Software-FCoE-Adapter, die den nativen FCoE-Stack in ESXi verwenden.

### Hardware-FCoE-Adapter

Diese Kategorie enthält vollständig verlagerte spezialisierte Converged Network Adapters (CNAs), die Netzwerk- und Fibre-Channel-Funktionalität auf derselben Karte enthalten.

Wenn solch ein Adapter installiert ist, erkennt Ihr Host beide CNA-Komponenten und kann diese verwenden. Im Client wird die Netzwerkkomponente als Standardnetzwerkadapter (vmnic) und die Fibre-Channel-Komponente als FCoE-Adapter (vmhba) angezeigt. Sie müssen den Hardware-FCoE-Adapter zum Verwenden nicht konfigurieren.

## Software-FCoE-Adapter

Ein Software-FCoE-Adapter verwendet den nativen FCoE-Protokoll-Stack in ESXi zum Verarbeiten von Protokollen. Der Software-FCoE-Adapter wird mit einer Netzwerkkarte verwendet, die DCB- (Data Center Bridging-) und E/A-Offload-Funktionen bietet. Intel X520 ist ein Beispiel für eine Netzwerkkarte dieser Art. Weitere Informationen zu Netzwerkkarten, die Software-FCoE unterstützen, finden Sie unter *VMware-Kompatibilitätshandbuch*.

Für den Software-FCoE-Adapter müssen Sie das Netzwerk ordnungsgemäß konfigurieren und anschließend den Adapter aktivieren.

---

**Hinweis** Die Anzahl an Software-FCoE-Adaptoren, die Sie aktivieren, entspricht der Anzahl der physischen Netzwerkkarten-Ports. ESXi unterstützt maximal vier Software-FCoE-Adapter auf einem Host.

---

## Konfigurationsrichtlinien für Software-FCoE

Befolgen Sie beim Einrichten einer Netzwerkumgebung für ESXi-Software-FCoE die Richtlinien und Best Practices von VMware.

### Richtlinien für Netzwerk-Switches

Befolgen Sie diese Richtlinien, wenn Sie einen Netzwerk-Switch für eine FCoE-Softwareumgebung konfigurieren:

- Deaktivieren Sie das Spanning-Tree-Protokoll (STP) auf den Ports, die mit Ihrem ESXi-Host kommunizieren. Durch das Aktivieren des STP wird möglicherweise die Antwort des FCoE-Initialisierungsprotokolls (FIP) am Switch verzögert und der Zustand „Keine Pfade verfügbar“ verursacht.  
  
FIP ist ein Protokoll, das FCoE zum Ermitteln und Initialisieren von FCoE-Elementen im Ethernet verwendet.
- Schalten Sie die prioritätsbasierte Flusssteuerung (Priority-based Flow Control, PFC) ein und legen Sie sie auf „AUTO“ fest.
- Vergewissern Sie sich, dass Sie über eine kompatible Firmware-Version auf dem FCoE-Switch verfügen.

### Netzwerkadapter - Best Practices

Wenn Sie planen, Software-FCoE-Adapter für den Einsatz mit Netzwerkadaptern zu aktivieren, gelten besondere Erwägungen.

- Stellen Sie sicher, dass auf dem FCoE-Netzwerkadapter der neueste Microcode installiert ist.
- Wenn der Netzwerkadapter über mehrere Ports verfügt, fügen Sie bei der Konfiguration von Netzwerken jeden Port zu einem eigenen vSwitch hinzu. Dadurch vermeiden Sie den Zustand „Keine Pfade verfügbar“, wenn ein störendes Ereignis, wie z. B. eine MTU-Änderung, eintritt.

- Verschieben Sie einen Netzwerkadapter-Port nicht von einem vSwitch zu einem anderen vSwitch, wenn der FCoE-Datenverkehr aktiv ist. Falls Sie diese Änderung vornehmen müssen, starten Sie danach den Host neu.
- Falls das Ändern des vSwitches für einen Netzwerkadapter-Port einen Ausfall verursacht, verschieben Sie den Port auf den ursprünglichen vSwitch zurück, um das Problem zu beheben.

## Einrichten des Netzwerks für Software-FCoE

Bevor Sie die Software-FCoE-Adapter aktivieren, müssen Sie VMkernel-Netzwerkadapter für alle physischen FCoE-Netzwerkkarten erstellen, die auf dem Host installiert sind.

Dieses Verfahren erklärt, wie ein einzelner VMkernel-Netzwerkadapter erstellt wird, der mit einem einzelnen physischen FCoE-Netzwerkadapter über einen vSphere Standard-Switch verbunden ist. Wenn Ihr Host mehrere Netzwerkadapter oder mehrere Ports auf dem Adapter hat, verbinden Sie jede FCoE-Netzwerkkarte mit einem getrennten Standard Switch. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

---

**Hinweis** ESXi unterstützt maximal vier Netzwerkadapter-Ports, die für Software-FCoE verwendet werden.

---

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.
- 3 Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.
- 5 Wählen Sie unter „Freie Adapter“ den Netzwerkadapter (vmnic#) aus, der FCoE unterstützt, und klicken Sie auf **Zuweisen**.

Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.

- 6 Geben Sie eine Netzwerkbezeichnung ein.

Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. „FCoE“.

- 7 Geben Sie eine VLAN-ID an und klicken Sie auf **Weiter**.

Da der FCoE-Datenverkehr ein isoliertes Netzwerk benötigt, stellen Sie sicher, dass sich die von Ihnen angegebene VLAN-ID von der ID unterscheidet, die für das reguläre Netzwerk auf Ihrem Host verwendet wird. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

- 8 Nach dem Abschließen der Konfiguration prüfen Sie die Informationen, und klicken Sie auf **Beenden**.

## Ergebnisse

Sie haben den virtuellen VMkernel-Adapter für den auf Ihrem Host installierten physischen FCoE-Netzwerkadapter erstellt.

---

**Hinweis** Um Störungen im FCoE-Datenverkehr zu vermeiden, sollten Sie den FCoE-Netzwerkadapter (vmnic #) nicht aus dem vSphere Standard-Switch entfernen, nachdem Sie das FCoE-Netzwerk eingerichtet haben.

---

## Hinzufügen von Software-FCoE-Adaptern

Sie müssen Software-FCoE-Adapter aktivieren, damit der Host sie für den Zugriff auf den Fibre-Channel-Speicher verwenden kann.

Die Anzahl an Software-FCoE-Adaptern, die Sie aktivieren können, entspricht der Anzahl der physischen FCoE-Netzwerkkarten-Ports auf Ihrem Host. ESXi unterstützt maximal vier Software-FCoE-Adapter auf einem Host.

### Voraussetzungen

Richten Sie das Netzwerk für den Software-FCoE-Adapter ein.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und anschließend auf das Symbol **Hinzufügen** (+).
- 4 Wählen Sie **Software-FCoE-Adapter**.
- 5 Wählen Sie im Dialogfeld „Hinzufügen von Software-FCoE-Adaptern“ eine entsprechende vmnic aus der Dropdown-Liste der physischen Netzwerkadapter aus.

Nur diejenigen Adapter, die noch nicht für den FCoE-Datenverkehr verwendet werden, werden aufgelistet.

- 6 Klicken Sie auf **OK**.

Der Software-FCoE-Adapter wird in der Liste der Speicheradapter angezeigt.

## Ergebnisse

Nachdem Sie den Software-FCoE-Adapter aktiviert haben, können Sie seine Eigenschaften anzeigen. Wenn Sie den Adapter nicht verwenden, können Sie ihn aus der Liste der Adapter entfernen.



# Starten von ESXi von einem Fibre-Channel-SAN

# 6

Wenn Sie Ihren Host so einrichten, dass er von einem SAN gestartet wird, wird das Start-Image des Hosts auf einer oder mehreren LUNs im SAN-Speichersystem gespeichert. Wenn der Host startet, wird er nicht von seiner lokalen Festplatte aus, sondern von der LUN im SAN aus gestartet.

ESXi unterstützt das Starten über einen Fibre-Channel-HBA oder einen FCoE-CNA.

Dieses Kapitel enthält die folgenden Themen:

- Vorteile beim Starten über ein SAN
- Anforderungen und Überlegungen beim Starten von Fibre-Channel-SAN
- Vorbereiten für das Starten über ein SAN
- Konfigurieren des Emulex HBAs für das Starten über ein SAN
- Konfigurieren des QLogic-HBAs für das Starten über ein SAN

## Vorteile beim Starten über ein SAN

Das Starten von SAN kann Ihrer Umgebung viele Vorteile bieten. In einigen Fällen sollten Sie das Starten von SAN jedoch nicht für ESXi-Hosts verwenden. Bevor Sie Ihr System zum Starten von einem SAN einrichten, sollten Sie zunächst überlegen, ob dies Ihrer Umgebung angemessen ist.

---

**Vorsicht** Wenn das Starten von SAN mit mehreren ESXi-Hosts erfolgt, muss jeder Host über eine eigene Start-LUN verfügen. Wenn Sie mehrere Hosts für die Verwendung derselben Start-LUN konfigurieren, werden wahrscheinlich ESXi-Images beschädigt.

---

Wenn Sie von SAN starten, gibt es u.a. folgende Vorteile für Ihre Umgebung:

- Günstigere Server. Höhere Serverdichte und bessere Ausführung ohne internen Speicher.
- Einfacherer Serveraustausch. Sie können Server problemlos austauschen und den neuen Server so einrichten, dass sie auf den alten Speicherort der Start-Image-Datei verweisen.
- Weniger ungenutzter Platz. Server ohne lokale Festplatten benötigen oft weniger Speicherplatz.

- Einfachere Sicherungsvorgänge. Sie können die Systemstart-Images im SAN als Teil der allgemeinen SAN-Sicherungsverfahren sichern. Außerdem können Sie fortschrittliche Array-Funktionen verwenden, wie z. B. Snapshots auf dem Start-Image.
- Verbesserte Verwaltung. Das Erstellen und Verwalten des Betriebssystem-Images ist einfacher und effizienter.
- Noch zuverlässiger. Sie können über mehrere Pfade auf das Startlaufwerk zugreifen, was verhindert, dass das Laufwerk zur einzelnen Fehlerquelle wird.

## Anforderungen und Überlegungen beim Starten von Fibre-Channel-SAN

Ihre ESXi-Startkonfiguration muss bestimmte Anforderungen erfüllen.

**Tabelle 6-1. Anforderungen für das Starten über ein SAN**

Anforderung	Beschreibung
Anforderungen an das ESXi-System	Halten Sie sich an die Herstellerempfehlungen für das Starten des Servers über ein SAN.
Adapteranforderungen	Aktivieren und konfigurieren Sie den Adapter ordnungsgemäß, damit er auf die Start-LUN zugreifen kann. Informationen finden Sie in der Dokumentation des Anbieters.
Zugriffssteuerung	<ul style="list-style-type: none"> <li>■ Jeder Host darf nur auf seine eigene LUN zugreifen, nicht auf die Start-LUNs anderer Hosts. Verwenden Sie Speichersystemsoftware, um sicherzustellen, dass der Host nur auf die designierte LUNs zugreift.</li> <li>■ Eine Diagnosepartition kann von mehreren Servern gemeinsam genutzt werden. Um dies zu erreichen, können Sie eine arrayspezifische LUN-Maskierung verwenden.</li> </ul>
Unterstützung von Multipathing	Das Multipathing auf eine Start-LUN auf Aktiv-Passiv-Arrays wird nicht unterstützt, weil das BIOS Multipathing nicht unterstützt und keinen Standby-Pfad aktivieren kann.
Überlegungen zum SAN	SAN-Verbindungen müssen über eine Switch-Topologie hergestellt werden, wenn das Array nicht für direkte Verbindungstopologie zertifiziert ist. Wenn das Array für direkte Verbindungstopologie zertifiziert ist, können die SAN-Verbindungen direkt zum Array hergestellt werden. Das Starten über SAN wird für die Switch-Topologie und für die direkte Verbindungstopologie unterstützt, wenn diese Topologien für das jeweilige Array zertifiziert sind.
Hardware-spezifische Überlegungen	Wenn sie ein eServer BladeCenter von IBM ausführen und das System über das SAN starten, müssen Sie die IDE-Laufwerke der Blades deaktivieren.

## Vorbereiten für das Starten über ein SAN

Wenn Sie Ihren Host für das Starten von einer SAN-Umgebung einrichten, führen Sie mehrere Aufgaben durch.

In diesem Abschnitt wird der generische Aktivierungsprozess zum Starten vom SAN auf den im Rack montierten Servern beschrieben. Weitere Informationen über das Aktivieren des Startens vom SAN auf Cisco Unified Computing System FCoE-Blade-Servern finden Sie in der Cisco-Dokumentation.

## Verfahren

### 1 Konfigurieren von SAN-Komponenten und des Speichersystems

Bevor Sie Ihren ESXi-Host zum Starten von einer SAN-LUN einrichten, konfigurieren Sie die SAN-Komponenten und ein Speichersystem.

### 2 Konfigurieren eines Speicheradapters für das Starten über ein SAN

Wenn Sie Ihren Host zum Starten über ein SAN einrichten, aktivieren Sie den Startadapter im BIOS des Hosts. Sie können den Startadapter zum Initiieren einer einfachen Verbindung mit der Ziel-Start-LUN konfigurieren.

### 3 Einrichten des Systems zum Starten vom Installationsmedium

Wenn Sie Ihren Host zum Starten vom SAN einrichten, starten Sie den Host zuerst vom VMware-Installationsmedium. Ändern Sie hierzu die Startreihenfolge in den BIOS-Einstellungen des Systems.

## Konfigurieren von SAN-Komponenten und des Speichersystems

Bevor Sie Ihren ESXi-Host zum Starten von einer SAN-LUN einrichten, konfigurieren Sie die SAN-Komponenten und ein Speichersystem.

Weil das Konfigurieren der SAN-Komponenten herstellerspezifisch ist, sollten Sie die Produktdokumentation eines jeden Elements zu Rate ziehen.

## Verfahren

- 1 Schließen Sie das Netzkabel an, wie in den Handbüchern der betreffenden Geräte beschrieben.

Überprüfen Sie ggf. die Switch-Verkabelung.

- 2 Konfigurieren Sie das Speicher-Array.

- a Machen Sie den ESXi-Host über das SAN-Speicher-Array für das SAN sichtbar. Dieser Vorgang wird häufig als das Erstellen eines Objekts bezeichnet.
- b Richten Sie den Host über das SAN-Speicher-Array so ein, sodass dieser die WWPNs der Hostadapter als Port- oder Knotennamen verwendet.
- c Erstellen Sie LUNs.
- d Weisen Sie LUNs zu.

- e Erfassen Sie die IP-Adressen der Switches und der Speicher-Arrays.
- f Erfassen Sie den WWPN für jeden Speicherprozessor.

---

**Vorsicht** Wenn die Installation von ESXi im Modus zum Starten über SAN per Skript erfolgt, müssen Sie bestimmte Schritte ausführen, um einen unerwünschten Datenverlust zu vermeiden.

---

## Konfigurieren eines Speicheradapters für das Starten über ein SAN

Wenn Sie Ihren Host zum Starten über ein SAN einrichten, aktivieren Sie den Startadapter im BIOS des Hosts. Sie können den Startadapter zum Initiieren einer einfachen Verbindung mit der Ziel-Start-LUN konfigurieren.

### Voraussetzungen

Bestimmen Sie den WWPN für den Speicheradapter.

### Verfahren

- ◆ Konfigurieren Sie den Speicheradapter für das Starten über ein SAN

Da die Konfiguration von Startadaptern herstellerabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Herstellers.

## Einrichten des Systems zum Starten vom Installationsmedium

Wenn Sie Ihren Host zum Starten vom SAN einrichten, starten Sie den Host zuerst vom VMware-Installationsmedium. Ändern Sie hierzu die Startreihenfolge in den BIOS-Einstellungen des Systems.

Weil das Ändern der Startsequenz im BIOS herstellerspezifisch ist, sollten Sie die entsprechenden Anweisungen in der Herstellerdokumentation zu Rate ziehen. Der folgende Vorgang erläutert, wie Sie die Startsequenz auf einem IBM-Host ändern können.

### Verfahren

- 1 Wechseln Sie beim Hochfahren des Systems in das Konfigurations- bzw. Installationsprogramm des System-BIOS.
- 2 Wählen Sie **Startup Options**, und drücken Sie die Eingabetaste.
- 3 Wählen Sie **Startup Sequence Options**, und drücken Sie die Eingabetaste.
- 4 Setzen Sie die Option von **First Startup Device** auf **[CD-ROM]**.

### Ergebnisse

Sie können jetzt ESXi installieren.

# Konfigurieren des Emulex HBAs für das Starten über ein SAN

Die Konfiguration des Emulex-BA-IOs zum Starten von einem SAN beinhaltet die Aktivierung der BIOS-Einstellung zur Startauswahl und die Aktivierung des BIOS.

## Verfahren

### 1 Aktivieren der BIOS-Einstellung zur Startauswahl

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie die BIOS-Einstellung zur Startauswahl aktivieren.

### 2 Aktivieren des BIOS

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie das BIOS aktivieren.

## Aktivieren der BIOS-Einstellung zur Startauswahl

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie die BIOS-Einstellung zur Startauswahl aktivieren.

## Verfahren

- 1 Führen Sie **lputil** aus.
- 2 Wählen Sie **3. Firmware Maintenance**.
- 3 Wählen Sie einen Adapter.
- 4 Wählen Sie **6. Boot BIOS Maintenance**.
- 5 Wählen Sie **1. Enable Boot BIOS**.

## Aktivieren des BIOS

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie das BIOS aktivieren.

## Verfahren

- 1 Starten Sie den Host neu.
- 2 Drücken Sie zum Konfigurieren der Adapterparameter ALT+E an der Emulex-Eingabeaufforderung und führen Sie diese Schritte aus.
  - a Wählen Sie einen Adapter (mit BIOS-Unterstützung).
  - b Wählen Sie **2. Configure This Adapter's Parameters**.
  - c Wählen Sie **1. Enable or Disable BIOS**.
  - d Wählen Sie **1**, um das BIOS zu aktivieren.
  - e Wählen Sie **x** zum Beenden und **Esc**, um zum Hauptmenü zurückzukehren.

- 3 Führen Sie zum Konfigurieren des Startgeräts diese Schritte vom Emulex-Hauptmenü aus.
  - a Wählen Sie denselben Adapter.
  - b Wählen Sie **1. Configure Boot Devices**.
  - c Wählen Sie den Speicherort für den Starteintrag aus.
  - d Geben Sie das zweistellige Startgerät ein.
  - e Geben Sie die zweistellige (HEX) Start-LUN ein (z. B. **08**).
  - f Wählen Sie die Start-LUN.
  - g Wählen Sie **1. WWPN**. (Starten Sie dieses Gerät mit WWPN, nicht DID).
  - h Wählen Sie **x** zum Beenden und **Y**, um neu zu starten.
- 4 Starten Sie im System-BIOS, und entfernen Sie zunächst Emulex aus der Start-Controller-Reihenfolge.
- 5 Führen Sie einen Neustart und die Installation auf einer SAN-LUN durch.

## Konfigurieren des QLogic-HBAs für das Starten über ein SAN

Mit diesem Beispiel wird erläutert, wie der QLogic-HBA für das Starten von ESXi über ein SAN konfiguriert wird. Die Prozedur umfasst die Aktivierung des QLogic-HBA-BIOS, die Aktivierung der Startauswahloption sowie die Auswahl der Start-LUN.

### Verfahren

- 1 Drücken Sie beim Starten des Servers **STRG+Q**, um das Fast!UTIL-Konfigurationsdienstprogramm zu starten.
- 2 Führen Sie, abhängig von der Anzahl an HBAs, die entsprechende Aktion aus.

Option	Beschreibung
<b>Ein HBA</b>	Wenn Sie über nur einen HBA (Host Bus Adapter) verfügen, wird die Seite mit den Fast!UTIL-Optionen angezeigt. Wechseln Sie zu <a href="#">Schritt 3</a> .
<b>Mehrere HBAs</b>	Wenn mehr als ein HBA vorhanden ist, wählen Sie den HBA manuell aus. <ol style="list-style-type: none"> <li>a Verwenden Sie auf der Seite „Select Host Adapter“ die Pfeiltasten, um den Cursor auf dem gewünschten HBA zu positionieren.</li> <li>b Drücken Sie die <b>Eingabetaste</b>.</li> </ol>

- 3 Wählen Sie auf der Seite mit den Fast!UTIL Options **Konfigurationseinstellungen** und drücken Sie die **Eingabetaste**.
- 4 Wählen Sie auf der Seite mit den Konfigurationseinstellungen die Option **Adaptoreinstellungen** und drücken Sie die **Eingabetaste**.

- 5 Stellen Sie das BIOS so ein, dass eine Suche nach SCSI-Geräten ausgeführt wird.
  - a Wählen Sie auf der Seite mit den Hostadaptoreinstellungen die Option **Host Adapter BIOS**.
  - b Drücken Sie die **Eingabetaste**, um den Wert auf Aktiviert zu setzen.
  - c Drücken Sie zum Beenden die **Esc**-Taste.
- 6 Aktivieren Sie die Startauswahl.
  - a Wählen Sie **Startauswahleinstellung** aus und drücken Sie die **Eingabetaste**.
  - b Wählen Sie auf der Seite für das auswählbare Starten die Option **Startauswahl**.
  - c Drücken Sie die **Eingabetaste**, um den Wert auf **Aktiviert** zu setzen.
- 7 Verwenden Sie die Pfeiltasten, um den Eintrag für den Namen des Startports in der Liste der Speicherprozessoren (SPs) auszuwählen, und drücken Sie die **Eingabetaste**, um den Bildschirm zur Auswahl des Fibre-Channel-Geräts zu öffnen.
- 8 Wählen Sie über die Pfeiltasten den gewünschten Speicherprozessor aus und drücken Sie die **Eingabetaste**.

Bei Verwendung eines Aktiv-Passiv-Speicher-Arrays muss sich der ausgewählte Speicherprozessor auf dem bevorzugten (aktiven) Pfad zur Start-LUN befinden. Wenn Sie nicht sicher sind, welcher Speicherprozessor sich auf dem aktiven Pfad befindet, können Sie diesen mithilfe der Speicher-Array-Verwaltungssoftware ermitteln. Die Ziel-IDs werden vom BIOS erstellt und können sich bei jedem Neustart ändern.

- 9 Führen Sie, abhängig von der Anzahl der dem Speicherprozessor zugeordneten HBAs, die entsprechende Aktion aus.

Option	Beschreibung
<b>Eine LUN</b>	Die LUN ist als Start-LUN ausgewählt. Sie müssen im Bildschirm für die Auswahl der LUN keine Auswahl vornehmen.
<b>Mehrere LUNs</b>	Der Bildschirm für die Auswahl der LUN wird geöffnet. Wählen Sie über die Pfeiltasten die Start-LUN aus und drücken Sie die <b>Eingabetaste</b> .

- 10 Sollten weitere Speicherprozessoren in der Liste angezeigt werden, drücken Sie **C**, um die Daten zu löschen.
- 11 Drücken Sie **ESC** zwei Mal, um den Bildschirm zu verlassen, und drücken Sie die **Eingabetaste**, um die Einstellung zu speichern.

# Starten von ESXi mit Software FCoE

# 7

ESXi unterstützt das Starten von FCoE-fähigen Netzwerkadaptern.

Wenn Sie ESXi von einem FCoE LUN installieren und starten, kann der Host einen VMware-Software FCoE-Adapter und einen Netzwerkadapter mit FCoE-Funktionen verwenden. Der Host benötigt keinen dedizierten FCoE HBA.

Sie führen die meisten Konfigurationen über die Option-ROM im Netzwerkadapter aus. Die Netzwerkadapter müssen eines der folgenden Formate unterstützen, die die Parameter über ein FCoE-Startgerät an VMkernel kommunizieren.

- FCoE Boot Firmware Table (FBFT). FBFT ist Eigentum von Intel.
- FCoE Boot Parameter Table (FBPT). FBPT wird von VMware für Drittanbieter definiert, um Software FCoE Boot zu implementieren.

Die Konfigurationsparameter werden im Option-ROM des Adapters festgelegt. Während einer ESXi-Installation oder einem nachfolgenden Startvorgang werden diese Parameter entweder im FBFT-Format oder im FBPT-Format in den Systemspeicher exportiert. Der VMkernel kann die Konfigurationseinstellungen lesen und diese zum Zugriff auf das Start-LUN verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen und Überlegungen für das Starten mit Software FCoE](#)
- [Best Practices für Software FCoE Boot](#)
- [Einrichten des Startens mit Software FCoE](#)
- [Durchführen der Fehlerbehebung für die Installation und Starten von Software-FCoE](#)

## Anforderungen und Überlegungen für das Starten mit Software FCoE

Wenn Sie den ESXi-Host aus SAN mit Software FCoE starten, gelten bestimmte Anforderungen und Überlegungen.

### Anforderungen

- ESXi 5.1 oder höher.



- Der Netzwerkadapter muss folgende Fähigkeiten aufweisen:
  - Er muss FCoE-fähig sein.
  - Er muss ESXi Open FCoE Stack unterstützen.
  - Er muss FCoE-Start-Firmware enthalten, die Startinformationen im FBFT-Format oder FBPT-Format exportieren kann.

## Überlegungen

- Sie können die Software FCoE-Startkonfiguration aus ESXi nicht ändern.
- Coredump wird auf keinen Software FCoE LUNs unterstützt, einschließlich der Start-LUN.
- Mehrfachpfade werden vor dem Start nicht unterstützt.
- Start-LUN kann mit anderen Hosts auch bei gemeinsam genutztem Speicher nicht gemeinsam genutzt werden.

## Best Practices für Software FCoE Boot

Mehrere Best Practices werden empfohlen, wenn Sie das System von einer Software FCoE LUN starten.

- Stellen Sie sicher, dass der Host Zugriff auf die gesamte Start-LUN hat. Die Start-LUN kann nicht mit anderen Hosts gemeinsam genutzt werden, auch nicht bei gemeinsam genutztem Speicher.
- Wenn Sie den Intel 10 Gigabit Ethernet Controller (Niantec) mit einem Cisco-Switch verwenden, konfigurieren Sie den Switch-Port in folgender Weise:
  - Aktivieren Sie das Spanning-Tree-Protokoll (STP).
  - Deaktivieren Sie `switchport trunk native vlan` für das VLAN, das für FCoE verwendet wird.

## Einrichten des Startens mit Software FCoE

Ihr ESXi-Host kann von einer FCoE LUN mit dem Software FCoE-Adapter einen Netzwerkadapter starten.

Wenn Sie Ihren Host für einen Software FCoE-Start konfigurieren, führen Sie eine Reihe von Aufgaben aus.

### Voraussetzungen

Der Netzwerkadapter hat folgende Fähigkeiten:

- Unterstützt teilweisen FCoE Offload (Software FCoE).
- Enthält eine FCoE Boot Firmware Table (FBFT) oder eine FCoE Boot Parameter Table (FBPT).

Informationen über Netzwerkkadappter, die Software FCoE-Starts unterstützen, finden Sie unter *VMware-Kompatibilitätshandbuch*.

## Verfahren

### 1 Konfigurieren der Parameter für das Starten mit Software FCoE

Ein Netzwerkkadappter auf Ihrem Host muss über eine speziell konfigurierte FCoE-Start-Firmware verfügen, um einen Software-FCoE-Startvorgang zu unterstützen. Wenn Sie die Firmware konfigurieren, aktivieren Sie den Adapter für den Software-FCoE-Start und geben Sie die Start-LUN-Parameter an.

### 2 Installieren und Starten von ESXi von Software FCoE LUN

Wenn Sie ein System einrichten, das von einer Software FCoE LUN startet, installieren Sie das ESXi-Image auf der Ziel-LUN. Sie können dann Ihren Host von dieser LUN starten.

## Konfigurieren der Parameter für das Starten mit Software FCoE

Ein Netzwerkkadappter auf Ihrem Host muss über eine speziell konfigurierte FCoE-Start-Firmware verfügen, um einen Software-FCoE-Startvorgang zu unterstützen. Wenn Sie die Firmware konfigurieren, aktivieren Sie den Adapter für den Software-FCoE-Start und geben Sie die Start-LUN-Parameter an.

## Verfahren

- ◆ Geben Sie in der Option ROM des Netzwerkkadapters die Software-FCoE-Start-Parameter an.  
Diese Parameter enthalten das Startziel, die Start-LUN, die VLAN-ID usw.  
Da die Konfiguration des Netzwerkkadapters anbieterabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Anbieters.

## Installieren und Starten von ESXi von Software FCoE LUN

Wenn Sie ein System einrichten, das von einer Software FCoE LUN startet, installieren Sie das ESXi-Image auf der Ziel-LUN. Sie können dann Ihren Host von dieser LUN starten.

## Voraussetzungen

- Konfigurieren Sie den Option-ROM des Netzwerkkadapters so, dass er auf eine Ziel-LUN zeigt, die Sie als Start-LUN verwenden möchten. Achten Sie darauf, dass Sie die Informationen über die hochfahrbare LUN haben.
- Ändern Sie die BIOS-Startsequenz im System-BIOS auf die folgende Sequenz:
  - a Netzwerkkadappter, den Sie für das Starten mit Software FCoE benutzen.
  - b ESXi-Installationsmedien.

Weitere Informationen hierzu finden Sie in der Anbieterdokumentation für Ihr System.

## Verfahren

- 1 Starten Sie eine interaktive Installation von der ESXi-Installations-CD/DVD.

Das ESXi-Installationsprogramm überprüft, dass das Starten mit FCoE im BIOS aktiviert ist, und erstellt erforderlichenfalls einen virtuellen Standard-Switch für den FCoE-fähigen Netzwerkadapter. Der Name des vSwitch ist VMware\_FCoE\_vSwitch. Das Installationsprogramm verwendet dann vorkonfigurierte FCoE-Startparameter zum Erkennen und Anzeigen aller verfügbaren FCoE LUNs.

- 2 Wählen Sie im Bildschirm **Festplatte auswählen** die Software FCoE LUN aus, die Sie in der Startparametereinstellung angegeben haben.

Wenn die Start-LUN in diesem Menü nicht erscheint, vergewissern Sie sich, dass Sie die Startparameter im Option-ROM des Netzwerkadapters richtig konfiguriert haben.

- 3 Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.

- 4 Starten Sie den Host neu.

- 5 Ändern Sie die Startreihenfolge im System-BIOS, sodass die FCoE-Boot-LUN das erste startbare Gerät ist.

ESXi setzt das Starten von der Software FCoE LUN fort, bis die Betriebsbereitschaft hergestellt ist.

## Nächste Schritte

Erforderlichenfalls können Sie den VMware\_FCoE\_vSwitch umbenennen und ändern, den das Installationsprogramm automatisch erstellt hat. Achten Sie darauf, dass der Cisco Discovery Protocol-Modus (CDP) auf „Überwachen“ oder „Beide“ eingestellt ist.

# Durchführen der Fehlerbehebung für die Installation und Starten von Software-FCoE

Wenn die Installation oder das Starten von ESXi über eine FCoE-LUN fehlschlägt, können Sie mehrere Fehlerbehebungsmethoden verwenden.

## Problem

Wenn Sie ESXi aus dem FCoE-Speicher mithilfe eines Software-FCoE-Adapters von VMware und eines Netzwerkadapters mit Funktionen für den teilweisen FCoE-Offload installieren oder starten, schlägt die Installation oder der Startvorgang fehl.

## Lösung

- Stellen Sie sicher, dass Sie die Startparameter im Option-ROM des FCoE-Netzwerkadapters richtig konfiguriert haben.
- Überwachen Sie während der Installation das BIOS des FCoE-Netzwerkadapters auf etwaige Fehler.

- Überprüfen Sie das VMkernel-Protokoll auf Fehler, falls dies möglich ist.
- Verwenden Sie den Befehl `esxcli`, um sich zu vergewissern, dass die Start-LUN vorhanden ist.

```
esxcli conn_options hardware bootdevice list
```

# Best Practices für Fibre-Channel-Speicher



Befolgen Sie bei der Verwendung von ESXi mit Fibre-Channel-SAN die Best Practices von VMware, um Leistungsbeeinträchtigungen zu verhindern.

Der vSphere Web Client bietet umfangreiche Funktionen für das Erfassen von Leistungsdaten. Die Informationen werden grafisch angezeigt und ständig aktualisiert.

Zudem können Sie das `resxtop`- oder das `esxtop`-Befehlszeilenprogramm verwenden. Die Dienstprogramme liefern detaillierte Informationen darüber, wie ESXi Ressourcen in Echtzeit verwendet. Weitere Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Erkundigen Sie sich bei Ihrem Speicheranbieter, ob Ihr Speichersystem die Hardwarebeschleunigungsfunktionen der Storage-APIs für die Array-Integration unterstützt. Wenn ja, suchen Sie in der Dokumentation Ihres Anbieters nach Informationen zur Aktivierung der Unterstützung für die Hardwarebeschleunigung auf dem Speichersystem. Weitere Informationen finden Sie unter [Kapitel 23 Speicherhardware-Beschleunigung](#).

Dieses Kapitel enthält die folgenden Themen:

- [Vermeiden von Fibre-Channel-SAN-Problemen](#)
- [Deaktivieren der automatischen Hostregistrierung](#)
- [Optimieren der Fibre-Channel-SAN-Speicherleistung](#)

## Vermeiden von Fibre-Channel-SAN-Problemen

Bei Verwendung von ESXi in Verbindung mit einem Fibre-Channel-SAN müssen Sie bestimmte Richtlinien befolgen, um SAN-Probleme zu vermeiden.

In diesem Abschnitt erhalten Sie einige Tipps, wie sich Probleme mit der SAN-Konfiguration verhindern lassen:

- Platzieren Sie nur einen einzigen VMFS-Datenspeicher in jeder LUN.
- Ändern Sie die vom System festgelegte Pfadrichtlinie nur, wenn Sie die Auswirkungen dieser Änderung kennen und verstehen.
- Erstellen Sie eine ausführliche Dokumentation. Notieren Sie Informationen zu Zoning, Zugriffssteuerung, Speicher, Switch, Server und FC-HBA-Konfiguration, Software- und Firmware-Versionen sowie zum Speicherkabelplan.

- Erstellen Sie einen Notfallplan bei Ausfällen:
  - Kopieren Sie Ihre Topologiezuordnungen mehrfach. Ermitteln Sie für jedes Element, welche Auswirkungen ein Ausfall dieses Elements auf das SAN hat.
  - Stellen Sie mithilfe einer Liste aller Verbindungen, Switches, HBAs und anderen Elemente sicher, dass Sie keine wichtige Fehlerstelle in Ihrem Design übersehen haben.
- Stellen Sie sicher, dass die FC-HBAs an den geeigneten Steckplätzen des Hosts installiert sind (basierend auf Steckplatz- und Busgeschwindigkeit). Richten Sie einen PCI-Bus-Lastenausgleich für alle Busse des Servers ein.
- Machen Sie sich mit den verschiedenen Überwachungspunkten in Ihrem Speichernetzwerk an allen Sichtbarkeitspunkten vertraut (einschließlich Leistungsdiagrammen für Hosts sowie Statistiken zu FC-Switches und Speicherleistung).
- Seien Sie beim Ändern der IDs der LUNs vorsichtig, die über von Ihrem ESXi-Host verwendete VMFS-Datenspeicher verfügen. Wenn Sie die ID ändern, wird der Datenspeicher inaktiv und seine virtuellen Maschinen fallen aus. Sie können den Datenspeicher neu signieren, um ihn wieder zu aktivieren. Weitere Informationen hierzu finden Sie unter [Verwalten von duplizierten VMFS-Datenspeichern](#).

Wenn sich keine laufenden virtuellen Maschinen auf dem VMFS-Datenspeicher befinden, nachdem Sie die ID der LUN geändert haben, müssen Sie zum Zurücksetzen der ID auf dem Host eine erneute Prüfung durchführen. Weitere Informationen über das erneute Prüfen finden Sie unter [Vorgänge zum Aktualisieren und zur erneuten Prüfung von Speichern](#).

## Deaktivieren der automatischen Hostregistrierung

Für bestimmte Speicher-Arrays ist die Registrierung der ESXi-Hosts bei den Arrays erforderlich. ESXi führt die Hostregistrierung automatisch aus, indem es den Namen und die IP-Adresse des Hosts an das Array sendet. Schalten Sie die ESXi-Funktion für die automatische Registrierung aus, wenn Sie es vorziehen, die Registrierung manuell mithilfe von Speicherverwaltungssoftware durchzuführen.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Systemeinstellungen“ den Parameter **Disk.EnableNaviReg** aus und klicken Sie auf das Symbol **Bearbeiten**.
- 5 Ändern Sie den Wert in 0.

### Ergebnisse

Die standardmäßig aktivierte automatische Hostregistrierungsfunktion wird dadurch deaktiviert.

## Optimieren der Fibre-Channel-SAN-Speicherleistung

Bei der Optimierung einer typischen SAN-Umgebung müssen verschiedene Faktoren berücksichtigt werden.

Wenn die Umgebung ordnungsgemäß konfiguriert ist, leisten die SAN-Fabric-Komponenten (insbesondere die SAN-Switches) aufgrund ihrer geringen Latenz im Vergleich zu Servern und Speicher-Arrays lediglich einen geringen Beitrag. Stellen Sie sicher, dass die Pfade durch das Switch-Fabric nicht ausgelastet sind, d. h. das Switch-Fabric wird mit dem höchsten Durchsatz ausgeführt.

### Speicher-Array-Leistung

Einer der wichtigsten Faktoren für die Optimierung einer kompletten iSCSI-Umgebung ist die Speicher-Array-Leistung.

Bei Problemen mit der Speicher-Array-Leistung sollten Sie unbedingt die entsprechende Dokumentation des Speicher-Array-Herstellers lesen.

Befolgen Sie diese allgemeinen Richtlinien, um die Array-Leistung in der vSphere-Umgebung zu erhöhen:

- Bedenken Sie beim Zuweisen von LUNs, dass über verschiedene Hosts auf jede LUN zugegriffen werden kann und dass auf jedem Host mehrere virtuelle Maschinen ausgeführt werden können. Auf einer LUN, die von einem Host verwendet wird, sind E/A-Vorgänge von einer Vielzahl von unterschiedlichen Anwendungen möglich, die unter verschiedenen Betriebssystemen ausgeführt werden. Aufgrund dieser unterschiedlichen Arbeitslast sollte die RAID-Gruppe mit den ESXi-LUNs keine LUNs enthalten, die von anderen Servern verwendet werden, auf denen nicht ESXi ausgeführt wird.
- Stellen Sie sicher, dass die Lese- oder Schreibcache aktiviert ist.
- SAN-Speicher-Arrays müssen kontinuierlich neu ausgelegt und optimiert werden, um sicherzustellen, dass die E/A-Last auf alle Speicher-Array-Pfade verteilt ist. Um diese Anforderung zu erfüllen, verteilen Sie die Pfade zu den LUNs auf alle Speicherprozessoren. Das Ergebnis ist ein optimaler Lastenausgleich. Eine sorgfältige Überwachung zeigt an, wann die LUN-Verteilung ausgeglichen werden muss.

Bei der Optimierung von Speicher-Arrays mit statischem Lastenausgleich ist die Überwachung der spezifischen Leistungsstatistiken (beispielsweise E/A-Vorgänge pro Sekunde, Blocks pro Sekunde und Reaktionszeit) und Verteilung der LUN-Arbeitslast auf alle Speicherprozessoren von größter Bedeutung.

---

**Hinweis** Der dynamische Lastenausgleich wird mit ESXi gegenwärtig nicht unterstützt.

---

### Serverleistung mit Fibre-Channel

Um eine optimale Serverleistung sicherzustellen, müssen verschiedene Faktoren berücksichtigt werden.

Der Zugriff jeder Serveranwendung auf den integrierten Speicher muss mit den folgenden Bedingungen gewährleistet sein:

- Hohe E/A-Rate (Anzahl an E/A-Vorgängen pro Sekunde)
- Hoher Durchsatz (MB pro Sekunde)
- Minimale Latenz (Reaktionszeiten)

Da für jede Anwendung andere Anforderungen gelten, können Sie diese Ziele erreichen, indem Sie eine geeignete RAID-Gruppe für das Speicher-Array wählen. Zum Erreichen von Leistungszielen führen Sie die folgenden Aufgaben aus:

- Platzieren Sie jede LUN in einer RAID-Gruppe, welche die erforderlichen Leistungsebenen bietet. Beachten Sie Aktivitäten und Ressourcennutzung von anderen LUNs in der zugewiesenen RAID-Gruppe. Mit einer hochleistungsfähigen RAID-Gruppe mit zu vielen Anwendungen, die eine E/A-Last verursachen, können die Leistungsziele möglicherweise nicht erreicht werden, die für eine Anwendung auf dem ESXi-Host erforderlich sind.
- Stellen Sie sicher, dass jeder Server über eine ausreichende Anzahl an HBAs verfügt, um einen maximalen Durchsatz für alle Anwendungen zu ermöglichen, die während der Spitzenzeiten auf dem Server gehostet werden. Bei Verteilung der E/A-Last auf mehrere HBAs wird ein höherer Durchsatz und eine geringere Latenz für jede Anwendung erreicht.
- Um Redundanz für den Fall eines HBA-Ausfalls bereitzustellen, sollten Sie den Server mit einem doppelten redundanten Fabric verbinden.
- Beim Zuweisen von LUNs oder RAID-Gruppen für ESXi-Systeme werden diese Ressourcen durch mehrere Betriebssysteme gemeinsam verwendet. Daher kann die erforderliche Leistung jeder LUN im Speichersubsystem beim Einsatz von ESXi-Systemen deutlich höher sein als bei Verwendung von physischen Maschinen. Wenn Sie z. B. die Ausführung von vier E/A-intensiven Anwendungen planen, weisen Sie die vierfache Leistungskapazität für die ESXi-LUNs zu.
- Bei der gemeinsamen Verwendung mehrerer ESXi-Systeme mit vCenter Server steigt die erforderliche Leistung für das Speichersubsystem entsprechend.
- Die Anzahl an ausstehenden E/A-Vorgängen von Anwendungen, die auf einem ESXi-System ausgeführt werden, sollte mit der Anzahl an E/A-Vorgängen übereinstimmen, die der HBA und das Speicher-Array verarbeiten können.



# Verwenden von ESXi mit iSCSI-SAN

## 9

Sie können ESXi in Verbindung mit einem SAN (Storage Area Network) verwenden, einem speziellen Hochgeschwindigkeitsnetzwerk, das Computersysteme mit Hochleistungsspeicher-Subsystemen verbindet. Der Einsatz von ESXi zusammen mit einem SAN bietet zusätzlichen Speicher für Konsolidierungen, steigert die Zuverlässigkeit und unterstützt Sie bei der Notfallwiederherstellung.

Die effiziente Nutzung von ESXi mit einem SAN setzt voraus, dass Sie über Anwendungserfahrungen mit ESXi-Systemen und SAN-Konzepten verfügen. Darüber hinaus ist es erforderlich, bei der Einrichtung von ESXi-Hosts für die Verwendung von iSCSI (Internet SCSI)-SAN-Speichersystemen bestimmte Überlegungen anzustellen.

Dieses Kapitel enthält die folgenden Themen:

- [iSCSI-SAN-Konzepte](#)
- [Zugriff auf Daten in einem iSCSI-SAN durch virtuelle Maschinen](#)

## iSCSI-SAN-Konzepte

Wenn Sie Administrator sind und die ESXi-Hosts für die Zusammenarbeit mit iSCSI-SANs einrichten möchten, müssen Sie über Anwendungserfahrungen mit iSCSI-Konzepten verfügen.

iSCSI-SANs verwenden Ethernet-Verbindungen zwischen Computersystemen oder Hostservern und Hochleistungsspeichersystemen. Zu den SAN-Komponenten zählen iSCSI-Hostbusadapter (HBAs) oder Netzwerkkarten in den Hostservern, Switches und Routern, die Speicherdatenverkehr weiterleiten, in der Verkabelung, in den Speicherprozessoren (SP) und in den Festplattenspeichersystemen.

iSCSI-SAN verwendet eine Client-Server-Architektur. Der Client, der so genannte iSCSI-Initiator, ist auf Ihrem Host in Betrieb. Er initiiert iSCSI-Sitzungen, indem er SCSI-Befehle ausgibt und diese in das iSCSI-Protokoll eingekapselt an den Server überträgt. Der Server ist als iSCSI-Ziel bekannt. Dieses iSCSI-Ziel stellt ein physisches Speichersystem auf dem Netzwerk dar. Es kann auch von einem virtuellen iSCSI-SAN bereitgestellt werden, z. B. einem in einer virtuellen Maschine ausgeführten iSCSI-Zielemulator. Das iSCSI-Ziel reagiert auf die Befehle des Initiators, indem es die erforderlichen iSCSI-Daten überträgt.

## iSCSI-Multipathing

Bei der Datenübertragung zwischen dem Hostserver und dem Speicher nutzt das SAN eine Technik, die als Multipathing bezeichnet wird. Multipathing bietet die Möglichkeit, mehr als einen physischen Pfad vom ESXi-Host zu einer LUN in einem Speichersystem bereitzustellen.

In der Regel besteht ein einzelner Pfad von einem Host zu einer LUN aus einem iSCSI-Adapter oder der Netzwerkkarte, Switch-Ports, Verbindungskabeln und dem Speicher-Controller-Port. Falls eine Komponente des Pfads ausfällt, wählt der Host für E/A-Vorgänge einen anderen verfügbaren Pfad. Der Prozess der Erkennung eines ausgefallenen Pfads und des Wechsels auf einen anderen Pfad wird als Pfad-Failover bezeichnet.

Weitere Informationen zum Multipathing finden Sie unter [Kapitel 17 Grundlegendes zu Multipathing und Failover](#).

## Ports im iSCSI-SAN

Ein einzelnes erkennbares Element auf dem iSCSI-SAN, z. B. ein Initiator oder ein Ziel, stellt einen iSCSI-Knoten dar. Jeder Knoten besitzt mindestens einen Port, der mit dem SAN verbunden wird.

iSCSI-Ports sind Endpunkte einer iSCSI-Sitzung. Jeder Knoten kann auf mehrere Arten ermittelt werden.

### IP-Adresse

Jeder iSCSI-Knoten kann über eigene IP-Adresse verfügen, sodass Router und Switches im Netzwerk eine Verbindung zwischen dem Server und dem Speicher aufbauen können. Diese Adresse ist mit der IP-Adresse vergleichbar, die Sie Ihrem Computer zuweisen, um auf das Unternehmensnetzwerk oder das Internet zugreifen zu können.

### iSCSI-Name

Ein weltweit eindeutiger Name zum Identifizieren des Knotens. iSCSI verwendet die Formate IQN (iSCSI Qualified Name) und EUI (Extended Unique Identifier).

Standardmäßig generiert ESXi eindeutige iSCSI-Namen für Ihre iSCSI-Initiatoren, zum Beispiel `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Der Standardwert muss daher nicht geändert werden. Wenn Sie ihn dennoch ändern, stellen Sie sicher, dass der neue iSCSI-Name eindeutig ist.

### iSCSI-Alias

Ein Name für ein iSCSI-Gerät oder einen iSCSI-Port, der einfach zu verwalten ist und statt dem iSCSI-Namen verwendet wird. iSCSI-Aliase sind nicht eindeutig und sollen als benutzerfreundliche Namen dienen, die mit einem Port verknüpft werden können.

## iSCSI-Benennungskonventionen

iSCSI verwendet einen speziellen, eindeutigen Bezeichner zum Identifizieren eines iSCSI-Knotens, sei es ein Ziel oder ein Initiator. Dieser Name entspricht dem WWN (WorldWide Name), der mit Fibre-Channel-Geräten verknüpft ist und zur allgemeinen Knotenidentifikation dient.

iSCSI-Namen können zwei verschiedene Formate aufweisen. Das geläufigste Format ist IQN.

Weitere Informationen zu Benennungskonventionen und Zeichenfolgenprofilen finden Sie unter iSCSI-Ben RFC 3721 und RFC 3722 auf der IETF-Website.

## Das IQN-Format (iSCSI Qualified Name)

IQN hat das Format `iqn.jjjj-mm.Namensvergabestelle:eindeutiger Name`, wobei:

- `yyyy-mm` gibt Jahr und Monat an, in dem die Stelle für die Namensvergabe (Naming Authority) eingerichtet wurde.
- `Namensvergabestelle` ist üblicherweise die Syntax des Internetdomännennames der Namensvergabestelle in umgekehrter Reihenfolge. Zum Beispiel könnte die Namensvergabestelle `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 Namensvergabestelle 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`

## Das EUI-Format (Enterprise Unique Identifier)

EUI hat das Format `eui.16 hexadezimale Ziffern`.

Beispiel: `eui.0123456789ABCDEF`.

Bei den 16 Hexadezimalstellen handelt es sich um die Textdarstellung einer 64-Bit-Zahl eines IEEE-EUI-Schemas (Extended Unique Identifier). Die oberen 24 Bit identifizieren die Unternehmens-ID, die das IEEE einem bestimmten Unternehmen zuordnet. Die unteren 40 Bit werden durch die Entität zugewiesen, der diese Unternehmens-ID zugeordnet ist, und müssen eindeutig sein.

## iSCSI-Initiatoren

Für den Zugriff auf iSCSI-Ziele verwendet Ihr Host iSCSI-Initiatoren. Die Initiatoren übertragen SCSI-Anforderungen und Antworten, die in das iSCSI-Protokoll eingekapselt sind, zwischen dem Host und dem iSCSI-Ziel.

Ihr Host unterstützt verschiedene Initiatortypen.

Weitere Informationen zum Konfigurieren und Verwenden der iSCSI-Adapter finden Sie unter [Kapitel 10 Konfigurieren von iSCSI-Adaptern und -Speichern](#).

## Software-iSCSI-Adapter

Ein Software-iSCSI-Adapter ist ein im VMkernel integrierter VMware-Code. Er ermöglicht die Verbindung Ihres Hosts mit dem iSCSI-Speichergerät über Standardnetzwerkadapter. Der Software iSCSI-Adapter dient der iSCSI-Verarbeitung und kommuniziert gleichzeitig mit dem Netzwerkadapter. Mit dem Software iSCSI-Adapter können Sie die iSCSI-Technologie verwenden, ohne besondere Hardware erwerben zu müssen.

## Hardware iSCSI-Adapter

Bei einem Hardware-iSCSI-Adapter handelt es sich um einen Adapter eines Drittanbieters, der die gesamte iSCSI- und Netzwerkverarbeitung von Ihrem Host auslagert. Hardware-iSCSI-Adapter werden in Kategorien unterteilt.

### Abhängige Hardware-iSCSI-Adapter

Hängt vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen ab, die von VMware zur Verfügung gestellt werden.

Bei diesem Adaptertyp kann es sich um eine Karte handeln, die einen Standard-Netzwerkadapter und die iSCSI-Offload-Funktion für denselben Port bietet. Die iSCSI-Offload-Funktion ist hinsichtlich des Abrufens der IP- und der MAC-Adresse sowie anderer Parameter für iSCSI-Sitzungen von der Netzwerkkonfiguration des Hosts abhängig. Ein Beispiel für einen abhängigen Adapter ist die iSCSI-lizenzierte Broadcom 5709-Netzwerkkarte.

### Unabhängige Hardware-iSCSI-Adapter

Implementiert ein eigenes Netzwerk und eigene iSCSI-Konfigurations- und -Verwaltungsschnittstellen.

Ein Beispiel für einen unabhängigen Hardware-iSCSI-Adapter ist eine Karte, die entweder nur die iSCSI-Offload-Funktion oder die iSCSI-Offload-Funktion und die standardmäßige Netzwerkkarten-Funktion bietet. Die iSCSI-Offload-Funktion besitzt eine unabhängige Konfigurationsverwaltung, die die IP- und die MAC-Adresse sowie andere Parameter für die iSCSI-Sitzungen zuweist. Ein Beispiel für einen unabhängigen Adapter ist der QLogic QLA4052-Adapter.

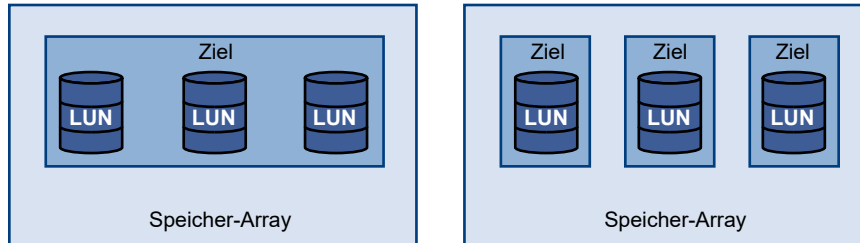
Hardware-iSCSI-Adapter müssen möglicherweise lizenziert werden. Anderenfalls werden sie im Client oder in vSphere-CLI nicht angezeigt. Fragen Sie Ihren Anbieter nach Lizenzierungsinformationen.

## Herstellen von iSCSI-Verbindungen

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

Verschiedene iSCSI-Speicheranbieter verwenden unterschiedliche Methoden, um Speicher für Server bereitzustellen. Einige Anbieter stellen mehrere LUNs auf einem einzigen Ziel dar, während andere Anbieter mehrere Ziele mit je einer LUN verknüpfen. Wenngleich die Speichernutzung durch einen ESXi-Host ähnlich ist, ist dennoch die Darstellungsweise der Informationen durch Verwaltungsprogramme unterschiedlich.

**Abbildung 9-1. Ziel im Vergleich zu LUN-Darstellungen**



Im vorliegenden Beispiel 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 Speichervolume. Im zweiten Fall werden dem Host drei unterschiedliche Ziele mit je einer LUN angezeigt.

Hostbasierte iSCSI-Initiatoren richten nur Verbindungen zu jedem Ziel ein. Das bedeutet, dass sich der LUN-Datenverkehr bei Speichersystemen mit einem Ziel, das mehrere LUNs umfasst, auf diese eine Verbindung konzentriert. Sind in einem System drei Ziele mit je einer LUN vorhanden, bestehen drei Verbindungen zwischen einem Host und den drei verfügbaren LUNs. Diese Information ist hilfreich, um den Speicherdatenverkehr auf mehreren Verbindungen des Hosts mit mehreren iSCSI-HBAs zusammenzufassen, wobei der Datenverkehr für ein Ziel auf einen bestimmten HBA festgelegt und gleichzeitig für den Datenverkehr zu einem anderen Ziel ein anderer HBA genutzt werden kann.

## iSCSI-Speichersystemtypen

ESXi unterstützt verschiedene Speichersysteme und Arrays.

Zu den Speichertypen, die Ihr Host unterstützt, gehören Aktiv-Aktiv, Aktiv-Passiv und ALUA-konform.

### Aktiv-Aktiv-Speichersystem

Ermöglicht den gleichzeitigen Zugriff auf die LUNs über alle Speicherports, die ohne wesentlichen Leistungsabfall verfügbar sind. Alle Pfade sind jederzeit aktiv (es sei denn, ein Pfad fällt aus).

### Aktiv-Passiv-Speichersystem

Ein System, in dem ein Speicherprozessor aktiv den Zugriff auf eine vorhandene LUN ermöglicht. Die anderen Prozessoren fungieren als Sicherung für die LUN und können den Zugriff auf andere LUN-E/A-Vorgänge aktiv bereitstellen. E/A-Daten können ausschließlich an einen aktiven Port gesendet werden. Falls der Zugriff über den aktiven Speicherport

fehlschlägt, kann einer der passiven Speicherprozessoren durch die Server, die auf ihn zugreifen, aktiviert werden.

### Asymmetrisches Speichersystem

Unterstützt Asymmetric Logical Unit Access (ALUA). ALUA-konforme Speichersysteme bieten verschiedene Zugriffsebenen für einzelne Ports. ALUA ermöglicht es Hosts, den Status von Zielports festzustellen und Pfade zu priorisieren. Der Host verwendet einige der aktiven Pfade als primäre Pfade, andere als sekundäre Pfade.

### Speichersystem mit virtuellem Port

Ermöglicht den Zugriff auf alle verfügbaren LUNs über einen einzigen virtuellen Port. Dies sind Aktiv/Aktiv-Speichergeräte, die jedoch die Vielzahl der Verbindungen durch einen einzigen Port verdecken. ESXi-Multipathing stellt nicht standardmäßig mehrere Verbindungen von einem bestimmten Port zu dem Speichersystem her. Einige Speicheranbieter bieten Sitzungs-Manager an, um mehrere Verbindungen zu den von ihnen vertriebenen Speichersystemen herzustellen und zu verwalten. Port-Failover und der Verbindungsausgleich werden von diesen Speichersystemen transparent verarbeitet. Dieser Vorgang wird häufig als „transparentes Failover“ bezeichnet.

## Erkennung, Authentifizierung und Zugriffssteuerung

Sie können mehrere Mechanismen verwenden, um Ihren Speicher zu erkennen und den Zugriff darauf zu beschränken.

Damit die Richtlinie für die Speicherzugriffssteuerung unterstützt wird, müssen Sie den Host und das iSCSI-Speichersystem konfigurieren.

### Erkennung

Eine Erkennungssitzung ist Teil des iSCSI-Protokolls und gibt die auf einem iSCSI-Speichersystem verfügbaren Ziele zurück. ESXi bietet zwei verschiedene Erkennungsmethoden: dynamisch und statisch. Bei der dynamischen Erkennung wird eine Liste der verfügbaren Ziele aus dem iSCSI-Speichersystem abgerufen, wohingegen Sie bei der statischen Erkennung lediglich versuchen können, über den Zielnamen und die Adresse auf ein bestimmtes Ziel zuzugreifen.

Weitere Informationen finden Sie unter [Konfigurieren von Erkennungsadressen für iSCSI-Adapter](#).

### Authentifizierung

Die Authentifizierung durch iSCSI-Speichersysteme erfolgt nach Name und Schlüsselpaar. ESXi unterstützt das CHAP-Protokoll, das VMware für die SAN-Implementierung empfiehlt. Sowohl für den ESXi-Host als auch für das iSCSI-Speichersystem muss das CHAP-Protokoll aktiviert sein und beide müssen die gleichen Anmeldeinformationen verwenden, um die CHAP-Authentifizierung verwenden zu können.

Informationen zum Aktivieren von CHAP finden Sie unter [Konfigurieren von CHAP-Parametern für iSCSI-Adapter](#).

## Zugriffssteuerung

Zugriffssteuerung ist eine auf dem iSCSI-Speichersystem eingerichtete Richtlinie. Eine Vielzahl der Implementierungen unterstützen mindestens eine der drei folgenden Arten der Zugriffssteuerung:

- Nach Initiatorname
- Nach IP-Adresse
- Nach dem CHAP-Protokoll

Nur Initiatoren, die alle Richtlinien einhalten, können auf das iSCSI-Volume zugreifen.

Die ausschließliche Verwendung von CHAP für die Zugriffssteuerung kann zu einer Verlangsamung von erneuten Prüfungen führen, da ESXi zwar alle Ziele ermitteln kann, aber bei der Authentifizierung fehlschlägt. iSCSI kann schneller neu prüfen, wenn der Host nur die Ziele ermittelt, die er authentifizieren kann.

## Fehlerkorrektur

Um die Integrität von iSCSI-Headern und -Daten zu schützen, legt das iSCSI-Protokoll Methoden zur Fehlerkorrektur fest, die als Header- und Daten-Digests bezeichnet werden.

Beide Parameter sind standardmäßig deaktiviert, können aber von Benutzern aktiviert werden. Diese Digests beziehen sich auf den Header bzw. die SCSI-Daten, die zwischen iSCSI-Initiatoren und Zielen in beiden Richtungen übertragen werden.

Header- und Daten-Digests überprüfen die durchgängige Integrität unverschlüsselter Daten. Diese Prüfung geht über die Integritätsprüfungen hinaus, die andere Netzwerkebenen bereitstellen (z.B. TCP und Ethernet). Header- und Daten-Digests prüfen den gesamten Kommunikationspfad mit allen Elementen, die den Datenverkehr auf Netzwerkebene ändern können, wie Router, Switches und Proxys.

Die Bereitstellung und Art dieser Digests wird verhandelt, sobald eine iSCSI-Verbindung aufgebaut wird. Wenn der Initiator und das Ziel einer Digest-Konfiguration zustimmen, muss dieses Digest für den gesamten Datenverkehr zwischen diesem Initiator und dem Ziel verwendet werden.

Die Aktivierung von Header- und Daten-Digests erfordert eine zusätzliche Verarbeitung durch den Initiator und das Ziel, was zu einer Beeinträchtigung des Durchsatzes und der CPU-Leistung führen kann.

---

**Hinweis** Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen aus und reduzieren damit die Auswirkungen auf die Leistung.

---

Weitere Informationen zum Aktivieren von Header-Digests und Daten-Digests finden Sie unter [Konfigurieren erweiterter Parameter für iSCSI](#).

## Zugriff auf Daten in einem iSCSI-SAN durch virtuelle Maschinen

ESXi speichert Festplattendateien einer virtuellen Maschine in einem VMFS-Datenspeicher, der sich auf einem SAN-Speichergerät befindet. Sobald Gastbetriebssysteme der virtuellen Maschine SCSI-Befehle an die virtuellen Festplatten senden, übersetzt die SCSI-Virtualisierungsebene diese Befehle in VMFS-Dateivorgänge.

Wenn eine virtuelle Maschine mit seinen auf einem SAN gespeicherten virtuellen Festplatten interagiert, finden die folgenden Prozesse statt:

- 1 Wenn das Gastbetriebssystem in einer virtuellen Maschine zum Lesen oder Schreiben auf eine SCSI-Festplatte zugreifen muss, sendet dieses SCSI-Befehle an die virtuelle Festplatte.
- 2 Gerätetreiber im Betriebssystem der virtuellen Maschine kommunizieren mit den virtuellen SCSI-Controllern.
- 3 Der virtuelle SCSI-Controller leitet den Befehl an den VMkernel weiter.
- 4 Der VMkernel führt die folgenden Aufgaben aus.
  - a Sucht die Datei, die der Festplatte der virtuellen Gastmaschine entspricht, im VMFS-Volume.
  - b ordnet die Anforderungen für die Blöcke auf der virtuellen Festplatte den Blöcken auf dem entsprechenden physischen Gerät zu.
  - c sendet die geänderte E/A-Anforderung vom Gerätetreiber im VMkernel an den iSCSI-Initiator (Hardware oder Software).
- 5 Handelt es sich bei dem iSCSI-Initiator um einen Hardware-iSCSI-Adapter (unabhängig oder abhängig), führt der Adapter die folgenden Aufgaben aus.
  - a kapselt die E/A-Anforderungen in iSCSI-PDUs (Protocol Data Units).
  - b kapselt iSCSI-PDUs in TCP/IP-Pakete.
  - c sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.
- 6 Handelt es sich bei dem iSCSI-Initiator um einen Software-iSCSI-Adapter, findet der folgende Prozess statt.
  - a Der iSCSI-Initiator kapselt E/A-Anforderungen in iSCSI-PDUs.
  - b Der Initiator sendet SCSI-PDUs über TCP/IP-Verbindungen.
  - c Der VMkernel-TCP/IP-Stack gibt TCP/IP-Pakete an eine physische Netzwerkkarte weiter.
  - d Die physische Netzwerkkarte sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.
- 7 Abhängig davon, welchen Port der iSCSI-Initiator für die Verbindung zum Netzwerk verwendet, übermitteln Ethernet-Switches und Router die Anforderung an das Speichergerät, auf das der Host zugreifen möchte.



# Konfigurieren von iSCSI-Adaptern und -Speichern

# 10

Bevor Sie ESXi in einem SAN verwenden können, müssen Sie die iSCSI-Adapter und -Speicher installieren.

Hierzu müssen Sie zunächst bestimmte Grundanforderungen und dann die die Best Practices zum Installieren und Einrichten von Hardware- oder Software-iSCSI-Adaptern beachten, um auf das SAN zuzugreifen.

In der folgenden Tabelle werden die iSCSI-Adapter (vmhbas) aufgelistet, die ESXi unterstützt. Zudem wird angegeben, ob eine Netzwerkkonfiguration des VMkernels erforderlich ist.

**Tabelle 10-1. Unterstützte iSCSI-Adapter**

iSCSI-Adapter (vmhba)	Beschreibung	VMkernel-Netzwerk
Software	Verwendet Standardnetzwerkkarten, um Ihren Host mit einem Remote-iSCSI-Ziel auf dem IP-Netzwerk zu verbinden.	Erforderlich
Unabhängige Hardware	Adapter eines Drittanbieters, der die iSCSI- und Netzwerk-Verarbeitung und -Verwaltung vom Host verlagert.	Nicht erforderlich
Abhängige Hardware	Adapter eines Drittanbieters, der vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen abhängt.	Erforderlich

Nach dem Einrichten der iSCSI-Adapter können Sie einen Datenspeicher auf dem iSCSI-Speicher erstellen. Weitere Informationen zum Erstellen und Verwalten von Datenspeichern finden Sie unter [Erstellen von Datenspeichern](#).

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen an ESXi-iSCSI-SAN](#)
- [Einschränkungen bei ESXi-iSCSI-SAN](#)
- [Festlegen der LUN-Zuordnungen für iSCSI](#)
- [Netzwerkkonfiguration und Authentifizierung](#)
- [Einrichten von unabhängigen Hardware-iSCSI-Adaptern](#)
- [Informationen zu abhängigen Hardware-iSCSI-Adaptern](#)

- Informationen zum Software-iSCSI-Adapter
- Ändern der allgemeinen Eigenschaften für iSCSI-Adapter
- Einrichten des iSCSI-Netzwerks
- Verwenden von Jumbo-Frames mit iSCSI
- Konfigurieren von Erkennungsadressen für iSCSI-Adapter
- Konfigurieren von CHAP-Parametern für iSCSI-Adapter
- Konfigurieren erweiterter Parameter für iSCSI
- iSCSI-Sitzungsverwaltung

## Anforderungen an ESXi-iSCSI-SAN

Vor der ordnungsgemäßen Verwendung eines ESXi-Hosts mit einem SAN müssen bestimmte Anforderungen erfüllt sein.

- Stellen Sie sicher, dass die Hardware- und Firmware-Kombinationen für Ihren SAN-Speicher in Verbindung mit ESXi-Systemen unterstützt werden. Eine aktuelle Liste finden Sie unter *VMware-Kompatibilitätshandbuch*.
- Konfigurieren Sie Ihr System so, dass nur ein VMFS-Datenspeicher für jede LUN vorhanden ist.
- Sofern Sie keine festplattenlosen Server einsetzen, richten Sie eine Diagnose-Partition auf einem lokalen Speicher ein. Wenn Sie über festplattenlose Server verfügen, die von einem iSCSI-SAN gestartet werden, finden Sie weitere Informationen über Diagnosepartitionen mit iSCSI unter [Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN](#).
- Verwenden Sie RDMS für den Zugriff auf eine beliebige Raw-Festplatte. Weitere Informationen hierzu finden Sie unter [Kapitel 18 Raw-Gerätezuordnung](#).
- Installieren Sie den SCSI Controller-Treiber im Gastbetriebssystem, damit Sie eine ausreichende Größe der Warteschlange festlegen können. Weitere Informationen über das Ändern der Warteschlangentiefe für iSCSI-Adapter und virtuelle Maschinen finden Sie unter *vSphere-Fehlerbehebung*.
- Erhöhen Sie den Wert des SCSI-Parameters `TimeoutValue` für virtuelle Maschinen, auf denen Microsoft Windows ausgeführt wird, damit Windows aus Pfad-Failover resultierende E/A-Verzögerungen besser toleriert. Weitere Informationen hierzu finden Sie unter [Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen](#).

## Einschränkungen bei ESXi-iSCSI-SAN

Bei der Verwendung von ESXi mit einem iSCSI-SAN gelten einige Einschränkungen.

- ESXi unterstützt keine über iSCSI verbundenen Bandlaufwerke.

- Sie können keine Multipathing-Software für virtuelle Maschinen verwenden, um einen E/A-Lastausgleich für eine einzelne physische LUN durchzuführen.
- ESXi unterstützt kein Multipathing, wenn Sie unabhängige Hardwareadapter mit Software- oder abhängigen Hardwareadaptern kombinieren.

## Festlegen der LUN-Zuordnungen für iSCSI

Wenn Sie Ihr ESXi-System zur Verwendung des iSCSI SAN-Speichers vorbereiten, müssen Sie zunächst LUN-Zuordnungen vornehmen.

Beachten Sie Folgendes:

- **Speicherbereitstellung.** Damit der Host die LUNs beim Start erkennt, müssen alle iSCSI-Speicherziele so konfiguriert werden, dass Ihr Host darauf zugreifen und sie verwenden kann. Konfigurieren Sie Ihren Host auch in der Weise, dass er alle verfügbaren iSCSI-Ziele erkennen kann.
- **vMotion und VMware DRS.** Wenn Sie vCenter Server und vMotion oder DRS verwenden, sollten Sie sicherstellen, dass die LUNs für die virtuellen Maschinen allen Hosts bereitgestellt werden. Diese Konfiguration bietet die höchste Flexibilität beim Verschieben virtueller Maschinen.
- **Aktiv/Aktiv-** im Vergleich zu Aktiv/Passiv-Arrays. Bei der Verwendung von vMotion oder DRS mit einem SAN-Speichergerät vom Typ „Aktiv/Passiv“ sollten Sie sicherstellen, dass alle Hosts über einheitliche Pfade zu allen Speicherprozessoren verfügen. Anderenfalls kann es bei vMotion-Migrationen zu einem Pfad-Thrashing kommen.

Für Aktiv/Passiv-Speicher-Arrays, die in der Speicher-/SAN-Kompatibilität nicht aufgelistet sind, werden keine Speicherport-Failover von VMware unterstützt. Sie müssen den Server am aktiven Port des Speichersystems anschließen. Durch diese Konfiguration wird sichergestellt, dass die LUNs dem Host angezeigt werden.

## Netzwerkkonfiguration und Authentifizierung

Bevor Ihr ESXi-Host den iSCSI-Speicher erkennen kann, müssen die iSCSI-Initiatoren konfiguriert werden. Möglicherweise muss auch die Authentifizierung eingerichtet werden.

- Für Software- und abhängiges Hardware-iSCSI muss die Vernetzung für den VMkernel konfiguriert werden. Mit dem Dienstprogramm `vmkping` können Sie die Netzwerkkonfiguration überprüfen. Bei Software-iSCSI und abhängigem iSCSI werden IPv4- und IPv6-Protokolle unterstützt.
- Für den Einsatz von unabhängigem Hardware-iSCSI müssen auf dem HBA Netzwerkparameter wie IP-Adresse, Subnetzmaske und Standard-Gateway konfiguriert werden. Sie können außerdem ein Netzwerkprotokoll, IPv4 oder IPv6, für den Adapter angeben.
- Überprüfen und ändern Sie ggf. den standardmäßigen Initiator-Namen.

- Die Adresse der dynamischen oder der statischen Erkennung und der Zielname des Speichersystems müssen festgelegt sein. Für Software- und abhängiges Hardware-iSCSI muss die Adresse mithilfe von `vmkping` angepingt werden können.
- Um die CHAP-Authentifizierung zu verwenden, aktivieren Sie diese auf Seiten des Initiators und des Speichersystems. Nach dem Aktivieren der Authentifizierung gilt diese ausschließlich für alle Ziele, die noch nicht erkannt wurden (nicht aber für bereits erkannte Ziele). Wurde schließlich die Erkennungsadresse festgelegt, werden die neu erkannten Ziele angezeigt und können verwendet werden.

Weitere Informationen zur Verwendung des Befehls `vmkping` finden Sie in der VMware-Knowledgebase.

## Einrichten von unabhängigen Hardware-iSCSI-Adaptern

Ein unabhängiger Hardware-iSCSI-Adapter ist ein spezielle Adapter von Drittanbietern, die über TCP/IP auf iSCSI-Speicher zugreifen kann. Dieser iSCSI-Adapter steuert die gesamte iSCSI- und Netzwerk-Verarbeitung und -Verwaltung für das ESXi-System.

### Voraussetzungen

- Prüfen Sie, ob der Adapter lizenziert werden muss.
- Installieren Sie den Adapter.

Informationen zur Lizenzierung, Installation sowie zu Firmware-Updates finden Sie in der Herstelldokumentation.

### Verfahren

#### 1 [Anzeigen abhängiger Hardware-iSCSI-Adapter](#)

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

#### 2 [Ändern der allgemeinen Eigenschaften für iSCSI-Adapter](#)

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

#### 3 [Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI](#)

Nach der Installation eines unabhängigen Hardware-iSCSI-Adapters müssen Sie möglicherweise die Standardnetzwerkeinstellungen ändern, damit der Adapter ordnungsgemäß für iSCSI SAN konfiguriert ist.

#### 4 Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

##### Nächste Schritte

Konfigurieren Sie bei Bedarf CHAP-Parameter und Jumbo-Frames.

## Anzeigen abhängiger Hardware-iSCSI-Adapter

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

Nachdem Sie einen unabhängigen Hardware-iSCSI-Adapter auf einem Host installiert haben, wird er in der Liste der Speicheradapter angezeigt, die zum Konfigurieren zur Verfügung stehen. Seine Eigenschaften können angezeigt werden.

##### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

##### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter**.

Falls installiert, sollte der Hardware-iSCSI-Adapter in der Liste der Speicheradapter angezeigt werden.

- 4 Wählen Sie die anzuzeigenden Adapter aus.

Die standardmäßigen Details für den Adapter werden angezeigt, darunter das Modell, der iSCSI-Name, iSCSI-Alias, IP-Adresse sowie Ziel- und Pfadinformationen.

## Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

---

**Wichtig** Wenn Sie Standardeigenschaften für Ihre iSCSI-Adapter ändern, achten Sie darauf, dass ihre Namen und IP-Adressen das richtige Format haben.

---

##### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften** und klicken Sie auf **Bearbeiten** im Bereich „Allgemein“.
- 5 Um den Standard-iSCSI-Namen für den Adapter zu ändern, geben Sie einen neuen Namen ein.

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

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

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

## Ergebnisse

Wenn Sie den iSCSI-Namen ändern, wird der angegebene Name für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

## Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI

Nach der Installation eines unabhängigen Hardware-iSCSI-Adapters müssen Sie möglicherweise die Standardnetzwerkeinstellungen ändern, damit der Adapter ordnungsgemäß für iSCSI SAN konfiguriert ist.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerkeinstellungen** und klicken Sie auf **Bearbeiten**.

- 5 Deaktivieren Sie „IPv6“ im Abschnitt „IPv4-Einstellungen“ oder wählen Sie die Methode zum Abrufen von IP-Adressen aus.

**Hinweis** Die automatische DHCP-Option und die statische Option schließen sich gegenseitig aus.

Option	Beschreibung
Keine IPv4-Einstellungen	Deaktivieren Sie IPv4.
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden.
Statische IPv4-Einstellungen verwenden	Geben Sie die IPv4 IP-Adresse, die Subnetzmaske und das Standard-Gateway für den iSCSI-Adapter ein.

- 6 Deaktivieren Sie „IPv6“ im Abschnitt „IPv6-Einstellungen“ oder wählen Sie eine geeignete Option zum Abrufen von IPv6-Adressen aus.

**Hinweis** Automatische Optionen und die statische Option schließen sich gegenseitig aus.

Option	Beschreibung
Keine IPv6-Einstellungen	Deaktivieren Sie IPv6.
IPv6 aktivieren	Wählen Sie eine Option zum Abrufen von IPv6-Adressen aus.
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Verbindungslokale Adresse für IPv6 überschreiben	Überschreiben Sie die Link-Local IP-Adresse durch Konfigurieren einer statischen IP-Adresse.
Statische IPv6-Adressen	<ul style="list-style-type: none"> <li>a Klicken Sie auf <b>Hinzufügen</b>, um eine neue IPv6-Adresse hinzuzufügen.</li> <li>b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf <b>OK</b>.</li> </ul>

- 7 Geben Sie im Abschnitt „DNS-Einstellungen“ IP-Adressen für einen bevorzugten DNS-Server und einen alternativen DNS-Server an.

Sie müssen beide Werte angeben.

## Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Wenn Sie die statische oder dynamische Erkennung einrichten, können Sie nur neue iSCSI-Ziele hinzufügen. Sie können keine Parameter eines vorhandenen Ziels ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie den zu konfigurierenden iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Ziele**.
- 5 Konfigurieren Sie die Erkennungsmethode.

Option	Beschreibung
<b>Dynamische Erkennung</b>	<ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Dynamische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ol> <p>Nach dem Einrichten der SendTargets-Sitzung mit dem iSCSI-System füllt Ihr Host die Liste „Statische Erkennung“ mit allen neu erkannten Zielen.</p>
<b>Statische Erkennung</b>	<ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Statische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die Daten des Ziels ein, und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ol>

## Informationen zu abhängigen Hardware-iSCSI-Adaptern

Ein abhängiger Hardware-iSCSI-Adapter ist ein Drittanbieter-Adapter, der vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen abhängt, die von VMware zur Verfügung gestellt werden.

Ein Beispiel für einen abhängigen iSCSI-Adapter ist eine Broadcom 5709-Netzwerkkarte. Wenn er auf einem Host installiert ist, präsentiert er seine beiden Komponenten, einen Standard-Netzwerkadapter und eine iSCSI-Engine, demselben Port. Die iSCSI-Engine wird als iSCSI-Adapter in der Liste der Speicheradapter (vmhba) angezeigt. Der iSCSI-Adapter ist zwar standardmäßig aktiviert. Damit er funktionsfähig ist, müssen Sie ihn jedoch zuerst über einen virtuellen VMkernel-Adapter (vmk) mit einem ihm zugeordneten physischen Netzwerkadapter (vmnic) verbinden. Anschließend können Sie den iSCSI-Adapter konfigurieren.



Nachdem Sie den abhängigen Hardware-iSCSI-Adapter konfiguriert haben, werden die Ermittlungs- und Authentifizierungsdaten über die Netzwerkverbindung geleitet, während der iSCSI-Datenverkehr unter Umgehung des Netzwerks über die iSCSI-Engine geleitet wird.

## Überlegungen zu abhängigen Hardware-iSCSI-Adapttern

Wenn Sie abhängige Hardware-iSCSI-Adapter für ESXi verwenden, muss Folgendes beachtet werden.

- Wenn Sie einen abhängigen Hardware-iSCSI-Adapter verwenden, zeigt der Leistungsbericht für eine dem Adapter zugewiesene Netzwerkkarte möglicherweise wenig oder keine Aktivität, selbst wenn eine große Menge an iSCSI-Datenverkehr vorhanden ist. Dieses Verhalten tritt auf, weil der iSCSI-Datenverkehr den regulären Netzwerkstack umgeht.
- Falls Sie einen virtuellen Switch eines Drittanbieters einsetzen, z. B. Cisco Nexus 1000V DVS, deaktivieren Sie das automatische Binden. Verwenden Sie stattdessen das manuelle Binden und stellen Sie dabei sicher, dass Sie einen VMkernel-Adapter (vmk) mit einer entsprechenden physischen Netzwerkkarte (vmnic) verbinden. Weitere Informationen finden Sie in der Herstellerdokumentation zu Ihrem virtuellen Switch.
- Der Broadcom iSCSI-Adapter führt eine Datenumwandlung in Hardware mit begrenztem Pufferspeicher durch. Wenn Sie den Broadcom iSCSI-Adapter in einem ausgelasteten oder überlasteten Netzwerk verwenden, aktivieren Sie die Flusssteuerung, damit die Leistung nicht beeinträchtigt wird.

Die Flusssteuerung überwacht die Datenübertragungsrate zwischen zwei Knoten und verhindert, dass ein langsamer Empfänger von einem schnellen Sender überrannt wird. Um optimale Ergebnisse zu erzielen, aktivieren Sie die Flusssteuerung an den Endpunkten des E/A-Pfads, d. h. auf den Hosts und den iSCSI-Speichersystemen.

Verwenden Sie den Befehl `esxcli system module parameters`, um die Flusskontrolle für den Host zu aktivieren. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1013413>.

- Abhängige Hardware-Adapter unterstützen IPv4 und IPv6.

## Konfigurieren von abhängigen Hardware-iSCSI-Adapttern

Der gesamte Installations- und Konfigurationsprozess für die abhängigen Hardware-iSCSI-Adapter besteht aus mehreren Schritten. Nach dem Einrichten des Adapters müssen Sie möglicherweise CHAP-Parameter und Jumbo-Frames konfigurieren.

### Verfahren

#### 1 Abhängige Hardware-iSCSI-Adapter anzeigen

Zeigen Sie einen abhängigen Hardware-iSCSI-Adapter an, um zu überprüfen, ob er korrekt geladen ist.

## 2 Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

## 3 Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern

Netzwerkverbindungen dienen dazu, abhängige iSCSI- und physische Netzwerkadapter zu binden. Um die Verbindungen ordnungsgemäß zu erstellen, müssen Sie den Namen der physischen Netzwerkkarte ermitteln, der der abhängige Hardware-iSCSI-Adapter zugewiesen werden soll.

## 4 Erstellen von Netzwerkverbindungen für iSCSI

Konfigurieren Sie Verbindungen für den Datenverkehr zwischen den Software- oder den abhängigen Hardware-iSCSI-Adaptern und den physischen Netzwerkadaptern.

## 5 Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

### Nächste Schritte

Konfigurieren Sie bei Bedarf CHAP-Parameter und Jumbo-Frames.

## Abhängige Hardware-iSCSI-Adapter anzeigen

Zeigen Sie einen abhängigen Hardware-iSCSI-Adapter an, um zu überprüfen, ob er korrekt geladen ist.

Der abhängige Hardware-iSCSI-Adapter (vmhba#) wird, wenn er installiert ist, in der Liste der Speicheradapter unter Kategorien wie z. B. „Broadcom iSCSI Adapter“ angezeigt. Falls der abhängige Hardware-Adapter nicht in der Liste der Speicheradapter angezeigt wird, überprüfen Sie, ob er lizenziert werden muss. Informationen finden Sie in der Dokumentation des Anbieters.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter**.
- 4 Wählen Sie die anzuzeigenden Adapter (vmhba#) aus.

Es werden die standardmäßigen Detailinformationen zu dem Adapter angezeigt, etwa iSCSI-Namen, iSCSI-Alias und Status.

## Nächste Schritte

Obwohl der abhängige iSCSI-Adapter standardmäßig aktiviert ist, müssen Sie, damit er funktionsbereit ist, eine Vernetzung für den iSCSI-Datenverkehr einrichten und den Adapter an den entsprechenden VMkernel-iSCSI-Port binden. Konfigurieren Sie dann die Erkennungsadressen und die CHAP-Parameter.

## Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

---

**Wichtig** Wenn Sie Standardeigenschaften für Ihre iSCSI-Adapter ändern, achten Sie darauf, dass ihre Namen und IP-Adressen das richtige Format haben.

---

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften** und klicken Sie auf **Bearbeiten** im Bereich „Allgemein“.
- 5 Um den Standard-iSCSI-Namen für den Adapter zu ändern, geben Sie einen neuen Namen ein.

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

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

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

### Ergebnisse

Wenn Sie den iSCSI-Namen ändern, wird der angegebene Name für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

## Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern

Netzwerkverbindungen dienen dazu, abhängige iSCSI- und physische Netzwerkadapter zu binden. Um die Verbindungen ordnungsgemäß zu erstellen, müssen Sie den Namen der

physischen Netzwerkkarte ermitteln, der der abhängige Hardware-iSCSI-Adapter zugewiesen werden soll.

### Voraussetzungen

Navigieren Sie im vSphere Web Client zum abhängigen Hardware-iSCSI-Adapter (vmhba#). Siehe [Abhängige Hardware-iSCSI-Adapter anzeigen](#).

### Verfahren

- 1 Wählen Sie den iSCSI-Adapter (vmhba#) aus und klicken Sie auf die Registerkarte **Netzwerk-Port-Bindung** unter „Adapterdetails“.
- 2 Klicken Sie auf **Hinzufügen**.

Der Netzwerkadapter (vmnic#), der dem abhängigen iSCSI-Adapter zugeordnet ist, wird in der Spalte „Physischer Netzwerkadapter“ aufgeführt.

### Nächste Schritte

Wenn die Spalte „VMkernel-Adapter“ leer ist, erstellen Sie einen VMkernel-Adapter (vmk#) für den physischen Netzwerkadapter (vmnic#) und binden Sie beide an den zugewiesenen abhängigen Hardware-iSCSI. Siehe [Einrichten des iSCSI-Netzwerks](#).

## Erstellen von Netzwerkverbindungen für iSCSI

Konfigurieren Sie Verbindungen für den Datenverkehr zwischen den Software- oder den abhängigen Hardware-iSCSI-Adaptoren und den physischen Netzwerkadaptern.

Die folgenden Aufgaben beschreiben die iSCSI-Netzwerkkonfiguration mit einem vSphere Standard-Switch.

Wenn Sie einen vSphere Distributed Switch mit mehreren Uplink-Ports für die Port-Bindung verwenden, erstellen Sie für jede physische Netzwerkkarte eine separate verteilte Portgruppe. Legen Sie anschließend die Teamrichtlinie so fest, dass jede verteilte Portgruppe nur einen aktiven Uplink-Port besitzt. Weitere Informationen zu vSphere Distributed Switches finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

### Verfahren

- 1 [Erstellen eines einzelnen VMkernel-Adapters für iSCSI](#)

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

- 2 [Erstellen zusätzlicher VMkernel-Adapter für iSCSI](#)

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkadapter für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

### 3 Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

### 4 Binden von iSCSI- und VMkernel-Adaptoren

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

### 5 Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Erstellen eines einzelnen VMkernel-Adapters für iSCSI

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.
- 3 Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.
- 5 Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie den Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.

Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.

---

**Wichtig** Wenn Sie einen VMkernel-Adapter für den abhängigen Hardware-iSCSI-Adapter erstellen, wählen Sie den Netzwerkadapter aus, der zu der iSCSI-Komponente gehört. Siehe [Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern](#).

---

- 6 Geben Sie eine Netzwerkbezeichnung ein.

Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. iSCSI.

- 7 Geben Sie die IP-Einstellungen an.
- 8 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

### Ergebnisse

Sie haben den virtuellen VMkernel-Adapter (vmk#) für einen physischen Netzwerkadapter (vmnic#) auf Ihrem Host erstellt.

### Nächste Schritte

Wenn Ihr Host über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügt, müssen Sie den virtuellen Adapter, den Sie erstellt haben, an den iSCSI-Adapter binden.

Wenn Sie über mehrere Netzwerkkadaper verfügen, erstellen Sie zusätzliche VMkernel-Adapter und führen Sie dann die iSCSI-Bindung durch. Die Anzahl an virtuellen Adaptern muss mit der Anzahl an physischen Adaptern auf dem Host übereinstimmen.

### Erstellen zusätzlicher VMkernel-Adapter für iSCSI

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkkadaper für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

#### Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der einen VMkernel-iSCSI-Adapter einem einzelnen physischen Netzwerkkadaper zuordnet, der für den iSCSI-Datenverkehr vorgesehen ist.

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
- 4 Verbinden Sie zusätzliche Netzwerkkadaper mit dem Switch.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **Physische Netzwerkkadaper** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie mindestens einen Netzwerkkadaper (vmnic#) aus, den Sie für iSCSI verwenden möchten.  
  
Wählen Sie für abhängige Hardware-iSCSI-Adapter nur die Netzwerkkarten aus, die eine entsprechende iSCSI-Komponente besitzen.
  - e Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.
- 5 Erstellen Sie iSCSI-VMkernel-Adapter für alle hinzugefügten physischen Netzwerkkadaper.  
  
Die Anzahl an VMkernel-Schnittstellen muss mit der Anzahl an physischen Netzwerkkadapern auf dem vSphere Standard-Switch übereinstimmen.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **VMkernel-Netzwerkkadaper** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.

## Nächste Schritte

Ändern Sie die Netzwerkrichtlinie für alle VMkernel-Adapter dahin gehend, dass pro VMkernel-Adapter nur ein physischer Netzwerkadapter aktiv ist. Sie können dann die iSCSI-VMkernel-Adapter an die Software-iSCSI- oder an die abhängigen Hardware-iSCSI-Adapter binden.

## Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

Standardmäßig werden für jeden VMkernel-Adapter auf dem vSphere Standard-Switch alle Netzwerkadapter als aktiv angezeigt. Sie müssen dieses Setup überschreiben, damit jeder VMkernel-Adapter lediglich einer aktiven physischen Netzwerkkarte zugeordnet wird. Beispielsweise wird „vmk1“ der Netzwerkkarte „vmnic1“ zugeordnet, „vmk2“ wird „vmnic2“ zugeordnet usw.

## Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der VMkernel mit physischen Netzwerkadaptern verbindet, die für den iSCSI-Datenverkehr vorgesehen sind. Die Anzahl an VMkernel-Adaptern muss mit der Anzahl an physischen Adaptern auf dem vSphere Standard-Switch übereinstimmen.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
- 4 Wählen Sie auf dem vSwitch-Diagramm den VMkernel-Adapter aus und klicken Sie auf das Symbol **Einstellungen bearbeiten**.
- 5 Klicken Sie im Assistenten **Einstellungen bearbeiten** auf **Teaming und Failover** und klicken Sie unter „Failover-Reihenfolge“ auf **Außer Kraft setzen**.
- 6 Wählen Sie nur einen physischen Adapter als aktiv aus und verschieben Sie alle übrigen Adapter in die Kategorie **Nicht verwendete Adapter**.
- 7 Wiederholen Sie [Schritt 4](#) bis [Schritt 6](#) für jede iSCSI-VMkernel-Schnittstelle auf dem vSphere Standard-Switch.

## Beispiel: iSCSI-Netzwerkrichtlinie

Die folgende Tabelle illustriert die ordnungsgemäße iSCSI-Zuordnung, bei der nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

VMkernel-Adapter (vmk#)	Physischer Netzwerkadapter (vmnic#)
vmk1	<b>Aktive Adapter</b> vmnic1
	<b>Nicht verwendete Adapter</b> vmnic2
vmk2	<b>Aktive Adapter</b> vmnic2
	<b>Nicht verwendete Adapter</b> vmnic1

### Nächste Schritte

Binden Sie nach dem Ausführen dieser Aufgabe die virtuellen VMkernel-Adapter an die Software-iSCSI- oder abhängigen Hardware-iSCSI-Adapter.

### Binden von iSCSI- und VMkernel-Adapttern

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

### Voraussetzungen

Erstellen Sie einen virtuellen VMkernel-Adapter für jeden physischen Netzwerkadapter auf Ihrem Host. Wenn Sie mehrere VMkernel-Adapter verwenden, richten Sie die korrekte Netzwerkrichtlinie ein.

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter** und wählen Sie die zu konfigurierende Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung** und klicken Sie dann auf **Hinzufügen**.
- 5 Wählen Sie einen VMkernel-Adapter zur Bindung mit dem iSCSI-Adapter aus.

**Hinweis** Stellen Sie sicher, dass die Netzwerkrichtlinie für den VMkernel-Adapter die Anforderungen für das Binden erfüllt.

Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter ist nur ein VMkernel-Adapter verfügbar, der mit der richtigen physischen Netzwerkkarte verknüpft ist.

- 6 Klicken Sie auf **OK**.



## Ergebnisse

Die Netzwerkverbindung wird in der Liste der VMkernel-Portbindungen für den iSCSI-Adapter angezeigt.

## Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie die Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung**, und klicken Sie auf **Detailansicht**.
- 5 Prüfen Sie die VMkernelAdapterinformationen durch das Wechseln zwischen verfügbaren Registerkarten.

## Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Wenn Sie die statische oder dynamische Erkennung einrichten, können Sie nur neue iSCSI-Ziele hinzufügen. Sie können keine Parameter eines vorhandenen Ziels ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

## Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie den zu konfigurierenden iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Ziele**.

## 5 Konfigurieren Sie die Erkennungsmethode.

Option	Beschreibung
<b>Dynamische Erkennung</b>	<ul style="list-style-type: none"> <li>a Klicken Sie auf <b>Dynamische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ul> <p>Nach dem Einrichten der SendTargets-Sitzung mit dem iSCSI-System füllt Ihr Host die Liste „Statische Erkennung“ mit allen neu erkannten Zielen.</p>
<b>Statische Erkennung</b>	<ul style="list-style-type: none"> <li>a Klicken Sie auf <b>Statische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die Daten des Ziels ein, und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ul>

## Informationen zum Software-iSCSI-Adapter

Bei der softwarebasierten iSCSI-Implementierung können Sie Standard-Netzwerkkarten verwenden, um Ihren Host mit einem externen iSCSI-Ziel im IP-Netzwerk zu verbinden. Der in ESXi integrierte Software-iSCSI-Adapter ermöglicht diese Verbindung, indem er über den Netzwerkstapel mit den physischen Netzwerkkarten kommuniziert.

Bevor Sie den Software-iSCSI-Adapter verwenden können, müssen Sie ein Netzwerk einrichten, den Adapter aktivieren und Parameter, wie z. B. Erkennungsadressen und CHAP, konfigurieren.

**Hinweis** Legen Sie einen separaten Netzwerkkartenadapter für iSCSI fest. Verwenden Sie iSCSI nicht bei Adaptern mit 100 MBit/s oder weniger.

## Konfigurieren des Software-iSCSI-Adapters

Der Workflow zur Konfiguration des Software-iSCSI-Adapters umfasst die folgenden Schritte.

### Verfahren

#### 1 Aktivieren des Software-iSCSI-Adapters

Sie müssen Ihren Software-iSCSI-Adapter aktivieren, damit er von Ihrem Host für den Zugriff auf den iSCSI-Speicher verwendet werden kann.

#### 2 Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptoren zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

#### 3 Erstellen von Netzwerkverbindungen für iSCSI

Konfigurieren Sie Verbindungen für den Datenverkehr zwischen den Software- oder den abhängigen Hardware-iSCSI-Adaptoren und den physischen Netzwerkkarten.

#### 4 Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

##### Nächste Schritte

Konfigurieren Sie bei Bedarf CHAP-Parameter und Jumbo-Frames.

#### Aktivieren des Software-iSCSI-Adapters

Sie müssen Ihren Software-iSCSI-Adapter aktivieren, damit er von Ihrem Host für den Zugriff auf den iSCSI-Speicher verwendet werden kann.

Sie können nur einen Software-iSCSI-Adapter aktivieren.

##### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

---

**Hinweis** Wenn Sie von iSCSI mithilfe des Software-iSCSI-Adapters starten, wird der Adapter aktiviert und die Netzwerkkonfiguration wird beim ersten Boot-Vorgang erstellt. Wenn Sie den Adapter deaktivieren, wird er bei jedem Neustart des Hosts erneut aktiviert.

---

##### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und anschließend auf das Symbol **Hinzufügen** (+).
- 4 Wählen Sie **Software-iSCSI-Adapter** aus und bestätigen Sie, dass Sie den Adapter hinzufügen möchten.

##### Ergebnisse

Der Software-iSCSI-Adapter (vmhba#) wird aktiviert und erscheint in der Liste der Speicheradapter. Nachdem Sie den Adapter aktiviert haben, weist ihm der Host den Standard-iSCSI-Namen zu. Falls Sie den Standardnamen ändern müssen, befolgen Sie die iSCSI-Namenskonventionen.

##### Nächste Schritte

Wählen Sie den Adapter aus und verwenden Sie zum Konfigurieren den Abschnitt „Adapterdetails“.

## Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

---

**Wichtig** Wenn Sie Standardeigenschaften für Ihre iSCSI-Adapter ändern, achten Sie darauf, dass ihre Namen und IP-Adressen das richtige Format haben.

---

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften** und klicken Sie auf **Bearbeiten** im Bereich „Allgemein“.
- 5 Um den Standard-iSCSI-Namen für den Adapter zu ändern, geben Sie einen neuen Namen ein.

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

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

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

### Ergebnisse

Wenn Sie den iSCSI-Namen ändern, wird der angegebene Name für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

## Erstellen von Netzwerkverbindungen für iSCSI

Konfigurieren Sie Verbindungen für den Datenverkehr zwischen den Software- oder den abhängigen Hardware-iSCSI-Adaptern und den physischen Netzwerkadaptern.

Die folgenden Aufgaben beschreiben die iSCSI-Netzwerkkonfiguration mit einem vSphere Standard-Switch.

Wenn Sie einen vSphere Distributed Switch mit mehreren Uplink-Ports für die Port-Bindung verwenden, erstellen Sie für jede physische Netzwerkkarte eine separate verteilte Portgruppe. Legen Sie anschließend die Teamrichtlinie so fest, dass jede verteilte Portgruppe nur einen aktiven Uplink-Port besitzt. Weitere Informationen zu vSphere Distributed Switches finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

## Verfahren

### 1 Erstellen eines einzelnen VMkernel-Adapters für iSCSI

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

### 2 Erstellen zusätzlicher VMkernel-Adapter für iSCSI

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkadapter für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

### 3 Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

### 4 Binden von iSCSI- und VMkernel-Adapttern

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

### 5 Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Erstellen eines einzelnen VMkernel-Adapters für iSCSI

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.
- 3 Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.

- 5 Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie den Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.

Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.

---

**Wichtig** Wenn Sie einen VMkernel-Adapter für den abhängigen Hardware-iSCSI-Adapter erstellen, wählen Sie den Netzwerkadapter aus, der zu der iSCSI-Komponente gehört. Siehe [Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern](#).

---

- 6 Geben Sie eine Netzwerkbezeichnung ein.

Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. iSCSI.

- 7 Geben Sie die IP-Einstellungen an.

- 8 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

### Ergebnisse

Sie haben den virtuellen VMkernel-Adapter (vmk#) für einen physischen Netzwerkadapter (vmnic#) auf Ihrem Host erstellt.

### Nächste Schritte

Wenn Ihr Host über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügt, müssen Sie den virtuellen Adapter, den Sie erstellt haben, an den iSCSI-Adapter binden.

Wenn Sie über mehrere Netzwerkadapter verfügen, erstellen Sie zusätzliche VMkernel-Adapter und führen Sie dann die iSCSI-Bindung durch. Die Anzahl an virtuellen Adaptern muss mit der Anzahl an physischen Adaptern auf dem Host übereinstimmen.

### Erstellen zusätzlicher VMkernel-Adapter für iSCSI

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkadapter für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

### Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der einen VMkernel-iSCSI-Adapter einem einzelnen physischen Netzwerkadapter zuordnet, der für den iSCSI-Datenverkehr vorgesehen ist.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.

- 4 Verbinden Sie zusätzliche Netzwerkadapter mit dem Switch.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **Physische Netzwerkadapter** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie mindestens einen Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.  
  
Wählen Sie für abhängige Hardware-iSCSI-Adapter nur die Netzwerkkarten aus, die eine entsprechende iSCSI-Komponente besitzen.
  - e Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.
- 5 Erstellen Sie iSCSI-VMkernel-Adapter für alle hinzugefügten physischen Netzwerkadapter.  
  
Die Anzahl an VMkernel-Schnittstellen muss mit der Anzahl an physischen Netzwerkadaptern auf dem vSphere Standard-Switch übereinstimmen.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.

#### Nächste Schritte

Ändern Sie die Netzwerkrichtlinie für alle VMkernel-Adapter dahin gehend, dass pro VMkernel-Adapter nur ein physischer Netzwerkadapter aktiv ist. Sie können dann die iSCSI-VMkernel-Adapter an die Software-iSCSI- oder an die abhängigen Hardware-iSCSI-Adapter binden.

#### Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

Standardmäßig werden für jeden VMkernel-Adapter auf dem vSphere Standard-Switch alle Netzwerkadapter als aktiv angezeigt. Sie müssen dieses Setup überschreiben, damit jeder VMkernel-Adapter lediglich einer aktiven physischen Netzwerkkarte zugeordnet wird. Beispielsweise wird „vmk1“ der Netzwerkkarte „vmnic1“ zugeordnet, „vmk2“ wird „vmnic2“ zugeordnet usw.

#### Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der VMkernel mit physischen Netzwerkadaptern verbindet, die für den iSCSI-Datenverkehr vorgesehen sind. Die Anzahl an VMkernel-Adaptern muss mit der Anzahl an physischen Adaptern auf dem vSphere Standard-Switch übereinstimmen.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
- 4 Wählen Sie auf dem vSwitch-Diagramm den VMkernel-Adapter aus und klicken Sie auf das Symbol **Einstellungen bearbeiten**.
- 5 Klicken Sie im Assistenten **Einstellungen bearbeiten** auf **Teaming und Failover** und klicken Sie unter „Failover-Reihenfolge“ auf **Außer Kraft setzen**.
- 6 Wählen Sie nur einen physischen Adapter als aktiv aus und verschieben Sie alle übrigen Adapter in die Kategorie **Nicht verwendete Adapter**.
- 7 Wiederholen Sie [Schritt 4](#) bis [Schritt 6](#) für jede iSCSI-VMkernel-Schnittstelle auf dem vSphere Standard-Switch.

## Beispiel: iSCSI-Netzwerkrichtlinie

Die folgende Tabelle illustriert die ordnungsgemäße iSCSI-Zuordnung, bei der nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

VMkernel-Adapter (vmk#)	Physischer Netzwerkadapter (vmnic#)
vmk1	<b>Aktive Adapter</b> vmnic1
	<b>Nicht verwendete Adapter</b> vmnic2
vmk2	<b>Aktive Adapter</b> vmnic2
	<b>Nicht verwendete Adapter</b> vmnic1

## Nächste Schritte

Binden Sie nach dem Ausführen dieser Aufgabe die virtuellen VMkernel-Adapter an die Software-iSCSI- oder abhängigen Hardware-iSCSI-Adapter.

## Binden von iSCSI- und VMkernel-Adaptoren

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

## Voraussetzungen

Erstellen Sie einen virtuellen VMkernel-Adapter für jeden physischen Netzwerkadapter auf Ihrem Host. Wenn Sie mehrere VMkernel-Adapter verwenden, richten Sie die korrekte Netzwerkrichtlinie ein.

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**



## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter** und wählen Sie die zu konfigurierende Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung** und klicken Sie dann auf **Hinzufügen**.
- 5 Wählen Sie einen VMkernel-Adapter zur Bindung mit dem iSCSI-Adapter aus.

---

**Hinweis** Stellen Sie sicher, dass die Netzwerkrichtlinie für den VMkernel-Adapter die Anforderungen für das Binden erfüllt.

---

Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter ist nur ein VMkernel-Adapter verfügbar, der mit der richtigen physischen Netzwerkkarte verknüpft ist.

- 6 Klicken Sie auf **OK**.

## Ergebnisse

Die Netzwerkverbindung wird in der Liste der VMkernel-Portbindungen für den iSCSI-Adapter angezeigt.

## Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie die Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung**, und klicken Sie auf **Detailansicht**.
- 5 Prüfen Sie die VMkernelAdapterinformationen durch das Wechseln zwischen verfügbaren Registerkarten.

## Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der

dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Wenn Sie die statische oder dynamische Erkennung einrichten, können Sie nur neue iSCSI-Ziele hinzufügen. Sie können keine Parameter eines vorhandenen Ziels ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie den zu konfigurierenden iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Ziele**.
- 5 Konfigurieren Sie die Erkennungsmethode.

Option	Beschreibung
Dynamische Erkennung	<ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Dynamische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ol> <p>Nach dem Einrichten der SendTargets-Sitzung mit dem iSCSI-System füllt Ihr Host die Liste „Statische Erkennung“ mit allen neu erkannten Zielen.</p>
Statische Erkennung	<ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Statische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die Daten des Ziels ein, und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ol>

## Software-iSCSI-Adapter deaktivieren

Wenn Sie den Software-iSCSI-Adapter nicht benötigen, können Sie ihn deaktivieren.

Durch Deaktivierung des Software-iSCSI-Adapters wird dieser zum Entfernen markiert. Der Adapter wird beim nächsten Neustart des Hosts vom Host entfernt. Nach dem Entfernen kann der Host nicht mehr auf die virtuellen Maschinen und die anderen Daten auf den Speichergeräten zugreifen, die diesem Adapter zugeordnet sind.

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

**Verfahren**

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter** und wählen Sie den Software-iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie auf **Deaktivieren** und bestätigen Sie, dass Sie den Adapter deaktivieren möchten.  
Der Status zeigt an, dass der Adapter deaktiviert wurde.
- 6 Starten Sie den Host neu.  
Nach dem Neustart wird der Adapter nicht mehr in der Liste der Speicheradapter angezeigt.

**Ergebnisse**

Der iSCSI-Software-Adapter ist nicht mehr verfügbar und auf die diesem Adapter zugeordneten Speichergeräte kann nicht mehr zugegriffen werden. Sie können den Adapter zu einem späteren Zeitpunkt aktivieren.

## Ändern der allgemeinen Eigenschaften für iSCSI-Adapter

Sie können den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

---

**Wichtig** Wenn Sie Standardeigenschaften für Ihre iSCSI-Adapter ändern, achten Sie darauf, dass ihre Namen und IP-Adressen das richtige Format haben.

---

**Voraussetzungen**

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

**Verfahren**

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften** und klicken Sie auf **Bearbeiten** im Bereich „Allgemein“.

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

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

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

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

### Ergebnisse

Wenn Sie den iSCSI-Namen ändern, wird der angegebene Name für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

## Einrichten des iSCSI-Netzwerks

Software- und abhängige Hardware-iSCSI-Adapter sind vom VMkernel-Netzwerk abhängig. Wenn Sie die Software- oder abhängigen Hardware-iSCSI-Adapter verwenden, müssen Sie Verbindungen für den Datenverkehr zwischen der iSCSI-Komponente und den physischen Netzwerkadaptern konfigurieren.

Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Anschließend muss der VMkernel-Adapter mit einem entsprechenden iSCSI-Adapter verknüpft werden. Dieser Vorgang wird Port-Bindung genannt.

Spezifische Überlegungen, wann und wie Netzwerkverbindungen mit Software-iSCSI verwendet werden, finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2038869>.

## Mehrere Netzwerkadapter in der iSCSI-Konfiguration

Wenn Ihr Host mehrere physische Netzwerkadapter für Software- und abhängige Hardware-iSCSI hat, verwenden Sie die Adapter für das Multipathing.

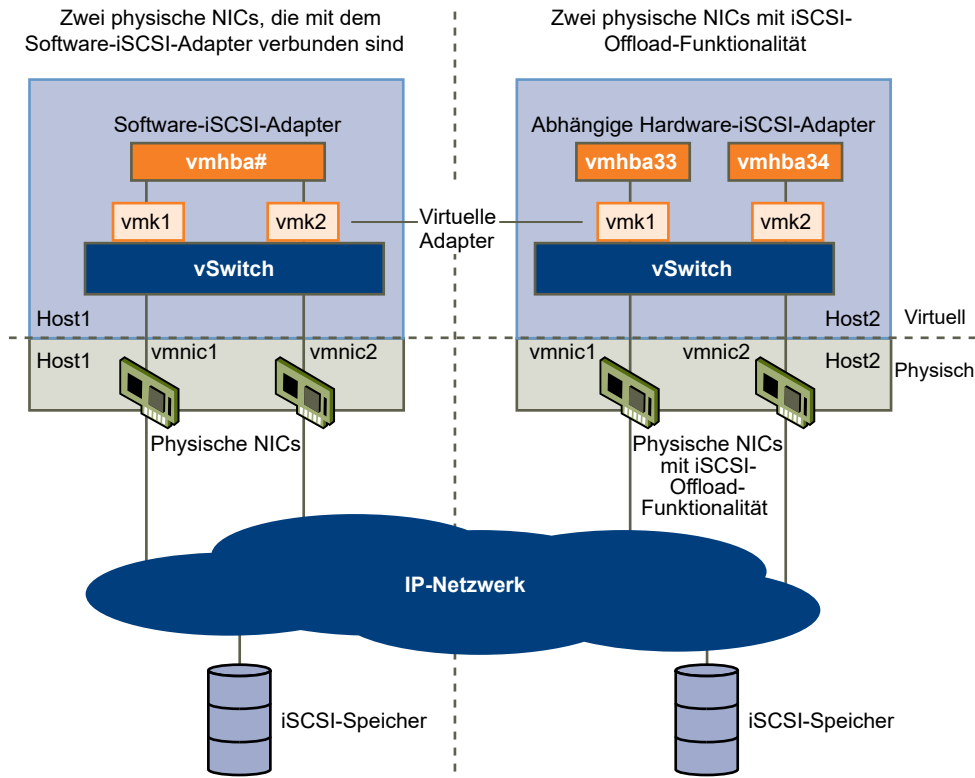
Sie können den Software-iSCSI-Adapter mit allen auf Ihrem Host verfügbaren physischen Netzwerkkarten verbinden. Die abhängigen iSCSI-Adapter müssen nur mit ihren eigenen physischen Netzwerkkarten verbunden sein.

---

**Hinweis** Physische Netzwerkkarten müssen sich in demselben Subnetz befinden wie das iSCSI-Speichersystem, mit dem sie verbunden werden.

---

Abbildung 10-1. Netzwerk mit iSCSI



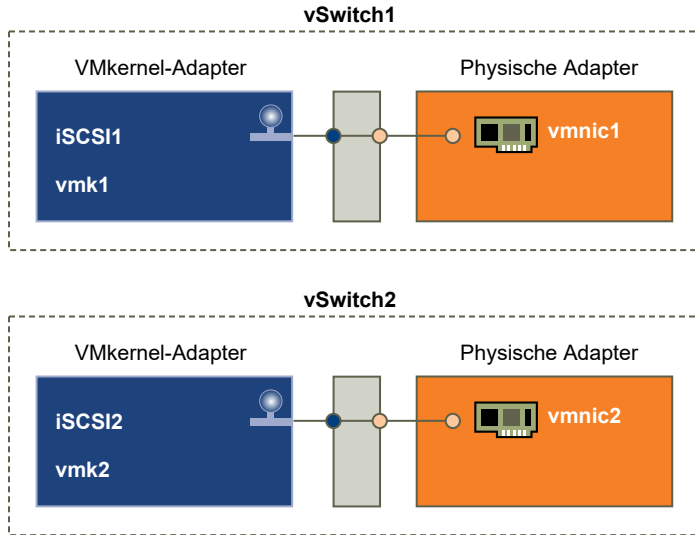
Der iSCSI-Adapter und die physische Netzwerkkarte werden über einen virtuellen VMkernel-Adapter verbunden, der auch als virtueller Netzwerkadapter oder VMkernel-Port bezeichnet wird. Sie erstellen einen VMkernel-Adapter (vmk) auf einem vSphere-Switch (vSwitch) mithilfe einer 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter.

Eine Möglichkeit, die 1:1-Zuordnung zu erreichen, wenn mehrere Netzwerkkarten vorhanden sind, besteht darin, für jedes V2P-Adapterpaar (Virtual-To-Physical) einen separaten vSphere-Switch auszuwählen.

**Hinweis** Wenn Sie separate vSphere-Switches verwenden, müssen Sie sie mit unterschiedlichen IP-Subnetzen verbinden. Anderenfalls können bei VMkernel-Adaptoren Verbindungsprobleme auftreten und der Host kann keine iSCSI-LUNs erkennen.

Die folgenden Beispiele zeigen Konfigurationen, die vSphere Standard-Switches verwenden. Sie können jedoch auch Distributed Switches verwenden. Weitere Informationen zu vSphere Distributed Switches finden Sie in der Dokumentation *vSphere-Netzwerk*.

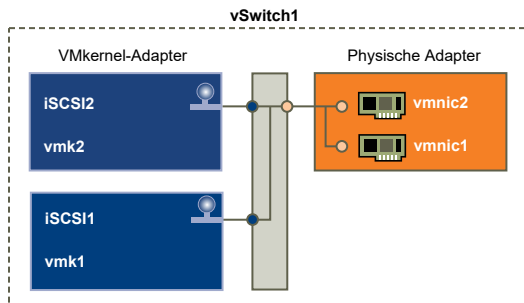
Abbildung 10-2. 1:1-Adapterzuordnung auf separaten vSphere Standard-Switches



Eine Alternative besteht darin, alle Netzwerkkarten und VMkernel-Adapter zu einem einzelnen vSphere Standard-Switch hinzuzufügen. In diesem Fall müssen Sie die Standardnetzwerkeinrichtung außer Kraft setzen und sicherstellen, dass jeder VMkernel-Adapter nur einem entsprechenden aktiven physischen Adapter zugeordnet wird.

**Hinweis** Sie müssen die Konfiguration mit einem einzelnen vSwitch verwenden, wenn sich VMkernel-Adapter in demselben Subnetz befinden.

Abbildung 10-3. 1:1-Adapterzuordnung auf einem einzelnen vSphere Standard-Switch



Die folgende Tabelle fasst die in diesem Thema beschriebene iSCSI-Netzwerkconfiguration zusammen.

Tabelle 10-2. Netzwerkkonfiguration für iSCSI

iSCSI-Adapter	VMkernel-Adapter (Ports)	Physische Adapter (NICs)
Software-iSCSI		
vmhba32	vmk1	vmnic1
	vmk2	vmnic2
Abhängige Hardware-iSCSI		

**Tabelle 10-2. Netzwerkkonfiguration für iSCSI (Fortsetzung)**

iSCSI-Adapter	VMkernel-Adapter (Ports)	Physische Adapter (NICs)
vmhba33	vmk1	vmnic1
vmhba34	vmk2	vmnic2

## Richtlinien für die Verwendung der iSCSI-Port-Bindung in ESXi

Sie können mehrere an iSCSI gebundene VMkernel-Adapter verwenden, um über mehrere Pfade zu einem iSCSI-Array zu verfügen, das eine einzelne IP-Adresse übermittelt.

Wenn Sie Port-Bindung für Multipathing verwenden, befolgen Sie diese Leitlinien:

- Die iSCSI-Ports des Array-Ziels müssen sich in derselben Broadcast-Domäne und demselben IP-Subnetz wie die VMkernel-Adapter befinden.
- Alle für die iSCSI-Port-Bindung verwendeten VMkernel-Adapter müssen sich in derselben Broadcast-Domäne und demselben IP-Subnetz befinden.
- Alle für die iSCSI-Konnektivität verwendeten VMkernel-Adapter müssen sich in demselben virtuellen Switch befinden.
- Die Port-Bindung unterstützt das Netzwerk-Routing nicht.

Verwenden Sie die Port-Bindung nicht, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- Array-Ziel-iSCSI-Ports befinden sich in einer anderen Broadcast-Domäne und einem anderen IP-Subnetz.
- Für die iSCSI-Konnektivität verwendete VMkernel-Adapter befinden sich in verschiedenen Broadcast-Domänen und IP-Subnetzen oder verwenden verschiedene virtuelle Switches.
- Für den Zugriff auf das iSCSI-Array ist Routing erforderlich.

## Erstellen von Netzwerkverbindungen für iSCSI

Konfigurieren Sie Verbindungen für den Datenverkehr zwischen den Software- oder den abhängigen Hardware-iSCSI-Adaptoren und den physischen Netzwerkadaptern.

Die folgenden Aufgaben beschreiben die iSCSI-Netzwerkkonfiguration mit einem vSphere Standard-Switch.

Wenn Sie einen vSphere Distributed Switch mit mehreren Uplink-Ports für die Port-Bindung verwenden, erstellen Sie für jede physische Netzwerkkarte eine separate verteilte Portgruppe. Legen Sie anschließend die Teamrichtlinie so fest, dass jede verteilte Portgruppe nur einen aktiven Uplink-Port besitzt. Weitere Informationen zu vSphere Distributed Switches finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

## Verfahren

### 1 Erstellen eines einzelnen VMkernel-Adapters für iSCSI

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

### 2 Erstellen zusätzlicher VMkernel-Adapter für iSCSI

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkadapter für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

### 3 Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

### 4 Binden von iSCSI- und VMkernel-Adapttern

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

### 5 Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Erstellen eines einzelnen VMkernel-Adapters für iSCSI

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte an.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.
- 3 Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.



- 5 Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie den Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.

Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.

---

**Wichtig** Wenn Sie einen VMkernel-Adapter für den abhängigen Hardware-iSCSI-Adapter erstellen, wählen Sie den Netzwerkadapter aus, der zu der iSCSI-Komponente gehört. Siehe [Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern](#).

---

- 6 Geben Sie eine Netzwerkbezeichnung ein.

Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. iSCSI.

- 7 Geben Sie die IP-Einstellungen an.

- 8 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

### Ergebnisse

Sie haben den virtuellen VMkernel-Adapter (vmk#) für einen physischen Netzwerkadapter (vmnic#) auf Ihrem Host erstellt.

### Nächste Schritte

Wenn Ihr Host über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügt, müssen Sie den virtuellen Adapter, den Sie erstellt haben, an den iSCSI-Adapter binden.

Wenn Sie über mehrere Netzwerkadapter verfügen, erstellen Sie zusätzliche VMkernel-Adapter und führen Sie dann die iSCSI-Bindung durch. Die Anzahl an virtuellen Adaptern muss mit der Anzahl an physischen Adaptern auf dem Host übereinstimmen.

## Erstellen zusätzlicher VMkernel-Adapter für iSCSI

Verwenden Sie dieses Verfahren, wenn zwei oder mehr physische Netzwerkadapter für iSCSI vorhanden sind und Sie alle physischen Adapter mit einem einzigen vSphere Standard-Switch verbinden möchten. In dieser Aufgabe fügen Sie physische Adapter und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

### Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der einen VMkernel-iSCSI-Adapter einem einzelnen physischen Netzwerkadapter zuordnet, der für den iSCSI-Datenverkehr vorgesehen ist.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.

- 4 Verbinden Sie zusätzliche Netzwerkadapter mit dem Switch.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **Physische Netzwerkadapter** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie mindestens einen Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.  
  
Wählen Sie für abhängige Hardware-iSCSI-Adapter nur die Netzwerkkarten aus, die eine entsprechende iSCSI-Komponente besitzen.
  - e Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.
- 5 Erstellen Sie iSCSI-VMkernel-Adapter für alle hinzugefügten physischen Netzwerkadapter.  
  
Die Anzahl an VMkernel-Schnittstellen muss mit der Anzahl an physischen Netzwerkadaptern auf dem vSphere Standard-Switch übereinstimmen.
  - a Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.
  - b Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
  - c Stellen Sie sicher, dass Sie den vorhandenen Switch verwenden, und klicken Sie auf **Weiter**.
  - d Führen Sie die Konfiguration durch und klicken Sie auf **Beenden**.

#### Nächste Schritte

Ändern Sie die Netzwerkrichtlinie für alle VMkernel-Adapter dahin gehend, dass pro VMkernel-Adapter nur ein physischer Netzwerkadapter aktiv ist. Sie können dann die iSCSI-VMkernel-Adapter an die Software-iSCSI- oder an die abhängigen Hardware-iSCSI-Adapter binden.

### Ändern der Netzwerkrichtlinie für iSCSI

Wenn Sie über einen einzelnen vSphere Standard-Switch mehrere VMkernel-Adapter an mehrere Netzwerkadapter anschließen, richten Sie die Netzwerkrichtlinie ein, sodass nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

Standardmäßig werden für jeden VMkernel-Adapter auf dem vSphere Standard-Switch alle Netzwerkadapter als aktiv angezeigt. Sie müssen dieses Setup überschreiben, damit jeder VMkernel-Adapter lediglich einer aktiven physischen Netzwerkkarte zugeordnet wird. Beispielsweise wird „vmk1“ der Netzwerkkarte „vmnic1“ zugeordnet, „vmk2“ wird „vmnic2“ zugeordnet usw.

#### Voraussetzungen

Erstellen Sie einen vSphere Standard-Switch, der VMkernel mit physischen Netzwerkadaptern verbindet, die für den iSCSI-Datenverkehr vorgesehen sind. Die Anzahl an VMkernel-Adaptern muss mit der Anzahl an physischen Adaptern auf dem vSphere Standard-Switch übereinstimmen.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
- 4 Wählen Sie auf dem vSwitch-Diagramm den VMkernel-Adapter aus und klicken Sie auf das Symbol **Einstellungen bearbeiten**.
- 5 Klicken Sie im Assistenten **Einstellungen bearbeiten** auf **Teaming und Failover** und klicken Sie unter „Failover-Reihenfolge“ auf **Außer Kraft setzen**.
- 6 Wählen Sie nur einen physischen Adapter als aktiv aus und verschieben Sie alle übrigen Adapter in die Kategorie **Nicht verwendete Adapter**.
- 7 Wiederholen Sie [Schritt 4](#) bis [Schritt 6](#) für jede iSCSI-VMkernel-Schnittstelle auf dem vSphere Standard-Switch.

## Beispiel: iSCSI-Netzwerkrichtlinie

Die folgende Tabelle illustriert die ordnungsgemäße iSCSI-Zuordnung, bei der nur ein physischer Netzwerkadapter für jeden VMkernel-Adapter aktiv ist.

VMkernel-Adapter (vmk#)	Physischer Netzwerkadapter (vmnic#)
vmk1	<b>Aktive Adapter</b> vmnic1
	<b>Nicht verwendete Adapter</b> vmnic2
vmk2	<b>Aktive Adapter</b> vmnic2
	<b>Nicht verwendete Adapter</b> vmnic1

## Nächste Schritte

Binden Sie nach dem Ausführen dieser Aufgabe die virtuellen VMkernel-Adapter an die Software-iSCSI- oder abhängigen Hardware-iSCSI-Adapter.

## Binden von iSCSI- und VMkernel-Adaptoren

Binden Sie einen iSCSI-Adapter an einen VMkernel-Adapter.

## Voraussetzungen

Erstellen Sie einen virtuellen VMkernel-Adapter für jeden physischen Netzwerkadapter auf Ihrem Host. Wenn Sie mehrere VMkernel-Adapter verwenden, richten Sie die korrekte Netzwerkrichtlinie ein.

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter** und wählen Sie die zu konfigurierende Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung** und klicken Sie dann auf **Hinzufügen**.
- 5 Wählen Sie einen VMkernel-Adapter zur Bindung mit dem iSCSI-Adapter aus.

---

**Hinweis** Stellen Sie sicher, dass die Netzwerkkrichtlinie für den VMkernel-Adapter die Anforderungen für das Binden erfüllt.

---

Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter ist nur ein VMkernel-Adapter verfügbar, der mit der richtigen physischen Netzwerkkarte verknüpft ist.

- 6 Klicken Sie auf **OK**.

## Ergebnisse

Die Netzwerkverbindung wird in der Liste der VMkernel-Portbindungen für den iSCSI-Adapter angezeigt.

## Überprüfen der Port-Bindungsdetails

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI-Adapter verbunden ist.

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie die Software oder den abhängigen iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung**, und klicken Sie auf **Detailansicht**.
- 5 Prüfen Sie die VMkernelAdapterinformationen durch das Wechseln zwischen verfügbaren Registerkarten.

## Verwalten des iSCSI-Netzwerks

Besondere Berücksichtigung finden sowohl physische als auch VMkernel-Netzwerkadapter, die einem iSCSI-Adapter zugeordnet sind.

Nachdem Sie Netzwerkverbindungen für iSCSI erstellt haben, wird bei mehreren Netzwerk-Dialogfeldern eine iSCSI-Kontrollanzeige aktiviert. Diese Kontrollanzeige zeigt, dass ein bestimmter virtueller oder physischer Netzwerkadapter iSCSI-gebunden ist. Befolgen Sie zur Vermeidung von Störungen des iSCSI-Datenverkehrs diese Richtlinien und Überlegungen bei der Verwaltung von iSCSI-gebundenen virtuellen und physischen Netzwerkadaptern:

- Stellen Sie sicher, dass den VMkernel-Netzwerkadaptern Adressen in dem Subnetz zugewiesen werden, in dem sich auch das iSCSI-Speicher-Portal befindet, zu dem sie eine Verbindung herstellen.
- iSCSI-Adapter, die VMkernel-Adapter verwenden, können keine Verbindungen zu iSCSI-Ports auf unterschiedlichen Subnetzen herstellen, selbst wenn diese Ports von den iSCSI-Adaptern ermittelt wurden.
- Stellen Sie bei der Verwendung von separaten vSphere-Switches zum Verbinden von physischen Netzwerkadaptern und VMkernel-Adaptern sicher, dass die vSphere-Switches Verbindungen zu unterschiedlichen IP-Subnetzen herstellen.
- Wenn sich VMkernel-Adapter in demselben Subnetz befinden, müssen Sie mit einem einzelnen vSwitch verbunden sein.
- Wenn Sie VMkernel-Adapter auf einen anderen vSphere-Switch migrieren, verschieben Sie die zugewiesenen physischen Adapter.
- Nehmen Sie keine Änderungen an der Konfiguration von iSCSI-gebundenen VMkernel-Adaptern oder physischen Netzwerkadaptern vor.
- Nehmen Sie keine Änderungen vor, die die Zuweisungen von VMkernel-Adaptern und physischen Netzwerkadaptern aufheben könnten. Sie können die Zuweisung aufheben, wenn Sie einen der Adapter oder den vSphere-Switch, der sie verbindet, entfernen oder die 1:1-Netzwerkrichtlinie für die Verbindung ändern.

## Fehler im iSCSI-Netzwerk beheben

Ein Warnhinweis deutet auf eine nicht übereinstimmende Portgruppenrichtlinie für einen iSCSI-gebundenen VMkernel-Adapter hin.

### Problem

Die Portgruppenrichtlinie des VMkernel-Adapters wird in den folgenden Fällen als nicht übereinstimmend betrachtet:

- Der VMkernel-Adapter ist mit keinem aktiven physischen Netzwerkadapter verbunden.
- Der VMkernel-Adapter ist mit mehreren physischen Netzwerkadaptern verbunden.
- Der VMkernel-Adapter ist mit mindestens einem physischen Standby-Adapter verbunden.
- Der aktive physische Adapter wurde geändert.

## Lösung

Folgen Sie den Anweisungen in [Ändern der Netzwerkrichtlinie für iSCSI](#) zum Einrichten der richtigen Netzwerkrichtlinie für den iSCSI-gebundenen VMkernel-Adapter.

## Verwenden von Jumbo-Frames mit iSCSI

ESXi unterstützt die Verwendung von Jumbo-Frames mit iSCSI.

Jumbo-Frames sind Ethernet-Frames mit einer Größe, die 1500 Byte überschreitet. Der Parameter „Maximum Transmission Unit“ (MTU) wird in der Regel dazu verwendet, die Größe der Jumbo-Frames zu messen. ESXi ermöglicht Jumbo-Frames mit einer MTU von bis zu 9000 Byte.

Wenn Sie Jumbo-Frames für den iSCSI-Datenverkehr verwenden, sollten Sie Folgendes in Betracht ziehen:

- Das Netzwerk muss Jumbo-Frames durchgängig unterstützen, damit diese Technologie eingesetzt werden kann.
- Informieren Sie sich bei Ihrem Anbieter, ob Ihre physischen Netzwerkkarten und iSCSI-HBAs Jumbo-Frames unterstützen.
- Zu Fragen zum Einrichten und Überprüfen physischer Netzwerk-Switches für Jumbo-Frames konsultieren Sie Ihre Anbieterdokumentation.

Die folgende Tabelle erläutert den Grad der Unterstützung, den ESXi für Jumbo-Frames bietet.

**Tabelle 10-3. Unterstützung für Jumbo-Frames**

Typ des iSCSI-Adapters	Unterstützung für Jumbo-Frames
Software-iSCSI	Unterstützt
Abhängige Hardware-iSCSI	Wird unterstützt. Fragen Sie den Anbieter.
Unabhängige Hardware-iSCSI	Wird unterstützt. Fragen Sie den Anbieter.

## Aktivieren von Jumbo-Frames für Software-iSCSI und abhängige Hardware-iSCSI

Um Jumbo-Frames für Software- und abhängige Hardware-iSCSI-Adapter im vSphere Web Client zu aktivieren, ändern Sie den Standardwert des MTU-Parameters (maximale Übertragungseinheiten).

Sie ändern den MTU-Parameter auf dem vSphere-Switch, den Sie für iSCSI-Datenverkehr verwenden. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.

- 3 Klicken Sie auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
- 4 Klicken Sie auf das Symbol **Einstellungen bearbeiten**.
- 5 Ändern Sie auf der Seite „Eigenschaften“ den MTU-Parameter.

Mit diesem Schritt wird die MTU für alle physischen Netzwerkkarten auf diesem Standard-Switch festgelegt. Legen Sie als MTU-Wert die größte MTU-Größe von allen Netzwerkkarten fest, die mit dem Standard-Switch verbunden sind. ESXi unterstützt eine MTU-Größe von bis zu 9000 Byte.

## Aktivieren von Jumbo-Frames für unabhängige Hardware-iSCSI

Um Jumbo-Frames für unabhängige Hardware-iSCSI-Adapter im vSphere Web Client zu aktivieren, ändern Sie den Standardwert des MTU-Parameters (maximale Übertragungseinheiten).

Verwenden Sie die Einstellungen unter „Erweiterte Optionen“, um den MTU-Parameter für den iSCSI-HBA zu ändern.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie in der Liste der Adapter den unabhängigen Hardware-iSCSI-Adapter aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Erweiterte Optionen**, und klicken Sie auf **Bearbeiten**.
- 5 Ändern Sie den Wert des MTU-Parameters.

ESXi unterstützt eine MTU-Größe von bis zu 9000 Byte.

## Konfigurieren von Erkennungsadressen für iSCSI-Adapter

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

Das ESXi-System unterstützt diese Erkennungsmethoden:

### Dynamische Erkennung

Wird auch als „SendTargets“-Erkennung bezeichnet. Immer wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, übermittelt der Initiator eine „SendTargets“-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 iSCSI-Adapters oder durch einen Neustart des Hosts erneut zur Liste hinzugefügt werden.

---

**Hinweis** Bei Software-iSCSI und davon abhängiger Hardware-iSCSI filtert ESXi die Zieladressen anhand der IP-Familie der angegebenen iSCSI-Serveradresse. Wenn die Adresse im IPv4-Format vorliegt, werden eventuelle IPv6-Adressen in der SendTargets-Antwort des iSCSI-Servers herausgefiltert. Wenn die Angabe eines iSCSI-Servers über DNS-Namen erfolgt oder die SendTargets-Antwort des iSCSI-Servers DNS-Namen aufweist, bezieht sich ESXi auf die IP-Familie des ersten aufgelösten Eintrags im DNS-Lookup.

---

## Statische Erkennung

Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben. Der iSCSI-Adapter verwendet zur Kommunikation mit dem iSCSI-Server eine von Ihnen bereitgestellte Liste von Zielen.

## Einrichten der dynamischen oder statischen Erkennung für iSCSI

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Wenn Sie die statische oder dynamische Erkennung einrichten, können Sie nur neue iSCSI-Ziele hinzufügen. Sie können keine Parameter eines vorhandenen Ziels ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie den zu konfigurierenden iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Ziele**.



## 5 Konfigurieren Sie die Erkennungsmethode.

Option	Beschreibung
<b>Dynamische Erkennung</b>	<ul style="list-style-type: none"> <li>a Klicken Sie auf <b>Dynamische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ul> <p>Nach dem Einrichten der SendTargets-Sitzung mit dem iSCSI-System füllt Ihr Host die Liste „Statische Erkennung“ mit allen neu erkannten Zielen.</p>
<b>Statische Erkennung</b>	<ul style="list-style-type: none"> <li>a Klicken Sie auf <b>Statische Erkennung</b> und klicken Sie anschließend auf <b>Hinzufügen</b>.</li> <li>b Geben Sie die Daten des Ziels ein, und klicken Sie auf <b>OK</b>.</li> <li>c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.</li> </ul>

## Entfernen dynamischer oder statischer iSCSI-Ziele

Entfernen Sie die iSCSI-Server in der Liste der Ziele.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter**, und wählen Sie den zu ändernden iSCSI-Adapter aus der Liste aus.
- 4 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Ziele**.
- 5 Wechseln Sie zwischen **Dynamische Erkennung** und **Statische Erkennung**.
- 6 Wählen Sie einen iSCSI-Server zum Entfernen aus und klicken Sie auf **Entfernen**.
- 7 Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Wenn Sie ein dynamisch erkanntes statisches Ziel entfernen, müssen Sie es vor der erneuten Prüfung aus dem Speichersystem entfernen. Sonst erkennt Ihr Host das Ziel automatisch und fügt es der Liste der statischen Ziele hinzu, wenn Sie den Adapter erneut prüfen.

## Konfigurieren von CHAP-Parametern für iSCSI-Adapter

Da die IP-Netzwerke, die die iSCSI-Technologie zum Verbinden mit Remotezielen verwendet, die von ihnen übertragenen Daten nicht schützen, muss die Sicherheit der Verbindung gewährleistet werden. Eines der von iSCSI implementierten Protokolle ist das CHAP (Challenge Handshake Authentication Protocol), das die jeweiligen Berechtigungen der Initiatoren, die auf Ziele im Netzwerk zugreifen, überprüft.

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- und abhängige Hardware-iSCSI-Adapter unterstützt ESXi auch die zielbasierte CHAP-Authentifizierung, die 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 alle Typen von iSCSI-Initiatoren und bidirektionales CHAP für Software- und abhängige Hardware-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.

### Bidirektionales CHAP

Bei der bidirektionalen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels. VMware unterstützt diese Methode nur für Software- und abhängige Hardware-iSCSI-Adapter.

Für Software- und abhängige Hardware-iSCSI-Adapter können Sie unidirektionales und bidirektionales CHAP für die einzelnen Adapter oder auf der Zielebene festlegen. Unabhängige Hardware-iSCSI unterstützt CHAP nur auf der Adapterebene.

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

---

**Hinweis** Wenn Sie die CHAP-Sicherheitsebene angeben, ist die Reaktion des Speicher-Arrays anbieterspezifisch und hängt von der CHAP-Implementierung des Arrays ab. Weitere Informationen über das Verhalten der CHAP-Authentifizierung in verschiedenen Initiator- und Zielkonfigurationen finden Sie in der Array-Dokumentation.

---

Tabelle 10-4. CHAP-Sicherheitsstufe

CHAP-Sicherheitsstufe	Beschreibung	Unterstützt
Keine	Der Host verwendet keine CHAP-Authentifizierung. Wählen Sie diese Option aus, um die Authentifizierung zu deaktivieren, wenn sie derzeit aktiviert ist.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
Unidirektionales CHAP verwenden, wenn vom Ziel gefordert	Der Host bevorzugt eine Nicht-CHAP-Verbindung, er kann jedoch eine CHAP-Verbindung verwenden, wenn das Ziel dies erfordert.	Software-iSCSI Abhängige Hardware-iSCSI
Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es	Der Host bevorzugt CHAP, er kann jedoch Nicht-CHAP-Verbindungen verwenden, wenn das Ziel CHAP nicht unterstützt.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
Unidirektionales CHAP verwenden	Für den Host ist eine erfolgreiche CHAP-Authentifizierung erforderlich. Die Verbindung schlägt fehl, wenn die CHAP-Aushandlung fehlschlägt.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
Bidirektionales CHAP verwenden	Der Host und das Ziel unterstützen bidirektionales CHAP.	Software-iSCSI Abhängige Hardware-iSCSI

## Einrichten von CHAP für iSCSI-Adapter

Wenn Sie den CHAP-Namen und -Schlüssel auf der Ebene des iSCSI-Adapters einrichten, empfangen alle Ziele denselben Parameter vom Adapter. Standardmäßig übernehmen alle Erkennungsadressen und statischen Ziele die CHAP-Parameter, die Sie auf der Adapterebene einrichten.

Der CHAP-Name darf nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen. Einige Adapter, z. B. der QLogic-Adapter, haben möglicherweise niedrigere Grenzen: 255 für den CHAP-Namen und 100 für den CHAP-Schlüssel.

### Voraussetzungen

- Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI oder abhängige Hardware-iSCSI fest, ob unidirektionales oder bidirektionales CHAP konfiguriert werden soll. Abhängige Hardware-iSCSI-Adapter unterstützen das bidirektionale CHAP nicht.
- Überprüfen Sie die auf der Speicherseite konfigurierten CHAP-Parameter. Parameter, die Sie konfigurieren, müssen zu denen auf der Speicherseite passen.
- Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Zeigen Sie Speicheradapter an, und wählen Sie den zu konfigurierenden iSCSI-Adapter aus.
- 2 Klicken Sie unter „Adapterdetails“ auf die Registerkarte **Eigenschaften**, und klicken Sie auf **Bearbeiten** im Bereich „Authentifizierung“.

### 3 Legen Sie die Authentifizierungsmethode fest.

- **Keine**
- **Unidirektionales CHAP verwenden, wenn vom Ziel gefordert**
- **Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es**
- **Unidirektionales CHAP verwenden**
- **Verwenden Sie bidirektionales CHAP.** Um bidirektionales CHAP zu konfigurieren, müssen Sie diese Option auswählen.

### 4 Geben Sie den ausgehenden 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-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden (Use initiator name)**.
- Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Textfeld **Name** ein.

### 5 Geben Sie einen ausgehenden CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.

### 6 Wenn Sie bidirektionales CHAP konfigurieren, geben Sie eingehende CHAP-Anmeldedaten an.

Für ausgehendes und eingehendes CHAP müssen Sie verschiedene Schlüssel verwenden.

### 7 Klicken Sie auf **OK**.

### 8 Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

## Ergebnisse

Wenn Sie die Parameter für 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 für Ziele

Wenn Sie Software- und abhängige Hardware-iSCSI-Adapter verwenden, können Sie verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.

Der CHAP-Name darf 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 oder abhängige Hardware-iSCSI fest, ob unidirektionales oder bidirektionales CHAP konfiguriert werden soll.
- Überprüfen Sie die auf der Speicherseite konfigurierten CHAP-Parameter. Parameter, die Sie konfigurieren, müssen zu denen auf der Speicherseite passen.
- Greifen Sie auf Speicheradapter zu.
- Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

## Verfahren

- 1 Wählen Sie den zu konfigurierenden iSCSI-Adapter aus, und klicken Sie auf die Registerkarte **Ziele** unter „Adapterdetails“.
- 2 Klicken Sie auf **Dynamische Erkennung** oder **Statische Erkennung**.
- 3 Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Authentifizierung**.
- 4 Heben Sie die Auswahl von **Einstellungen von übergeordnetem Element übernehmen** auf und legen Sie die Authentifizierungsmethode fest.

- **Keine**
- **Unidirektionales CHAP verwenden, wenn vom Ziel gefordert**
- **Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es**
- **Unidirektionales CHAP verwenden**
- **Verwenden Sie bidirektionales CHAP.** Um bidirektionales CHAP zu konfigurieren, müssen Sie diese Option auswählen.

- 5 Geben Sie den ausgehenden 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-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden (Use initiator name)**.
- Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Textfeld **Name** ein.

- 6 Geben Sie einen ausgehenden CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.
- 7 Wenn Sie bidirektionales CHAP konfigurieren, geben Sie eingehende CHAP-Anmeldedaten an.

Für ausgehendes und eingehendes CHAP müssen Sie verschiedene Schlüssel verwenden.

- 8 Klicken Sie auf **OK**.
- 9 Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

### Ergebnisse

Wenn Sie die Parameter für 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 Host neu starten, Sie die Sitzung über die Befehlszeile beenden oder das Speichersystem eine Abmeldung erzwingt. Nachdem die Sitzung beendet wurde, können Sie keine Verbindungen mehr zu Zielen herstellen, die CHAP benötigen.

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Öffnen Sie das Dialogfeld „CHAP-Anmeldedaten“.
- 2 Wenn Sie für Software- und abhängige Hardware-iSCSI-Adapter nur das beiderseitige CHAP deaktivieren, das unidirektionale CHAP jedoch beibehalten möchten, wählen Sie im Bereich „Beiderseitiges CHAP“ **CHAP nicht verwenden** aus.
- 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 erweiterter 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.

In der folgenden Tabelle sind die erweiterten iSCSI-Parameter aufgelistet, die Sie mit dem vSphere Web Client konfigurieren können. Darüber hinaus können Sie die vSphere-CLI-Befehle verwenden, um einige der erweiterten Parameter zu konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu *Erste Schritte mit vSphere Command-Line Interfaces*.

---

**Wichtig** Nehmen Sie keine Änderungen an den erweiterten iSCSI-Einstellungen vor, es sei denn, dies erfolgt unter Anleitung des VMware-Supports oder des Speicheranbieters.

---

Tabelle 10-5. 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 Abhängige Hardware-iSCSI
Daten-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.  <b>Hinweis</b> 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 Abhängige Hardware-iSCSI
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 Abhängige Hardware-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 Abhängige Hardware-iSCSI
Maximale Burstlänge	Die maximale SCSI-Datenlast in einer Data-In- oder einer angeforderten Data-Out-iSCSI-Sequenz in Byte.	Software-iSCSI Abhängige Hardware-iSCSI
Maximal empfangbare Datensegmentlänge	Die maximale Datensegmentlänge in Byte, die in einer iSCSI-PDU empfangen werden kann.	Software-iSCSI Abhängige Hardware-iSCSI
Zeitüberschreitung bei der Sitzungswiederherstellung	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor eine Sitzung wiederhergestellt werden kann. Wird der angegebene Zeitraum überschritten, beendet der iSCSI-Initiator die Sitzung.	Software-iSCSI Abhängige Hardware-iSCSI
No-Op-Intervall	Gibt das Zeitintervall in Sekunden an, in dem NOP-Out-Anforderungen von Ihrem iSCSI-Initiator an ein iSCSI-Ziel gesendet werden. Mithilfe der NOP-Out-Anforderungen kann verifiziert werden, ob zwischen dem iSCSI-Initiator und dem iSCSI-Ziel eine aktive Verbindung besteht.	Software-iSCSI Abhängige Hardware-iSCSI
No-Op-Zeitüberschreitung	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor Ihr Host eine NOP-In-Meldung erhält. Die Meldung wird vom iSCSI-Ziel als Antwort auf die NOP-Out-Anforderung gesendet. Wenn der Grenzwert für die No-Op-Zeitüberschreitung erreicht wurde, beendet der Initiator die aktuelle und startet eine neue Sitzung.	Software-iSCSI Abhängige Hardware-iSCSI

Tabelle 10-5. Zusätzliche Parameter für iSCSI-Initiatoren (Fortsetzung)

Erweiterte Parameter	Beschreibung	Konfigurierbar auf
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.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
Verzögerte Quittierung (ACK)	Ermöglicht Systemen die Verzögerung der Bestätigung empfangener Datenpakete.	Software-iSCSI Abhängige Hardware-iSCSI

## Konfigurieren erweiterter Parameter für iSCSI

Die erweiterten iSCSI-Einstellungen steuern Parameter wie „Header-Digest“, „Data Digest“, „ARP-Umleitung“, „Verzögerte Quittierung (ACK)“ usw.

**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.

### Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
- 4 Konfigurieren Sie die erweiterten Parameter.
  - Klicken Sie zum Konfigurieren erweiterter Parameter auf der Adapterebene unter „Adapterdetails“ auf die Registerkarte **Erweiterte Optionen** und klicken Sie dann auf **Bearbeiten**.
  - Konfigurieren Sie erweiterte Parameter auf der Zielebene.
    - a Klicken Sie auf die Registerkarte **Ziele** und klicken Sie entweder auf **Dynamische Erkennung** oder auf **Statische Erkennung**.
    - b Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Erweiterte Optionen**.
- 5 Geben Sie die erforderlichen Werte für die erweiterten Parameter ein, die Sie ändern möchten.



## iSCSI-Sitzungsverwaltung

Um miteinander zu kommunizieren, richten iSCSI-Initiatoren und -Ziele iSCSI-Sitzungen ein. Sie können iSCSI-Sitzungen mithilfe der vSphere-CLI prüfen und verwalten.

Standardmäßig starten Software-iSCSI- und abhängige Hardware-iSCSI-Initiatoren eine iSCSI-Sitzung zwischen jedem Initiatorport und jedem Zielport. Wenn Ihr iSCSI-Initiator oder -Ziel über mehrere Ports verfügt, können auf Ihrem Host mehrere Sitzungen eingerichtet sein. Die Standardanzahl an Sitzungen für jedes Ziel entspricht dem Produkt aus der Anzahl an Ports auf dem iSCSI-Adapter und der Anzahl an Zielports.

Mit vSphere CLI können Sie alle aktuellen Sitzungen anzeigen, um sie zu analysieren und zu debuggen. Wenn Sie weitere Pfade zu Speichersystemen erstellen möchten, können Sie die Standardanzahl an Sitzungen erhöhen, indem Sie die bestehenden Sitzungen zwischen dem iSCSI-Adapter und den Zielports duplizieren.

Sie können auch eine Sitzung mit einem bestimmten Zielport einrichten. Diese Sitzung kann nützlich sein, wenn Ihr Host eine Verbindung zu einem Speichersystem mit einem einzigen Port herstellt, das Ihrem Initiator standardmäßig nur einen Zielport präsentiert, aber zusätzliche Sitzungen auf einen anderen Zielport umleiten kann. Durch das Einrichten einer neuen Sitzung zwischen Ihrem iSCSI-Initiator und einem anderen Zielport wird ein zusätzlicher Pfad zum Speichersystem erstellt.

Für die iSCSI-Sitzungsverwaltung muss Folgendes beachtet werden:

- Einige Speichersysteme bieten keine Unterstützung für mehrere Sitzungen von demselben Initiatornamen oder Endpunkt aus. Wenn Sie versuchen, mehrere Sitzungen mit solchen Zielen zu erstellen, kann dies zu unvorhersehbarem Verhalten Ihrer iSCSI-Umgebung führen.
- Speicheranbieter können automatische Sitzungs-Manager bereitstellen. Die Verwendung des automatischen Sitzungs-Managers zum Hinzufügen oder Löschen von Sitzungen garantiert keine nachhaltigen Ergebnisse und kann die Speicherleistung beeinträchtigen.

## Überprüfen von iSCSI-Sitzungen

Verwenden Sie den vCLI-Befehl, um iSCSI-Sitzungen zwischen einem iSCSI-Adapter und einem Speichersystem anzuzeigen.

In dem Vorgang wird der Zielsystem durch **--server=Servername** angegeben. Der angegebene Zielsystem fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um iSCSI-Sitzungen aufzulisten:

```
esxcli --server=Servername iscsi session list
```

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
<b>-A --adapter=</b> <i>str</i>	Der Name des iSCSI-Adapters, z. B. vmhba34.
<b>-s --isid=</b> <i>str</i>	Der Bezeichner der iSCSI-Sitzung.
<b>-n --name=</b> <i>str</i>	Der Name des iSCSI-Ziels, z. B. iqn.X.

## Hinzufügen von iSCSI-Sitzungen

Verwenden Sie die vCLI, um eine iSCSI-Sitzung für das von Ihnen angegebene Ziel hinzuzufügen oder um eine vorhandene Sitzung zu duplizieren. Durch das Duplizieren von Sitzungen erhöhen Sie die Standardanzahl an Sitzungen und erstellen zusätzliche Pfade zu Speichersystemen.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um eine iSCSI-Sitzung hinzuzufügen oder zu duplizieren:

```
esxcli --server=server_name iscsi session add
```

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
<b>-A --adapter=</b> <i>str</i>	Der Name des iSCSI-Adapters, z. B. vmhba34. Diese Option ist erforderlich.
<b>-s --isid=</b> <i>str</i>	Die ISID einer zu duplizierenden Sitzung. Sie finden diese, indem Sie alle Sitzungen auflisten.
<b>-n --name=</b> <i>str</i>	Der Name des iSCSI-Ziels, z. B. iqn.X.

### Nächste Schritte

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

## Entfernen von iSCSI-Sitzungen

Verwenden Sie den vCLI-Befehl, um eine iSCSI-Sitzung zwischen einem iSCSI-Adapter und einem Ziel zu entfernen.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

### Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um eine Sitzung zu entfernen:

```
esxcli --server=Servername iscsi session remove
```

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
<b>-A --adapter=</b> <i>str</i>	Der Name des iSCSI-Adapters, z. B. vmhba34. Diese Option ist erforderlich.
<b>-s --isid=</b> <i>str</i>	Die ISID einer zu entfernenden Sitzung. Sie finden diese, indem Sie alle Sitzungen auflisten.
<b>-n --name=</b> <i>str</i>	Der Name des iSCSI-Ziels, z. B. iqn.X.

### Nächste Schritte

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

# Starten von einem iSCSI-SAN

# 11

Wenn Sie Ihren Host so einrichten, dass er von einem SAN gestartet wird, wird das Start-Image des Hosts auf einer oder mehreren LUNs im SAN-Speichersystem gespeichert. Wenn der Host startet, wird er nicht von seiner lokalen Festplatte aus, sondern von der LUN im SAN aus gestartet.

Sie können das Starten vom SAN verwenden, wenn Sie keinen lokalen Speicher warten möchten oder Hardwarekonfigurationen ohne Festplatten haben, wie z. B. Blade-Systeme.

ESXi unterstützt verschiedene Methoden zum Starten vom iSCSI-SAN.

**Tabelle 11-1. Unterstützung für das Starten vom iSCSI-SAN**

Unabhängige Hardware-iSCSI	Software-iSCSI und abhängige Hardware-iSCSI
Konfigurieren Sie den iSCSI-HBA für das Starten vom SAN. Informationen zur HBA-Konfiguration finden Sie unter <a href="#">Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN</a>	Verwenden Sie den Netzwerkadapter, der iBFT unterstützt. Weitere Informationen hierzu finden Sie unter <a href="#">iBFT-iSCSI-Start - Überblick</a> .

Dieses Kapitel enthält die folgenden Themen:

- [Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN](#)
- [Vorbereiten des iSCSI-SAN](#)
- [Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN](#)
- [iBFT-iSCSI-Start - Überblick](#)

## Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN

Wenn Sie eine iSCSI-LUN als Startgerät für Ihren Host einrichten und verwenden möchten, müssen Sie einige allgemeine Richtlinien befolgen.

Es gelten die folgenden Richtlinien für das Starten von unabhängigem Hardware-iSCSI und iBFT.

- Prüfen Sie die Herstellerempfehlungen für die Hardware, die Sie in Ihrer Startkonfiguration verwenden.

- Weitere Informationen zu Installationsvoraussetzungen und -anforderungen finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.
- Verwenden Sie statische IP-Adressen, um das Auftreten von DHCP-Konflikten zu vermeiden.
- Verwenden Sie für VMFS-Datenspeicher und Startpartitionen verschiedene LUNs.
- Konfigurieren Sie auf Ihrem Speichersystem ordnungsgemäße ACLs.
  - Die Start-LUN sollte nur für den Host sichtbar sein, der die LUN verwendet. Auf diese Start-LUN sollten andere Hosts im SAN nicht zugreifen dürfen.
  - Wenn eine LUN für einen VMFS-Datenspeicher verwendet wird, kann sie von mehreren Hosts gemeinsam verwendet werden. Dies wird durch ACLs im Speichersystem ermöglicht.
- Konfigurieren Sie eine Diagnosepartition.
  - Nur bei unabhängigen Hardware-iSCSI können Sie die Diagnosepartition auf der Start-LUN platzieren. Wenn Sie die Diagnosepartition in der Start-LUN konfigurieren, kann diese LUN nicht von mehreren Hosts verwendet werden. Wenn eine separate LUN für eine Diagnosepartition verwendet wird, kann sie von mehreren Hosts gemeinsam verwendet werden.
  - Wenn Sie mithilfe von iBFT vom SAN starten, können Sie keine Diagnosepartition auf einer SAN-LUN einrichten. Verwenden Sie vSphere ESXi Dump Collector auf einem Remoteserver, um die Diagnoseinformationen Ihres Hosts zu erfassen. Informationen zu ESXi Dump Collector finden Sie unter *Installations- und Einrichtungshandbuch für vSphere* und *vSphere-Netzwerk*.

## Vorbereiten des iSCSI-SAN

Bevor Sie Ihren Host zum Starten von einer iSCSI-LUN konfigurieren, müssen Sie Ihr SAN vorbereiten und konfigurieren.

---

**Vorsicht** Wenn Sie über ein SAN starten und die Installation von ESXi per Skript erfolgt, müssen Sie bestimmte Schritte ausführen, um einen unerwünschten Datenverlust zu vermeiden.

---

### Verfahren

- 1 Schließen Sie die Netzkabel an, wie in den Handbüchern der betreffenden Geräte beschrieben.
- 2 Stellen Sie die IP-Verbindung zwischen dem Speichersystem und dem Server sicher.  
 Hierzu gehört ebenfalls die ordnungsgemäße Konfiguration aller Router und Switches im Speichernetzwerk. Speichersysteme müssen ein Ping-Signal an die iSCSI-Adapter in den Hosts senden können.

### 3 Konfigurieren Sie das Speichersystem.

- a Erstellen Sie ein Volume (oder eine LUN) im Speichersystem für Ihren Host, von dem gebootet werden soll.
- b Konfigurieren Sie das Speichersystem, sodass Ihr Host auf die zugewiesene LUN zugreifen kann.

Hierzu ist möglicherweise ein Update der ACLs mit den IP-Adressen, den iSCSI-Namen und dem CHAP-Authentifizierungsparameter, den Sie auf Ihrem Host verwenden, erforderlich. Auf einigen Speichersystemen müssen Sie nicht nur die Zugriffsdaten für den ESXi-Host angeben, sondern auch die zugewiesene LUN ausdrücklich mit dem Host verknüpfen.

- c Stellen Sie sicher, dass die LUN dem Host ordnungsgemäß präsentiert wird.
- d Stellen Sie sicher, dass kein anderes System auf die konfigurierte LUN zugreifen kann.
- e Schreiben Sie sich den iSCSI-Namen und die IP-Adresse der Ziele auf, die dem Host zugewiesen sind.

Sie benötigen diese Informationen für die Konfiguration Ihrer iSCSI-Adapter.

## Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN

Wenn Ihr ESXi-Host einen unabhängigen Hardware-iSCSI-Adapter verwendet, wie z. B. einen QLogic-HBA, müssen Sie den Adapter so konfigurieren, dass er vom SAN startet.

Dieses Verfahren erläutert, wie der QLogic-iSCSI-HBA für das Starten vom SAN aktiviert wird. Weitere Informationen und aktuelle Einzelheiten zu den QLogic-Adapter-Konfigurationseinstellungen finden Sie auf der QLogic-Website.

### Voraussetzungen

Da Sie zuerst vom VMware-Installationsmedium starten müssen, richten Sie Ihren Host so ein, dass er von CD/DVD-ROM startet. Ändern Sie hierzu die Startreihenfolge in den BIOS-Einstellungen des Systems.

### Verfahren

- 1 Legen Sie die Installations-CD/DVD in das CD/DVD-ROM-Laufwerk ein und starten Sie den Host neu.
- 2 Stellen Sie im BIOS ein, dass der Host zuerst vom CD/DVD-ROM-Laufwerk aus gestartet wird.
- 3 Drücken Sie während des Server-POST die Tastenkombination Strg+q, um das QLogic-iSCSI-HBA-Konfigurationsmenü zu öffnen.
- 4 Wählen Sie den zu konfigurierenden E/A-Port.

Standardmäßig ist „Adapterstartmodus“ auf „Deaktivieren“ gesetzt.

- 5 Konfigurieren Sie den HBA.
  - a Wählen Sie aus dem Menü **Fast!UTIL-Optionen** die Option **Konfigurationseinstellungen > Hostadaptereinstellungen** aus.
  - b Konfigurieren Sie die folgenden Einstellungen für Ihren Hostadapter: Initiator-IP-Adresse, Subnetzmaske, Gateway, Initiator-iSCSI-Name und CHAP (falls erforderlich).
- 6 Konfigurieren Sie die iSCSI-Einstellungen.
 

Weitere Informationen hierzu finden Sie unter [Konfigurieren der iSCSI-Starteinstellungen](#).
- 7 Speichern Sie die Änderungen, und starten Sie das System neu.

## Konfigurieren der iSCSI-Starteinstellungen

Wenn Sie den ESXi-Host zum Starten von iSCSI einrichten, müssen Sie die iSCSI-Starteinstellungen konfigurieren.

### Verfahren

- 1 Wählen Sie aus dem Menü **Fast!UTIL-Optionen** die Option **Konfigurationseinstellungen > iSCSI-Starteinstellungen** aus.
- 2 Bevor Sie SendTargets festlegen können, setzen Sie „Adapterstartmodus“ auf **Manuell**.
- 3 Aktivieren Sie **Primäre Startgeräteinstellungen**.
  - a Geben Sie **Ziel-IP** und **Zielport** für die Zielerkennung ein.
  - b Die Felder **Start-LUN (Boot LUN)** und **iSCSI-Name (iSCSI Name)** müssen nicht ausgefüllt werden, wenn nur ein iSCSI-Ziel und eine LUN für die angegebene Adresse vorhanden sind, über die der Start erfolgen soll. Anderenfalls müssen Sie diese Felder ausfüllen, um sicherzustellen, dass der Start nicht über ein Volume oder ein anderes System durchgeführt wird. Nachdem das Zielspeichersystem erreicht wurde, werden diese Felder nach einem erneuten Prüfen ausgefüllt angezeigt.
  - c Speichern Sie die Änderungen.
- 4 Wählen Sie im Menü **iSCSI-Starteinstellungen (iSCSI Boot Settings)** das primäre Startgerät. Zur Suche nach neuen Ziel-LUNs wird ein erneuter Prüfvorgang des HBA ausgeführt.
- 5 Wählen Sie das iSCSI-Ziel.

---

**Hinweis** Wenn mehr als eine LUN im Ziel vorhanden ist, können Sie eine bestimmte LUN-ID wählen, indem Sie nach Auswahl des iSCSI-Gerätes die **Eingabetaste** drücken.

---

- 6 Öffnen Sie das Menü **Primäre Startgeräteeeinstellungen (Primary Boot Device Setting)**. Nach der erneuten Prüfung sind die Felder **Start-LUN (Boot LUN)** und **iSCSI-Name (iSCSI Name)** ausgefüllt. Ändern Sie den Wert von **Start-LUN (Boot LUN)** in die gewünschte LUN-ID.

## iBFT-iSCSI-Start - Überblick

ESXi-Hosts können mithilfe von Software- oder abhängigen Hardware-iSCSI-Adaptoren und Netzwerkadaptern von einer iSCSI-SAN gestartet werden.

Der Host muss über einen Netzwerkadapter verfügen, der das Starten von iSCSI und das iBFT-Format (iBFT, iSCSI-Start-Firmware-Tabelle) unterstützt, um ESXi bereitzustellen und vom iSCSI-SAN starten zu können. Die iBFT ist eine Methode zur Übermittlung von Parametern zum iSCSI-Startgerät an ein Betriebssystem.

Bevor Sie ESXi installieren und vom iSCSI-SAN starten, konfigurieren Sie das Netzwerk und die iSCSI-Startparameter auf dem Netzwerkadapter und aktivieren Sie den Adapter für das Starten von iSCSI. Da die Konfiguration des Netzwerkadapters herstellerabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Herstellers.

Beim ersten Starten über iSCSI verbindet sich die iSCSI-Start-Firmware auf Ihrem System mit einem iSCSI-Ziel. Wenn die Anmeldung erfolgreich ist, speichert die Firmware die Netzwerk- und iSCSI-Start-Parameter in der iBFT und die Tabelle im Arbeitsspeicher des Systems. Das System verwendet diese Tabelle zur Konfiguration seiner eigenen iSCSI-Verbindung und seines iSCSI-Netzwerks sowie zum Starten.

Die iBFT-iSCSI-Startsequenz wird in der folgenden Liste beschrieben.

- 1 Beim Neustart erkennt das System-BIOS die iSCSI-Start-Firmware auf dem Netzwerkadapter.
- 2 Die iSCSI-Start-Firmware verwendet zum Verbinden mit dem angegebenen iSCSI-Ziel die vorkonfigurierten Startparameter.
- 3 Wenn die Verbindung mit dem iSCSI-Ziel hergestellt wurde, schreibt die iSCSI-Start-Firmware die Netzwerk- und iSCSI-Startparameter in die iBFT und speichert die Tabelle im Systemarbeitsspeicher.

---

**Hinweis** Das System verwendet diese Tabelle zur Konfiguration seiner eigenen iSCSI-Verbindung und seines iSCSI-Netzwerks sowie zum Starten.

---

- 4 Das BIOS startet das Startgerät.
- 5 Der VMkernel startet den Ladevorgang und übernimmt den Startvorgang.
- 6 Der VMkernel verwendet die Startparameter aus der iBFT zum Herstellen einer Verbindung mit dem iSCSI-Ziel.
- 7 Nach Herstellung der iSCSI-Verbindung wird das System gestartet.



## iBFT-iSCSI-Start - Überlegungen

Wenn Sie mithilfe von iBFT-aktivierten Netzwerkadaptern einen ESXi-Host von iSCSI starten, muss Folgendes beachtet werden.

- Aktualisieren Sie mithilfe der vom Anbieter bereitgestellten Tools den Startcode Ihrer Netzwerkkarte und die iBFT-Firmware, bevor Sie versuchen, VMware ESXi zu installieren und zu starten. Informationen über den unterstützten Startcode und die iBFT-Firmware-Versionen für den VMware ESXi-iBFT-Start finden Sie in der Anbieterdokumentation und VMware HCL.
- Der iBFT iSCSI-Start unterstützt kein Failover für die iBFT-aktivierten Netzwerkadapter.
- Nach dem Einrichten des Hosts für das Starten von iBFT-iSCSI gelten die folgenden Einschränkungen:
  - Sie können den Software-iSCSI-Adapter nicht deaktivieren. Wenn die iBFT-Konfiguration im BIOS vorhanden ist, aktiviert der Host den Software-iSCSI-Adapter bei jedem Neustart neu.

---

**Hinweis** Wenn Sie den iBFT-fähigen Netzwerkadapter nicht für den iSCSI-Start verwenden und nicht möchten, dass der Software-iSCSI-Adapter immer aktiviert ist, entfernen Sie die iBFT-Konfiguration aus dem Netzwerkadapter.

---

- Sie können das iBFT-iSCSI-Startziel nicht mit dem vSphere Web Client entfernen. Das Ziel erscheint auf der Liste der statischen Ziele des Adapters.

## Konfigurieren des Startens von iBFT über ein SAN

Sie können mithilfe des Software-iSCSI-Adapters oder eines abhängigen Hardware-iSCSI-Adapters und eines Netzwerkadapters vom iSCSI-SAN aus starten. Der Netzwerkadapter muss die iBFT unterstützen.

Wenn Sie Ihren Host für das Starten mit iBFT einrichten, führen Sie mehrere Aufgaben durch.

### Verfahren

#### 1 Konfigurieren der iSCSI-Startparameter

Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte iSCSI-Start-Firmware verfügen, um den iSCSI-Startvorgang zu starten. Wenn Sie die Firmware konfigurieren, geben Sie die Netzwerk- und iSCSI-Parameter an und aktivieren Sie den Adapter für den iSCSI-Start.

#### 2 Ändern der Startsequenz im BIOS

Wenn Sie Ihren Host so einrichten, dass er vom iBFT-iSCSI gestartet wird, ändern Sie die Startsequenz, sodass Ihr Host in der entsprechenden Reihenfolge gestartet wird.

#### 3 Installieren von ESXi auf dem iSCSI-Ziel

Sie müssen beim Einrichten Ihres Hosts zum Starten von iBFT-iSCSI das ESXi-Image auf der Ziel-LUN installieren.

#### 4 Starten von ESXi vom iSCSI-Ziel

Nachdem Sie den Host für den iBFT-iSCSI-Start vorbereitet und die ESXi-Images auf das iSCSI-Ziel kopiert haben, führen Sie den eigentlichen Startvorgang durch.

### Konfigurieren der iSCSI-Startparameter

Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte iSCSI-Start-Firmware verfügen, um den iSCSI-Startvorgang zu starten. Wenn Sie die Firmware konfigurieren, geben Sie die Netzwerk- und iSCSI-Parameter an und aktivieren Sie den Adapter für den iSCSI-Start.

Die Konfiguration auf dem Netzwerkadapter kann dynamisch oder statisch sein. Wenn Sie die dynamische Konfiguration verwenden, geben Sie an, dass alle Ziel- und Initiator-Startparameter über DHCP bezogen werden. Bei der statischen Konfiguration geben Sie Daten manuell ein, zu denen die IP-Adresse und der Initiator-IQN Ihres Hosts sowie die Zielparameter gehören.

#### Verfahren

- ◆ Geben Sie auf dem Netzwerkadapter, den Sie zum Starten von iSCSI verwenden, die Netzwerk- und iSCSI-Parameter an.

Da die Konfiguration des Netzwerkadapters herstellerabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Herstellers.

### Ändern der Startsequenz im BIOS

Wenn Sie Ihren Host so einrichten, dass er vom iBFT-iSCSI gestartet wird, ändern Sie die Startsequenz, sodass Ihr Host in der entsprechenden Reihenfolge gestartet wird.

Ändern Sie die BIOS-Startsequenz auf die folgende Sequenz:

- iSCSI
- DVD-ROM

Weil das Ändern der Startsequenz im BIOS herstellerspezifisch ist, sollten Sie die entsprechenden Anweisungen in der Herstellerdokumentation zu Rate ziehen. In der nachfolgenden Beispielprozedur wird veranschaulicht, wie die Startsequenz eines Dell-Hosts mit einem Broadcom-Netzwerkadapter geändert wird.

#### Verfahren

- 1 Schalten Sie den Host ein.
- 2 Drücken Sie F2 während der Selbstdiagnose des Einschaltvorgangs (POST = Power-On Self-Test), um das BIOS-Setup aufzurufen.
- 3 Wählen Sie im BIOS-Setup **Boot Sequence** und drücken Sie die Eingabetaste.
- 4 Ordnen Sie im Startsequenz-Menü die startbaren Elemente so, dass iSCSI dem DVD-ROM voransteht.
- 5 Drücken Sie ESC, um das Startsequenz-Menü zu verlassen.
- 6 Drücken Sie die ESC-Taste, um das BIOS-Setup zu beenden.

- 7 Wählen Sie **Änderungen speichern** und klicken Sie auf **Beenden**, um das BIOS-Setup-Menü zu beenden.

## Installieren von ESXi auf dem iSCSI-Ziel

Sie müssen beim Einrichten Ihres Hosts zum Starten von iBFT-iSCSI das ESXi-Image auf der Ziel-LUN installieren.

### Voraussetzungen

- Konfigurieren Sie die iSCSI-Start-Firmware auf Ihrer Start-Netzwerkkarte, um auf die Ziel-LUN zu verweisen, die Sie als Start-LUN verwenden möchten.
- Ändern Sie die Startsequenz im BIOS, sodass iSCSI dem DVD-Laufwerk vorangestellt wird.
- Falls Sie Broadcom-Adapter verwenden, legen Sie die Option **Boot to iSCSI target** auf **Disabled** fest

### Verfahren

- 1 Legen Sie das Installationsmedium in das CD/DVD-ROM-Laufwerk ein und starten Sie den Host neu.
- 2 Wenn das Installationsprogramm startet, führen Sie die Standardinstallationsprozedur aus.
- 3 Wählen Sie die iSCSI-LUN als Installationsziel aus, wenn Sie dazu aufgefordert werden.  
Das Installationsprogramm kopiert das ESXi-Start-Image in die iSCSI-LUN.
- 4 Entfernen Sie nach dem Neustart des Systems die Installations-DVD aus dem Laufwerk.

## Starten von ESXi vom iSCSI-Ziel

Nachdem Sie den Host für den iBFT-iSCSI-Start vorbereitet und die ESXi-Images auf das iSCSI-Ziel kopiert haben, führen Sie den eigentlichen Startvorgang durch.

### Voraussetzungen

- Konfigurieren Sie die iSCSI-Start-Firmware auf Ihrer Start-Netzwerkkarte, um auf die Ziel-LUN zu verweisen.
- Ändern Sie die Startsequenz im BIOS, sodass iSCSI dem Startgerät vorangestellt wird.
- Falls Sie Broadcom-Adapter verwenden, legen Sie die Option **Boot to iSCSI target** auf **Enabled** fest

### Verfahren

- 1 Starten Sie den Host neu.  
  
Der Host startet mithilfe von iBFT-Daten vom iSCSI-LUN. Beim Erststart richtet das iSCSI-Initialisierungsskript das Standardnetzwerk ein. Das Netzwerk-Setup überdauert nachfolgende Neustarts.
- 2 (Optional) Passen Sie die Netzwerkkonfiguration mithilfe des vSphere Web Client an.

## Best Practices für Netzwerke

Um den ESXi-Host mithilfe von iBFT über iSCSI zu starten, müssen Sie das Netzwerk ordnungsgemäß konfigurieren.

Für eine höhere Sicherheit und größere Leistung sollten auf dem Host redundante Netzwerkadapter vorhanden sein.

Wie Sie alle Netzwerkadapter einrichten, hängt davon ab, ob Ihre Umgebung für den iSCSI-Datenverkehr und den Hostverwaltungs-Datenverkehr freigegebene oder isolierte Netzwerke verwendet.

### Freigegebene iSCSI- und Verwaltungsnetzwerke

Konfigurieren Sie die Netzwerk- und iSCSI-Parameter auf dem ersten Netzwerkadapter auf dem Host. Nach dem Starten des Hosts können Sie sekundäre Netzwerkadapter zur Standard-Portgruppe hinzufügen.

### Isolierte iSCSI- und Verwaltungsnetzwerke

Befolgen Sie diese Richtlinien, wenn Sie isolierte iSCSI- und Verwaltungsnetzwerke konfigurieren.

- Ihre isolierten Netzwerke müssen sich in verschiedenen Subnetzen befinden.
- Wenn Sie zum Isolieren der Netzwerke VLANs verwenden, müssen diese verschiedene Subnetze haben, um die ordnungsgemäße Einrichtung der Routing-Tabellen sicherzustellen.
- Es wird empfohlen, die Konfiguration so vorzunehmen, dass sich der iSCSI-Adapter und das Ziel in demselben Subnetz befinden. Es gelten die folgenden Einschränkungen, wenn Sie den iSCSI-Adapter und das Ziel in unterschiedlichen Subnetzen einrichten:
  - Das Standard-VMkernel-Gateway muss in der Lage sein, sowohl den Verwaltungs- als auch den iSCSI-Datenverkehr weiterzuleiten.
  - Nachdem Sie Ihren Host gestartet haben, können Sie den iBFT-aktivierten Netzwerkadapter nur für iBFT verwenden. Sie können den Adapter nicht für anderen iSCSI-Datenverkehr verwenden.
- Verwenden Sie den ersten physischen Netzwerkadapter für das Verwaltungsnetzwerk.
- Verwenden Sie den zweiten physischen Netzwerkadapter für das iSCSI-Netzwerk. Stellen Sie sicher, dass Sie die iBFT konfigurieren.
- Nach dem Starten des Hosts können Sie sekundäre Netzwerkadapter zu den Verwaltungs- und iSCSI-Netzwerken hinzufügen.

### Ändern von iBFT-iSCSI-Starteinstellungen

Falls sich auf dem iSCSI-Speicher oder Ihrem Host Einstellungen ändern, wie z. B. der IQN-Name oder die IP-Adresse, aktualisieren Sie die iBFT. Für diese Aufgabe wird vorausgesetzt, dass die Start-LUN und die auf der LUN gespeicherten Daten intakt bleiben.

## Verfahren

- 1 Fahren Sie den ESXi-Host herunter.
- 2 Ändern Sie die iSCSI-Speichereinstellungen.
- 3 Aktualisieren Sie die iBFT auf dem Host mit den neuen Einstellungen.
- 4 Starten Sie den Host neu.

Der Host startet mit den neuen Informationen, die in der iBFT gespeichert sind.

## iBFT-iSCSI-Start - Fehlerbehebung

In den Themen dieses Abschnitts wird beschrieben, wie Sie Probleme identifizieren und beheben, die beim Verwenden des iBFT-iSCSI-Startvorgangs auftreten können.

### Verlust des Gateways des Systems verursacht einen Ausfall der Netzwerkverbindung

Die Netzwerkverbindung geht verloren, wenn Sie eine dem iBFT-Netzwerkadapter zugewiesene Portgruppe löschen.

#### Problem

Die Netzwerkverbindung geht nach dem Löschen einer Portgruppe verloren.

#### Ursache

Wenn Sie während der Installation von ESXi ein Gateway im iBFT-aktivierten Netzwerkadapter angeben, wird dieses Gateway zum Standard-Gateway des Systems. Das Standard-Gateway des Systems geht verloren, wenn Sie die dem Netzwerkadapter zugewiesene Portgruppe löschen. Diese Aktion verursacht den Verlust der Netzwerkverbindung.

#### Lösung

Legen Sie ein iBFT-Gateway daher nur dann fest, wenn es erforderlich ist. Wenn das Gateway erforderlich ist, legen Sie nach der Installation das Standard-Gateway des Systems auf das Gateway fest, das das Verwaltungsnetzwerk verwendet.

### Ändern der iSCSI-Startparameter sorgt dafür, dass ESXi in statusfreiem Modus startet

Durch das Ändern der iSCSI-Startparameter auf dem Netzwerkadapter nach dem Erststart wird die iSCSI- und Netzwerkkonfiguration auf dem ESXi-Host nicht aktualisiert.

#### Problem

Wenn Sie nach dem ersten ESXi-Start von iSCSI die iSCSI-Startparameter auf dem Netzwerkadapter ändern, startet der Host in einem statusfreien Modus.

### **Ursache**

Die Firmware verwendet die aktualisierte Startkonfiguration und kann eine Verbindung mit dem iSCSI-Ziel herstellen und das ESXi-Image laden. Wenn geladen, greift das System jedoch nicht auf die neuen Parameter zurück, sondern verwendet weiterhin die dauerhaften Netzwerk- und iSCSI-Parameter aus dem vorherigen Startvorgang. Infolgedessen kann der Host keine Verbindung zum Ziel herstellen und startet im statusfreien Modus.

### **Lösung**

- 1 Stellen Sie über den vSphere Web Client eine Verbindung mit dem ESXi-Host her.
- 2 Konfigurieren Sie iSCSI und das Netzwerk auf dem Host neu, sodass sie mit den iBFT-Parametern übereinstimmen.
- 3 Führen Sie eine erneute Prüfung durch.

# Best Practices für iSCSI-Speicher

# 12

Befolgen Sie bei der Verwendung von ESXi mit iSCSI-SAN die Best Practices von VMware, um Probleme zu vermeiden.

Erkundigen Sie sich bei Ihrem Speicheranbieter, ob Ihr Speichersystem die Hardwarebeschleunigungsfunktionen der Storage-APIs für die Array-Integration unterstützt. Wenn ja, suchen Sie in der Dokumentation Ihres Anbieters nach Informationen zur Aktivierung der Unterstützung für die Hardwarebeschleunigung auf dem Speichersystem. Weitere Informationen finden Sie unter [Kapitel 23 Speicherhardware-Beschleunigung](#).

Dieses Kapitel enthält die folgenden Themen:

- [Vermeiden von iSCSI-SAN-Problemen](#)
- [Optimieren der iSCSI-SAN-Speicherleistung](#)
- [Überprüfen von Ethernet-Switch-Statistiken](#)

## Vermeiden von iSCSI-SAN-Problemen

Bei Verwendung von ESXi in Verbindung mit einem SAN müssen Sie bestimmte Richtlinien befolgen, um SAN-Probleme zu vermeiden.

In diesem Abschnitt erhalten Sie einige Tipps, wie sich Probleme mit der SAN-Konfiguration vermeiden lassen:

- Platzieren Sie nur einen einzigen VMFS-Datenspeicher in jeder LUN. Mehrere VMFS-Datenspeicher in einer LUN werden nicht empfohlen.
- Ändern Sie die vom System festgelegte Pfadrichtlinie nur, wenn Sie die Auswirkungen dieser Änderung kennen und verstehen.
- Erstellen Sie eine ausführliche Dokumentation. Notieren Sie Informationen zu Konfiguration, Zugriffssteuerung, Speicher, Switch, Server und iSCSI-HBA-Konfiguration, Software- und Firmware-Versionen sowie zum Speicherkabelplan.
- Erstellen Sie einen Notfallplan bei Ausfällen:
  - Kopieren Sie Ihre Topologiezuordnungen mehrfach. Ermitteln Sie für jedes Element, welche Auswirkungen ein Ausfall dieses Elements auf das SAN hat.

- Stellen Sie mithilfe einer Liste aller Verbindungen, Switches, HBAs und anderen Elemente sicher, dass Sie keine wichtige Fehlerstelle in Ihrem Design übersehen haben.
- Stellen Sie sicher, dass die iSCSI-HBAs an den geeigneten Steckplätzen des ESXi-Hosts installiert sind (basierend auf Steckplatz- und Busgeschwindigkeit). Richten Sie einen PCI-Bus-Lastenausgleich für alle Busse des Servers ein.
- Machen Sie sich mit den verschiedenen Überwachungspunkten in Ihrem Speichernetzwerk an allen Sichtbarkeitspunkten vertraut (einschließlich ESXi-Leistungsdiagramme sowie Statistiken zu Ethernet-Switches und Speicherleistung).
- Seien Sie beim Ändern der IDs der LUNs vorsichtig, die über von Ihrem Host verwendete VMFS-Datenspeicher verfügen. Wenn Sie die ID ändern, schlagen die auf dem VMFS-Datenspeicher ausgeführten virtuellen Maschinen fehl.

Wenn sich keine laufenden virtuellen Maschinen auf dem VMFS-Datenspeicher befinden, nachdem Sie die ID der LUN geändert haben, müssen Sie zum Zurücksetzen der ID auf dem Host eine erneute Prüfung durchführen. Weitere Informationen über das erneute Prüfen finden Sie unter [Vorgänge zum Aktualisieren und zur erneuten Prüfung von Speichern](#).

- Wenn Sie den standardmäßigen iSCSI-Namen Ihres iSCSI-Adapters ändern müssen, stellen Sie sicher, dass der Name, den Sie eingeben, weltweit eindeutig und ordnungsgemäß formatiert ist. Um Speicherzugriffsprobleme zu vermeiden, weisen Sie unterschiedlichen Adaptern niemals denselben iSCSI-Namen zu, auch nicht auf unterschiedlichen Hosts.

## Optimieren der iSCSI-SAN-Speicherleistung

Bei der Optimierung einer typischen SAN-Umgebung müssen verschiedene Faktoren berücksichtigt werden.

Bei ordnungsgemäßer Konfiguration der Netzwerkumgebung sollten die iSCSI-Komponenten einen ausreichenden Durchsatz und eine ausreichend geringe Latenz für iSCSI-Initiatoren und -Ziele bieten. Wenn das Netzwerk überlastet und die maximale Leistung von Verbindungen, Switches oder Routern erreicht ist, ist die iSCSI-Leistung beeinträchtigt und möglicherweise nicht mehr ausreichend für ESXi-Umgebungen.

## Speichersystemleistung

Einer der wichtigsten Faktoren für die Optimierung einer kompletten iSCSI-Umgebung ist die Speichersystemleistung.

Bei Problemen mit der Speichersystemleistung lesen Sie die entsprechende Dokumentation des Speichersystem-Anbieters.



Bedenken Sie beim Zuweisen von LUNs, dass über verschiedene Hosts auf jede gemeinsam genutzte LUN zugegriffen werden kann und dass auf jedem Host mehrere virtuelle Maschinen ausgeführt werden können. Auf einer LUN, die vom ESXi-Host verwendet wird, sind E/A-Vorgänge von einer Vielzahl von unterschiedlichen Anwendungen möglich, die unter verschiedenen Betriebssystemen ausgeführt werden. Aufgrund dieser unterschiedlichen Arbeitslast sollte die RAID-Gruppe mit den ESXi-LUNs keine LUNs enthalten, die von anderen Hosts verwendet werden, auf denen nicht ESXi für E/A-intensive Anwendungen ausgeführt wird.

Aktivieren Sie die Lese- und Schreibcache.

Lastenausgleich ist der Vorgang zum Verteilen von E/A-Anforderungen eines Servers auf alle verfügbaren Speicherprozessoren und die verknüpften Hostserverpfade. Das Ziel ist die Optimierung der Leistung im Hinblick auf den Durchsatz (E/A pro Sekunde, MB pro Sekunde oder Reaktionszeiten).

SAN-Speichersysteme müssen kontinuierlich neu ausgelegt und optimiert werden, um sicherzustellen, dass die E/A-Last auf alle Speichersystempfade verteilt ist. Um diese Anforderung zu erfüllen, verteilen Sie die Pfade zu den LUNs auf alle Speicherprozessoren. Das Ergebnis ist ein optimaler Lastenausgleich. Eine sorgfältige Überwachung zeigt an, wenn die LUN-Verteilung manuell angepasst werden muss.

Bei der Optimierung von Speichersystemen mit statischem Lastenausgleich ist die Überwachung der spezifischen Leistungsstatistiken (beispielsweise E/A-Vorgänge pro Sekunde, Blocks pro Sekunde und Reaktionszeit) und Verteilung der LUN-Arbeitslast auf alle Speicherprozessoren von größter Bedeutung.

## Serverleistung mit iSCSI

Um eine optimale Serverleistung sicherzustellen, müssen verschiedene Faktoren berücksichtigt werden.

Der Zugriff jeder Serveranwendung auf den integrierten Speicher muss mit den folgenden Bedingungen gewährleistet sein:

- Hohe E/A-Rate (Anzahl an E/A-Vorgängen pro Sekunde)
- Hoher Durchsatz (MB pro Sekunde)
- Minimale Latenz (Reaktionszeiten)

Da für jede Anwendung andere Anforderungen gelten, können Sie diese Ziele erreichen, indem Sie eine geeignete RAID-Gruppe für das Speichersystem wählen. Zum Erreichen von Leistungszielen führen Sie die folgenden Aufgaben aus:

- Platzieren Sie jede LUN in einer RAID-Gruppe, welche die erforderlichen Leistungsebenen bietet. Beachten Sie Aktivitäten und Ressourcennutzung von anderen LUNs in der zugewiesenen RAID-Gruppe. Mit einer hochleistungsfähigen RAID-Gruppe mit zu vielen Anwendungen, die eine E/A-Last verursachen, können die Leistungsziele möglicherweise nicht erreicht werden, die für eine Anwendung auf dem ESXi-Host erforderlich sind.

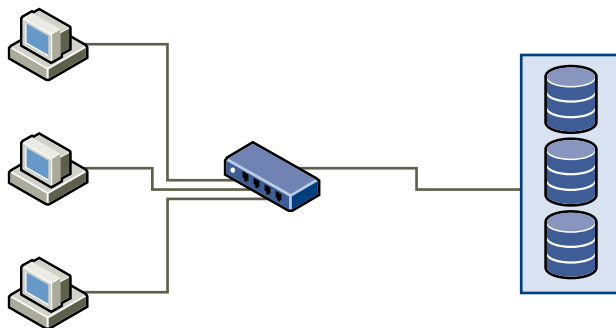
- Stellen Sie jeden Server mit einer ausreichenden Anzahl an iSCSI-Hardware-Adaptern bereit, um einen maximalen Durchsatz für alle Anwendungen zu ermöglichen, die während der Spitzenzeiten auf dem Server gehostet werden. Bei Verteilung der E/A-Last auf mehrere Ports wird ein höherer Durchsatz und eine geringere Latenz für jede Anwendung erreicht.
- Um für Software-iSCSI Redundanz zu bieten, verbinden Sie den Initiator mit allen Netzwerkadaptern, die für die iSCSI-Konnektivität verwendet werden.
- Beim Zuweisen von LUNs oder RAID-Gruppen für ESXi-Systeme werden diese Ressourcen durch mehrere Betriebssysteme gemeinsam verwendet. Daher kann die erforderliche Leistung jeder LUN im Speichersubsystem beim Einsatz von ESXi-Systemen deutlich höher sein als bei Verwendung von physischen Maschinen. Wenn Sie z. B. die Ausführung von vier E/A-intensiven Anwendungen planen, weisen Sie die vierfache Leistungskapazität für die ESXi-LUNs zu.
- Bei der gemeinsamen Verwendung mehrerer ESXi-Systeme mit vCenter Server, steigt die erforderliche Leistung für das Speichersubsystem entsprechend.
- Die Anzahl an ausstehenden E/A-Vorgängen von Anwendungen, die auf einem ESXi-System ausgeführt werden, sollte mit der Anzahl an E/A-Vorgängen übereinstimmen, die das SAN verarbeiten kann.

## Netzwerkleistung

Ein typisches SAN umfasst verschiedene Computer, die über ein Netzwerk aus Switches mit verschiedenen Speichersystemen verbunden sind. Mehrere Computer greifen häufig auf denselben Speicher zu.

„Eine einzige Ethernet-Verbindung mit dem Speicher“ zeigt mehrere Computersysteme, die über einen Ethernet-Switch mit einem Speichersystem verbunden sind. In dieser Konfiguration sind die einzelnen Systeme über eine einzige Ethernet-Verbindung mit dem Switch verbunden, der ebenfalls über eine einzige Ethernet-Verbindung mit dem Speichersystem verbunden ist. In den meisten Konfigurationen, mit modernen Switches und typischem Datenverkehr, stellt dies kein Problem dar.

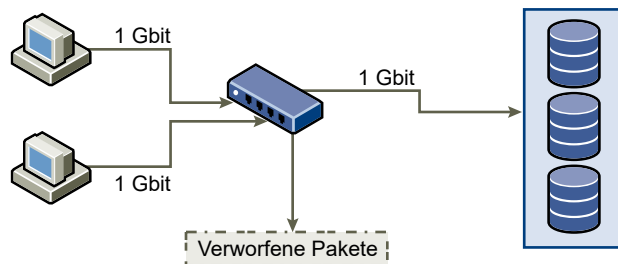
Abbildung 12-1. Eine einzige Ethernet-Verbindung mit dem Speicher



Wenn Systeme Daten aus dem Speicher lesen, ist die maximale Antwort des Speichers, genügend Daten zu senden, um die Verbindung zwischen den Speichersystemen und dem Ethernet-Switch zu füllen. Es ist unwahrscheinlich, dass ein einziges System oder eine einzige virtuelle Maschine die Netzwerkgeschwindigkeit vollständig nutzen kann. Wenn mehrere Systeme ein Speichergerät gemeinsam verwenden, ist dies jedoch die erwartete Situation.

Beim Schreiben von Daten in den Speicher versuchen möglicherweise mehrere Systeme oder virtuelle Maschinen, ihre Datenträger zu füllen. Wie „Verworfen Pakete“ zeigt, gehen in dieser Situation Daten zwischen den Systemen und dem Speichersystem verloren. Der Grund dafür ist, dass die zu übertragende Datenmenge die Kapazität einer einzigen Verbindung mit dem Speichersystem überschreitet. In diesem Fall verwirft der Switch Netzwerkpakete, da die Datenmenge, die übertragen werden kann, durch die Geschwindigkeit der Verbindung zwischen Switch und Speichersystem eingeschränkt ist.

**Abbildung 12-2. Verworfen Pakete**



Das Wiederherstellen von verworfenen Netzwerkpaketen führt zu einer erheblichen Leistungsbeeinträchtigung. Neben der Zeit zur Ermittlung, dass Daten verloren gegangen sind, ist für die erneute Übermittlung Netzwerkbandbreite erforderlich, die anderenfalls für aktuelle Transaktionen verwendet werden könnte.

iSCSI-Datenverkehr wird innerhalb des Netzwerks über TCP (Transmission Control Protocol) übermittelt. Bei TCP handelt es sich um ein zuverlässiges Übertragungsprotokoll, mit dem Sie sicherstellen, dass wiederholt versucht wird, verworfene Pakete zu übermitteln, bis diese ihr Ziel erreichen. TCP ist für eine Wiederherstellung und schnelle und problemlose Übermittlung von verworfenen Paketen konzipiert. Wenn der Switch jedoch regelmäßig Pakete verwirft, ist der Netzwerkdurchsatz deutlich reduziert. Das Netzwerk ist aufgrund von Anforderungen für ein erneutes Senden der Daten und durch die erneut gesendeten Pakete überlastet, und es werden letztendlich weniger Daten übertragen als in einem Netzwerk, das nicht überlastet ist.

Die meisten Ethernet-Switches können Daten puffern oder speichern, sodass jedes Gerät, das versucht Daten zu senden, die gleiche Möglichkeit hat, dieses Ziel zu erreichen. Diese Möglichkeit zum Puffern von Übertragungen erlaubt es, in Kombination mit einer Vielzahl an Systemen, die die Anzahl von ausstehenden Befehlen einschränken, kleine Datenpakete von mehreren Systemen der Reihe nach an ein Speichersystem zu senden.

Wenn bei umfangreichen Transaktionen mehrere Server versuchen, Daten über einen einzigen Switch-Port zu senden, kann die Kapazität des Switches zum Puffern einer Anforderung überschritten werden, während eine andere Anforderung übermittelt wird. In diesem Fall werden die Daten, die der Switch nicht senden kann, verworfen, und das Speichersystem muss die

erneute Übermittlung des verworfenen Pakets anfordern. Wenn ein Ethernet-Switch an einem Eingangsport beispielsweise 32 KB puffern kann, der mit dem Switch verbundene Server jedoch annimmt, das 256 KB an das Speichergerät gesendet werden können, gehen einige Daten verloren.

Die meisten verwalteten Switches bieten Informationen zu verworfenen Paketen, die in etwa den folgenden Angaben entsprechen:

```
*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

**Tabelle 12-1. Beispiel zu Switch-Informationen**

Schnittstelle	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

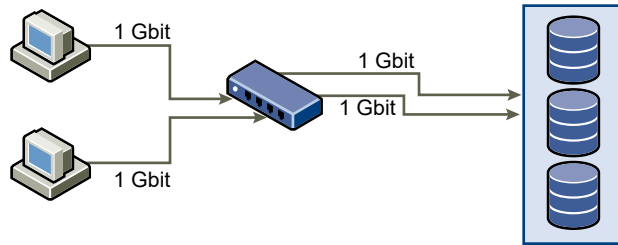
In diesem Beispiel eines Cisco-Switches lautet die verwendete Bandbreite 476303000 Bit/s, also weniger als die Hälfte der Kabelgeschwindigkeit. Trotzdem puffert die Schnittstelle eingehende Pakete, und es wurden einige Pakete verworfen. Die letzte Zeile dieser Schnittstellenübersicht zeigt, dass diese Schnittstelle bereits fast 10.000 eingehende Pakete in der IQD-Spalte verworfen hat.

Um dieses Problem zu verhindern, sind Konfigurationsänderungen erforderlich. Stellen Sie dabei sicher, dass eingehende Ethernet-Verbindungen nicht zu einer ausgehenden Verbindung zusammengefasst werden, sodass die Verbindung „überbucht“ wird. Wenn mehrere Verbindungen, deren Datenverkehr bereits fast die maximale Kapazität erreicht, zu einer kleineren Anzahl von Verbindungen zusammengefasst werden, ist eine Überbuchung möglich.

Im Allgemeinen sollten Anwendungen oder Systeme, die große Datenmengen in den Speicher schreiben (z. B. Datenerfassungs- oder Transaktionsprotokollierungssysteme) keine gemeinsamen Ethernet-Verbindungen zu einem Speichergerät verwenden. Für diese Anwendungstypen wird mit mehreren Verbindungen zu Speichergeräten eine optimale Leistung erzielt.

„Mehrere Verbindungen zwischen Switch und Speicher“ zeigt mehrere Verbindungen vom Switch zum Speicher.

Abbildung 12-3. Mehrere Verbindungen zwischen Switch und Speicher



Die Verwendung von VLANs oder VPNs ist keine geeignete Lösung für das Problem von überlasteten Verbindungen in Konfigurationen mit gemeinsam verwendeten Komponenten. VLANs und andere Konfigurationen zur virtuellen Partitionierung von Netzwerken bieten eine Möglichkeit für den logischen Aufbau eines Netzwerks, ändern jedoch nicht die physischen Kapazitäten von Verbindungen und Trunks zwischen Switches. Wenn für den Speicherdatenverkehr und anderen Netzwerkverkehr gemeinsame physische Verbindungen verwendet werden (wie in einem VPN), besteht das Risiko von überlasteten Verbindungen und Paketverlust. Gleiches gilt für VLANs mit gemeinsamen Interswitch-Trunks. Für die Leistungsberechnungen in einem SAN müssen die physischen Grenzen des Netzwerks, nicht die logischen Zuordnungen berücksichtigt werden.

## Überprüfen von Ethernet-Switch-Statistiken

Eine Vielzahl von Ethernet-Switches bieten verschiedene Methoden zur Überwachung des Switch-Status.

Switches mit Ports, welche die meiste Zeit einen fast maximalen Durchsatz erzielen, bieten keine optimale Leistung. Wenn Sie in Ihrem iSCSI-SAN über solche Ports verfügen, reduzieren Sie die Last. Wenn der Port mit einem ESXi-System oder iSCSI-Speicher verbunden ist, kann die Last über einen manuellen Lastenausgleich reduziert werden.

Wenn der Port mit mehreren Switches oder Routern verbunden ist, ziehen Sie die Installation zusätzlicher Verbindungen zwischen diesen Komponenten in Betracht, um eine höhere Last verarbeiten zu können. Ethernet-Switches bieten darüber hinaus meist Informationen zu Übertragungsfehlern, in der Warteschlange platzierten Paketen und verworfenen Ethernet-Paketen. Wenn ein Switch diese Bedingungen regelmäßig für Ports anzeigt, die für den iSCSI-Datenverkehr verwendet werden, bietet das iSCSI-SAN eine schlechte Leistung.

Verwalten des lokalen und vernetzten Speichergeräts, auf das Ihr ESXi-Host zugreifen kann.

Dieses Kapitel enthält die folgenden Themen:

- [Eigenschaften des Speichergeräts](#)
- [Grundlegendes zur Benennung von Speichergeräten](#)
- [Vorgänge zum Aktualisieren und zur erneuten Prüfung von Speichern](#)
- [Identifizieren von Problemen hinsichtlich der Gerätekonnektivität](#)
- [Aktivieren oder Deaktivieren der Locator-LED auf Speichergeräten](#)

## Eigenschaften des Speichergeräts

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 die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

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

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

**Tabelle 13-1. Informationen zum Speichergerät**

Informationen zum Speichergerät	Beschreibung
Name	Auch als Anzeigenamen bezeichnet. Es ist ein 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.
Betriebszustand	Gibt an, ob das Gerät gemountet bzw. nicht gemountet ist. Weitere Informationen finden Sie unter <a href="#">Speichergeräte trennen</a> .
LUN	Logical Unit Number (LUN) innerhalb des SCSI-Ziels. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.

Tabelle 13-1. Informationen zum Speichergerät (Fortsetzung)

Informationen zum Speichergerät	Beschreibung
Laufwerkstyp	Gibt an, ob das Gerät ein Flash-Laufwerk oder ein reguläres HDD-Laufwerk ist. Weitere Informationen zur Verwendung von Flash-Laufwerken finden Sie unter <a href="#">Kapitel 14 Arbeiten mit Flash-Geräten</a> .
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet. Das Protokoll hängt vom Typ des verwendeten Speichers ab. Siehe <a href="#">Physische Speichertypen</a> .
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten der Pfade zum Speichergerät verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In. Weitere Informationen finden Sie unter <a href="#">Verwalten mehrerer Pfade</a> .
Hardwarebeschleunigung	Informationen dazu, ob das Speichergerät den Host bei Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen finden Sie unter <a href="#">Kapitel 23 Speicherhardware-Beschleunigung</a> .
Speicherort	Ein Pfad zum Speichergerät im Verzeichnis <code>/vmfs/devices/</code> .
Partitionsformat	Ein Partitionsschema, das vom Speichergerät verwendet wird. Es kann sich hierbei um einen Master Boot Record (MBR) oder eine GUID-Partitionstabelle (GPT) handeln. Die GPT-Geräte unterstützen Datenspeicher größer als 2 TB. Weitere Informationen finden Sie unter <a href="#">VMFS-Datenspeicher und Speicherfestplattenformate</a> .
Partitionen	Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.
Multipathing-Richtlinien (VMFS-Datenspeicher)	Pfadauswahlrichtlinie und Speicher-Array-Typ-Richtlinie, die der Host für die Pfade zum Speicher verwendet. Weitere Informationen finden Sie unter <a href="#">Kapitel 17 Grundlegendes zu Multipathing und Failover</a> .
Pfade (VMFS-Datenspeicher)	Pfade, die zum Zugriff auf den Speicher verwendet werden, und ihr Status.

## Anzeigen von Speichergeräten für einen Host

Zeigen Sie alle für einen Host verfügbaren Speichergeräte an. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

In der Ansicht „Speichergeräte“ können Sie die Speichergeräte des Hosts anzeigen, ihre Informationen analysieren und ihre Eigenschaften ändern.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

Alle für den Host verfügbaren Speichergeräte werden unter „Speichergeräte“ aufgeführt.

- 4 Wählen Sie ein Gerät in der Liste aus, um Details zu diesem Gerät anzuzeigen.
- 5 Auf den Registerkarten unter „Gerätedetails“ können Sie auf zusätzliche Informationen zugreifen und Eigenschaften für das ausgewählte Gerät ändern.

Registerkarte	Beschreibung
Eigenschaften	Anzeigen von Geräteeigenschaften und -merkmalen. Anzeigen und Ändern von Multipathing-Richtlinien für das Gerät.
Pfade	Anzeigen der für das Gerät verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads.

## Anzeigen von Speichergeräten für einen Adapter

Zeigen Sie eine Liste der Speichergeräte an, auf die über einen bestimmten Speicheradapter auf dem Host zugegriffen werden kann.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf „Speicheradapter“.  
Alle auf dem Host installierten Speicheradapter werden unter „Speicheradapter“ aufgeführt.
- 4 Wählen Sie den Adapter in der Liste aus und klicken Sie auf die Registerkarte **Geräte**.  
Die Speichergeräte, auf die der Host über den Adapter zugreifen kann, werden angezeigt.

## Grundlegendes zur Benennung von Speichergeräten

Jedes Speichergerät oder jede LUN wird durch mehrere Namen identifiziert.

### Gerätebezeichner

Je nach Art der Speicherung verwendet der ESXi-Host unterschiedliche Algorithmen und Konventionen zum Generieren eines Bezeichners für jedes Speichergerät.

#### SCSI INQUIRY-Bezeichner.

Der Host verwendet den SCSI INQUIRY-Befehl zum Abfragen eines Speichergeräts und verwendet die Ergebnisdaten, insbesondere die „Page 83“-Informationen, zum Generieren eines eindeutigen Bezeichners. Gerätebezeichner auf Basis der „Page 83“-Informationen sind auf allen Hosts eindeutig und dauerhaft und verfügen über eines der folgenden Formate:

- *naa.Nummer*
- *t10.Nummer*
- *eui.Nummer*



Diese Formate entsprechen den Standards des T10 Committee. Weitere Informationen finden Sie in der SCSI-3-Dokumentation auf der Website des T10 Committee.

### Pfadbasierter Bezeichner.

Wenn das Gerät nicht die „Page 83“-Informationen bietet, generiert der Host einen mpx.*Pfad*-Namen, wobei *Pfad* der erste Pfad zu dem Gerät ist. Beispiel: mpx.vmhba1:C0:T1:L3. Dieser Bezeichner kann auf dieselbe Weise verwendet werden wie der SCSI INQUIRY-Bezeichner.

Der mpx.-Bezeichner wird für lokale Geräte unter der Annahme erstellt, dass ihre Pfadnamen eindeutig sind. Allerdings ist dieser Bezeichner weder eindeutig noch dauerhaft und kann sich nach jedem Start ändern.

In der Regel hat der Pfad zu dem Gerät das folgende Format:

*vmhbaAdapter:CKanal:TZiel:LLUN*

- *vmhbaAdapter* ist der Name des Speicheradapters. Der Name bezieht sich auf den physischen Adapter auf dem Host, nicht auf den SCSI-Controller, den die virtuellen Maschinen verwenden.

- *CChannel* ist die Nummer des Speicherkanals.

Software-iSCSI-Adapter und abhängige Hardwareadapter verwenden die Kanalnummer, um mehrere Pfade zu demselben Ziel anzuzeigen.

- *TZiel* ist die Zielnummer. Die Zielnummerierung wird vom Host festgelegt und kann sich ändern, wenn es eine Änderung in der Zuordnung von Zielen gibt, die für den Host sichtbar sind. Von verschiedenen Hosts gemeinsam verwendete Ziele verfügen möglicherweise nicht über dieselbe Zielnummer.

- *LLUN* ist die LUN-Nummer, die die Position der LUN innerhalb des Ziels angibt. 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.

### Legacy-Bezeichner

Zusätzlich zu SCSI INQUIRY- oder mpx.-Bezeichnern generiert ESXi für jedes Gerät einen alternativen Legacy-Namen. Der Bezeichner hat das folgende Format:

*vml.Nummer*

Der Legacy-Bezeichner enthält mehrere Ziffern, die das Gerät eindeutig identifizieren und teilweise von den „Page 83“-Informationen abgeleitet werden können, falls diese zur Verfügung stehen. Für nicht lokale Geräte, die die „Page 83“-Informationen nicht unterstützen, wird der vml.-Name als einzig verfügbarer eindeutiger Bezeichner verwendet.

## Beispiel: Anzeigen von Gerätenamen in der vSphere-CLI

Mit dem Befehl `esxcli --server=Servername storage core device list` können Sie alle Gerätenamen in der vSphere-CLI anzeigen. Die Ausgabe lautet in etwa wie folgt:

```
# esxcli --server=server_name storage core device list
naa.number
    Display Name: DGC Fibre Channel Disk(naa.number)
    ...
    Other UUIDs:vml.number
```

## Umbenennen von Speichergeräten

Sie können den Anzeigenamen eines Speichergeräts ändern. Der Anzeigename wird vom ESXi-Host basierend auf dem Speichertyp und dem Hersteller zugewiesen.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.
- 4 Wählen Sie das umzubenennende Gerät und klicken Sie auf **Umbenennen**.
- 5 Ändern Sie den Gerätenamen auf einen aussagekräftigen Namen.

## Vorgänge zum Aktualisieren und zur erneuten Prüfung von Speichern

Mit dem Aktualisierungsvorgang für Datenspeicher, Speichergeräte und Speicheradapter werden die Listen und Speicherinformationen im vSphere Web Client aktualisiert. Es werden beispielsweise die Informationen zur Datenspeicherkapazität aktualisiert. Wenn Sie Datenspeichermanagementaufgaben durchführen oder Änderungen an der SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut prüfen.

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, z. B. das Erstellen eines VMFS-Datenspeichers oder RDMS, das Hinzufügen einer Erweiterung und das Vergrößern oder Löschen eines VMFS-Datenspeichers, wird Ihr Speicher von Ihrem Host oder dem vCenter Server automatisch neu geprüft und aktualisiert. Sie können die Funktion für die automatische Neuprüfung deaktivieren, indem Sie den Filter für das erneute Prüfen eines Hosts ausschalten. Siehe [Ausschalten von Speicherfiltern](#).

In bestimmten Fällen müssen Sie die erneute Prüfung manuell durchführen. Sie können erneut alle verfügbaren Speicher Ihres Hosts oder, wenn Sie den vCenter Server verwenden, aller Hosts in einem Ordner, Cluster oder Datencenter prüfen.

Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, die über einen bestimmten Adapter verbunden sind, führen Sie eine erneute Prüfung dieses Adapters durch.

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

- Festlegen der Zone eines neuen Festplatten-Arrays auf einem SAN.
- Erstellen von neuen LUNs in einem SAN.
- Ändern Sie die Pfadmaskierung auf einem Host.
- Erneutes Verbinden eines Kabels.
- CHAP-Einstellungen ändern (nur iSCSI).
- Hinzufügen oder Entfernen von Erkennungsadressen oder statischen Adressen (nur iSCSI).
- Hinzufügen eines einzelnen Hosts zu vCenter Server, nachdem Sie einen Datenspeicher, der von den vCenter Server-Hosts und dem einzelnen Host gemeinsam genutzt wird, bearbeitet oder vom vCenter Server entfernt haben.

**Wichtig** Wenn bei einer erneuten Prüfung kein Pfad verfügbar ist, entfernt der Host den Pfad aus der Liste der Pfade zu dem Gerät. Der Pfad wird erneut in der Liste angezeigt, sobald er verfügbar und wieder einsatzbereit ist.

## Durchführen einer erneuten Speicherprüfung

Wenn Sie Änderungen an Ihrer Host- oder SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut prüfen. Sie können eine erneute Prüfung des für den Host, den Cluster oder das Datacenter verfügbaren Speichers durchführen. Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, auf die über einen bestimmten Host zugegriffen wird, führen Sie eine erneute Prüfung nur dieses Hosts durch.

### Verfahren

- 1 Gehen Sie im Objektnavigator des vSphere Web Client zu einem Host, einem Cluster, einem Datacenter oder einem Ordner, der bzw. das Hosts enthält.
- 2 Wählen Sie **Speicher > Speicher erneut prüfen** im Kontextmenü aus.
- 3 Geben Sie den Umfang der erneuten Prüfung an.

Option	Beschreibung
<b>Auf neue Speichergeräte prüfen</b>	Prüfen Sie alle Adapter erneut auf neu hinzugefügte Speichergeräte. Wenn neue Geräte erkannt werden, werden sie in der Geräteliste angezeigt.
<b>Auf neue VMFS-Volumes prüfen</b>	Prüfen Sie alle Speichergeräte neu, um neue Datenspeicher zu suchen, die seit der letzten Prüfung hinzugefügt wurden. Alle neuen Datenspeicher werden in der Datenspeicherliste angezeigt.

## Durchführen einer erneuten Adapterprüfung

Wenn Sie Änderungen an Ihrer SAN-Konfiguration vornehmen und diese Änderungen auf Speicher beschränken, auf die über einen bestimmten Adapter zugegriffen wird, führen Sie eine erneute Prüfung nur dieses Adapters durch.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speicheradapter** und wählen Sie den erneut zu prüfenden Adapter aus der Liste aus.
- 4 Klicken Sie auf das Symbol **Adapter erneut prüfen**.

## Ändern der Anzahl gescannter Speichergeräte

Der Zugriff eines ESXi-Hosts ist zwar auf 256 SCSI-Speichergeräte begrenzt, aber der mögliche LUN-ID-Bereich liegt zwischen 0 und 1023. ESXi ignoriert LUN-IDs ab 1024. Dieser Grenzwert wird durch den Parameter `Disk.MaxLUN` bestimmt, der den Standardwert „1024“ aufweist.

Der Wert von `Disk.MaxLUN` bestimmt außerdem, wie viele LUNs der SCSI-Scancode mithilfe einzelner INQUIRY-Befehle zu ermitteln versucht, wenn das SCSI-Ziel die direkte Erkennung mithilfe von REPORT\_LUNS nicht unterstützt.

Den Parameter `Disk.MaxLUN` können Sie in Abhängigkeit von Ihren Anforderungen ändern. Wenn beispielsweise in Ihrer Umgebung wenige Speichergeräte mit LUN-IDs zwischen 0 und 100 vorhanden sind, können Sie den Wert „101“ festlegen, um die Geschwindigkeit der Geräteerkennung für Ziele ohne Unterstützung von REPORT\_LUNS zu optimieren. Durch einen niedrigeren Wert kann die Zeit zum erneuten Prüfen und Starten verkürzt werden. Die Zeit zum erneuten Prüfen der Speichergeräte hängt jedoch von verschiedenen Faktoren ab, wie beispielsweise dem Typ des Speichersystems und der Auslastung des Speichersystems.

In anderen Situationen müssen Sie möglicherweise diesen Wert erhöhen, wenn in Ihrer Umgebung LUN-IDs über 1023 hinaus verwendet werden.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Systemeinstellungen“ **Disk.MaxLUN** und klicken Sie auf das Symbol **Bearbeiten**.
- 5 Ändern Sie den vorhandenen Wert in einen Wert Ihrer Wahl und klicken Sie auf **OK**.

Der eingegebene Wert gibt die LUN-ID nach der letzten LUN an, die Sie suchen möchten.

Wenn Sie beispielsweise nach LUN-IDs von 0 bis 100 suchen möchten, setzen Sie **Disk.MaxLUN** auf „101.

## Identifizieren von Problemen hinsichtlich der Gerätekonnektivität

Wenn bei Ihrem ESXi-Host ein Problem bei der Verbindung mit einem Speichergerät auftritt, behandelt der Host das Problem abhängig von bestimmten Faktoren als permanent oder temporär.

Verbindungsprobleme bei Speichergeräten haben verschiedene Ursachen. Obwohl ESXi die Ursache für die Nichtverfügbarkeit eines Speichergeräts oder seiner Pfade nicht immer ermitteln kann, unterscheidet der Host zwischen dem Status des permanenten Geräteverlusts (Permanent Device Loss, PDL) des Geräts und einem vorübergehenden Status „Keine Pfade verfügbar“ (All Paths Down, APD).

### Permanenter Geräteverlust (Permanent Device Loss, PDL)

Dies ist ein Zustand, der eintritt, wenn ein Speichergerät dauerhaft ausfällt oder vom Administrator entfernt oder ausgeschlossen wird. Es wird nicht erwartet, dass es verfügbar wird. Wenn das Gerät dauerhaft nicht mehr zur Verfügung steht, empfängt ESXi Erkennungs-codes oder eine Verweigerung der Anmeldung aus Speicher-Arrays und erkennt einen permanenten Geräteverlust.

### Keine Pfade verfügbar (All Paths Down, APD)

Ein Zustand, der eintritt, wenn ein Speichergerät für den Host nicht mehr verfügbar ist und keine Pfade zu dem Gerät verfügbar sind. ESXi behandelt dies als flüchtigen Zustand, weil in der Regel die Probleme mit dem Gerät temporär sind und anzunehmen ist, dass das Gerät wieder verfügbar wird.

## Erkennen von PDL-Bedingungen

Einem Speichergerät wird der Zustand PDL (Permanent Device Loss, dauerhafter Geräteverlust) zugeschrieben, wenn es für den ESXi-Host dauerhaft nicht verfügbar ist.

Die PDL-Bedingung tritt typischerweise ein, wenn ein Gerät versehentlich entfernt wird, wenn seine eindeutige ID sich ändert oder wenn ein nicht behebbarer Hardwarefehler auftritt.

Wenn das Speicher-Array bestimmt, dass das Gerät dauerhaft nicht verfügbar ist, sendet es SCSI-Erkennungs-codes an den ESXi-Host. Anhand der Erkennungs-Codes kann der Host erkennen, dass das Gerät ausgefallen ist, und den Gerätezustand PDL registrieren. Die Erkennungs-Codes müssen auf allen Pfaden zum Gerät erhalten werden, damit es als dauerhaft verloren betrachtet wird.

Wenn für das Gerät der Zustand PDL registriert wurde, versucht der Host nicht mehr, eine Verbindung mit dem Gerät herzustellen oder Befehle an das Gerät zu senden, um nicht blockiert zu werden bzw. seine Reaktionsfähigkeit nicht zu verlieren.

Der vSphere Web Client zeigt folgende Informationen für das Gerät an:

- Der Betriebszustand des Geräts wird in *Verbindung unterbrochen* geändert.
- Alle Pfade werden als *Ausgefallen* angezeigt.
- Die Datenspeicher auf dem Gerät werden grau dargestellt.

Der Host entfernt automatisch das PDL-Gerät und alle Pfade zu dem Gerät, falls keine offenen Verbindungen zu dem Gerät vorhanden sind, oder nachdem die letzte Verbindung getrennt wurde. Sie können das automatische Entfernen von Pfaden deaktivieren, indem Sie den erweiterten Hostparameter `Disk.AutoremoveOnPDL` auf „0“ festlegen. Weitere Informationen finden Sie unter [Festlegen von erweiterten Hostattributen](#).

Wenn die PDL-Bedingung für das Gerät nicht mehr vorhanden ist, kann es vom Host erkannt werden, wird aber als neues Gerät behandelt. Die Datenkonsistenz für virtuelle Maschinen auf dem wiederhergestellten Gerät ist nicht garantiert.

---

**Hinweis** Der Host kann die PDL-Bedingungen nicht erkennen und behandelt die Geräteverbindungsprobleme weiterhin als APD, wenn ein Speichergerät dauerhaft ausfällt, ohne dass entsprechende SCSI-Erkennungscode zurückgegeben werden oder die iSCSI-Anmeldung abgelehnt wird.

---

## Permanenter Geräteverlust (Permanent Device Loss, PDL) und SCSI-Erkennungscode

Im folgenden Beispiel für ein VMkernel-Protokoll gibt ein SCSI-Erkennungscode an, dass das Gerät den Zustand PDL aufweist.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Informationen zu SCSI-Erkennungscode finden Sie unter *Fehlerbehebung beim Speicher in vSphere-Fehlerbehebung*.

## Permanenter Geräteverlust (Permanent Device Loss, PDL) und iSCSI

Bei iSCSI-Arrays mit einer einzelnen LUN pro Ziel wird der Zustand PDL daran erkannt, dass die iSCSI-Anmeldung fehlschlägt. Ein iSCSI-Speicher-Array lehnt die Versuche des Hosts zum Starten einer iSCSI-Sitzung mit dem Grund `Ziel nicht verfügbar` ab. Wie bei den Erkennungs-Codes muss diese Antwort auf allen Pfaden empfangen werden, damit das Gerät als dauerhaft verloren betrachtet wird.

## Permanenter Geräteverlust (Permanent Device Loss, PDL) und virtuelle Maschinen

Wenn für das Gerät der Zustand PDL registriert wurde, beendet der Host alle Eingaben/Ausgaben von virtuellen Maschinen. vSphere HA kann PDL erkennen und ausgefallene virtuelle Maschinen neu starten. Weitere Informationen finden Sie unter [Gerätekonnektivitätsprobleme und Hochverfügbarkeit](#).

## Durchführen des geplanten Entfernens von Speichergeräten

Falls ein Speichergerät nicht ordnungsgemäß funktioniert, können Sie PDL- (Permanent Device Loss, „dauerhafter Ausfall eines Geräts“) oder APD-Zustände (All Paths Down, „keine Pfade verfügbar“) vermeiden und eine geplante Entfernung und erneute Verbindung eines Speichergeräts durchführen.

Das geplante Entfernen eines Geräts ist eine beabsichtigte Trennung eines Speichergeräts. Sie können ein Gerät auch aus einem bestimmten Grund entfernen, zum Beispiel, weil Sie Ihre Hardware aktualisieren oder Ihre Speichergeräte neu konfigurieren möchten. Wenn Sie eine ordnungsgemäße Entfernung und erneute Verbindung eines Speichergeräts durchführen, führen Sie mehrere Aufgaben durch.

- 1 Migrieren Sie die virtuelle Maschinen von dem Gerät, das Sie trennen möchten.  
Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.
- 2 Unmounten Sie den auf dem Gerät verwendeten Datenspeicher.  
Weitere Informationen hierzu finden Sie unter [Unmounten von Datenspeichern](#).
- 3 Trennen Sie das Speichergerät.  
Weitere Informationen hierzu finden Sie unter [Speichergeräte trennen](#).
- 4 Im Falle eines iSCSI-Geräts mit einer einzelnen LUN pro Ziel löschen Sie den Eintrag für das statische Ziel aus jedem iSCSI-HBA, der einen Pfad zum Speichergerät aufweist.  
Weitere Informationen hierzu finden Sie unter [Entfernen dynamischer oder statischer iSCSI-Ziele](#).
- 5 Über die Array-Konsole können Sie eine notwendige Neukonfiguration des Speichergeräts durchführen.
- 6 Schließen Sie das Speichergerät erneut an.  
Weitere Informationen hierzu finden Sie unter [Speichergeräte anhängen](#).
- 7 Mounten Sie den Datenspeicher und starten Sie die virtuelle Maschinen neu. Weitere Informationen hierzu finden Sie unter [Mounten von Datenspeichern](#).

### Speichergeräte trennen

Trennen Sie das Speichergerät sicher von Ihrem Host.

Möglicherweise müssen Sie das Gerät trennen, um es für Ihren Host unzugänglich zu machen, wenn Sie beispielsweise ein Upgrade der Speicherhardware durchführen.

#### Voraussetzungen

- Das Gerät enthält keine Datenspeicher.
- Keine virtuelle Maschinen nutzen das Gerät als RDM-Festplatte.
- Das Gerät enthält keine Diagnosepartition oder Scratch-Partition.

## Verfahren

- 1 Zeigen Sie im vSphere Web Client Speichergeräte an.
- 2 Wählen Sie das zu trennende Gerät aus und klicken Sie auf das Symbol **Trennen**.

## Ergebnisse

Auf das Gerät kann nicht mehr zugegriffen werden. Der Betriebszustand des Geräts wird in „Nicht gemountet“ geändert.

## Nächste Schritte

Wenn mehrere Hosts das Gerät teilen, trennen Sie das Gerät von jedem Host.

## Speichergeräte anhängen

Verbinden Sie das Speichergerät wieder, das Sie zuvor getrennt haben.

## Verfahren

- 1 Zeigen Sie im vSphere Web Client Speichergeräte an.
- 2 Wählen Sie das getrennte Speichergerät aus und klicken Sie auf das Symbol **Anhängen**.

## Ergebnisse

Das Gerät wird verfügbar.

## Wiederherstellen nach PDL-Bedingungen

Ein ungeplanter permanenter Geräteverlust (Permanent Device Loss, PDL) tritt ein, wenn ein Speichergerät dauerhaft nicht mehr verfügbar ist, ohne vom ESXi-Host getrennt worden zu sein.

Die folgenden Elemente in vSphere Web Client zeigen an, dass sich das Gerät im PDL-Status befindet:

- Der auf dem Gerät angezeigte Datenspeicher ist nicht verfügbar.
- Der Betriebszustand des Geräts ändert sich auf „Verbindung unterbrochen“.
- Alle Pfade werden als „Ausgefallen“ angezeigt.
- In der VMkernel-Protokolldatei wird in einer Warnung angezeigt, dass das Gerät dauerhaft unzugänglich ist.

Um einen nicht geplanten PDL-Status zu beheben und das nicht mehr verfügbare Gerät vom Host zu entfernen, müssen Sie mehrere Aufgaben ausführen.

- 1 Schalten Sie alle virtuellen Maschinen ab, die auf dem von der PDL-Bedingung betroffenen Datenspeicher laufen, und heben Sie ihre Registrierung auf.
- 2 Unmounten Sie den Datenspeicher.

Weitere Informationen hierzu finden Sie unter [Unmounten von Datenspeichern](#).

- 3 Führen Sie eine erneute Prüfung auf allen ESXi-Hosts durch, die Zugriff auf das Gerät hatten.



Weitere Informationen hierzu finden Sie unter [Durchführen einer erneuten Speicherprüfung](#).

**Hinweis** Wenn die erneute Prüfung nicht erfolgreich ist und der Host das Gerät weiterhin auflistet, sind vielleicht noch ausstehende E/A-Vorgänge oder aktive Verweise auf das Gerät vorhanden. Prüfen Sie, ob virtuelle Maschinen, Vorlagen, ISO-Images, Zuordnungen für Raw-Geräte usw. vorhanden sind, bei denen ein aktiver Verweis auf das Gerät oder den Datenspeicher existiert.

## Handhabung vorübergehender APD-Bedingungen

Ein Speichergerät wird als im Status „Keine Pfade verfügbar“ (All Paths Down, APD) befindlich angesehen, wenn es für Ihren ESXi-Host über eine nicht spezifizierte Zeitdauer nicht verfügbar ist.

Die Ursache für einen APD-Status kann beispielsweise ein ausgefallener Switch oder ein nicht angeschlossenes Speicherkabel sein.

Im Gegensatz zum Status „permanenter Geräteverlust“ (Permanent Device Loss, PDL) verarbeitet der Host den APD-Status als vorübergehend und erwartet, dass das Gerät wieder verfügbar wird.

Der Host versucht zeitlich unbegrenzt, die Befehle erneut abzusetzen, um die Verbindung mit dem Gerät wiederherzustellen. Wenn das erneute Absetzen der Befehle durch den Host über einen längeren Zeitpunkt fehlschlägt, besteht beim Host und seinen virtuellen Maschinen das Risiko von Leistungsbeeinträchtigungen und eines möglichen Ausfalls.

Um diese Probleme zu vermeiden, verfügt Ihr Host über eine Standard-APD-Behandlungsfunktion. Wenn ein Gerät in den APD-Status wechselt, aktiviert das System sofort eine Zeitmessungsfunktion und lässt für eine begrenzte Zeitdauer zu, dass der Host Befehle für nicht virtuelle Maschinen erneut abzusetzen versucht.

Standardmäßig ist die APD-Zeitüberschreitung mit 140 Sekunden festgelegt. Diese Dauer ist in der Regel länger als die Zeit, die ein Gerät zur Wiederherstellung nach einem Verbindungsausfall benötigt. Wenn das Gerät während dieser Zeitspanne wieder verfügbar wird, laufen der Host und seine virtuelle Maschine ohne Probleme weiter.

Wenn die Wiederherstellung durch das Gerät nicht funktioniert und die Zeitüberschreitung eintritt, stoppt der Host seine Neuversuche und beendet alle nicht virtuellen Maschinen-E/A-Befehle. Die virtuellen Maschinen-E/A-Befehle werden weiterhin abgesetzt. Der vSphere Web Client zeigt die folgenden Informationen für das Gerät, bei dem die APD-Zeitüberschreitung aufgetreten ist:

- Der Betriebszustand des Geräts wird in `Ausgefallen` oder `Fehler` geändert.
- Alle Pfade werden als `Ausgefallen` angezeigt.
- Die Datenspeicher auf dem Gerät werden abgeblendet.

Obwohl das Gerät und die Datenspeicher nicht verfügbar sind, reagieren virtuelle Maschinen. Sie können die virtuellen Maschinen deaktivieren oder auf einen anderen Datenspeicher oder Host migrieren.

Wenn später ein oder mehr Gerätepfade wieder arbeiten, werden nachfolgende E/A-Befehle an das Gerät wieder normal abgesetzt und die spezielle APD-Verarbeitung wird beendet.

## Deaktivieren der Speicher-APD-Behandlung

Die Speicher-APD-Behandlung (All Paths Down, keine Pfade verfügbar) auf dem ESXi-Host ist standardmäßig aktiviert. Wenn diese Option aktiviert ist, versucht der Host für eine begrenzte Zeit erneut, E/A-Befehle nicht virtueller Maschinen an ein Speichergerät im APD-Zustand zu senden. Wenn diese Zeit abgelaufen ist, stellt der Host diese Versuche ein und beendet alle E/A-Aktivitäten nicht virtueller Maschinen. Sie können die Funktion zur APD-Behandlung auf dem Host deaktivieren.

Wenn Sie die APD-Behandlung deaktivieren, versucht der Host immer wieder erneut, Befehle zu senden, um die Verbindung mit dem APD-Gerät wiederherzustellen. Dieses Verhalten entspricht dem Verhalten in ESXi Version 5.0. Es kann dazu führen, dass für virtuelle Maschinen auf dem Host eine interne E/A-Zeitüberschreitung eintritt, sodass sie ausfallen bzw. nicht mehr reagieren. Der Host kann vom vCenter Server getrennt werden.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Systemeinstellungen“ den Parameter **Misc.APDHandlingEnable** aus und klicken Sie auf das Symbol **Bearbeiten**.
- 5 Ändern Sie den Wert in 0.

### Ergebnisse

Wenn Sie die APD-Behandlung deaktiviert haben, können Sie sie wieder aktivieren, wenn ein Gerät zum APD-Zustand wechselt. Die Funktion zur internen APD-Behandlung wird sofort aktiviert und der Timer startet mit dem aktuellen Zeitüberschreitungswert für jedes Gerät im APD-Zustand.

## Ändern der Grenzwerte für die Zeitüberschreitung für Speicher-APD

Der Parameter für die Zeitüberschreitung steuert, wie viele Sekunden der ESXi-Host im Zustand „Keine Pfade verfügbar“ (APD) wiederholt versucht, E/A-Befehle für nicht virtuelle Maschinen auf ein Speichergerät anzuwenden. Bei Bedarf können Sie den Standardwert für die Zeitüberschreitung ändern.

Der Timer wird sofort gestartet, nachdem das Gerät in den APD-Zustand versetzt wurde. Nach Eintreten der Zeitüberschreitung kennzeichnet der Host das APD-Gerät als nicht erreichbar und alle ausstehenden oder neuen E/A-Vorgänge nicht virtueller Maschinen schlagen fehl. Es wird weiterhin versucht, E/A-Vorgänge virtueller Maschinen auszuführen.

Der Parameter für den Standardwert der Zeitüberschreitung auf Ihrem Host beträgt 140 Sekunden. Sie können den Zeitüberschreitungswert erhöhen, wenn beispielsweise Speichergeräte, die mit Ihrem ESXi-Host verbunden sind, länger als 140 Sekunden benötigen, um nach einem Verbindungsverlust eine neue Verbindung herzustellen.

---

**Hinweis** Wenn Sie den Zeitüberschreitungswert ändern, während ein APD ausgeführt wird, wirkt sich diese Änderung nicht auf den Zeitüberschreitungswert dieses APD aus.

---

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Systemeinstellungen“ den **Misc.APDTimeout**-Parameter aus und klicken Sie auf das Symbol *Bearbeiten*.
- 5 Ändern Sie den Standardwert.

Sie können einen Wert zwischen 20 und 99999 Sekunden eingeben.

## Überprüfen des Verbindungsstatus eines Speichergeräts

Verwenden Sie den `esxcli`-Befehl, um den Verbindungsstatus eines bestimmten Speichergeräts zu überprüfen.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

#### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

#### Verfahren

- 1 Führen Sie den Befehl `esxcli --server=Servername storage core device list -d=Geräte-ID` aus.
- 2 Überprüfen Sie den Verbindungsstatus im Feld `Status`:
  - `Ein` – Das Gerät ist verbunden.
  - `Ausgefallen` – Das Gerät hat den APD-Zustand. Der APD-Timer wird gestartet.
  - `APD-Zeitüberschreitung` – Der APD-Timer ist abgelaufen.

- **Nicht verbunden** – Das Gerät befindet sich im PDL-Zustand.

## Gerätekonnektivitätsprobleme und Hochverfügbarkeit

Wenn ein Gerät in den Status „Permanenter Geräteverlust (Permanent Device Loss, PDL)“ oder „Keine Pfade verfügbar (All Paths Down, APD)“ wechselt, kann vSphere High Availability (HA) Konnektivitätsprobleme erkennen und eine automatisierte Wiederherstellung für betroffene virtuelle Maschinen ausführen.

vSphere HA verwendet VM-Komponentenschutz zum Schützen virtueller Maschinen, die auf einem Host in einem vSphere HA-Cluster ausgeführt werden, vor Fehlern beim Datenzugriff. Weitere Informationen zum VM-Komponentenschutz und zum Konfigurieren von Antworten für Datenspeicher und virtuelle Maschinen, wenn eine APD- oder PDL-Bedingung auftritt, finden Sie in der Dokumentation *Handbuch zur Verfügbarkeit in vSphere*.

## Aktivieren oder Deaktivieren der Locator-LED auf Speichergeräten

Verwenden Sie die Locator-LED, um spezifische Speichergeräte zu identifizieren, damit Sie diese unter anderen Geräten finden können. Sie können die Locator-LED ein- oder ausschalten.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.
- 4 Wählen Sie aus der Liste der Speichergeräte eine oder mehrere Festplatten aus, und aktivieren bzw. deaktivieren Sie den Locator-LED-Indikator.

Option	Beschreibung
<b>Aktivieren</b>	Klicken Sie auf das Symbol <b>Locator-LED einschalten</b> .
<b>Deaktivieren</b>	Klicken Sie auf das Symbol <b>Locator-LED ausschalten</b> .

Abgesehen von regulären Speicher-Festplattenlaufwerken (HDDs) unterstützt vSphere auch Flash-Speichergeräte.

Anders als die regulären Festplatten (HDDs), bei denen es sich um elektromechanische Geräte mit beweglichen Teilen handelt, verwenden Flash-Geräte Halbleiter als Speichermedium und enthalten keine beweglichen Teile. In der Regel sind Flash-Geräte sehr widerstandsfähig und bieten einen schnelleren Zugriff auf Daten.

Zur Erkennung von Flash-Geräten verwendet ESXi einen Abfragemechanismus, der auf T10-Standards basiert. Der ESXi-Host kann Flash-Geräte bei einer Reihe von Speicher-Arrays erkennen. Erkundigen Sie sich bei Ihrem Anbieter, ob Ihr Speicher-Array die Erkennung von Flash-Geräten durch den ESXi-Mechanismus unterstützt.

Nachdem der Host die Flash-Geräte erkannt hat, können Sie diese für verschiedene Aufgaben und Funktionen verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden von Flash-Geräten mit vSphere](#)
- [Markieren der Speichergeräte](#)
- [Überwachen von Flash-Geräten](#)
- [Best Practices für Flash-Geräte](#)
- [Informationen zu vFlash-Ressourcen](#)
- [Konfigurieren des Hostauslagerungs-Caches](#)

## Verwenden von Flash-Geräten mit vSphere

In Ihrer vSphere-Umgebung können Sie Flash-Geräte für verschiedene Funktionen verwenden.

Tabelle 14-1. Verwenden von Flash-Geräten mit vSphere

Funktionalität	Beschreibung
Virtual SAN	Virtual SAN erfordert Flash-Geräte. Weitere Informationen finden Sie in der Dokumentation <i>Verwalten von VMware Virtual SAN</i> .
VMFS-Datenspeicher	<p>Sie können VMFS-Datenspeicher auf Flash-Geräten erstellen. Verwenden Sie die Datenspeicher für folgende Zwecke:</p> <ul style="list-style-type: none"> <li>■ Speichern virtueller Maschinen. Bestimmte Gastbetriebssysteme können virtuelle Festplatten, die sich auf diesen Datenspeichern befinden, als vFlash-Festplatten identifizieren. Siehe <a href="#">Identifizieren von vFlash-Festplatten</a>.</li> <li>■ Teilen Sie Datenspeicherplatz für den ESXi-Hostauslagerungs-Cache zu. Siehe <a href="#">Konfigurieren des Hostauslagerungs-Caches</a>.</li> </ul>
Virtuelle Flash-Ressource (VFFS)	<p>Richten Sie eine vFlash-Ressource ein und verwenden Sie sie für folgende Funktionen:</p> <ul style="list-style-type: none"> <li>■ Verwenden Sie sie als vFlash-Lesecache für Ihre virtuellen Maschinen. Siehe <a href="#">Kapitel 15 Informationen zu VMware vSphere Flash Read Cache</a>.</li> <li>■ Teilen Sie die vFlash-Ressource für den ESXi-Hostauslagerungs-Cache zu. Dies ist eine alternative Methode zur Host-Cache-Konfiguration, bei der VFFS-Datenträger anstelle von VMFS-Datenspeichern verwendet werden. Siehe <a href="#">Konfigurieren des Hostauslagerungs-Cache mit der vFlash-Ressource</a>.</li> <li>■ Soweit dies Ihr Anbieter erfordert, verwenden Sie die vFlash-Ressource für E/A-Cache-Filter. Siehe <a href="#">Kapitel 21 Filtern der E/A einer virtuellen Maschine</a>.</li> </ul>

## Identifizieren von vFlash-Festplatten

Gastbetriebssysteme können virtuelle Festplatten, die sich auf Flash-Datenspeichern befinden, als vFlash-Festplatten identifizieren.

Um zu überprüfen, ob diese Funktion aktiviert ist, können Gastbetriebssysteme die standardmäßigen Abfragebefehle wie z. B. SCSI VPD Page (B1h) für SCSI-Geräte und ATA IDENTIFY DEVICE (Word 217) für IDE-Geräte verwenden.

Für verknüpfte Klone, native Snapshots und Delta-Festplatten melden die Abfragebefehle den virtuellen Flash-Status der Basisfestplatte.

Betriebssysteme können eine virtuelle Festplatte unter folgenden Bedingungen als Flash-Festplatte erkennen:

- Das Erkennen von vFlash-Festplatten wird auf Hosts von ESXi 5.x oder höher und der virtuellen Hardwareversion 8 oder höher unterstützt.
- Das Erkennen von vFlash-Festplatten wird nur von VMFS5 oder höher unterstützt.
- Wenn sich virtuelle Festplatten auf gemeinsam genutzten VMFS-Datenspeichern mit Flash-Geräteerweiterungen befinden, muss das Gerät auf allen Hosts als Flash-Gerät markiert sein.
- Damit eine virtuelle Festplatte als virtueller Flash identifiziert wird, sollten alle zugrunde liegenden physischen Erweiterungen Flash-gestützt sein.

## Markieren der Speichergeräte

Sie können den vSphere Web Client verwenden, um Speichergeräte zu markieren, die nicht automatisch als lokale Flash-Geräte erkannt werden.

Wenn Sie Virtual SAN konfigurieren oder eine virtuelle Flash-Ressource einrichten, muss Ihre Speicherumgebung lokale Flash-Geräte enthalten.

Es kann jedoch vorkommen, dass ESXi bestimmte Speichergeräte nicht als Flash-Geräte erkennt, wenn deren Anbieter die automatische Flash-Geräteerkennung nicht unterstützen. Es kann auch vorkommen, dass andere als SATA-SAS-Flash-Geräte nicht als lokale Geräte erkannt werden. Wenn Geräte nicht als lokale Flash-Geräte erkannt werden, werden sie aus der Liste der für Virtual SAN oder die virtuelle Flash-Ressource angebotenen Geräte ausgeschlossen. Wenn diese Geräte als lokale Flash-Geräte markiert werden, stehen sie für Virtual SAN und für die virtuelle Flash-Ressource zur Verfügung.

## Markieren der Speichergeräte als Flash-Gerät

Falls ESXi Geräte nicht automatisch als Flash-Geräte erkennt, markieren Sie sie als Flash-Geräte.

ESXi erkennt bestimmte Geräte nicht als Flash-Festplatten, wenn die Hersteller die automatische Flash-Festplatten-Erkennung nicht unterstützen. In der Spalte „Laufwerktyp“ wird für die Geräte „HDD“ als Typ angezeigt.

---

**Vorsicht** Das Markieren von HDD-Festplatten als Flash-Festplatten kann die Leistung von Datenspeichern und Diensten, die sie verwenden, verschlechtern. Markieren Sie Festplatten nur dann als Flash-Festplatten, wenn Sie sicher sind, dass es sich dabei um Flash-Festplatten handelt.

---

### Voraussetzungen

Stellen Sie sicher, dass das Gerät nicht verwendet wird.

### Verfahren

- 1 Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Speicher**.
- 3 Klicken Sie auf **Speichergeräte**.
- 4 Wählen Sie in der Liste der Speichergeräte eines oder mehrere HDD-Geräte aus, die als Flash-Geräte erkannt werden müssen, und klicken Sie auf das Symbol **Als Flash-Festplatte markieren** (F).
- 5 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

### Ergebnisse

Der Gerätetyp wird in „Flash“ geändert.

## Nächste Schritte

Wenn das Flash-Gerät, das Sie markieren, von mehreren Hosts gemeinsam genutzt wird, stellen Sie sicher, dass Sie das Gerät von allen Hosts aus markieren, die das Gerät gemeinsam nutzen.

## Markieren der Speichergeräte als lokal

ESXi ermöglicht Ihnen das Markieren von Geräten als lokal. Dies ist nützlich, wenn ESXi nicht ermitteln kann, ob bestimmte Geräte lokal sind.

### Voraussetzungen

- Stellen Sie sicher, dass das Gerät nicht gemeinsam genutzt wird.
- Schalten Sie auf dem Gerät befindliche virtuelle Maschinen aus und unmounten Sie einen zugewiesenen Datenspeicher.

### Verfahren

- 1 Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Speicher**.
- 3 Klicken Sie auf **Speichergeräte**.
- 4 Wählen Sie in der Liste der Speichergeräte eines oder mehrere Remotegeräte aus, die als lokal markiert werden müssen, und klicken Sie auf das Symbol **Als lokal relativ zum Host markieren** aus.
- 5 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

## Überwachen von Flash-Geräten

Sie können von einem ESXi-Host bestimmte kritische Flash-Geräte-Parameter überwachen, darunter den Indikator für Medienabnutzung (Media Wearout Indicator), Temperatur und Anzahl der erneut zugeordneten Sektoren (Reallocated Sector Count).

Verwenden Sie den `esxcli`-Befehl, um Flash-Geräte zu überwachen.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.



## Verfahren

- ◆ Führen Sie folgenden Befehl aus, um Flash-Geräte-Statistiken anzuzeigen:

```
esxcli server=Servername storage core device smart get -d=Flash-Geräte-ID
```

## Best Practices für Flash-Geräte

Befolgen Sie diese Best Practices, wenn Sie Flash-Geräte in einer vSphere-Umgebung verwenden.

- Stellen Sie sicher, dass Sie mit Flash-Geräten die neueste Firmware verwenden. Erkundigen Sie sich regelmäßig bei Ihren Speicheranbietern nach Updates.
- Achten Sie sorgfältig darauf, wie intensiv Sie das Flash-Gerät nutzen, und berechnen Sie dessen geschätzte Lebensdauer. Die Lebenserwartung hängt davon ab, wie aktiv Sie das Flash-Gerät weiterhin nutzen.

## Geschätzte Lebensdauer von Flash-Geräten

Überwachen Sie beim Arbeiten mit Flash-Geräten, wie aktiv Sie sie verwenden, und berechnen Sie ihre geschätzte Lebensdauer.

In der Regel bieten Speicheranbieter zuverlässige Schätzungen zur Lebensdauer für ein Flash-Gerät unter idealen Bedingungen. Beispielsweise garantiert ein Anbieter eine Lebensdauer von 5 Jahren unter der Bedingung, dass es 20 GB an Schreibvorgängen pro Tag gibt. Allerdings hängt die tatsächliche Lebenserwartung des Geräts davon ab, wie viele Schreibvorgänge pro Tag Ihr ESXi-Host tatsächlich generiert. Führen Sie die folgenden Schritte aus, um die Lebensdauer des Flash-Geräts zu berechnen.

### Voraussetzungen

Notieren Sie die Anzahl der Tage, die seit dem letzten Neustart des ESXi-Hosts vergangen sind. Beispiel: 10 Tage.

### Verfahren

- 1 Ermitteln Sie die Gesamtzahl der Blöcke, die seit dem letzten Neustart auf das Flash-Gerät geschrieben wurden.

Führen Sie den folgenden Befehl aus: **esxcli storage core device stats get -d=device\_ID** Beispiel:

```
~ # esxcli storage core device stats get -d t10.aaaaaaaaaaaaaaaa
Device: t10.aaaaaaaaaaaaaaaa
Successful Commands: xxxxxxxx
Blocks Read: xxxxxxxx
Blocks Written: 629145600
Read Operations: xxxxxxxx
```

Das Element „Blocks Written“ (Geschriebene Blöcke) in der Ausgabe zeigt die Anzahl der Blöcke, die seit dem letzten Neustart auf das Gerät geschrieben wurden. In diesem Beispiel ist der Wert 629.145.600. Nach jedem Neustart wird der Zähler auf 0 zurückgesetzt.

- 2 Berechnen Sie die Gesamtzahl der Schreibvorgänge und wandeln Sie diese in GB um.

Ein Block umfasst 512 Byte. Um die Gesamtzahl der Schreibvorgänge zu berechnen, multiplizieren Sie den Wert von „Blocks Written“ (Geschriebene Blöcke) mit 512. Wandeln Sie dann den Ergebniswert in GB um.

In diesem Beispiel beträgt die Gesamtzahl der Schreibvorgänge seit dem letzten Neustart ca. 322 GB.

- 3 Schätzen Sie die durchschnittliche Anzahl der Schreibvorgänge pro Tag in GB.

Dividieren Sie die Gesamtzahl der Schreibvorgänge durch die Anzahl der Tage seit dem letzten Neustart.

Wenn der letzte Neustart vor 10 Tagen erfolgt ist, erhalten Sie 32 GB Schreibvorgänge pro Tag. Anhand dieser Anzahl können Sie den Durchschnitt über einen bestimmten Zeitraum ermitteln.

- 4 Schätzen Sie die Lebensdauer Ihres Geräts anhand der folgenden Formel:

*Vom Anbieter angegebene Anzahl der Schreibvorgänge pro Tag mal die vom Anbieter angegebene Lebensdauer geteilt durch die tatsächliche durchschnittliche Anzahl der Schreibvorgänge pro Tag*

Wenn der Anbieter beispielsweise eine Lebensdauer von 5 Jahren garantiert unter der Bedingung, dass es 20 GB an Schreibvorgängen pro Tag gibt, und die tatsächliche Anzahl an Schreibvorgängen pro Tag 30 GB ist, beträgt die Lebensdauer Ihres Flash-Geräts ungefähr 3,3 Jahre.

## Informationen zu vFlash-Ressourcen

Sie können lokale Flash-Geräte auf einem ESXi-Host zu einem einzelnen virtualisierten Zwischenspeicher-Layer, der so genannten vFlash-Ressource, zusammenfassen.

Wenn Sie die vFlash-Ressource einrichten, erstellen Sie ein neues Dateisystem, das virtuelle Flash-Dateisystem (Virtual Flash File System, VFFS). Das VFFS ist eine Ableitung des VMFS, das für Flash-Geräte optimiert ist und zum Gruppieren der physischen Flash-Geräte zu einem einzelnen Zwischenspeicherressourcenpool verwendet wird. Als nicht dauerhafte Ressource kann es nicht zum Speichern von virtuellen Maschinen verwendet werden.

Für die folgenden vSphere-Funktionen ist die vFlash-Ressource erforderlich:

- Lesecache der virtuellen Maschine. Siehe [Kapitel 15 Informationen zu VMware vSphere Flash Read Cache](#).
- Hostauslagerungs-Cache. Siehe [Konfigurieren des Hostauslagerungs-Cache mit der vFlash-Ressource](#).

- E/A-Cache-Filter, soweit dies Ihre Anbieter erfordern. Siehe [Kapitel 21 Filtern der E/A einer virtuellen Maschine](#).

Stellen Sie vor dem Einrichten der vFlash-Ressource sicher, dass Sie Geräte verwenden, die im *VMware-Kompatibilitätshandbuch* als geeignet aufgeführt sind.

## Überlegungen zu vFlash-Ressourcen

Wenn Sie eine virtuelle Flash-Ressource konfigurieren, die von ESXi-Hosts und virtuellen Maschinen belegt wird, müssen mehrere Gesichtspunkte berücksichtigt werden.

- Auf jedem ESXi-Host kann nur eine virtuelle Flash-Ressource, auch als VFFS-Volume bezeichnet, vorhanden sein. Die virtuelle Flash-Ressource wird nur auf Hostebene verwaltet.
- Sie können die virtuelle Flash-Ressource nicht zum Speichern von virtuellen Maschinen verwenden. Die virtuelle Flash-Ressource ist nur eine Zwischenspeicherebene.
- Sie können nur lokale Flash-Geräte für die virtuelle Flash-Ressource verwenden.
- Sie können die virtuelle Flash-Ressource von gemischten Flash-Geräten aus verwenden. Alle Gerätetypen werden gleich behandelt, und es wird nicht zwischen SAS-, SATA- oder PCI Express-Verbindungen unterschieden. Wenn die Ressource aus gemischten Flash-Geräten erstellt wird, müssen Sie Geräte mit vergleichbarer Leistung zusammen gruppieren, um die Leistung zu maximieren.
- Sie können nicht die gleichen Flash-Geräte für die virtuelle Flash-Ressource und Virtual SAN verwenden. Diese benötigen jeweils ein eigenes, dediziertes Flash-Gerät.
- Nach dem Einrichten einer virtuellen Flash-Ressource kann die gesamte verfügbare Kapazität von ESXi-Hosts als Hostauslagerungs-Cache und von virtuellen Maschinen als Lese-Cache verwendet werden.
- Sie können keine einzelnen Flash-Geräte auswählen, um entweder als Auslagerungs-Cache oder als Lese-Cache verwendet zu werden. Alle Flash-Geräte sind in einer Einheit als Flash-Ressource kombiniert.

## Einrichten der vFlash-Ressource

Sie können eine vFlash-Ressource einrichten oder einer vorhandenen vFlash-Ressource Kapazität hinzufügen.

Zum Einrichten einer virtuellen Flash-Ressource verwenden Sie lokale Flash-Geräte, die mit dem Host verbunden sind. Wenn Sie die Kapazität der virtuellen Flash-Ressource erhöhen möchten, können Sie weitere Geräte hinzufügen. Die maximale Anzahl der Geräte ist in der Dokumentation *Maximalwerte für die Konfiguration* angegeben. Ein einzelnes Flash-Gerät muss der virtuellen Flash-Ressource exklusiv zugeteilt werden und kann nicht gemeinsam mit einem anderen vSphere-Dienst (z. B. Virtual SAN oder VMFS) genutzt werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.

- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie unter „Virtueller Flash“ die Option **vFlash-Ressourcenverwaltung** und klicken Sie auf **Kapazität hinzufügen**.
- 4 Wählen Sie aus der Liste der verfügbaren Flash-Geräte eines oder mehrere zur Verwendung durch die virtuelle Flash-Ressource aus und klicken Sie auf **OK**.

Unter bestimmten Bedingungen kann es sein, dass in der Liste keine Flash-Geräte angezeigt werden. Weitere Informationen finden Sie im Abschnitt über die Fehlerbehebung bei Flash-Geräten in der Dokumentation zu *vSphere-Fehlerbehebung*.

### Ergebnisse

Die vFlash-Ressource wird erstellt. Im Bereich „Geräte-Backing“ werden alle Geräte aufgelistet, die für die virtuelle Flash-Ressource verwendet werden.

### Nächste Schritte

Sie können die vFlash-Ressource für die Cache-Konfiguration auf dem Host sowie für die Konfiguration des Flash-Lesecaches auf virtuellen Festplatten verwenden. Darüber hinaus ist für E/A-Cache-Filter, die über vSphere APIs für E/A-Filter entwickelt wurden, möglicherweise die vFlash-Ressource erforderlich.

Durch Hinzufügen weiterer Flash-Geräte zur virtuellen Flash-Ressource können Sie die Kapazität erhöhen.

## Entfernen der vFlash-Ressource

Sie müssen möglicherweise eine auf lokalen Flash-Geräten bereitgestellte vFlash-Ressource entfernen, um die Geräte für andere Dienste verfügbar zu machen.

Sie können keine vFlash-Ressource entfernen, die mit Hostauslagerungs-Cache konfiguriert ist, oder wenn der Host virtuelle Maschinen mit Flash-Lesecache konfiguriert hat, die eingeschaltet sind.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host, bei dem virtueller Flash konfiguriert ist.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie unter „Virtueller Flash“ die Option **vFlash-Ressourcenverwaltung** aus und klicken Sie auf **Alle entfernen**.

### Ergebnisse

Nachdem Sie die vFlash-Ressource entfernt und das Flash-Gerät gelöscht haben, ist das Gerät für andere Vorgänge verfügbar.

## Erweiterte Einstellungen für virtuellen Flash

Die erweiterten Optionen für virtuelles Flash können geändert werden.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie die gewünschte Einstellung aus und klicken Sie auf **Bearbeiten**.

Option	Beschreibung
<b>VFLASH.VFlashResourceUsageThreshold</b>	Das System löst den Alarm <i>Host-vFlash-Ressourcennutzung</i> aus, sobald die Nutzung einer virtuellen Flash-Ressource den Schwellenwert überschreitet. Der Standardschwellenwert ist 80 %. Sie können den Schwellenwert an Ihre Anforderungen anpassen. Der Alarm wird automatisch zurückgesetzt, wenn die Nutzung der virtuellen Flash-Ressource wieder unter den Schwellenwert fällt.
<b>VFLASH.MaxResourceGBForVmCache</b>	Ein ESXi-Host speichert die Metadaten des Flash Read Cache im Arbeitsspeicher. Das Standardlimit der Gesamt-Cachegröße der virtuellen Maschine beträgt 2 TB. Diese Einstellung können Sie ändern. Damit die neue Einstellung wirksam wird, muss der Host neu gestartet werden.

- 5 Klicken Sie auf **OK**.

## Konfigurieren des Hostauslagerungs-Caches

Ihre ESXi-Hosts können einen Teil des Flash-gestützten Speicherelements als Auslagerungs-Cache verwenden, der von allen virtuellen Maschinen gemeinsam genutzt wird.

Der Cache auf Hostebene besteht aus Dateien auf einer niedriglatenten Festplatte, die von ESXi als Write-Back-Cache für Auslagerungsdateien der virtuellen Maschinen verwendet wird. Der Cache wird von allen virtuellen Maschinen gemeinsam verwendet, die auf dem Host ausgeführt werden. Durch das Auslagern von Seiten der virtuellen Maschinen kann der potenziell beschränkte Speicherplatz auf Flash-Geräten optimal genutzt werden.

Je nach Ihrer Umgebung und Ihres Lizenzierungspakets stehen Ihnen folgende Methoden zum Konfigurieren des Hostauslagerungs-Cache zur Verfügung. Beide Methoden führen zu vergleichbaren Ergebnissen.

- Sie können einen VMFS-Datenspeicher auf einem Flash-Gerät erstellen und diesen dann verwenden, um dem Host-Cache Speicherplatz zuzuweisen. Der Host reserviert eine bestimmte Menge an Speicherplatz für die Auslagerung in den Hostcache.
- Wenn Ihre vSphere-Lizenz die Einrichtung und Verwaltung von virtuellen Flash-Ressourcen erlaubt, können Sie den Auslagerungs-Cache auf dem Host mithilfe einer dieser Ressourcen konfigurieren. Der Hostauslagerungscache wird aus einem Teil der vFlash-Ressource zugewiesen.

## Konfigurieren des Host-Caches mit VMFS-Datenspeicher

Aktivieren Sie die Fähigkeit des Hosts zur Auslagerung in den Host-Cache. Sie können auch den Prozentsatz des Speicherplatzes ändern, der dem Host-Cache zugeteilt ist.

Führen Sie diese Aufgabe durch, wenn Sie keine geeignete Lizenz zum Einrichten und Verwalten einer virtuellen Flash-Ressource besitzen. Wenn Sie hingegen eine solche Lizenz besitzen, verwenden Sie die virtuelle Flash-Ressource zur Konfiguration des Host-Cache.

### Voraussetzungen

Erstellen Sie einen Flash-gestützten VMFS-Datenspeicher. Siehe [Erstellen eines VMFS-Datenspeichers](#).

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Host-Cache-Konfiguration**.
- 4 Wählen Sie den Datenspeicher in der Liste aus und klicken Sie auf das Symbol **Speicher für den Host-Cache zuteilen**.
- 5 Wenn Sie die Fähigkeit des Hosts zur Auslagerung in den Host-Cache auf Datenspeicherbasis aktivieren möchten, aktivieren Sie das Kontrollkästchen **Speicher für den Host-Cache zuteilen**.

Standardmäßig wird dem Host-Cache der maximal verfügbare Speicherplatz zugewiesen.

- 6 (Optional) Zum Ändern der Host-Cache-Größe wählen Sie **Benutzerdefinierte Größe** und nehmen die gewünschten Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Konfigurieren des Hostauslagerungs-Cache mit der vFlash-Ressource

Sie können eine bestimmte Menge der vFlash-Ressource für den Hostauslagerungs-Cache reservieren.

### Voraussetzungen

Richten Sie eine vFlash-Ressource ein. [Einrichten der vFlash-Ressource](#).

---

**Hinweis** Wenn sich ein mit virtuellem Flash konfigurierter ESXi-Host im Wartungsmodus befindet, können Sie einen Hostauslagerungs-Cache weder hinzufügen noch ändern. Sie müssen zuerst den Wartungsmodus auf dem Host beenden, bevor Sie einen Hostauslagerungs-Cache konfigurieren können.

---

## Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Wählen Sie unter vFlash **Konfiguration des vFlash-Hostauslagerungs-Cache** und klicken Sie auf **Bearbeiten**.
- 4 Aktivieren Sie das Kontrollkästchen **vFlash-Hostauslagerungs-Cache aktivieren**.
- 5 Geben Sie die Größe der vFlash-Ressource ein, die für den Hostauslagerungs-Cache reserviert werden soll.
- 6 Klicken Sie auf **OK**.

# Informationen zu VMware vSphere Flash Read Cache

15

Mit Flash Read Cache™ kann die Leistung der virtuellen Maschine verbessert und beschleunigt werden, indem Flash-Geräte, die sich auf dem Host befinden, als Cache verwendet werden.

Flash Read Cache kann für jede virtuelle Festplatte einzeln reserviert werden. Der Flash Read Cache wird erst erstellt, wenn eine virtuelle Maschine eingeschaltet wird, und wieder verworfen, sobald die virtuelle Maschine angehalten oder ausgeschaltet wird. Beim Migrieren einer virtuellen Maschine haben Sie die Möglichkeit, den Cache zu migrieren. Standardmäßig wird der Cache migriert, wenn die vFlash-Module auf Quell- und Zielhosts kompatibel sind. Wenn Sie den Cache nicht migrieren, wird er auf dem Zielhost erneut aufgebaut („aufgewärmt“). Sie können die Cachegröße ändern, während die virtuelle Maschine eingeschaltet ist. In diesem Fall wird der vorhandene Cache verworfen und ein neuer Durchschreibcache erstellt, was zu einer Cache-Aktualisierungsspanne führt. Das Erstellen eines neuen Caches hat den Vorteil, dass die Cachegröße besser auf die aktiven Daten der Anwendung abgestimmt werden kann.

Flash Read Cache unterstützt Write-Through-Caching oder Caching für Lesevorgänge. Write-Back-Caching oder Caching für Schreibvorgänge wird nicht unterstützt. Datenlesevorgänge erfolgen über den Cache (falls vorhanden). Datenschreibvorgänge werden an den Hintergrundspeicher (z. B. SAN oder NAS) gesendet. Alle Daten, die aus dem Hintergrundspeicher gelesen oder in diesen geschrieben werden, werden ohne Einschränkungen im Cache gespeichert.

RDMs im physischen Kompatibilitätsmodus werden vom Flash Read Cache nicht unterstützt. RDMs im virtuellen Kompatibilitätsmodus werden vom Flash Read Cache unterstützt.

Das Video enthält weitere Informationen über Flash Read Cache.



Konfigurieren von vSphere Flash Read Cache



([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_pbinee4w/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_pbinee4w/uiConfId/49694343/))

---

**Hinweis** Nicht bei allen Arbeitslasten können die Vorteile eines Flash Read Cache genutzt werden. Die Leistungsverbesserung hängt von Ihrem Arbeitslastmuster und der Working-Set-Größe ab. Bei leseintensiven Arbeitslasten mit Working-Sets, die in den Cache passen, können die Vorteile einer Konfiguration mit Flash Read Cache genutzt werden. Durch die Konfiguration des Flash Read Cache für leseintensive Arbeitslasten werden im gemeinsam genutzten Speicher zusätzliche E/A-Ressourcen verfügbar. Dies kann zu einer Leistungsverbesserung für andere Arbeitslasten führen, auch wenn für diese die Verwendung des Flash Read Cache nicht konfiguriert ist.

---

Dieses Kapitel enthält die folgenden Themen:

- [DRS-Unterstützung für Flash-Lesecache](#)
- [vSphere High Availability-Unterstützung für Flash-Lesecache](#)
- [Konfigurieren des Flash-Lesecaches für eine virtuelle Maschine](#)
- [Migrieren von virtuellen Maschinen mit Flash Read Cache](#)

## DRS-Unterstützung für Flash-Lesecache

DRS unterstützt den virtuellen Flash als Ressource.

DRS verwaltet virtuelle Maschinen mit Flash-Lesecache-Reservierungen. Jedes Mal, wenn Sie DRS ausführen, wird die vom ESXi-Host gemeldete, verfügbare vFlash-Kapazität angezeigt. Jeder Host unterstützt eine vFlash-Ressource. DRS wählt einen Host aus, der über ausreichend vFlash-Kapazität verfügt, um eine virtuelle Maschine starten zu können. DRS behandelt eingeschaltete virtuelle Maschinen mit einem Flash-Lesecache als leicht affin zu ihrem aktuellen Host und verschiebt sie nur aus schwerwiegenden Gründen oder, um gegebenenfalls eine übermäßige Hostnutzung zu korrigieren.

## vSphere High Availability-Unterstützung für Flash-Lesecache

Flash-Lesecache wird von High Availability (HA) unterstützt.

Wenn vSphere HA eine virtuelle Maschine neu startet, für die Flash-Lesecache konfiguriert ist, wird die virtuelle Maschine auf einem Host im Cluster neu gestartet, für den die Flash-Lesecache-, CPU-, Arbeitsspeicher- und Overhead-Reservierungen erfüllt sind. vSphere HA startet eine virtuelle Maschine nicht neu, wenn der nicht reservierte Flash-Speicher die Reservierung für virtuellen Flash nicht erfüllt. Sie müssen eine virtuelle Maschine manuell neu konfigurieren, um den Flash-Lesecache zu reduzieren oder zu löschen, falls auf dem Zielhost nicht genügend vFlash-Ressourcen verfügbar sind.

# Konfigurieren des Flash-Lesecaches für eine virtuelle Maschine

Sie können den Flash-Lesecache für eine virtuelle Maschine konfigurieren, die mit ESXi 5.5 oder höher kompatibel ist.

Durch Aktivieren des Flash-Lesecaches können Sie die Blockgröße und die zu reservierende Cachegröße angeben.

Die Blockgröße ist die Mindestanzahl von zusammenhängenden Byte, die im Cache gespeichert werden können. Diese Blockgröße kann größer als die nominale Festplatten-Blockgröße von 512 Byte sein und zwischen 4 KB und 1024 KB betragen. Falls ein Gastbetriebssystem einen einzelnen Datenträgerblock mit 512 Byte schreibt, werden die über die Cache-Blockgröße hinausgehenden Byte zwischengespeichert. Sie sollten die Cache-Blockgröße nicht mit der Festplatten-Blockgröße verwechseln.

Bei der Reservierung handelt es sich um die zu reservierende Größe für Cache-Blöcke. Es gibt mindestens 256 Cache-Blöcke. Bei einer Cache-Blockgröße von 1 MB beträgt die Mindestcachegröße 256 MB. Bei einer Cache-Blockgröße von 4 K beträgt die Mindestcachegröße 1 MB.

Um weitere Informationen zu Größenanpassungsrichtlinien zu erhalten, suchen Sie auf der VMware-Website nach dem Whitepaper *Performance of vSphere Flash Read Cache in VMware vSphere*.

## Voraussetzungen

- Richten Sie die virtuelle vFlash-Ressource ein.
- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 5.5 oder höher kompatibel ist.

## Verfahren

- 1 Wählen Sie zum Suchen einer virtuellen Maschine ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool, einen Host oder eine vApp aus.
- 2 Klicken Sie auf der Registerkarte **Verwandte Objekte** und klicken Sie dann auf **Virtuelle Maschinen**.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 4 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte**, um die Festplattenoptionen anzuzeigen.
- 5 Um den Flash-Lesecache für die virtuelle Maschine zu aktivieren, geben Sie einen Wert in das Textfeld **vFlash-Lesecache** ein.

- 6 Klicken Sie auf **Erweitert**, und geben Sie die folgenden Parameter an.

Option	Beschreibung
Reservierung	Wählen Sie einen Wert für die zu reservierende Cachegröße aus.
Blockgröße	Wählen Sie eine Blockgröße aus.

- 7 Klicken Sie auf **OK**.

## Migrieren von virtuellen Maschinen mit Flash Read Cache

Beim Migrieren einer eingeschalteten virtuellen Maschine von einem Host zu einem anderen können Sie angeben, ob Flash Read Cache-Inhalte zusammen mit den virtuellen Festplatten migriert werden sollen.

### Voraussetzungen

Falls Sie planen, Flash Read Cache-Inhalte zu migrieren, müssen Sie eine ausreichende vFlash-Ressource auf dem Zielhost konfigurieren.

### Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf die ausgeführte virtuelle Maschine und wählen Sie **Migrieren** aus.
- 2 Geben Sie den Migrationstyp an.

Option	Beschreibung
Nur Computing-Ressource ändern	Migriert virtuelle Maschinen auf einen anderen Host oder Cluster.
Sowohl Computing- als auch Speicherressourcen ändern	Migrieren Sie die virtuellen Maschinen auf einen bestimmten Host oder Cluster und deren Speicher auf einen bestimmten Datenspeicher oder Datenspeicher-Cluster.

- 3 Wählen Sie den Zielhost aus und klicken Sie auf **Weiter**.
- 4 Geben Sie eine Migrationseinstellung für alle mit Virtual Flash Read Cache konfigurierten virtuellen Festplatten an. Dieser Migrationsparameter wird nicht angezeigt, wenn Sie nur den Datenspeicher und nicht den Host ändern.

Migrationseinstellungen für den Flash-Lesecache	Beschreibung
Cache-Inhalte immer migrieren	Das Migrieren virtueller Maschinen wird nur fortgesetzt, wenn der gesamte Cache-Inhalt auf den Zielhost migriert werden kann. Diese Option ist hilfreich für einen kleinen Cache oder wenn die Cachegröße weitgehend mit den aktiven Daten der Anwendung übereinstimmt.
Cache-Inhalte nicht migrieren	Write-Through-Cache wird geleert. Der Cache wird auf dem Zielhost neu erstellt. Diese Option ist hilfreich für einen großen Cache oder wenn der Cache größer als die aktiven Daten der Anwendung ist.

- 5 Wenn Sie über mehrere virtuelle Festplatten mit Flash Read Cache verfügen, können Sie die Migrationseinstellung für jede einzelne Festplatte anpassen.
  - a Klicken Sie auf **Erweitert**.
  - b Wählen Sie eine virtuelle Festplatte aus, für die Sie die Migrationseinstellung ändern möchten.
  - c Wählen Sie im Dropdown-Menü in der Spalte **Migrationseinstellung für Virtual Flash Read Cache** eine entsprechende Option aus.
- 6 Schließen Sie die Migrationskonfiguration ab und klicken Sie auf **Beenden**.

#### Nächste Schritte

Überprüfen Sie auf der Registerkarte **Übersicht** der virtuellen Maschine, ob die Migration erfolgreich war:

- Vergewissern Sie sich, ob auf der Registerkarte die richtige IP-Adresse des Zielhosts angezeigt wird.
- Vergewissern Sie sich, dass im VM-Hardwarebereich die richtigen Virtual Flash Read Cache-Informationen für jede virtuelle Festplatte angezeigt werden.

Datenspeicher sind besondere logische Container (analog zu Dateisystemen), bei denen Angaben zu physischen Speichern 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.

Je nach dem verwendeten Speicher können Datenspeicher folgende Typen aufweisen:

- VMFS-Datenspeicher, denen das Virtual Machine File System-Format zugrunde liegt. Siehe [Grundlegende Informationen VMFS-Datenspeicher](#).
- NFS-Datenspeicher, denen das Network File System-Format (NFS) zugrunde liegt. Siehe [Grundlegende Informationen zu NFS-Datenspeichern](#).
- Datenspeicher für Virtual SAN. Informationen finden Sie in der Dokumentation *Verwalten von VMware Virtual SAN*.
- Datenspeicher mit virtuellen Volumes. Siehe [Kapitel 19 Arbeiten mit virtuellen Volumes](#).

Nach dem Erstellen von Datenspeichern können Sie für die Datenspeicher mehrere Verwaltungsvorgänge durchführen. Bestimmte Vorgänge wie das Umbenennen eines Datenspeichers stehen für alle Datenspeichertypen zur Verfügung. Andere gelten für bestimmte Datenspeichertypen.

Sie können die Datenspeicher auch auf verschiedene Weisen organisieren. Sie können beispielsweise eine Gruppierung in Ordnern nach Geschäftsmethoden vornehmen. Damit ist es möglich, allen Datenspeichern einer Gruppe im gleichen Vorgang dieselben Berechtigungen und Alarmer zuzuweisen.

Datenspeicher lassen sich auch zu Datenspeicher-Clustern hinzufügen. Ein Datenspeicher-Cluster ist eine Sammlung von Datenspeichern mit gemeinsam genutzten Ressourcen und einer gemeinsamen Verwaltungsoberfläche. Wenn Sie einen Datenspeicher-Cluster erstellen, können Sie Speicher-DRS zum Verwalten von Speicherressourcen verwenden. Weitere Informationen zu Datenspeicher-Clustern finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegende Informationen VMFS-Datenspeicher](#)
- [Grundlegende Informationen zu NFS-Datenspeichern](#)

- Erstellen von Datenspeichern
- Verwalten von duplizierten VMFS-Datenspeichern
- Upgrade von VMFS-Datenspeichern
- Erhöhen der VMFS-Datenspeicherkapazität
- Verwaltungsvorgänge für Datenspeicher
- Dynamische Festplattenspiegelung einrichten
- Erfassen von Diagnoseinformationen für ESXi-Hosts auf einem Speichergerät
- Überprüfen der Metadatenkonsistenz mit VOMA
- Konfigurieren des Cachespeichers für VMFS-Zeigerblöcke

## Grundlegende Informationen VMFS-Datenspeicher

Zum Speichern virtueller Festplattendateien verwendet ESXi Datenspeicher. Datenspeicher sind logische Container, bei denen Angaben zu den einzelnen Speichergeräten verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Auf Blockspeichergeräten bereitgestellte Datenspeicher verwenden das vSphere VMFS-Format, ein spezielles Hochleistungsdateisystem für die Speicherung virtueller Maschinen.

Seit der Einführung wurden mehrere Versionen des VMFS-Dateisystems veröffentlicht. In der folgenden Tabelle werden Beziehungen zwischen dem Host und der VMFS-Version dargestellt.

**Tabelle 16-1. Hostzugriff auf die VMFS-Version**

VMFS	ESX/ESXi 3.x-Host	ESX/ESXi 4.x-Host	ESXi 5.x-Host	ESXi 6.x-Host
VMFS2	RO	RO	N	N
VMFS3	RW	RW	RW	RW
				<b>Hinweis</b> Sie können vorhandene VMFS3-Datenspeicher weiter verwenden, aber keine neuen erstellen. Führen Sie für vorhandene VMFS3-Datenspeicher ein Upgrade auf VMFS5 aus.
VMFS5	N	N	RW	RW

- RW: Vollständige Unterstützung von Lese- und Schreibberechtigungen. Sie können virtuelle Maschinen erstellen und einschalten.
- RO: Nur Unterstützung für Leseberechtigungen. Sie können virtuelle Maschinen nicht erstellen und einschalten.

- N: Kein Zugriff Hosts der Versionen ESXi 5.x und höher unterstützen VMFS2 nicht. Wenn der Datenspeicher mit VMFS2 formatiert ist, führen Sie zunächst mit den Legacy-Hosts ein Upgrade des Datenspeichers auf VMFS3 durch.

Mit dem vSphere Web Client können Sie im Voraus einen VMFS-Datenspeicher auf einem blockbasierten Speichergerät einrichten, das Ihr ESXi-Host erkennt. Ein VMFS-Datenspeicher kann sich über mehrere physische Erweiterungsgeräte erstrecken, einschließlich SAN-LUNs und lokale Speicher. Diese Funktion ermöglicht Ihnen die Zusammenfassung von Speicher und gibt Ihnen bei der Erstellung des für die virtuelle Maschine erforderlichen Datenspeichers die notwendige Flexibilität.

---

**Hinweis** Durch das Poolen ATS-fähiger Hardware wird ein zusammengefasster VMFS-Datenspeicher erstellt, der den Sperrmechanismus „Nur ATS“ verwenden kann. Wenn ein Gerät nicht ATS-fähig ist, kann der Datenspeicher nicht „Nur ATS“ sein, sondern verwendet ATS+SCSI-Sperre.

---

Die Kapazität des Datenspeichers kann während der Ausführung von virtuelle Maschinen im Datenspeicher erhöht werden. Auf diese Weise lässt sich entsprechend den aktuellen Anforderungen der virtuellen Maschine stets neuer Speicherplatz zu VMFS-Volumes hinzufügen. VMFS wurde für den gleichzeitigen Zugriff mehrerer physischer Maschinen konzipiert und erzwingt eine geeignete Zugriffsteuerung für VM-Dateien.

## Eigenschaften von VMFS5-Datenspeichern

VMFS5 bietet zahlreiche Verbesserungen bei Skalierbarkeit und Leistung.

VMFS5 weist die folgenden Merkmale auf:

- Speichergeräte mit einer Kapazität von mehr als 2 TB für jede VMFS5-Erweiterung
- Unterstützung von virtuellen Maschinen mit virtuellen Festplatten mit hoher Kapazität oder von Festplatten mit mehr als 2 TB.
- Erhöhte Ressourcenlimits, wie z. B. Dateideskriptoren.
- Standard-Dateisystemblockgröße von 1 MB mit Unterstützung für virtuelle Festplatten mit einer Kapazität von 2 TB.
- Festplattengröße von mehr als 2 TB für RDMs.
- Unterstützung von kleinen Dateien von 1 KB.
- Möglichkeit des Öffnens aller Dateien, die sich in einem VMFS5-Datenspeicher befinden, in einem Modus für die gemeinsame Nutzung durch maximal 32 Hosts
- Skalierbarkeitsverbesserungen bei Speichergeräten, welche die Hardwarebeschleunigung unterstützen. Weitere Informationen hierzu finden Sie unter [Kapitel 23 Speicherhardware-Beschleunigung](#).
- Standardmäßige Verwendung von Nur-ATS-Sperrmechanismen auf Speichergeräten mit ATS-Unterstützung. Informationen zur Nur-ATS-Sperrung und dem Upgrade darauf finden Sie unter [VMFS-Sperrmechanismen](#).

- Die Möglichkeit, physischen Speicherplatz auf Thin-bereitgestellten Speichergeräten zurückzugewinnen. Weitere Informationen hierzu finden Sie unter [Array-Thin Provisioning und VMFS-Datenspeicher](#).
- Online-Upgrade-Prozess, der vorhandene Datenspeicher aktualisiert, ohne die derzeitige Ausführung von Hosts oder virtuellen Maschinen zu unterbrechen. Weitere Informationen hierzu finden Sie unter [Upgrade von VMFS-Datenspeichern](#).

Informationen über Blockgrößenbeschränkungen eines VMFS-Datenspeichers finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1003565>.

## VMFS-Datenspeicher und Speicherfestplattenformate

Die vom Host unterstützten Speichergeräte können sowohl das Format Master Boot Record (MBR) als auch das Format GUID-Partitionstabelle (GPT) verwenden.

Beim Erstellen eines neuen VMFS5-Datenspeichers wird das Gerät mit GPT formatiert. Das GPT-Format erlaubt das Erstellen von Datenspeichern in der Größe zwischen 2 TB und 64 TB für eine einzelne Erweiterung.

VMFS3 nutzen für ihre Speichergeräte weiterhin das MBR-Format. Beachten Sie beim Umgang mit VMFS3-Datenspeichern folgende Punkte:

- Für VMFS3-Datenspeicher gilt das 2 TB-Limit auch dann, wenn das Speichergerät eine Kapazität von mehr als 2 TB hat. Um die gesamte Speicherkapazität nutzen zu können, führen Sie ein Upgrade des VMFS3-Datenspeichers auf VMFS5 durch. Die Konvertierung des MBR-Formats in GPT erfolgt erst, nachdem Sie den Datenspeicher auf über 2 TB erweitert haben.
- Wenn Sie ein Upgrade des VMFS3-Datenspeichers auf VMFS5 durchführen, verwendet der Datenspeicher das MBR-Format. Die Konvertierung in GPT erfolgt erst, nachdem Sie den Datenspeicher auf über 2 TB erweitert haben.
- Entfernen Sie beim Upgrade eines VMFS-Datenspeichers alle Partitionen des Speichergeräts, die von ESXi nicht erkannt werden, beispielsweise Partitionen in den Formaten EXT2 oder EXT3. Andernfalls kann der Host die Geräte nicht mit GPT formatieren und das Upgrade schlägt fehl.
- VMFS3-Datenspeicher auf Geräten mit GPT-Partitionsformat können nicht erweitert werden.

## VMFS-Datenspeicher als Repositorys

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

Mit VMFS5 verfügen Sie über bis zu 256 VMFS-Datenspeicher pro Host mit der maximalen Größe von 64 TB. Die erforderliche Mindestgröße für einen VMFS-Datenspeicher beträgt 1,3 GB, die empfohlene Mindestgröße beträgt jedoch 2 GB.

---

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

---



Sie können mehrere virtuelle Maschinen auf demselben VMFS-Datenspeicher 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 virtuelle Maschinen ausgeführt werden.

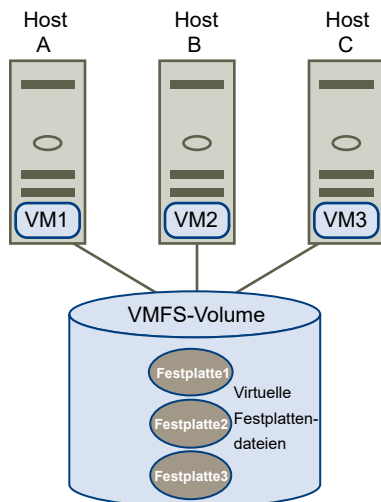
Wenn mehrere virtuelle Maschinen ausgeführt werden, bietet VMFS spezielle Sperrmechanismen für Dateien virtueller Maschinen, damit der sichere Betrieb auch in SAN-Umgebungen möglich ist, in der mehrere ESXi-Hosts auf denselben VMFS-Datenspeicher zugreifen.

Neben virtuelle Maschinen können auf VMFS-Datenspeichern auch andere Dateien, beispielsweise Vorlagen für virtuelle Maschinen und ISO-Images gespeichert werden.

## Gemeinsames Nutzen eines VMFS-Datenspeichers durch mehrere Hosts

Als Clusterdateisystem ermöglicht VMFS mehreren ESXi-Hosts, parallel auf denselben VMFS-Datenspeicher zuzugreifen.

Abbildung 16-1. Gemeinsames Nutzen eines VMFS-Datenspeichers durch mehrere Hosts



Informationen zur maximal zulässigen Anzahl von Hosts, die eine Verbindung mit einem einzelnen VMFS-Datenspeicher herstellen können, finden Sie im Dokument *Maximalwerte für die Konfiguration*.

Um sicherzustellen, dass nicht mehrere Hosts gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine festplatteninterne Sperrung.

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

- Sie können vSphere Distributed Resource Scheduling (DRS) und VMware High Availability (HA) verwenden.

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. Bei einem Störfall wird die festplatteninterne Sperre für die einzelnen virtuellen Maschinen aufgehoben. Weitere Informationen zu VMware DRS finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*. Informationen zu VMware HA finden Sie in der Dokumentation *Handbuch zur Verfügbarkeit in vSphere*.

- Mit vMotion können Sie virtuelle Maschinen bei laufendem Betrieb von einem physischen Server auf einen anderen migrieren. Informationen zur Migration von virtuellen Maschinen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Um einen freigegebenen Datenspeicher zu erstellen, mounten Sie den Datenspeicher auf den ESXi-Hosts, die Zugriff auf den Datenspeicher benötigen. Weitere Informationen hierzu finden Sie unter [Mounten von Datenspeichern](#).

## Updates von VMFS-Metadaten

Ein VMFS-Datenspeicher enthält Dateien der virtuellen Maschine, Verzeichnisse, symbolische Links, RDM-Deskriptor-Dateien usw. Der Datenspeicher verwaltet ebenfalls eine konsistente Ansicht aller Zuordnungsinformationen für diese Objekte. Diese Zuordnungsinformationen werden als Metadaten bezeichnet.

Metadaten werden jedes Mal aktualisiert, wenn Verwaltungsvorgänge des Datenspeichers oder der virtuellen Maschine durchgeführt werden. Einige Beispiele für Vorgänge, die eine Aktualisierung der Metadaten erfordern:

- Erstellen, Erweitern oder Sperren einer Datei einer virtuellen Maschine.
- Ändern von Dateieigenschaften
- Ein- bzw. Ausschalten einer virtuellen Maschine
- Erstellen oder Löschen eines VMFS-Datenspeichers
- Vergrößern von VMFS-Datenspeichern
- Erstellen einer Vorlage
- Bereitstellen einer virtuellen Maschine anhand einer Vorlage
- Migrieren einer virtuellen Maschine mit vMotion

Wenn Änderungen der Metadaten in einer Umgebung mit gemeinsam genutztem Speicher stattfinden, verwendet VMFS spezielle Sperrmechanismen, um die Daten zu schützen und zu verhindern, dass mehrere Hosts gleichzeitig Schreibzugriff auf die Metadaten erhalten.

## VMFS-Sperrmechanismen

In Umgebungen mit gemeinsam genutztem Speicher, bei denen mehrere Hosts auf denselben VMFS-Datenspeicher zugreifen, werden bestimmte Sperrmechanismen eingesetzt.

Diese Sperrmechanismen verhindern den gleichzeitigen Schreibzugriff mehrerer Hosts auf die Metadaten und stellen sicher, dass keine Daten beschädigt werden.

Je nach seiner Konfiguration und dem Typ des zugrunde liegenden Speichers kann ein VMFS-Datenspeicher den ATS (Atomic Test and Set)-Sperrmechanismus („Nur ATS“) exklusiv verwenden oder eine Kombination von ATS und SCSI-Reservierungen (ATS+SCSI) verwenden.

## Mechanismus „Nur ATS“

Bei Speichergeräten, die die auf dem T10-Standard basierten VAAI-Spezifikationen unterstützen, bietet VMFS ATS-Sperrung, auch als hardwaregestütztes Sperren bezeichnet. Der ATS-Algorithmus unterstützt ein differenziertes Sperren von Festplatten auf Sektorbasis. Alle neu formatierten VMFS5-Datenspeicher verwenden den Mechanismus „Nur ATS“, wenn er vom zugrunde liegenden Speicher unterstützt wird, und verwenden nie SCSI-Reservierungen.

Wenn Sie einen Datenspeicher mit mehreren Erweiterungen erstellen, in dem ATS verwendet wird, filtert vCenter Server Nicht-ATS-Geräte heraus. Dieses Filtern ermöglicht Ihnen, nur solche Geräte zu verwenden, die das ATS-Primitiv unterstützen.

In bestimmten Fällen ist für VMFS5-Datenspeicher die Einstellung „Nur ATS“ zu deaktivieren. Weitere Informationen hierzu finden Sie unter [Ändern des Sperrmechanismus zu ATS+SCSI](#).

## Mechanismus „ATS+SCSI“

Ein VMFS-Datenspeicher, der den Mechanismus „ATS+SCSI“ unterstützt, ist für die Verwendung von ATS konfiguriert und versucht, es zu verwenden, sofern möglich. Wenn ATS fehlschlägt, kehrt der VMFS-Datenspeicher zu SCSI-Reservierungen zurück. Im Gegensatz zur ATS-Sperrung wird bei der SCSI-Reservierung ein Speichergerät vollständig gesperrt, während ein Vorgang durchgeführt wird, der den Schutz von Metadaten erfordert. Nach dem Abschluss des Vorgangs hebt VMFS die Reservierung auf und blockierte Vorgänge können fortgesetzt werden.

Zu den Datenspeichern, die den Mechanismus „ATS+SCSI“ verwenden, gehören VMFS5-Datenspeicher, die von VMFS3 aktualisiert wurden. Außerdem verwenden neue VMFS5-Datenspeicher auf Speichergeräten, die ATS nicht unterstützen, den Mechanismus „ATS+SCSI“.

Wenn Ihr VMFS-Datenspeicher zu SCSI-Reservierungen zurückkehrt, bemerken Sie möglicherweise einen Leistungsabfall, der durch übermäßige SCSI-Reservierungen verursacht wird. Informationen über Möglichkeiten, die Anzahl der SCSI-Reservierungen zu verringern, finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

## Anzeigen von Informationen zu VMFS-Sperren

Verwenden Sie den `esxcli`-Befehl zum Abrufen von Informationen zu dem Sperrmechanismus, den ein VMFS-Datenspeicher verwendet.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Zum Anzeigen von Informationen in Bezug auf VMFS-Sperrmechanismen führen Sie den folgenden Befehl aus:

```
esxcli --server=Servername storage vmfs lockmode list.
```

## Ergebnisse

Die Tabelle enthält Elemente, die bei der Ausgabe des Befehls enthalten sein können.

**Tabelle 16-2. Informationen zu VMFS-Sperren**

Felder	Werte	Beschreibungen
Sperrmodus		Zeigt die Sperrkonfiguration des Datenspeichers an.
	Nur ATS	Gemäß der Konfiguration des Datenspeichers wird nur ATS verwendet.
	ATS+SCSI	Der Datenspeicher ist für die Verwendung von ATS konfiguriert, er kann aber auf SCSI zurückgreifen, wenn ATS nicht funktioniert oder nicht unterstützt wird.
	ATS-Upgrade steht aus	Beim Datenspeicher wird gerade ein Online-Upgrade auf „Nur ATS“ ausgeführt.
	ATS-Downgrade steht aus	Beim Datenspeicher wird gerade ein Online-Downgrade auf ATS+SCSI ausgeführt.
ATS-kompatibel		Zeigt an, ob der Datenspeicher für „Nur ATS“ konfiguriert werden kann.
ATS-Upgrade-Modi		Zeigt die Art des Upgrades an, das der Datenspeicher unterstützt.
	Keine	Der Datenspeicher ist nicht zu „Nur ATS“ kompatibel.
	Online	Der Datenspeicher kann während des Upgrades auf „Nur ATS“ verwendet werden.

Tabelle 16-2. Informationen zu VMFS-Sperren (Fortsetzung)

Felder	Werte	Beschreibungen
	Offline	Der Datenspeicher kann während des Upgrades auf „Nur ATS“ nicht verwendet werden.
Grund für ATS-Inkompatibilität		Wenn der Datenspeicher nicht zu „Nur ATS“ kompatibel ist, wird hier der Grund für die Inkompatibilität angezeigt.

## Ändern von VMFS-Sperren in „Nur ATS“

Wenn Ihre VMFS5-Datenspeicher mit dem Sperrmechanismus ATS+SCSI arbeiten, können Sie den Sperrmechanismus auf „Nur ATS“ setzen.

VMFS5-Datenspeicher, die aus VMFS3 aktualisiert wurden, verwenden üblicherweise den Sperrmechanismus ATS+SCSI. Wenn diese Datenspeicher auf ATS-aktivierter Hardware implementiert werden, ist in der Regel ein Upgrade auf die Nur-ATS-Sperrung möglich. Abhängig von Ihrer vSphere-Umgebung können Sie einen der folgenden Upgrademodi verwenden:

- Das Online-Upgrade auf Nur-ATS ist für die meisten VMFS5-Datenspeicher mit nur einer Erweiterung verfügbar. Während des Online-Upgrades eines Ihrer Hosts können andere Hosts den Datenspeicher weiter verwenden.
- Bei VMFS5-Datenspeichern mit mehreren physischen Erweiterungen muss ein Offline-Upgrade auf Nur-ATS durchgeführt werden. Für Datenspeicher mit mehreren physischen Erweiterungen ist das Online-Upgrade nicht verfügbar. Der Grund ist, dass bei diesen Datenspeichern während des Upgrades keine Hosts mit ihnen verbunden sein dürfen.

### Verfahren

#### 1 Vorbereiten eines Upgrades auf „Nur ATS“

Sie müssen mehrere Schritte durchführen, um Ihre Umgebung auf ein Online- oder Offline-Upgrade auf „Nur ATS“-Sperrung vorzubereiten.

#### 2 Upgrade des Sperrmechanismus auf „Nur ATS“

Bei Nur-ATS-kompatiblen VMFS-Datenspeichern können Sie den Sperrmechanismus von ATS+SCSI auf Nur ATS aktualisieren.

### Vorbereiten eines Upgrades auf „Nur ATS“

Sie müssen mehrere Schritte durchführen, um Ihre Umgebung auf ein Online- oder Offline-Upgrade auf „Nur ATS“-Sperrung vorzubereiten.

### Verfahren

- 1 Führen Sie ein Upgrade für alle Hosts, die auf den VMFS5-Datenspeicher zugreifen, auf die neueste vSphere-Version durch.

- Bestimmen Sie, ob der Datenspeicher sich für ein Upgrade seines aktuellen Sperrmechanismus eignet, indem Sie den Befehl `esxcli storage vmfs lockmode list` ausführen.

Die folgenden Felder der Beispielausgabe geben an, dass sich der Datenspeicher für ein Upgrade eignet, zeigen den aktuellen Sperrmechanismus und einen Upgrade-Modus, der für den Datenspeicher zur Verfügung steht.

```

Locking Mode   ATS Compatible   ATS Upgrade Modes
-----
ATS+SCSI       true               Online or Offline

```

- Je nach dem für den Datenspeicher verfügbaren Upgrade-Modus führen Sie eine der folgenden Aktionen durch:

Upgrade-Modus	Aktion
Online	Überprüfen Sie, dass alle Hosts konsistente Speicherverbindung zum VMFS-Datenspeicher aufweisen.
Offline	Überprüfen Sie, dass keine Hosts den Datenspeicher aktiv nutzen.

### Upgrade des Sperrmechanismus auf „Nur ATS“

Bei Nur-ATS-kompatiblen VMFS-Datenspeichern können Sie den Sperrmechanismus von ATS+SCSI auf Nur ATS aktualisieren.

Bei den meisten Datenspeichern, die sich nicht über mehrere Erweiterungen erstrecken, sind Online-Upgrades möglich. Während des Online-Upgrades eines Ihrer ESXi-Hosts können andere Hosts den Datenspeicher weiter verwenden. Der Online-Upgrade wird erst dann abgeschlossen, wenn alle Hosts den Datenspeicher geschlossen haben.

#### Voraussetzungen

Wenn Sie das Upgrade des Sperrmechanismus abschließen möchten, indem Sie den Datenspeicher in den Wartungsmodus versetzen, deaktivieren Sie Storage DRS. Dies bezieht sich nur auf Online-Upgrades.

#### Verfahren

- Führen Sie das Upgrade des Sperrmechanismus mit dem folgenden Befehl durch:

```

esxcli storage vmfs lockmode set -a|--ats -l|--volume-label= VMFS label -u|--volume-uuid= VMFS UUID.

```

## 2 Beim Online-Upgrade sind weitere Schritte notwendig.

- a Schließen Sie den Datenspeicher auf allen Hosts, die Zugriff darauf haben, sodass der Host die Änderung erkennen kann.

Dazu können Sie eine der folgenden Methoden verwenden:

- Unmounten Sie den Datenspeicher und mounten Sie ihn erneut.
- Versetzen Sie den Datenspeicher in den Wartungsmodus und verlassen Sie den Wartungsmodus.

- b Prüfen Sie, dass der Sperrungsstatus des Datenspeichers zu „Nur ATS“ geändert wurde, indem Sie folgenden Befehl ausführen:

```
esxcli storage vmfs lockmode list
```

- c Wenn der Sperrungsmodus irgendein einen anderen Status aufweist, etwa ATS UPGRADE PENDING, sehen Sie nach, welcher Host das Upgrade noch nicht durchgeführt hat. Verwenden Sie dazu folgenden Befehl:

```
esxcli storage vmfs host list
```

## Ändern des Sperrmechanismus zu ATS+SCSI

Wenn Sie einen VMFS5-Datenspeicher auf einem Gerät erstellen, das die ATS (Atomic Test and Set)-Sperrung unterstützt, wird der Datenspeicher so eingestellt, dass nur der ATS-Sperrmechanismus verwendet wird. Unter bestimmten Umständen müssen Sie möglicherweise ein Downgrade vom Sperrmodus „Nur ATS“ auf „ATS+SCSI“ ausführen.

Möglicherweise müssen Sie zum Sperrmechanismus „ATS+SCSI“ wechseln, wenn beispielsweise ein Downgrade auf Ihrem Speichergerät durchgeführt wird oder Firmware-Updates fehlschlagen und das Gerät ATS nicht mehr unterstützt.

Der Downgrade-Vorgang verläuft ähnlich wie das Upgrade auf „Nur ATS“. Wie beim Upgrade können Sie je nach Ihrer Speicherkonfiguration das Downgrade im Online- oder Offline-Modus durchführen.

### Verfahren

- 1 Ändern Sie den Sperrmechanismus auf „ATS+SCSI“ durch Ausführen des folgenden Befehls:

```
esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label= VMFS-Bezeichnung -u|--volume-uuid= VMFS UUID.
```

- 2 Schließen Sie beim Online-Modus den Datenspeicher auf allen Hosts, die auf den Datenspeicher zugreifen können, damit die Hosts die Änderung erkennen können.

## Grundlegende Informationen zu NFS-Datenspeichern

In ESXi integrierte NFS-Clients verwenden das Network File System-Protokoll (NFS) über TCP/IP, um auf ein ausgewähltes NFS-Volume auf einem NAS-Server zuzugreifen. Der ESXi-Host kann

das Volume mounten und für seine Speicherzwecke nutzen. vSphere unterstützt die Versionen 3 und 4.1 des NFS-Protokolls.

Das NFS-Volume bzw. NFS-Verzeichnis wird von einem Speicheradministrator erstellt und aus dem NFS-Server exportiert. Das NFS-Volume muss nicht mit einem lokalen Dateisystem wie VMFS formatiert sein. Sie können das NFS-Volume direkt auf ESXi-Hosts mounten und virtuelle Maschinen auf dieselbe Art und Weise speichern und starten, wie Sie das mit VMFS-Datenspeichern tun würden.

Neben der Speicherung von virtuellen Festplatten in NFS-Datenspeichern können Sie NFS als zentrales Repository für ISO-Images, VM-Vorlagen usw. nutzen. 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.

ESXi unterstützt die folgenden Speicherfunktionen auf den meisten NFS-Volumes:

- vMotion und Storage vMotion
- High Availability (HA) und Distributed Resource Scheduler (DRS)
- Fault Tolerance (FT) und Host-Profile

---

**Hinweis** NFS 4.1 bietet keine Unterstützung für eine Fault Tolerance-Legacy-Version.

---

- ISO-Images, die virtuellen Maschinen als CD-ROMs angezeigt werden
- Snapshots einer virtuellen Maschine
- Virtuelle Maschinen mit virtuellen Festplatten mit hoher Kapazität oder aber Festplatten mit mehr als 2 TB. In NFS-Datenspeichern erstellte virtuelle Festplatten verwenden standardmäßig Thin Provisioning, es sei denn, Sie nutzen Hardwarebeschleunigung mit Unterstützung des Vorgangs „Speicherplatz reservieren“. NFS 4.1 bietet keine Unterstützung für Hardwarebeschleunigung. Weitere Informationen hierzu finden Sie unter [Hardwarebeschleunigung auf NAS-Geräten](#).

## Richtlinien und Anforderungen für NFS-Speicher

Bei der Verwendung des NFS-Speichers müssen Sie spezifische Richtlinien zu Konfiguration, Netzwerk und NFS-Datenspeicher befolgen.

### Richtlinien zur NFS-Serverkonfiguration

- Vergewissern Sie sich, dass die verwendeten NFS-Server in der *VMware HCL* gelistet sind. Achten Sie auf die korrekte Version der Server-Firmware.
- Befolgen Sie beim Konfigurieren des NFS-Speichers die Empfehlungen des Speicheranbieters.
- Exportieren Sie das NFS-Volume mithilfe von NFS über TCP.



- Vergewissern Sie sich, dass eine Freigabe vom NFS-Server entweder als NFS 3 oder als NFS 4.1, nicht aber mit beiden Protokollversionen gemeinsam exportiert wird. Diese Richtlinie muss vom Server durchgesetzt werden, da ESXi das Mounten ein und derselben Freigabe über unterschiedliche NFS-Versionen nicht verhindert.
- NFS 3 und NFS 4.1 ohne Kerberos bieten keine Unterstützung für delegierte Benutzer, über die der Zugriff auf NFS-Volumes mit Nicht-Root-Anmeldedaten möglich wäre. Wenn Sie NFS 3 oder NFS 4.1 ohne Kerberos verwenden, stellen Sie sicher, dass alle Hosts Rootzugriff auf das Volume besitzen. Diese Funktion wird bei verschiedenen Speicheranbietern unterschiedlich aktiviert, erfolgt üblicherweise aber auf den NAS-Servern über die Option `no_root_squash`. Wenn der NAS-Server keinen Rootzugriff zulässt, können Sie den NFS-Datenspeicher eventuell auf dem Host mounten. In diesem Fall können Sie jedoch im Datenspeicher keine virtuellen Maschinen erstellen.
- Falls das zugrunde liegende NFS-Volume, auf dem die Dateien gespeichert sind, schreibgeschützt ist, stellen Sie sicher, dass es vom 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.

## Richtlinien für NFS-Netzwerke

- Für die Netzwerkverbindung benötigt der Host einen Standardnetzwerkadapter.
- ESXi unterstützt Layer-2- und Layer-3-Netzwerk-Switches. Bei Layer-3-Switches müssen sich ESXi-Hosts und NFS-Speicherarrays in unterschiedlichen Subnetzen befinden und die Routing-Informationen müssen vom Netzwerk-Switch verarbeitet werden.
- Für den NFS-Speicher ist eine VMkernel-Portgruppe erforderlich. Neue VMkernel-Portgruppen können auf einem bereits vorhandenen virtuellen Switch (vSwitch) oder einem neuen vSwitch erstellt werden, nachdem dieser konfiguriert wurde. Beim vSwitch kann es sich um einen vSphere Standard Switch (VSS) oder einen vSphere Distributed Switch (VDS) handeln.
- Bei Verwendung mehrerer Ports für den NFS-Datenverkehr müssen Sie sicherstellen, dass alle virtuellen und physischen Switches korrekt konfiguriert sind. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Netzwerk*.
- NFS 3 und NFS 4.1 ohne Kerberos unterstützen IPv4 und IPv6.

## Richtlinien für den NFS-Datenspeicher

- Für NFS 4.1 müssen Sie ein Upgrade Ihrer vSphere-Umgebung auf Version 6.x durchführen. Es ist nicht möglich, NFS-4.1-Datenspeicher auf Hosts zu mounten, die Version 4.1 nicht unterstützen.
- Das Mounten ein und desselben Datenspeichers mit unterschiedlichen NFS-Versionen ist nicht möglich. NFS-3- und NFS-4.1-Clients arbeiten mit unterschiedlichen Sperrprotokollen. Das bedeutet, dass es beim Zugriff auf dieselbe virtuelle Festplatte über zwei nicht kompatible Clients zu unvorhersehbarem Verhalten und Datenbeschädigung kommen kann.

- NFS-3- und NFS-4.1-Datenspeicher können nebeneinander auf demselben Host existieren.
- vSphere bietet keine Unterstützung für Datenspeicherupgrades aus NFS Version 3 auf Version 4.1.
- Wenn Sie dasselbe NFS-3-Volume auf verschiedenen Hosts mounten, müssen Sie sicherstellen, dass Server- und Ordernamen auf allen Hosts identisch sind. Wenn die Namen nicht übereinstimmen, betrachten die Hosts das NFS-3-Volume als zwei separate Datenspeicher. Bei Funktionen wie vMotion kann dies zu einem Fehler führen. Ein Beispiel für eine solche Diskrepanz wäre `filer` als Servernamen auf einem Host und `filer.domain.com` auf dem anderen. Diese Richtlinie gilt nicht für NFS Version 4.1.
- Wenn Sie beim Benennen von Datenspeichern und virtuellen Maschinen Nicht-ASCII-Zeichen verwenden, stellen Sie sicher, dass der zugrunde liegende NFS-Server die Internationalisierung unterstützt. Wenn der Server keine Sonderzeichen unterstützt, verwenden Sie nur die Standard-ASCII-Zeichen, da andernfalls unvorhersehbare Fehler auftreten können.

## NFS-Protokolle und ESXi

ESXi unterstützt NFS-Protokolle der Versionen 3 und 4.1. Um beide Versionen unterstützen zu können, verwendet ESXi zwei unterschiedliche NFS-Clients.

### NFS-Protokoll Version 3

vSphere unterstützt NFS Version 3 in TCP. Bei Verwendung dieser Version sollten Sie Folgendes beachten:

- Der Speicherdatenverkehr wird bei NFS Version 3 in einem unverschlüsselten Format über das LAN übertragen. Aufgrund dieser Einschränkungen bei der Sicherheit sollten Sie die NFS-Speicherung ausschließlich in vertrauenswürdigen Netzwerken einsetzen und den Datenverkehr in getrennten physischen Switches isolieren. Sie können auch ein privates VLAN verwenden.
- NFS 3 nutzt für die E/A nur eine TCP-Verbindung. Aus diesem Grund unterstützt ESXi die E/A für den NFS-Server auf nur einer IP-Adresse oder einem Hostnamen und bietet keine Unterstützung für mehrere Pfade. Je nach Ihrer Netzwerkinfrastruktur und -konfiguration können Sie mithilfe von Netzwerk-Stacks mehrere Verbindungen mit den Speicherzielen konfigurieren. Dazu müssen Sie mehrere Datenspeicher betreiben, von denen jeder eine eigene Netzwerkverbindung zwischen Host und Speicher verwendet.
- Bei NFS 3 bietet ESXi keine Unterstützung für delegierte Benutzer, über die der Zugriff auf NFS-Volumes mit Nicht-Root-Anmeldedaten möglich wäre. Stellen Sie sicher, dass alle Hosts Root-Zugriff auf das Volume besitzen.
- NFS 3 unterstützt die Hardwarebeschleunigung, über die der Host mit NAS-Geräten integriert werden und mehrere vom NAS-Speicher bereitgestellte Hardwarevorgänge nutzen kann. Weitere Informationen finden Sie unter [Hardwarebeschleunigung auf NAS-Geräten](#).

- Wenn die Hardwarebeschleunigung unterstützt wird, können Sie virtuelle Festplatten mit Thick Provisioning auf NFS-3-Datenspeichern erstellen.
- Die NFS-3-Sperrung in ESXi verwendet nicht das Protokoll Network Lock Manager (NLM). Stattdessen liefert VMware ein eigenes Sperrprotokoll. NFS-3-Sperrungen werden durch Sperrdateien auf dem NFS-Server erzielt. Diese tragen den Namen `.lck-file_id..`

## NFS-Protokoll Version 4.1

Bei Verwendung von NFS 4.1 sollten Sie Folgendes beachten:

- NFS 4.1 unterstützt mehrere Pfade für Server mit unterstütztem Session Trunking. Wenn Trunking verfügbar ist, können Sie über mehrere IP-Adressen auf dasselbe NFS-Volumen zugreifen. Client-ID-Trunking wird nicht unterstützt.
- NFS 4.1 bietet keine Unterstützung für Hardwarebeschleunigung. Diese Einschränkung lässt die Erstellung von virtuellen Festplatten mit Thick Provisioning in NFS-4.1-Datenspeichern nicht zu.
- NFS 4.1 unterstützt das Authentifizierungsprotokoll Kerberos zur sicheren Kommunikation mit dem NFS-Server. Weitere Informationen finden Sie unter [Verwenden von Kerberos-Anmeldedaten für NFS 4.1](#).
- NFS 4.1 verwendet Freigabereservierungen als Sperrmechanismus.
- NFS 4.1 unterstützt die integrierte Dateisperrung.
- NFS 4.1 unterstützt den Dateizugriff durch Nicht-Root-Benutzer über Kerberos.
- NFS 4.1 unterstützt herkömmliches Mounten ohne Kerberos. Halten Sie sich dabei an die empfohlenen Richtlinien zu Sicherheit und Rootzugriff für NFS Version 3.
- Gleichzeitiges Mounten mit AUTH\_SYS und Kerberos wird nicht unterstützt.
- NFS 4.1 mit Kerberos bietet keine Unterstützung für IPv6. NFS 4.1 mit AUTH\_SYS unterstützt IPv4 und IPv6.

## NFS-Protokolle und vSphere-Lösungen

vSphere-Funktionen	NFS Version 3	NFS Version 4.1
vMotion und Storage vMotion	Ja	Ja
High Availability (HA)	Ja	Ja
Fault Tolerance (FT)	Ja	Ja
Distributed Resource Scheduler (DRS)	Ja	Ja
Hostprofile	Ja	Ja
Storage DRS	Ja	Nein
Storage I/O Control	Ja	Nein

vSphere-Funktionen	NFS Version 3	NFS Version 4.1
Site Recovery Manager	Ja	Nein
Virtuelle Volumes	Ja	Nein

## NFS-Versionsupgrades

vSphere bietet keine Unterstützung für automatische Datenspeicherkonvertierungen aus NFS Version 3 auf Version 4.1. Wenn Sie Ihren Datenspeicher aus NFS 3 aktualisieren möchten, haben Sie folgende Möglichkeiten:

- Sie können einen neuen NFS-4.1-Datenspeicher erstellen und mit Storage vMotion anschließend die virtuellen Maschinen aus dem alten in den neuen Datenspeicher migrieren.
- Verwenden Sie die von Ihrem NFS-Speicheranbieter vorgesehenen Konvertierungsmethoden. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.
- Unmounten Sie aus der einen Version und mounten Sie in der anderen.

**Vorsicht** Wenn Sie so vorgehen, achten Sie darauf, dass Sie den Datenspeicher von allen Hosts unmounten, die Zugriff auf den Datenspeicher haben. Ein Datenspeicher kann niemals mit zwei Protokollen gleichzeitig gemountet werden.

## Firewall-Konfigurationen für NFS-Speicher

ESXi enthält eine Firewall zwischen der Verwaltungsschnittstelle und dem Netzwerk. Die Firewall ist standardmäßig aktiviert. Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme der Standarddienste wie NFS der eingehende und ausgehende Datenverkehr blockiert wird.

Unterstützte Dienste, einschließlich NFS, sind in einer Regelsatzkonfigurationsdatei im ESXi-Firewall-Verzeichnis `/etc/vmware/firewall/` beschrieben. Die Datei enthält Firewallregeln und listet die Beziehung einer jeden Regel zu Ports und Protokollen auf.

Das Verhalten des NFS-Client-Regelsatzes (`nfsClient`) unterscheidet sich von dem Verhalten anderer Regelsätze. Wenn der NFS-Client-Regelsatz aktiviert ist, sind alle ausgehenden TCP-Ports für die Zielhosts in der Liste der zulässigen IP-Adressen offen.

Der NFS 4.1-Regelsatz öffnet ausgehende Verbindungen am Zielport 2049, dem Port, der in der Spezifikation für das Protokoll der Version 4.1 genannt ist. Die ausgehenden Verbindungen sind für alle IP-Adressen zum Zeitpunkt des ersten Mountens geöffnet. Dieser Port bleibt geöffnet, bis der ESXi-Host neu gestartet wird.

Weitere Informationen zu Firewall-Konfigurationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## NFS-Client-Firewallverhalten

Der NFS-Client-Firewallregelsatz weist ein anderes Verhalten als andere ESXi-Firewallregelsätze auf. ESXi konfiguriert NFS-Client-Einstellungen, wenn Sie einen NFS-Datenspeicher mounten oder unmounten. Das Verhalten unterscheidet sich je nach NFS-Version.

Beim Hinzufügen, Mounten und Unmounten eines NFS-Datenspeichers hängt das Verhalten von der NFS-Version ab.

### Firewallverhalten in NFS v3

Wenn Sie einen NFS-v3-Datenspeicher hinzufügen oder mounten, überprüft ESXi den Status des NFS-Client-Firewallregelsatzes (`nfsClient`).

- Wenn der Regelsatz `nfsClient` deaktiviert ist, aktiviert ihn ESXi und deaktiviert die Richtlinie „Alle IP-Adressen zulassen“, indem das Flag `allowedAll` auf `FALSE` gesetzt wird. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.
- Wenn `nfsClient` aktiviert ist, bleiben der Status des Regelsatzes und die Richtlinien der zugelassenen IP-Adressen unverändert. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.

---

**Hinweis** Wenn Sie vor oder nach dem Hinzufügen eines NFS-v3-Datenspeichers zum System den Regelsatz `nfsClient` manuell aktivieren oder die Richtlinie „Alle IP-Adressen zulassen“ manuell festlegen, werden Ihre Einstellungen nach dem Unmounten des letzten NFS-v3-Datenspeichers überschrieben. Der Regelsatz `nfsClient` wird nach dem Unmounten aller NFS-v3-Datenspeicher deaktiviert.

---

Beim Entfernen oder Unmounten eines NFS-v3-Datenspeichers führt ESXi eine der folgenden Aktionen aus.

- Wenn keiner der verbleibenden NFS-v3-Datenspeicher von dem Server gemountet werden, auf dem der ungemountete Datenspeicher angesiedelt ist, entfernt ESXi die IP-Adresse des Servers aus der Liste der ausgehenden IP-Adressen.
- Wenn nach dem Unmounten keine gemounteten NFS-v3-Datenspeicher mehr übrig bleiben, deaktiviert ESXi den Firewallregelsatz `nfsClient`.

### Firewallverhalten in NFS v4.1

Beim Mounten des ersten NFS-v4.1-Datenspeichers aktiviert ESXi den Regelsatz `nfs41client` und setzt das Flag `allowedAll` auf `TRUE`. Dabei wird Port 2049 für alle IP-Adressen geöffnet. Das Unmounten eines NFS-v4.1-Datenspeichers hat keine Auswirkungen auf den Status der Firewall. Das heißt, dass durch den ersten gemounteten NFS-v4.1-Datenspeicher Port 2049 geöffnet wird und dieser so lange geöffnet bleibt, bis Sie ihn explizit schließen.

## Überprüfen der Firewall-Ports für NFS-Clients

Um den Zugriff auf NFS-Speicher zu ermöglichen, öffnet ESXi automatisch Firewall-Ports für die NFS-Clients, wenn Sie einen NFS-Datenspeicher mounten. Zu Zwecken der Fehlerbehebung müssen Sie möglicherweise überprüfen, ob die Ports geöffnet sind.

### Verfahren

- 1 Wählen Sie im vSphere Web Client den ESXi-Host aus.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie **Sicherheitsprofil** im Bereich **System** aus und klicken Sie auf **Bearbeiten**.
- 4 Führen Sie einen Bildlauf nach unten zu einer passenden NFS-Version durch, um sicherzustellen, dass der Port geöffnet ist.

## Geroutete Schicht 3-Verbindungen für Zugriff auf NFS-Speicher verwenden

Wenn Sie geroutete Schicht 3 (L3)-Verbindungen für den Zugriff auf NFS-Speicher verwenden, müssen Sie bestimmte Anforderungen und Beschränkungen beachten.

Ihre Umgebung muss die folgenden Anforderungen erfüllen:

- Das HSRP-Protokoll von Cisco (Hot Standby Router Protocol) wird im IP-Router verwendet. Falls Sie einen anderen Router als den von Cisco verwenden, stellen Sie sicher, dass Sie das VRRP-Protokoll (Virtual Router Redundancy Protocol) verwenden.
- QoS (Quality of Service) wird für die Priorisierung des NFS L3-Datenverkehrs auf Netzwerken mit begrenzter Bandbreite oder auf überlasteten Netzwerken verwendet. Weitere Informationen hierzu finden Sie in der Dokumentation des Routers.
- Befolgen Sie die von Ihrem Speicheranbieter empfohlenen Best Practices für NFS L3. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.
- Deaktivieren der Netzwerk-E/A-Ressourcenverwaltung (NetIORM).
- Falls Sie vorhaben, Systeme mit Top-of-Rack-Switches oder der Switch-abhängigen E/A-Gerätepartitionierung einzusetzen, wenden Sie sich bezüglich Kompatibilität und Unterstützung an Ihren Systemanbieter.

In einer L3-Umgebung gelten die folgenden Beschränkungen:

- Die Umgebung unterstützt VMware Site Recovery Manager nicht.
- Die Umgebung unterstützt nur das NFS-Protokoll. Verwenden Sie keine anderen Speicherprotokolle, wie z. B. FCoE, in demselben physischen Netzwerk.
- Der NFS-Datenverkehr in dieser Umgebung unterstützt IPv6 nicht.
- Der NFS-Datenverkehr in dieser Umgebung kann nur über ein LAN geleitet werden. Andere Umgebungen, wie z. B. WAN, werden nicht unterstützt.

## Einrichten der NFS-Speicherumgebung

Es sind einige Konfigurationsschritte erforderlich, bevor ein NFS-Datenspeicher in vSphere gemountet werden kann.

### Voraussetzungen

- Machen Sie sich mit den Richtlinien in [Richtlinien und Anforderungen für NFS-Speicher](#) vertraut.
- Details zum Konfigurieren des NFS-Speichers erhalten Sie in der Dokumentation Ihres Speicheraanbieters.

### Verfahren

- 1 Konfigurieren Sie auf dem NFS-Server ein NFS-Volume und exportieren Sie es, damit es auf den ESXi-Hosts gemountet werden kann.
  - a Notieren Sie sich die IP-Adresse oder den DNS-Namen des NFS-Servers und den vollständigen Pfad oder Ordernamen der NFS-Freigabe.  
  
Bei NFS 4.1 können Sie mehrere IP-Adressen oder DNS-Namen erfassen und so die Mehrfachpfadfunktion in NFS-4.1-Datenspeichern nutzen. NFS 3 und NFS 4.1 ohne Kerberos unterstützen IPv4- und IPv6-Adressen.
  - b Wenn Sie NFS 4.1 mit Kerberos-Authentifizierung ausstatten möchten, geben Sie die Kerberos-Anmeldedaten ein, die von ESXi zur Authentifizierung verwendet werden sollen.
- 2 Konfigurieren Sie auf allen ESXi Hosts einen VMkernel-Netzwerkport für den NFS-Datenverkehr.  
  
Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.
- 3 Wenn Sie den NFS-4.1-Datenspeicher mit Kerberos-Authentifizierung ausstatten möchten, konfigurieren Sie die ESXi-Hosts für die Authentifizierung mit Kerberos.  
  
Stellen Sie sicher, dass jeder Host, auf dem dieser Datenspeicher gemountet wird, Teil einer Active Directory-Domäne ist und über konfigurierte Anmeldedaten für die NFS-Authentifizierung verfügt.

### Nächste Schritte

Jetzt können Sie einen NFS-Datenspeicher auf den ESXi-Hosts erstellen.

## Verwenden von Kerberos-Anmeldedaten für NFS 4.1

Mit NFS-Version 4.1 unterstützt ESXi den Kerberos-Authentifizierungsmechanismus.

Kerberos ist ein Authentifizierungsdienst, mit dem ein auf ESXi installierter NFS 4.1-Client vor dem Mounten einer NFS-Freigabe bei einem NFS-Server seine Identität nachweisen kann. Kerberos verwendet Kryptographie bei der Arbeit über eine ungesicherte Netzwerkverbindung. Die vSphere-Implementierung von Kerberos für NFS 4.1 unterstützt nur die Identitätsprüfung für den Client und den Server, stellt aber keine Datenintegrität oder Vertraulichkeitsdienste bereit.

Wenn Sie die Kerberos-Authentifizierung verwenden, ist Folgendes zu beachten:

- ESXi verwendet die Kerberos-Version 5 mit Active Directory-Domäne und KD-Center.
- Als vSphere-Administrator geben Sie Active Directory-Anmeldedaten an, um einem NFS-Benutzer Zugriff auf NFS 4.1-Kerberos-Datenspeicher zu erteilen. Ein einzelner Anmeldedatensatz wird zum Zugriff auf alle Kerberos-Datenspeicher, die auf diesem Host gemountet sind, verwendet.
- Wenn mehrere ESXi-Hosts denselben NFS 4.1-Datenspeicher nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Sie können dies durch Festlegen des Benutzers in Hostprofilen und Anwenden des Profils auf alle ESXi-Hosts automatisieren.
- NFS 4.1 unterstützt nicht gleichzeitige AUTH\_SYS- und Kerberos-Mounts.
- NFS 4.1 mit Kerberos bietet keine Unterstützung für IPv6. Nur IPv4 wird unterstützt.

## Konfigurieren der Kerberos-Authentifizierung für ESXi-Hosts

Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie verschiedene Aufgaben zum Einrichten Ihrer Hosts für Kerberos-Authentifizierung ausführen.

Wenn mehrere ESXi-Hosts denselben NFS 4.1-Datenspeicher nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Sie können dies durch Festlegen des Benutzers in Hostprofilen und Anwenden des Profils auf alle ESXi-Hosts automatisieren.

### Voraussetzungen

- Stellen Sie sicher, dass Microsoft Active Directory (AD) und NFS-Server für die Verwendung von Kerberos konfiguriert sind.
- Aktivieren Sie den DES-CBC-MD5-Verschlüsselungsmodus auf AD. Der NFS 4.1-Client unterstützt nur diesen Verschlüsselungsmodus.
- Stellen Sie sicher, dass die NFS-Server-Exporte so konfiguriert sind, dass Vollzugriff auf den Kerberos-Benutzer gewährt wird.

### Verfahren

#### 1 Konfigurieren von DNS für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie die DNS-Einstellungen auf ESXi-Hosts ändern, um auf den DNS-Server zu zeigen, der dafür konfiguriert wurde, DNS-Datensätze für das Kerberos-KD-Center auszuhändigen. Verwenden Sie zum Beispiel die Active Directory-Serveradresse, wenn AD als DNS-Server verwendet wird.

#### 2 Konfigurieren von NTP (Network Time Protocol) für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, konfigurieren Sie Network Time Protocol (NTP), um sicherzustellen, dass alle ESXi-Hosts auf dem vSphere-Netzwerk synchronisiert sind.



### 3 Aktivieren der Kerberos-Authentifizierung in Active Directory

Bei Verwendung des NFS-4.1-Speichers mit Kerberos müssen Sie jedem ESXi-Host eine Active Directory-Domäne hinzufügen und die Kerberos-Authentifizierung aktivieren. Kerberos wird in Active Directory integriert und ermöglicht Single Sign On sowie eine zusätzliche Schutzebene für unsichere Netzwerkverbindungen.

#### Nächste Schritte

Nach dem Konfigurieren Ihres Hosts für Kerberos können Sie einen NFS 4.1-Datenspeicher erstellen, in dem Kerberos aktiviert ist.

#### Konfigurieren von DNS für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie die DNS-Einstellungen auf ESXi-Hosts ändern, um auf den DNS-Server zu zeigen, der dafür konfiguriert wurde, DNS-Datensätze für das Kerberos-KD-Center auszuhändigen. Verwenden Sie zum Beispiel die Active Directory-Serveradresse, wenn AD als DNS-Server verwendet wird.

#### Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf die Registerkarte **Verwalten**, klicken Sie auf **Netzwerk** und wählen Sie **TCP/IP-Konfiguration** aus.
- 3 Wählen Sie **TCP/IP-Konfiguration** aus und klicken Sie auf das Symbol **Bearbeiten**.
- 4 Geben Sie die DNS-Einstellungsdaten ein.

Option	Beschreibung
Domäne	AD-Domänenname
Bevorzugter DNS-Server	AD-Server-IP
Domänen durchsuchen	AD-Domänenname

#### Konfigurieren von NTP (Network Time Protocol) für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, konfigurieren Sie Network Time Protocol (NTP), um sicherzustellen, dass alle ESXi-Hosts auf dem vSphere-Netzwerk synchronisiert sind.

#### Verfahren

- 1 Wählen Sie den Host in der vSphere-Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie im Abschnitt „System“ die Option **Uhrzeitkonfiguration** aus.
- 4 Klicken Sie auf **Bearbeiten** und richten Sie den NTP-Server ein.
  - a Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.
  - b Legen Sie die Starttrichtlinie für den NTP-Dienst fest.

- c Geben Sie die IP-Adressen der NTP-Server ein, mit denen synchronisiert werden soll.
- d Klicken Sie im Abschnitt „NTP-Dienststatus“ auf **Starten** oder **Neu starten**.

**5** Klicken Sie auf **OK**.

Der Host wird mit dem NTP-Server synchronisiert.

### Aktivieren der Kerberos-Authentifizierung in Active Directory

Bei Verwendung des NFS-4.1-Speichers mit Kerberos müssen Sie jedem ESXi-Host eine Active Directory-Domäne hinzufügen und die Kerberos-Authentifizierung aktivieren. Kerberos wird in Active Directory integriert und ermöglicht Single Sign On sowie eine zusätzliche Schutzebene für unsichere Netzwerkverbindungen.

#### Voraussetzungen

Richten Sie eine AD-Domäne und ein Domänenadministratorkonto mit Berechtigungen zum Hinzufügen von Hosts zur Domäne ein.

#### Verfahren

- 1** Fügen Sie einen ESXi-Host zu einer Active Directory-Domäne hinzu.
  - a Wählen Sie im vSphere Web Client den ESXi-Host aus.
  - b Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
  - c Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.
  - d Klicken Sie auf **Domäne beitreten**, geben Sie die Domäneneinstellungen ein, und klicken Sie auf **OK**.

Der Verzeichnisdiensttyp wird zu Active Directory geändert.

- 2** Konfigurieren oder bearbeiten Sie die Anmeldedaten eines NFS-Kerberos-Benutzers.

- a Klicken Sie unter „NFS-Kerberos-Anmeldedaten“ auf **Bearbeiten**.
- b Geben Sie einen Benutzernamen und ein Kennwort ein.

Der Zugriff auf die in allen Kerberos-Datenspeichern gespeicherten Dateien erfolgt über diese Anmeldedaten.

Der Status der NFS-Kerberos-Anmeldedaten ändert sich zu „Aktiviert“.

## Erstellen von Datenspeichern

Mit dem Assistenten für neue Datenspeicher erstellen Sie die Datenspeicher. Abhängig vom verwendeten Speichertyp in Ihrer Umgebung und von Ihren Speicheranforderungen können Sie einen VMFS-, NFS- oder virtuellen Datenspeicher erstellen.

Ein Virtual SAN-Datenspeicher wird automatisch erstellt, wenn Sie Virtual SAN aktivieren. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware Virtual SAN*.

Sie können auch den Assistenten für neue Datenspeicher verwenden, um VMFS-Datenspeicherkopien zu verwalten.

- [Erstellen eines VMFS-Datenspeichers](#)

VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte.

- [Erstellen eines NFS-Datenspeichers](#)

Sie können ein NFS-Volume mit dem **Assistenten für neue Datenspeicher** mounten.

- [Erstellen eines virtuellen Datenspeichers](#)

Neue Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

## Erstellen eines VMFS-Datenspeichers

VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte.

---

**Hinweis** Sie können keine VMFS3-Datenspeicher in vSphere 6.x erstellen. Selbst wenn vorhandene VMFS3-Datenspeicher weiterhin verfügbar sind und verwendet werden können, müssen Sie sie auf VMFS5 aktualisieren.

---

### Voraussetzungen

Installieren und konfigurieren Sie alle Adapter, die vom Speicher benötigt werden. Scannen Sie alle Adapter erneut auf neu hinzugefügte Speicher.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.
- 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.  
  
Der vSphere Web Client setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.
- 4 Wählen Sie „VMFS“ als Datenspeichertyp aus.
- 5 Wählen Sie das Gerät aus, das für den Datenspeicher verwendet werden soll.

---

**Wichtig** Für das Gerät, das Sie auswählen, dürfen keine Werte in der Spalte „Snapshot-Volume“ angezeigt werden. Wenn ein Wert vorhanden ist, enthält das Gerät eine Kopie des vorhandenen VMFS-Datenspeichers. Weitere Informationen zur Verwaltung von Datenspeicherkopien finden Sie unter [Verwalten von duplizierten VMFS-Datenspeichern](#).

---

## 6 Legen Sie die Konfiguration der Partition fest.

Option	Beschreibung
<b>Alle verfügbaren Partitionen verwenden</b>	Weist einem einzelnen VMFS-Datenspeicher die gesamte Festplatte zu. Bei Auswahl dieser Option werden die momentan auf diesem Gerät gespeicherten Dateisysteme und Daten dauerhaft gelöscht.
<b>Freien Speicherplatz verwenden</b>	Stellt einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereit.

## 7 (Optional) Wenn der für den Datenspeicher zugeteilte Speicherplatz für Ihre Zwecke zu groß ist, passen Sie die Kapazitätswerte im Feld „Größe des Datenspeichers“ an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zugeteilt.

## 8 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **Beenden**.

### Ergebnisse

Der Datenspeicher auf dem SCSI-basierten Gerät wird erstellt. Er ist für alle Hosts verfügbar, die auf das Gerät Zugriff haben.

## Erstellen eines NFS-Datenspeichers

Sie können ein NFS-Volume mit dem **Assistenten für neue Datenspeicher** mounten.

### Voraussetzungen

- Richten Sie die NFS-Speicherumgebung ein.
- Wenn Sie die Kerberos-Authentifizierung mit dem NFS 4.1-Datenspeicher verwenden möchten, müssen Sie für die ESXi-Hosts die Kerberos-Authentifizierung konfigurieren.

### Verfahren

#### 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.

#### 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.

#### 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.

Der vSphere Web Client setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.

#### 4 Wählen Sie „NFS“ als Datenspeichertyp aus.

#### 5 Geben Sie eine NFS-Version an.

- NFS 3

## ■ NFS 4.1

---

**Wichtig** Wenn mehrere Hosts auf denselben Datenspeicher zugreifen, müssen Sie dasselbe Protokoll auf allen Hosts verwenden.

---

- 6 Geben Sie den Servernamen oder die IP-Adresse und den Mount-Punkt-Ordernamen ein.  
Bei NFS 4.1 können Sie mehrere IP-Adressen oder Servernamen hinzufügen, wenn der Server Trunking unterstützt. Der Host verwendet diese Werte, um Multipathing bis zum Mount-Punkt des NFS-Servers zu erreichen.  
Sie können IPv4- oder IPv6-Adressen für NFS 3 und NFS 4.1 ohne Kerberos verwenden.
- 7 Wählen Sie **NFS schreibgeschützt mounten**, wenn das Laufwerk vom NFS-Server als schreibgeschützt exportiert wurde.
- 8 Wenn Sie Kerberos-Authentifizierung mit NFS 4.1 verwenden, aktivieren Sie Kerberos auf dem Datenspeicher.
- 9 Wenn Sie einen Datenspeicher auf Datencenter- oder Cluster-Ebene erstellen, wählen Sie Hosts aus, die den Datenspeicher mounten.
- 10 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

## Erstellen eines virtuellen Datenspeichers

Neue Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.
- 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.  
Achten Sie darauf, für jeden Datenspeicher in Ihrer Datenspeicherumgebung einen eindeutigen Namen zu vergeben.  
Beim Mounten eines virtuellen Datenspeichers auf mehreren Hosts muss der Datenspeichername auf allen Hosts gleich sein.
- 4 Wählen Sie **VVOL** als Datenspeichertyp.
- 5 Wählen Sie aus der Liste der Speichercontainer einen Backing-Speichercontainer aus.
- 6 Wählen Sie die Hosts aus, die Zugriff auf den Datenspeicher benötigen.
- 7 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

## Nächste Schritte

Nach der Erstellung des virtuellen Datenspeichers können Sie ihn umbenennen, Datenspeicherdateien durchsuchen, den Datenspeicher unmounten und weitere Datenspeicheraktionen ausführen.

Sie können den Datenspeicher nicht einem Datenspeicher-Cluster hinzufügen.

## Verwalten von duplizierten VMFS-Datenspeichern

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

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

Neben dem Erstellen eines Snapshots und der Replizierung der LUN können die folgenden Speichergerätvorgänge möglicherweise bewirken, dass ESXi den vorhandenen Datenspeicher auf dem Gerät als eine Kopie des ursprünglichen Datenspeichers markiert:

- LUN-ID-Änderungen
- Änderungen des SCSI-Gerätetyps, z. B. von SCSI-2 auf SCSI-3
- Aktivierung der SPC-2-Übereinstimmung

ESXi kann die Kopie des VMFS-Datenspeichers erkennen und sie im vSphere Web Client anzeigen. Sie haben die Option, die Datenspeicherkopie mit ihrer ursprünglichen UUID zu mounten oder die UUID zu ändern, was zu einer Neusignierung des Datenspeichers führt.

Ob Sie die Neusignierung oder das Mounten ohne Neusignierung wählen, hängt davon ab, wie die LUNs in der Speicherumgebung maskiert werden. Wenn Ihre Hosts beide Kopien der LUN sehen können, ist die Neusignierung die empfohlene Methode. Sonst ist das Mounten eine Option.

## Beibehalten der vorhandenen Datenspeichersignatur

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

Sie können die Signatur beispielsweise beibehalten, wenn Sie synchronisierte Kopien von virtuellen Maschinen als Teil eines Notfallplans auf einer sekundären Site unterhalten. Bei einem Notfall an der primären Site mounten Sie die Datenspeicherkopie und schalten die virtuelle Maschinen der sekundären Site ein.

## Voraussetzungen

- Führen Sie eine erneute Speicherprüfung auf Ihrem Host durch, um die Ansicht der Speichergeräte auf dem Host zu aktualisieren.
- Unmounten Sie den Original-VMFS-Datenspeicher, der dieselbe UUID hat wie die Kopie, die Sie mounten möchten. Sie können die VMFS-Datenspeicherkopie nur mounten, wenn sie nicht mit dem Original-VMFS-Datenspeicher kollidiert.

## Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.
- 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.
- 4 Wählen Sie „VMFS“ als Datenspeichertyp aus.
- 5 Wählen Sie aus der Liste der Speichergeräte das Gerät aus, dessen Wert in der Spalte „Snapshot-Volume“ angezeigt wird.

Der in der Spalte „Snapshot-Volume“ vorhandene Name gibt an, dass das Gerät 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 die Konfigurationsinformationen für den Datenspeicher, und klicken Sie auf **Beenden (Finish)**.

## Nächste Schritte

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

## Neusignieren einer VMFS-Datenspeicherkopie

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 Signatur (UUID) zu und mountet die Kopie als einen vom Original unabhängigen Datenspeicher. Alle Referenzen der Originalsignatur aus den Konfigurationsdateien der virtuellen Maschine werden aktualisiert.

Beachten Sie bei der Datenspeicher-Neusignierung Folgendes:

- Die Datenspeicher-Neusignierung kann nicht rückgängig gemacht werden.
- Nach der Neusignierung wird die Speichergerätekopie, die die VMFS-Kopie enthalten hat, nicht mehr als Replik 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 Speichergeräte-Snapshots, in Konflikt steht.

#### Voraussetzungen

- Unmounten Sie die Datenspeicherkopie.
- Führen Sie eine erneute Speicherprüfung auf Ihrem Host durch, um die Ansicht der Speichergeräte auf dem Host zu aktualisieren.

#### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.
- 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.
- 4 Wählen Sie „VMFS“ als Datenspeichertyp aus.
- 5 Wählen Sie aus der Liste der Speichergeräte das Gerät aus, dessen Wert in der Spalte „Snapshot-Volume“ angezeigt wird.  
  
Der in der Spalte „Snapshot-Volume“ vorhandene Name gibt an, dass das Gerät 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 die Konfigurationsinformationen für den Datenspeicher, und klicken Sie auf **Beenden (Finish)**.

## Upgrade von VMFS-Datenspeichern

Wenn Ihre Datenspeicher mit VMFS2 oder VMFS3 formatiert wurden, müssen Sie ein Upgrade der Datenspeicher auf VMFS5 durchführen.

Beachten Sie bei der Durchführung von Datenspeicher-Upgrades Folgendes:

- Verwenden Sie für ein Upgrade eines VMFS2-Datenspeichers ein Verfahren in zwei Schritten. Dieses beinhaltet, dass zunächst ein Upgrade von VMFS2 auf VMFS3 durchgeführt wird. Verwenden Sie für den Zugriff auf den VMFS2-Datenspeicher und die Konvertierung von VMFS2 zu VMFS3 einen Host der Version ESX/ESXi 4.x oder früher.  
  
Nach dem Upgrade des VMFS2-Datenspeichers auf VMFS3 steht der Datenspeicher auf dem ESXi 6.x-Host nicht mehr zur Verfügung, auf dem Sie das Upgrade auf VMFS5 abschließen.
- Sie können ein Upgrade von VMFS3 auf VMFS5 vornehmen, während der Datenspeicher mit eingeschalteten virtuellen Maschinen benutzt wird.



- Bei der Durchführen eines Upgrades behält Ihr Host alle Dateien im Datenspeicher.
- Das Datenspeicher-Upgrade ist ein Prozess, der nur in eine Richtung ausgeführt werden kann. Nach dem Upgrade des Datenspeichers können Sie ihn auf sein vorheriges VMFS-Format zurücksetzen.

Ein aktualisierter VMFS5-Datenspeicher weicht von einem neu formatierten VMFS5 ab.

**Tabelle 16-3. Aktualisierte und neu formatierte VMFS5-Datenspeicher im Vergleich**

Merkmale	Aktualisierter VMFS5	Formatierter VMFS5
Dateiblockgröße	1, 2, 4 oder 8 MB	1MB
Größe des untergeordneten Blocks	64KB	8 KB
Partitionsformat	MBR. Die Konvertierung in GPT erfolgt erst, nachdem Sie den Datenspeicher auf über 2 TB erweitert haben.	GPT
Datenspeichergrenzwerte	Behält die Beschränkungen des VMFS3-Datenspeichers bei.	
VMFS-Sperrmechanismus	ATS+SCSI	Nur ATS (auf Hardware, die ATS unterstützt) ATS+SCSI (auf Hardware, die ATS nicht unterstützt)

Weitere Informationen über VMFS-Sperrmechanismen und das Upgrade auf „Nur ATS“ finden Sie unter [VMFS-Sperrmechanismen](#).

## Upgrade eines Datenspeichers auf VMFS5

Wenn Sie VMFS3-Datenspeicher verwenden, müssen Sie sie auf VMFS5 aktualisieren.

Sie können ein Upgrade vornehmen, während der Datenspeicher mit eingeschalteten virtuellen Maschinen benutzt wird.

### Voraussetzungen

- Wenn Sie einen VMFS2-Datenspeicher haben, müssen Sie erst mit einem ESX/ESXi 3.x- oder ESX/ESXi 4.x-Host ein Upgrade auf VMFS3 vornehmen. Verwenden Sie den Client des vSphere-Hosts, um auf den Host zuzugreifen.
- Alle Hosts, die auf den Datenspeicher zugreifen, müssen VMFS5 unterstützen.
- Stellen Sie sicher, dass das zu aktualisierende Volume über mindestens 2 MB an freiem Speicherplatz verfügt. Diese Information finden Sie auf der Registerkarte „Übersicht“ des Datenspeichers.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf den Datenspeicher, der einem Upgrade unterzogen werden soll.

- 3 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 4 Klicken Sie auf **Upgrade auf VMFS5**.
- 5 Überprüfen Sie, dass die Hosts, die auf den Datenspeicher zugreifen, VMFS5 unterstützen.
- 6 Klicken Sie auf **OK**, um das Upgrade zu starten
- 7 Führen Sie auf allen Hosts, die dem Datenspeicher zugewiesen sind, eine erneute Prüfung durch.

#### Ergebnisse

Der Datenspeicher wird einem Upgrade auf VMFS5 unterzogen und ist für alle Hosts verfügbar, die mit dem Datenspeicher verbunden sind.

## Erhöhen der VMFS-Datenspeicherkapazität

Wenn Ihr VMFS-Datenspeicher mehr Speicherplatz benötigt, erhöhen Sie die Datenspeicherkapazität. Sie können die Kapazität dynamisch erhöhen, indem Sie eine Datenspeichererweiterung vergrößern oder eine neue Erweiterung hinzufügen.

Verwenden Sie zum Vergrößern der Datenspeicherkapazität eine der folgenden Methoden:

- Erweitern Sie dynamisch eine vergrößerbare Datenspeichererweiterung, damit der Datenspeicher die benachbarte Kapazität belegt. Die Erweiterung wird als vergrößerbar angesehen, wenn das zugrunde liegende Speichergerät unmittelbar hinter der Erweiterung über freien Speicherplatz verfügt.
- Fügen Sie dynamisch eine neue Erweiterung hinzu. Der Datenspeicher kann sich über bis zu 32 Erweiterungen mit einer Größe von jeweils mehr als 2 TB erstrecken und dennoch als ein einziges Volume erscheinen. Der zusammengefasste VMFS-Datenspeicher kann jederzeit jede einzelne oder alle seiner Erweiterungen verwenden. Es ist nicht notwendig, dass eine bestimmte Erweiterung aufgefüllt wird, bevor die nächste Erweiterung verwendet werden kann.

---

**Hinweis** Datenspeicher, die nur hardwaregestützte Sperren unterstützen, die auch als Atomic Test and Set-Mechanismus (ATS) bezeichnet werden, können sich über Nicht-ATS-Geräte erstrecken. Weitere Informationen finden Sie unter [VMFS-Sperrmechanismen](#).

---

## Erhöhen der VMFS-Datenspeicherkapazität

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

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.

## Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Wählen Sie den zu vergrößernden Datenspeicher aus und klicken Sie auf das Symbol „Datenspeicherkapazität erhöhen“.
- 3 Wählen Sie ein Gerät aus der Liste der Speichergeräte aus.

Die Auswahlmöglichkeiten hängen davon ab, ob ein erweiterbares Speichergerät verfügbar ist.

Option	Beschreibung
<b>So vergrößern Sie eine vorhandene Erweiterung</b>	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Ja“ hat. Ein Speichergerät wird als „Erweiterbar“ gemeldet, wenn es sofort nach der Erweiterung über freien Speicherplatz verfügt.
<b>So fügen Sie eine neue Erweiterung hinzu</b>	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Nein“ hat.

- 4 Prüfen Sie das **aktuelle Festplattenlayout** auf die verfügbaren Konfigurationen und klicken Sie auf **Weiter**.
- 5 Wählen Sie eine Konfigurationsoption im unteren Fenster aus.

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

Option	Beschreibung
<b>Freien Speicherplatz nutzen, um eine neue Erweiterung hinzuzufügen</b>	Fügt den freien Speicherplatz auf dieser Festplatte als neue Erweiterung hinzu.
<b>Freien Speicherplatz nutzen, um eine vorhandene Erweiterung zu erweitern</b>	Vergrößert eine vorhandene Erweiterung auf die erforderliche Kapazität.
<b>Freien Speicherplatz verwenden</b>	Stellt eine Erweiterung im verbleibenden freien Speicherplatz auf der Festplatte bereit. Diese Option ist nur verfügbar, wenn Sie eine Erweiterung hinzufügen.
<b>Alle verfügbaren Partitionen verwenden</b>	Weist einer einzelnen Erweiterung die gesamte Festplatte zu. Diese Option ist nur verfügbar, wenn Sie eine Erweiterung hinzufügen und die zu formatierende Festplatte nicht leer ist. Die Festplatte wird neu formatiert und dabei werden alle darauf enthaltenen Datenspeicher und Daten gelöscht.

- 6 Geben Sie die Kapazität der Erweiterung an.  
Die Mindesterweiterungsgröße ist 1,3 GB. Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.
- 7 Klicken Sie auf **Weiter**.
- 8 Überprüfen Sie das vorgeschlagene Layout und die neue Konfiguration des Datenspeichers, und klicken Sie anschließend auf **Beenden**.

## Verwaltungsvorgänge für Datenspeicher

Nach dem Erstellen von Datenspeichern können Sie für die Datenspeicher mehrere Verwaltungsvorgänge durchführen. Bestimmte Vorgänge wie das Umbenennen eines Datenspeichers stehen für alle Datenspeichertypen zur Verfügung. Andere beziehen sich auf bestimmte Typen von Datenspeichern.

- **Ändern des Datenspeichernamens**

Der Name eines vorhandenen Datenspeichers kann geändert werden. Sie können ohne negative Auswirkungen den Datenspeicher umbenennen, auf dem virtuelle Maschinen ausgeführt werden.

- **Unmounten von Datenspeichern**

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

- **Mounten von Datenspeichern**

Sie können einen zuvor ungemounteten Datenspeicher mounten. Sie können einen Datenspeicher auch auf weiteren Hosts mounten. Dadurch wird dieser zu einem gemeinsam genutzten Datenspeicher.

- **Entfernen von VMFS-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.

- **Verwenden des Datenspeicherbrowsers**

Verwenden Sie den Datenspeicherbrowser zum Verwalten des Inhalts Ihrer Datenspeicher. Sie können Ordner und Dateien durchsuchen, die im Datenspeicher gespeichert sind. Im Browser können Sie auch Dateien hochladen und Verwaltungsaufgaben für Ihre Dateien und Ordner durchführen.

- **Ausschalten von Speicherfiltern**

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, verwendet vCenter Server Standardspeicherschutzfilter. Die Filter helfen Ihnen Speicherschäden zu vermeiden, indem nur die Speichergeräte abgerufen werden, die für einen bestimmten Vorgang verwendet werden können. Ungeeignete Geräte werden nicht zur Auswahl angezeigt. Sie können die Filter deaktivieren, um alle Geräte anzuzeigen.

## Ändern des Datenspeichernamens

Der Name eines vorhandenen Datenspeichers kann geändert werden. Sie können ohne negative Auswirkungen den Datenspeicher umbenennen, auf dem virtuelle Maschinen ausgeführt werden.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.

- 2 Wählen Sie den umzubenennenden Datenspeicher aus.
- 3 Wählen Sie im Kontextmenü die Option **Umbenennen**.
- 4 Geben Sie einen neuen Datenspeichernamen ein.

Der vSphere Web Client setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.

#### Ergebnisse

Der neue Name erscheint auf allen Hosts, die Zugriff auf den Datenspeicher haben.

## Unmounten von Datenspeichern

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

Führen Sie während des Unmountens keine Konfigurationsvorgänge aus, die E/A-Datenspeichervorgänge zum Ergebnis haben könnten.

---

**Hinweis** Stellen Sie sicher, dass der Datenspeicher nicht für vSphere HA-Taktsignale verwendet wird. vSphere HA-Taktsignale verhindern das Unmounten des Datenspeichers nicht. Wenn jedoch der Datenspeicher für das Taktsignal verwendet wird, kann das Unmounten des Datenspeichers dazu führen, dass der Host ausfällt und eine aktive virtuelle Maschine neu gestartet wird.

---

#### Voraussetzungen

Stellen ggf. Sie vor dem Unmounten von Datenspeichern sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Es dürfen sich keine virtuelle Maschinen im Datenspeicher befinden.
- Der Datenspeicher wird nicht von Speicher-DRS verwaltet.
- Storage I/O Control für diesen Datenspeicher ist deaktiviert.

#### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie mit der rechten Maustaste auf den entsprechenden Datenspeicher und wählen Sie **Datenbank unmounten**.
- 3 Wenn der Datenspeicher gemeinsam genutzt wird, geben Sie an, welche Hosts nicht mehr auf den Datenspeicher zugreifen sollen.
- 4 Bestätigen Sie, dass Sie den Datenspeicher unmounten möchten.

## Ergebnisse

Nachdem Sie einen VMFS-Datenspeicher von allen Hosts ungemountet haben, wird der Datenspeicher als inaktiv markiert. Wenn Sie einen NFS- oder virtuellen Datenspeicher von allen Hosts unmounten, wird er in der Bestandsliste nicht mehr angezeigt.

## Nächste Schritte

Wenn Sie den VMFS-Datenspeicher im Zuge eines ordnungsgemäßen Verfahrens zum Entfernen eines Speichergeräts unmounten, können Sie jetzt das Speichergerät trennen, auf dem der Datenspeicher gesichert wird. Weitere Informationen hierzu finden Sie unter [Speichergeräte trennen](#).

## Mounten von Datenspeichern

Sie können einen zuvor ungemounteten Datenspeicher mounten. Sie können einen Datenspeicher auch auf weiteren Hosts mounten. Dadurch wird dieser zu einem gemeinsam genutzten Datenspeicher.

Ein VMFS-Datenspeicher, der auf allen Hosts ungemountet wurde, verbleibt zwar in der Bestandsliste, wird aber als unzugänglich markiert. Sie können diese Aufgabe zum Mounten des VMFS-Datenspeichers auf einem bestimmten Host oder mehreren Hosts verwenden.

Wenn Sie einen NFS- oder virtuellen Datenspeicher von allen Hosts unmounten, wird er in der Bestandsliste nicht mehr angezeigt. Zum Mounten eines NFS- oder virtuellen Datenspeichers, der aus der Bestandsliste entfernt wurde, verwenden Sie den Assistenten „Neuer Datenspeicher“.

Ein beliebiger Datenspeicher, der auf einigen Hosts ungemountet wird, während er auf anderen gemountet ist, wird in der Bestandsliste als aktiv angezeigt.

## Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher, der gemountet werden soll, und wählen Sie eine der folgenden Optionen aus:
  - **Datenspeicher mounten**
  - **Datenspeicher auf zusätzlichen Hosts mounten**

Von der Art des verwendeten Datenspeichers hängt ab, welche Optionen verfügbar sind.
- 3 Wählen Sie die Hosts aus, die Zugriff auf den Datenspeicher benötigen.

## Entfernen von VMFS-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.

---

**Hinweis** Der Datenspeicher-Löschvorgang löscht alle Dateien permanent, die virtuelle Maschinen auf dem Datenspeicher zugeordnet sind. Obwohl Sie den Datenspeicher ohne Unmounten löschen können, empfiehlt es sich, zuerst den Datenspeicher zu unmounten.

---

### Voraussetzungen

- Entfernen oder migrieren Sie alle virtuellen Maschinen aus dem Datenspeicher.
- Stellen Sie sicher, dass kein anderer Host auf den Datenspeicher zugreift.
- Deaktivieren Sie Speicher-DRS für den Datenspeicher.
- Deaktivieren Sie Storage I/O Control für den Datenspeicher.
- Stellen Sie sicher, dass der Datenspeicher nicht für vSphere HA-Taktsignale verwendet wird.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie zum Entfernen mit der rechten Maustaste auf den Datenspeicher.
- 3 Wählen Sie **Datenspeicher löschen** aus.
- 4 Bestätigen Sie, dass Sie den Datenspeicher entfernen möchten.

## Verwenden des Datenspeicherbrowsers

Verwenden Sie den Datenspeicherbrowser zum Verwalten des Inhalts Ihrer Datenspeicher. Sie können Ordner und Dateien durchsuchen, die im Datenspeicher gespeichert sind. Im Browser können Sie auch Dateien hochladen und Verwaltungsaufgaben für Ihre Dateien und Ordner durchführen.

- [Hochladen von Dateien in Datenspeicher](#)  
Verwenden Sie den Datenspeicher-Datei-Browser zum Hochladen von Dateien in Datenspeicher, auf die ESXi-Hosts zugreifen können.
- [Kopieren von Datenspeicherordnern oder -dateien](#)  
Verwenden Sie den Datenspeicherbrowser zum Kopieren von Ordnern oder Dateien an einen neuen Speicherort auf demselben oder einem anderen Datenspeicher.
- [Verschieben von Datenspeicherordnern oder -dateien](#)  
Verschieben Sie Ordner oder Dateien mit dem Datenspeicherbrowser an einen neuen Speicherort im selben oder einem anderen Datenspeicher.
- [Umbenennen von Datenspeicherordnern oder -dateien](#)  
Verwenden Sie den Datenspeicherbrowser, um Ordner oder Dateien umzubenennen.

## ■ Vergrößern virtueller Thin-Festplatten

Wenn Sie eine virtuelle Festplatte im Format „Thin-Bereitstellung“ erstellt haben, können Sie die Thin-Festplatte in das Format „Thick-Provision“ konvertieren.

### Verfahren

- 1 Öffnen Sie den Datenspeicherbrowser.
  - a Zeigen Sie den Datenspeicher in der Bestandsliste an.
  - b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen** (🔍) aus.
- 2 Untersuchen Sie den Inhalt des Datenspeichers, indem Sie zu vorhandenen Ordnern und Dateien navigieren.
- 3 Führen Sie Verwaltungsaufgaben mithilfe der entsprechenden Symbole und Optionen durch.

Symbole und Optionen	Beschreibungen
	Installiert das Client-Integrations-Plug-In oder lädt eine Datei in den Datenspeicher hoch. Weitere Informationen hierzu finden Sie unter <a href="#">Hochladen von Dateien in Datenspeicher</a> .
	Erstellt einen Ordner im Datenspeicher.
	Kopiert ausgewählte Ordner oder Dateien an einen neuen Speicherort, entweder im selben oder in einem anderen Datenspeicher. Weitere Informationen hierzu finden Sie unter <a href="#">Kopieren von Datenspeicherordnern oder -dateien</a> .
	Verschiebt ausgewählte Ordner oder Dateien an einen neuen Speicherort, entweder im selben oder in einem anderen Datenspeicher. Weitere Informationen hierzu finden Sie unter <a href="#">Verschieben von Datenspeicherordnern oder -dateien</a> .
	Benennt ausgewählte Dateien oder Ordner um. Weitere Informationen hierzu finden Sie unter <a href="#">Umbenennen von Datenspeicherordnern oder -dateien</a> .
	Löscht ausgewählte Dateien oder Ordner.
<b>Vergrößern</b>	Konvertiert eine ausgewählte virtuelle Festplatte vom Thin-Format in das Thick-Format. Diese Option gilt nur für per Thin Provisioning bereitgestellte Festplatten. Weitere Informationen hierzu finden Sie unter <a href="#">Vergrößern virtueller Thin-Festplatten</a> .

### Nächste Schritte

Weitere Informationen erhalten Sie in dem folgenden Video.



Verwenden des Datenspeicherbrowsers im vSphere Web Client

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_huoxztz17/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_huoxztz17/uiConfId/49694343/))



## Hochladen von Dateien in Datenspeicher

Verwenden Sie den Datenspeicher-Datei-Browser zum Hochladen von Dateien in Datenspeicher, auf die ESXi-Hosts zugreifen können.


Zusätzlich zur herkömmlichen Verwendung als Speicher für VM-Dateien können zu virtuellen Maschinen gehörende Daten oder Dateien in Datenspeichern gespeichert werden. Beispiel: Sie können ISO-Images von Betriebssystemen von einem lokalen Computer in einen Datenspeicher auf dem Host hochladen. Anschließend können Sie diese Images zum Installieren von Gastbetriebssystemen auf den neuen virtuellen Maschinen verwenden.

---



**Hinweis** Sie können keine Dateien direkt in die Virtual Volumes-Datenspeicher hochladen. Sie müssen zuerst einen Ordner im Virtual Volumes-Datenspeicher erstellen und dann die Dateien in den Ordner hochladen. Die erstellten Ordner in Virtual Volume-Datenspeichern für Blockspeicher haben eine begrenzte Speicherkapazität von 4 GB. vVols-Datenspeicher unterstützen direktes Hochladen von Ordnern.

---

### Voraussetzungen

- Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**
- Zeigen Sie auf das Symbol  und prüfen Sie die Bezeichnung. Wenn die Bezeichnung „Client-Integrations-Plug-In installieren“ angezeigt wird, müssen Sie das Plug-In installieren, um Dateien hochladen zu können. Klicken Sie auf das Symbol und befolgen Sie die Anweisungen. Nach der Installation ändert sich die Bezeichnung in „Eine Datei auf den Datenspeicher hochladen“.

### Verfahren

- 1 Öffnen Sie den Datenspeicherbrowser.
  - a Zeigen Sie den Datenspeicher in der Bestandsliste an.
  - b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**  aus.
- 2 (Optional) Erstellen Sie einen Ordner zum Speichern der Datei.
- 3 Wählen Sie den Zielordner aus und klicken Sie auf das Symbol **Eine Datei auf den Datenspeicher aktualisieren** .
- 4 Suchen Sie das Element zum Hochladen auf dem lokalen Computer und klicken Sie auf **Öffnen**.
- 5 Aktualisieren Sie den Dateibrowser des Datenspeichers, damit die hochgeladene Datei in der Liste angezeigt wird.

### Nächste Schritte

Möglicherweise treten Probleme auf, wenn Sie eine OVF-Vorlage bereitstellen, die Sie zuvor exportiert und dann in einen Datenspeicher hochgeladen haben. Einzelheiten dazu und eine Problemumgehung finden Sie im VMware-Knowledgebase-Artikel [2117310](#).

## Kopieren von Datenspeicherordnern oder -dateien

Verwenden Sie den Datenspeicherbrowser zum Kopieren von Ordnern oder Dateien an einen neuen Speicherort auf demselben oder einem anderen Datenspeicher.

Virtuelle Festplattendateien werden ohne Formatkonvertierung verschoben oder kopiert. Wenn Sie eine virtuelle Festplatte in einen Datenspeicher verschieben, der zu einem anderen Host als dem Quellhost gehört, müssen Sie die virtuelle Festplatte möglicherweise konvertieren. Andernfalls können Sie die Festplatte möglicherweise nicht verwenden.

VM-Dateien können nicht zwischen vCenter Server-Systemen kopiert werden.

### Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

### Verfahren

- 1 Öffnen Sie den Datenspeicherbrowser.
  - a Zeigen Sie den Datenspeicher in der Bestandsliste an.
  - b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen** (🔍) aus.
- 2 Navigieren Sie zu einem Objekt, das Sie kopieren möchten (einem Ordner oder einer Datei).
- 3 Wählen Sie das Objekt aus, und klicken Sie auf das Symbol **Auswahl an eine andere Stelle kopieren**.
- 4 Geben Sie den Zielort an.
- 5 (Optional) Wählen Sie **Überschreiben von Dateien und Ordnern mit passenden Namen am Zielort** aus.
- 6 Klicken Sie auf **OK**.

## Verschieben von Datenspeicherordnern oder -dateien

Verschieben Sie Ordner oder Dateien mit dem Datenspeicherbrowser an einen neuen Speicherort im selben oder einem anderen Datenspeicher.

---

**Hinweis** Virtuelle Festplattendateien werden ohne Formatkonvertierung verschoben oder kopiert. Wenn Sie eine virtuelle Festplatte in einen Datenspeicher eines Hosttyps verschieben, der sich vom Quellhost unterscheidet, müssen u. U. die virtuellen Festplatten konvertiert werden, bevor Sie diese verwenden können.

---

### Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

## Verfahren

- 1 Öffnen Sie den Datenspeicherbrowser.
  - a Zeigen Sie den Datenspeicher in der Bestandsliste an.
  - b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen** (🔍) aus.
- 2 Gehen Sie zu einem Objekt, das Sie verschieben möchten, entweder ein Ordner oder eine Datei.
- 3 Wählen Sie das Objekt aus und klicken Sie auf das Symbol **Auswahl an eine andere Stelle verschieben**.
- 4 Geben Sie den Zielort an.
- 5 (Optional) Wählen Sie **Überschreiben von Dateien und Ordnern mit passenden Namen am Zielort** aus.
- 6 Klicken Sie auf **OK**.

## Umbenennen von Datenspeicherordnern oder -dateien

Verwenden Sie den Datenspeicherbrowser, um Ordner oder Dateien umzubenennen.

### Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

## Verfahren

- 1 Öffnen Sie den Datenspeicherbrowser.
  - a Zeigen Sie den Datenspeicher in der Bestandsliste an.
  - b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen** (🔍) aus.
- 2 Navigieren Sie zu einem Objekt, das Sie umbenennen möchten (einem Ordner oder einer Datei).
- 3 Wählen Sie das Objekt aus und klicken Sie auf das Symbol **Auswahl umbenennen**.
- 4 Geben Sie den neuen Namen an und klicken Sie auf **OK**.

## Vergrößern virtueller Thin-Festplatten

Wenn Sie eine virtuelle Festplatte im Format „Thin-Bereitstellung“ erstellt haben, können Sie die Thin-Festplatte in das Format „Thick-Provision“ konvertieren.


Sie können mit dem Datenspeicherbrowser die virtuelle Festplatte vergrößern.

### Voraussetzungen

- Stellen Sie sicher, dass der Datenspeicher, in dem sich die virtuelle Maschine befindet, über ausreichend Speicherplatz verfügt.

- Stellen Sie zudem sicher, dass die virtuelle Festplatte das Thin-Format aufweist.
- Entfernen Sie Snapshots.
- Schalten Sie die virtuelle Maschine aus.

### Verfahren

- 1 Wechseln Sie zu dem Ordner der virtuellen Festplatte, die Sie vergrößern möchten.
  - a Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
  - b Doppelklicken Sie auf die virtuelle Maschine zum Anzeigen ihrer Informationen.
  - c Klicken Sie auf der Registerkarte **Verwandte Objekte** und klicken Sie auf **Datenspeicher**.  
 Der Datenspeicher, in dem die Dateien der virtuellen Maschine gespeichert sind, wird angezeigt.
  - d Wählen Sie den Datenspeicher aus und klicken Sie auf das Symbol **Navigieren zum Datei-Browser des Datenspeichers**.  
 Der Datenspeicherbrowser zeigt den Inhalt des Datenspeichers an.
- 2 Öffnen Sie den Ordner der virtuellen Maschine und navigieren Sie zu der virtuellen Festplattendatei, die Sie konvertieren möchten.  
 Die Datei hat die Erweiterung `.vmdk` und ist durch das Symbol für virtuelle Festplatten () gekennzeichnet.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Festplattendatei und wählen Sie **Vergrößern**.

---

**Hinweis** Die Option ist möglicherweise nicht verfügbar, wenn die virtuelle Festplatte das Thick-Format aufweist oder wenn die virtuelle Maschine ausgeführt wird.

---

### Ergebnisse

Die vergrößerte virtuelle Festplatte belegt den ganzen Datenspeicherplatz, der ursprünglich für sie bereitgestellt wurde.

## Ausschalten von Speicherfiltern

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, verwendet vCenter Server Standardspeicherschutzfilter. Die Filter helfen Ihnen Speicherschäden zu vermeiden, indem nur die Speichergeräte abgerufen werden, die für einen bestimmten Vorgang verwendet werden können. Ungeeignete Geräte werden nicht zur Auswahl angezeigt. Sie können die Filter deaktivieren, um alle Geräte anzuzeigen.

### Voraussetzungen

Wenden Sie sich an den VMware-Support, bevor Sie die Gerätefilter ändern. Sie können die Filter nur dann deaktivieren, wenn Sie über andere Methoden zum Verhindern von Gerätebeschädigungen verfügen.

## Verfahren

- 1 Navigieren Sie zum vCenter Server im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Einstellungen** auf **Erweiterte Einstellungen** und dann auf **Bearbeiten**.
- 4 Geben Sie den Filter an, der deaktiviert werden soll.
  - a Geben Sie im Textfeld **Name** im unteren Bereich der Seite einen geeigneten Filternamen ein.

Name	Beschreibung
config.vpxd.filter.vmdsFilter	VMFS-Filter
config.vpxd.filter.rdmFilter	RDM-Filter
config.vpxd.filter.sameHostsAndTranportsFilter	Filter für dieselben Hosts und Transporte
config.vpxd.filter.hostRescanFilter	Filter für das erneute Prüfen eines Hosts
	<b>Hinweis</b> Wenn Sie diesen Filter deaktivieren, führen Ihre Hosts weiterhin eine erneute Prüfung durch, sobald Sie für einen Host oder Cluster eine neue LUN bereitstellen.

- b Geben Sie im Textfeld **Wert** für den angegebenen Schlüssel **False** ein.
  - 5 Klicken Sie auf **Hinzufügen** und dann auf **OK**, um Ihre Änderungen zu speichern.
- Es ist nicht erforderlich, dass Sie das vCenter Server-System neu starten.

## Speicherfilterung

vCenter Server stellt Speicherfilter zur Verfügung, um eine Beschädigung von Speichergeräten oder Beeinträchtigung der Leistung zu vermeiden, die durch eine nicht unterstützte Nutzung von Speichergeräten verursacht werden kann. Diese Filter sind standardmäßig verfügbar.

**Tabelle 16-4. Speicherfilter**

Filtername	Beschreibung
config.vpxd.filter.vmdsFilter (VMFS-Filter)	Filtert Speichergeräte oder LUNs heraus, die bereits von einem VMFS-Datenspeicher auf einem von vCenter Server verwalteten Host verwendet werden. Die LUNs werden nicht als Kandidaten angezeigt, die mit einem anderen VMFS-Datenspeicher formatiert oder als RDM verwendet werden sollen.
config.vpxd.filter.rdmFilter (RDM-Filter)	Filtert LUNs heraus, auf die bereits von einer RDM-Datei auf einem von vCenter Server verwalteten Host verwiesen wird. Die LUNs werden nicht als Kandidaten angezeigt, die mit VMFS formatiert oder von einer anderen RDM-Datei verwendet werden sollen.  Damit Ihre virtuellen Maschinen auf dieselbe LUN zugreifen können, müssen die virtuellen Maschinen dieselbe RDM-Zuordnungsdatei nutzen. Informationen über diesen Konfigurationstyp finden Sie in der Dokumentation <i>Handbuch zur vSphere-Ressourcenverwaltung</i> .

Tabelle 16-4. Speicherfilter (Fortsetzung)

Filtername	Beschreibung
config.vpxd.filter.sameHostsAndTransportFilter (Filter für dieselben Hosts und Transporte)	<p>Filtert LUNs heraus, die aufgrund einer Inkompatibilität des Hosts oder des Speichertyps nicht zur Verwendung als VMFS-Datenspeichererweiterungen geeignet sind. Verhindert, dass Sie die folgenden LUNs als Erweiterungen hinzufügen:</p> <ul style="list-style-type: none"> <li>■ LUNs, die nicht für alle Hosts verfügbar gemacht werden, die den ursprünglichen VMFS-Datenspeicher gemeinsam nutzen.</li> <li>■ LUNs, die einen Speichertyp nutzen, der von demjenigen abweicht, den der ursprüngliche VMFS-Datenspeicher verwendet. Sie können beispielsweise keine Fibre Channel-Erweiterung zu einem VMFS-Datenspeicher auf einem lokalen Speichergerät hinzufügen.</li> </ul>
config.vpxd.filter.hostRescanFilter (Filter für das erneute Prüfen eines Hosts)	<p>Führt eine automatische erneute Prüfung und Aktualisierung von VMFS-Datenspeichern durch, nachdem Sie Vorgänge zur Verwaltung von Datenspeichern durchgeführt haben. Der Filter hilft bei der Bereitstellung einer einheitlichen Ansicht aller VMFS-Datenspeicher auf allen von vCenter Server verwalteten Hosts.</p> <p><b>Hinweis</b> Wenn Sie eine neue LUN für einen Host oder Cluster bereitstellen, führt der Host automatisch eine erneute Prüfung durch, unabhängig davon, ob der Filter zum erneuten Prüfen des Hosts aktiviert oder deaktiviert ist.</p>

## Dynamische Festplattenspiegelung einrichten

Mit dem logischen Volume-Manager der virtuellen Maschine ist die Spiegelung virtueller Festplatten normalerweise nicht möglich. Wenn Ihre virtuellen Microsoft Windows-Maschinen jedoch Unterstützung für dynamische Festplatten bieten, können Sie die virtuelle Maschinen vor einem ungeplanten Speichergeräteverlust schützen, indem Sie virtuelle Festplatten in zwei SAN-LUNs spiegeln.

### Voraussetzungen

- Verwenden Sie eine virtuelle Windows-Maschine, die dynamische Festplatten unterstützt.
- Erforderliche Berechtigung: **Erweitert**

### Verfahren

- 1 Erstellen Sie eine virtuelle Maschine mit zwei virtuellen Festplatten.  
Achten Sie darauf, die Festplatten in verschiedenen Datenspeichern zu platzieren.
- 2 Melden Sie sich an Ihre virtuelle Maschine an und konfigurieren Sie die Festplatten als dynamisch gespiegelte Festplatten.  
Weitere Informationen finden Sie in der Microsoft-Dokumentation.
- 3 Schalten Sie die virtuelle Maschine nach der Synchronisierung der Festplatten aus.

- 4 Ändern Sie die Einstellungen für die virtuelle Maschine, um die Verwendung der dynamischen Festplattenspiegelung zuzulassen.
  - a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
  - b Klicken Sie auf die Registerkarte **VM-Optionen**, und erweitern Sie das Menü **Erweitert**.
  - c Klicken Sie auf **Konfiguration bearbeiten** neben den Konfigurationsparametern.
  - d Klicken Sie auf **Zeile hinzufügen** und fügen Sie folgende Parameter hinzu:

Name	Wert
scsi#.returnNoConnectDuringAPD	Wahr
scsi#.returnBusyOnNoConnectStatus	Falsch

- e Klicken Sie auf **OK**.

## Erfassen von Diagnoseinformationen für ESXi-Hosts auf einem Speichergerät

Während eines Hostfehlers muss ESXi in der Lage sein, Diagnoseinformationen an einem vorkonfigurierten Speicherort zur Diagnose und für technischen Support zu speichern.

In der Regel wird eine Partition zum Erfassen von Diagnoseinformationen, auch als VMkernel-Core-Dump bezeichnet, auf einem lokalen Speichergerät während der ESXi-Installation erstellt. Sie können dieses Standardverhalten außer Kraft setzen, wenn Sie z. B. gemeinsam genutzte Speichergeräte anstelle von lokalem Speicher verwenden. Um das automatische Formatieren lokaler Geräte zu verhindern, trennen Sie die Geräte vom Host, bevor Sie ESXi installieren und den Host zum ersten Mal einschalten. Später können Sie einen Speicherort für die Erfassung von Diagnoseinformationen auf einem lokalen oder Remotespeichergerät einrichten.

Wenn Sie Speichergeräte verwenden, können Sie unter zwei Optionen zum Einrichten der Core-Dump-Erfassung wählen. Sie können eine vorkonfigurierte Diagnosepartition auf einem Speichergerät oder eine Datei in einem VMFS-Datenspeicher verwenden.

### ■ Einrichten einer Gerätepartition als Core-Dump-Speicherort

Erstellen Sie eine Diagnosepartition für Ihren ESXi-Host.

### ■ Einrichten einer Datei als Core-Dump-Speicherort

Wenn Ihre verfügbare Core-Dump-Partition nicht groß genug ist, können Sie ESXi zum Generieren des Core-Dumps als Datei konfigurieren.

## Einrichten einer Gerätepartition als Core-Dump-Speicherort

Erstellen Sie eine Diagnosepartition für Ihren ESXi-Host.

Beim Erstellen einer Diagnosepartition gelten die folgenden Gesichtspunkte:

- Sie können keine Diagnosepartition auf einer iSCSI-LUN erstellen, auf die über den Software-iSCSI- oder abhängigen Hardware-iSCSI-Adapter zugegriffen wird. Weitere Informationen zu Diagnosepartitionen mit iSCSI finden Sie unter [Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN](#).
- Sie können keine Diagnosepartition auf einer Software-FCoE-LUN erstellen.
- Sofern Sie keine festplattenlosen Server einsetzen, richten Sie eine Diagnose-Partition auf einem lokalen Speicher ein.
- Für jeden Host ist eine Diagnosepartition mit 2,5 GB erforderlich. Wenn mehrere Hosts eine Diagnosepartition auf einer SAN-LUN gemeinsam nutzen, sollte die Partition groß genug sein, um die Core-Dumps aller Hosts unterzubringen.
- Falls ein Host, der eine gemeinsame Diagnosepartition verwendet, ausfällt, starten Sie den Host neu und extrahieren Sie die Protokolldateien unmittelbar nach dem Ausfall. Andernfalls könnte der zweite Host, der ausfällt, bevor Sie die Diagnosedaten des ersten Hosts sammeln, nicht in der Lage sein, den Core-Dump zu speichern.

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie mit der rechten Maustaste auf den Host, und wählen Sie **Diagnosepartition hinzufügen** aus.

Wenn diese Option nicht angezeigt wird, ist auf dem Host bereits eine Diagnosepartition vorhanden.

- 3 Legen Sie den Diagnosepartitionstyp fest.

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

- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie das Gerät, das Sie für die Diagnosepartition verwenden möchten, und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Konfigurationsinformationen für die Partition, und klicken Sie auf **Beenden**.



## Verifizieren einer Diagnosepartition

Verwenden Sie den Befehl `esxcli`, um sich zu vergewissern, dass die Diagnosepartition eingestellt ist.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- ◆ Listen Sie die Partitionen auf, um zu überprüfen, dass eine Diagnosepartition festgelegt ist.

```
esxcli --server=Servername system coredump partition list
```

### Ergebnisse

Wenn eine Diagnosepartition festgelegt ist, zeigt der Befehl Informationen über sie an. Sonst zeigt der Befehl, dass keine Partition aktiviert und konfiguriert ist.

### Nächste Schritte

Verwenden Sie die vCLI-Befehle zum Verwalten der Diagnosepartition des Hosts. Siehe *Konzepte und Beispiele zur vSphere Command-Line Interface*.

## Einrichten einer Datei als Core-Dump-Speicherort

Wenn Ihre verfügbare Core-Dump-Partition nicht groß genug ist, können Sie ESXi zum Generieren des Core-Dumps als Datei konfigurieren.

Typischerweise wird eine 2,5 GB große Core-Dump-Partition während der Installation von ESXi erstellt. Bei Upgrades von ESXi 5.0 oder früheren Versionen aus ist die Core-Dump-Partition auf 100 MB beschränkt. Bei dieser Art von Upgrades erstellt das System möglicherweise während des Startvorgangs eine Core-Dump-Datei auf einem VMFS-Datenspeicher. Wenn keine Core-Dump-Datei erstellt wird, können Sie diese manuell erstellen.

---

**Hinweis** Software-iSCSI und Software-FCoE werden für Speicherorte von Core-Dump-Dateien nicht unterstützt.

---

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- 1 Erstellen Sie eine Core-Dump-Datei eines VMFS-Datenspeichers durch Ausführen des folgenden Befehls:

```
esxcli system coredump file add
```

Der Befehl verfügt über die folgenden Optionen, die jedoch nicht erforderlich sind und ausgelassen werden können:

Option	Beschreibung
<code>--datastore   -d</code> <i>Datenspeicher_UUID oder</i> <i>Datenspeichername</i>	Wenn Sie keine Angabe machen, wird ein Datenspeicher mit ausreichender Größe ausgewählt.
<code>--file   -f</code> <i>Dateiname</i>	Wenn Sie keine Angabe machen, wird ein eindeutiger Name für die Core-Dump-Datei ausgewählt.
<code>--size   -s</code> <i>Dateigröße_MB</i>	Wenn Sie keine Angabe machen, wird eine Datei mit einer Größe erstellt, die dem im Host vorhandenen Arbeitsspeicher entspricht.

- 2 Stellen Sie sicher, dass die Datei erstellt wurde:

```
esxcli system coredump file list
```

Es wird eine Ausgabe ähnlich der folgenden angezeigt:

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	false	false	104857600

- 3 Aktivieren Sie die Core-Dump-Datei für den Host:

```
esxcli system coredump file set
```

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
<code>--path   -p</code>	Der Pfad der zu verwendenden Core-Dump-Datei. Dies muss eine vorab zugeteilte Datei sein.
<code>--smart   -s</code>	Dieses Flag kann nur zusammen mit <code>--enable   -e=true</code> verwendet werden. Es bewirkt, dass die Datei mithilfe des intelligenten Auswahlalgorithmus ausgewählt wird.  Beispiel:  <b>esxcli system coredump file set --smart --enable true</b>

- 4 Stellen Sie sicher, dass die Core-Dump-Datei aktiv und konfiguriert ist:

```
esxcli system coredump file list
```

Eine Ausgabe ähnlich der Folgenden zeigt an, dass die Core-Dump-Datei aktiv und konfiguriert ist:

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	True	True	104857600

### Nächste Schritte

Informationen zu anderen Befehlen, die Sie zum Verwalten der Core-Dump-Dateien verwenden können, finden Sie in der Dokumentation *Referenz zur vSphere Command-Line Interface*.

## Deaktivieren und Löschen einer Core-Dump-Datei

Deaktivieren Sie eine konfigurierte Core-Dump-Datei und entfernen Sie sie bei Bedarf aus dem VMFS-Datenspeicher.

Sie können die Core-Dump-Datei temporär deaktivieren. Wenn Sie nicht beabsichtigen, die deaktivierte Datei zu verwenden, können Sie sie aus dem VMFS-Datenspeicher entfernen. Zum Entfernen der nicht aktivierten Datei können Sie den Befehl `esxcli system coredump file remove` mit der Option `--force | -F` verwenden.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Deaktivieren Sie die Core-Dump-Datei durch Ausführen des folgenden Befehls:

```
esxcli system coredump file set --unconfigure | -u
```

- 2 Entfernen Sie die Datei aus dem VMFS-Datenspeicher:

```
esxcli system coredump file remove --file | -f file_name
```

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
<code>--file   -f</code>	Gibt den Dateinamen der zu entfernenden Dump-Datei an. Wenn Sie den Dateinamen nicht angeben, wird die konfigurierte Core-Dump-Datei entfernt.
<code>--force   -F</code>	Deaktiviert die zu entfernende Dump-Datei und hebt deren Konfiguration auf. Diese Option ist erforderlich, wenn die Datei nicht zuvor deaktiviert wurde und aktiv ist.

## Ergebnisse

Die Core-Dump-Datei wird deaktiviert und aus dem VMFS-Datenspeicher entfernt.

# Überprüfen der Metadatenkonsistenz mit VOMA

Verwenden Sie vSphere On-disk Metadata Analyser (VOMA), um Metadatenbeschädigungen zu identifizieren und zu beheben, die Dateisysteme oder zugrunde liegende logische Volumes beeinträchtigen.

## Problem

Möglicherweise müssen Sie die Metadatenkonsistenz eines Dateisystems oder eines logischen Volumes überprüfen, das das Dateisystem unterstützt, wenn Probleme mit verschiedenen Funktionen in einem VMFS-Datenspeicher oder einer vFlash-Ressource auftreten. Beispielsweise sollten Sie in folgenden Situationen eine Metadatenprüfung durchführen:

- Es treten Speicherausfälle auf.
- Nach einer erneuten RAID-Erstellung oder dem Ersetzen einer Festplatte.
- Die Datei `vmkernel.log` enthält Metadatenfehler.
- Sie können nicht auf Dateien auf einem VMFS zugreifen.
- Für einen Datenspeicher wird auf der Registerkarte „Ereignisse“ von vCenter Server eine Beschädigung gemeldet.

## Lösung

Führen Sie zum Überprüfen der Metadatenkonsistenz VOMA von der Befehlszeilenschnittstelle eines ESXi-Hosts aus. Mit VOMA können Probleme mit Metadateninkonsistenzen für einen VMFS-Datenspeicher oder eine vFlash-Ressource überprüft und behoben werden. Wenden Sie sich an den VMware-Support, wenn von VOMA gemeldete Fehler behoben werden sollen.

Folgen Sie diesen Anweisungen, wenn Sie das VOMA-Tool verwenden:

- Stellen Sie sicher, dass der VMFS-Datenspeicher, den Sie analysieren, sich nicht über mehrere Erweiterungen erstreckt. Sie können VOMA nur auf einen Datenspeicher mit einer Erweiterung anwenden.
- Schalten Sie alle ausgeführten virtuellen Maschinen aus oder migrieren Sie sie in einen anderen Datenspeicher.

Das folgende Beispiel veranschaulicht die Überprüfung der VMFS-Metadatenkonsistenz mithilfe von VOMA.

- 1 Ermitteln Sie den Namen und die Partitionsnummer des Geräts, das den zu überprüfenden VMFS-Datenspeicher stützt.

```
#esxcli storage vmfs extent list
```

Der Gerätenamen und die Partitionsspalten in der Ausgabe geben das Gerät an. Beispiel:

```
Volume Name  XXXXXXXX  Device Name  Partition
1TB_VMFS5   XXXXXXXX  naa.600508e000000000b367477b3be3d703  3
```

## 2 Führen Sie VOMA aus, um auf VMFS-Fehler zu prüfen.

Geben Sie den absoluten Pfad zur Gerätepartition an, die den VMFS-Datenspeicher stützt. Geben Sie zudem eine Partitionsnummer mit dem Gerätenamen an. Beispiel:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/
naa.600508e000000000b367477b3be3d703:3
```

In der Ausgabe werden mögliche Fehler aufgelistet. Beispielsweise deutet die folgende Ausgabe darauf hin, dass die Taktsignaladresse ungültig ist.

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
  ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.

Total Errors Found:          1
```

Für das VOMA-Tool gibt es die folgenden Befehlsoptionen.

**Tabelle 16-5. VOMA-Befehlsoptionen**

Befehlsoption	Beschreibung
<code>-m   --module</code>	<p>Das auszuführende Modul:</p> <ul style="list-style-type: none"> <li>■ <code>vmfs</code>. Dies ist die Standardoption. Sie können VMFS3- und VMFS5-Datenspeicher überprüfen. Wenn Sie dieses Modul angeben, werden zudem Minimalüberprüfungen für LVM durchgeführt.</li> <li>■ <code>vmfsl</code>. Überprüft Dateisysteme, die vFlash-Volumes unterstützen.</li> <li>■ <code>lvm</code>. Überprüft logische Volumes, die VMFS-Datenspeicher unterstützen.</li> </ul>
<code>-f   --func</code>	<p>Durchzuführende Funktionen:</p> <ul style="list-style-type: none"> <li>■ <code>query</code>. Listet die vom Modul unterstützten Funktionen auf.</li> <li>■ <code>check</code>. Sucht nach Fehlern.</li> <li>■ <code>fix</code>. Sucht und behebt Fehler.</li> </ul>
<code>-d --device</code>	<p>Zu inspizierendes Gerät bzw. zu inspizierende Festplatte. Stellen Sie sicher, dass Sie den absoluten Pfad zur Gerätepartition angeben, die den VMFS-Datenspeicher stützt. Zum Beispiel: <code>/vmfs/devices/disks/naa.00000000000000000000000000000000:1</code>.</p>
<code>-s   --logfile</code>	<p>Geben Sie die Protokolldatei zum Ausgeben der Ergebnisse an.</p>

Tabelle 16-5. VOMA-Befehlsoptionen (Fortsetzung)

Befehlsoption	Beschreibung
<code>-v   --version</code>	Zeigt die VOMA-Version an.
<code>-h   --help</code>	Zeigt einen Hilfetext zum VOMA-Befehl an.

## Konfigurieren des Cachespeichers für VMFS-Zeigerblöcke

Sie können erweiterte VMFS-Parameter verwenden, um den Zeigerblock-Cachespeicher zu konfigurieren.

Während die Größe der VM-Dateien im VMFS-Datenspeicher wächst, steigt auch die Anzahl der von diesen Dateien verwendeten Zeigerblöcke. Die Zeigerblöcke dienen dazu, Dateiblöcke in großen VM-Dateien und auf virtuellen Festplatten im VMFS-Datenspeicher zu adressieren.

Sie können die minimale und maximale Größe des Zeigerblock-Cachespeichers auf jedem ESXi-Host konfigurieren. Wenn sich die Größe des Zeigerblock-Cachespeichers der konfigurierten maximalen Größe nähert, entfernt ein Bereinigungsmechanismus einige Zeigerblockeinträge aus dem Cache.

Wählen Sie die maximale Größe des Zeigerblock-Cachespeichers basierend auf der Arbeitsgröße aller geöffneten virtuellen Festplattendateien in den VMFS-Datenspeichern aus. Alle VMFS-Datenspeicher auf dem Host verwenden einen einzigen Zeigerblock-Cachespeicher.

Der Mindestwert basiert auf dem garantierten Mindest-Arbeitsspeicher, der dem Cache vom System zugeteilt wird. 1 TB Speicherplatz für geöffnete Dateien erfordert etwa 4 MB Arbeitsspeicher.

Konfigurieren Sie die Mindest- und Höchstwerte für den Zeigerblock-Cachespeicher im Dialogfeld **Erweiterte Systemeinstellungen** des vSphere Web Client.

Tabelle 16-6. Erweiterte Parameter zum Anpassen des Zeigerblock-Cachespeichers

Parameter	Werte	Beschreibung
<code>VMFS3.MaxAddressableSpaceTB</code>	Der Standardwert ist 32 (in TB).	Von VMFS-Cache unterstützte maximale Größe aller geöffneten Dateien, bevor die Bereinigung startet.
<code>VMFS3.MinAddressableSpaceTB</code>	Der Standardwert ist 10 (in TB).	Von VMFS-Cache garantiert unterstützte minimale Größe aller geöffneten Dateien.

Mit dem Befehl `esxcli storage vmfs pbcache` können Sie Informationen über die Größe des Zeigerblock-Cachespeichers und andere Statistiken erhalten. Diese Informationen helfen Ihnen dabei, die minimale und maximale Größe des Zeigerblock-Cachespeichers anzupassen, um maximale Leistung zu erzielen.

## Festlegen von erweiterten Hostattributen

Sie können für einen Host erweiterte Hostattribute festlegen.

**Vorsicht** Das Ändern der erweiterten Optionen wird nicht unterstützt, es sei denn, der technische Support von VMware oder ein KB-Artikel weisen Sie an, dies zu tun. In allen anderen Fällen wird das Ändern dieser Optionen als nicht unterstützt betrachtet. In den meisten Fällen werden mit den Standardeinstellungen bereits beste Ergebnisse erzielt.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Einstellungen“ den entsprechenden Eintrag.
- 5 Klicken Sie auf **Bearbeiten**, um den Wert zu bearbeiten.
- 6 Klicken Sie auf **OK**.

## Abrufen von Informationen für den Cachespeicher für VMFS-Zeigerblöcke

Sie können Informationen über die Nutzung des Cachespeichers für VMFS-Zeigerblöcke abrufen. Dadurch erfahren Sie, wie viel Speicherplatz der Zeigerblock-Cachespeicher verbraucht. Zudem können Sie ermitteln, ob Sie die Mindest- oder Höchstgröße des Zeigerblock-Cachespeichers anpassen müssen.

In dem Vorgang wird der Zielserver durch `--server=Servername` angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Mit dem folgenden Befehl können Sie Statistiken zum Zeigerblock-Cachespeicher abrufen oder zurücksetzen:

```
esxcli storage vmfs pbcache
```

Option	Beschreibung
<b>get</b>	Ruft die Statistik des Cachespeichers für VMFS-Zeigerblöcke ab.
<b>Zurücksetzen</b>	Setzt die Statistik des Cachespeichers für VMFS-Zeigerblöcke zurück.

## Beispiel: Abrufen von Statistiken für den Zeigerblock-Cachespeicher

```
#esxcli storage vmfs pbcache get
Cache Capacity Miss Ratio: 0 %
Cache Size: 0 MiB
Cache Size Max: 132 MiB
Cache Usage: 0 %
Cache Working Set: 0 TiB
Cache Working Set Max: 32 TiB
Vmfs Heap Overhead: 0 KiB
Vmfs Heap Size: 23 MiB
Vmfs Heap Size Max: 256 MiB
```



# Grundlegendes zu Multipathing und Failover

# 17

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

Beim Ausfall eines beliebigen Elements im SAN-Netzwerk, z. B. eines Adapters, Switches oder Kabels, kann ESXi zu einem anderen physischen Pfad wechseln, der die Failover-Komponente nicht verwendet. Der Prozess des Wechsels zu einem anderen Pfad, um fehlgeschlagene Komponenten zu vermeiden, wird als Pfad-Failover bezeichnet.

Neben dem Pfad-Failover bietet Multipathing Lastenausgleich. Lastenausgleich ist der Vorgang zum Aufteilen der E/A-Lasten auf mehrere physische Pfade. Mit diesem Verfahren können potenzielle Engpässe reduziert oder vermieden werden.

---

**Hinweis** Während eines Failovers kann es bei virtuellen Maschinen zu einer E/A-Verzögerung von bis zu sechs Sekunden kommen. Diese Verzögerung ist erforderlich, damit nach einer Topologieänderung ein stabiler Zustand des SAN hergestellt werden kann. Die E/A-Verzögerungen sind möglicherweise auf Aktiv/Passiv-Arrays länger und auf Aktiv-Aktiv-Arrays kürzer.

---

Dieses Kapitel enthält die folgenden Themen:

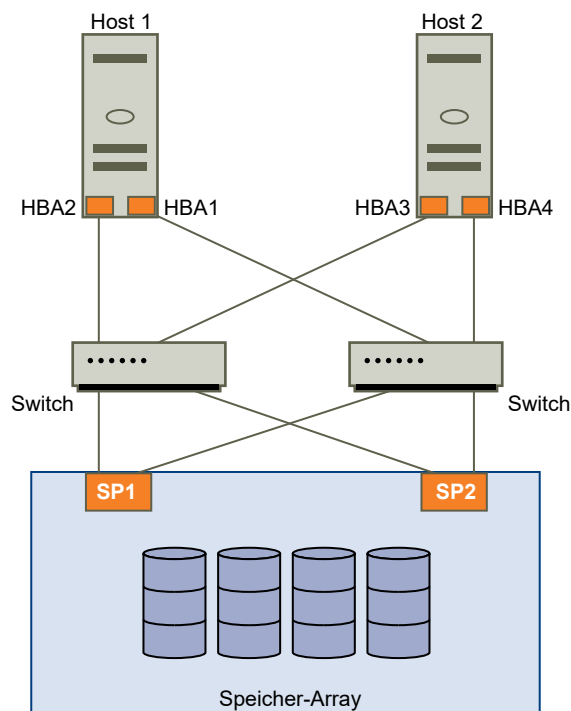
- Failover mit Fibre-Channel
- Hostbasiertes Failover mit iSCSI
- Array-basiertes Failover mit iSCSI
- Pfad-Failover und virtuelle Maschinen
- Verwalten mehrerer Pfade
- VMware Multipathing-Modul
- Prüfen und Beanspruchen von Pfaden
- Verwalten von Speicherpfaden und Multipathing-Plug-Ins
- Planungswarteschlangen für VM-E/A

## Failover mit Fibre-Channel

Zur Unterstützung von Multipathing verfügt Ihr Host normalerweise über zwei oder mehrere HBAs. Diese Konfiguration ergänzt die SAN-Multipathing-Konfiguration, die normalerweise mindestens einen Switch im SAN-Fabric und mindestens einen Speicherprozessor im Speicher-Array-Gerät selbst bereitstellt.

In der folgenden Abbildung wird dargestellt, wie jeder Server über mehrere physische Pfade mit dem Speichergerät verbunden ist. Wenn zum Beispiel HBA1 oder die Verbindung zwischen HBA1 und dem FC-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 17-1. Multipathing und Failover mit Fibre-Channel



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

## Hostbasiertes Failover mit iSCSI

Beim Einrichten Ihres ESXi-Hosts für das Multipathing und das Failover können Sie je nach Typ der iSCSI-Adapter auf Ihrem Host mehrere iSCSI-HBAs oder mehrere Netzwerkkarten verwenden.

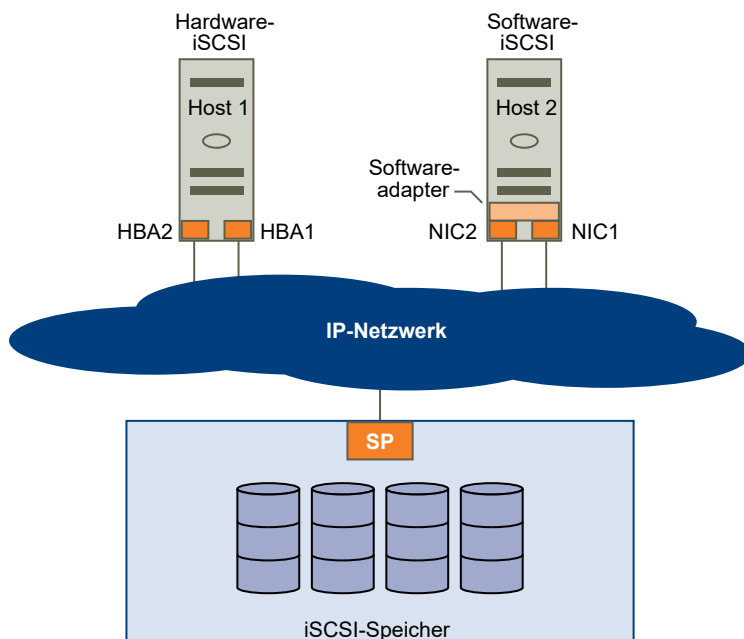
Weitere Informationen über verschiedene iSCSI-Adapertypen finden Sie unter [iSCSI-Initiatoren](#).

Bei der Verwendung von Multipathing muss Folgendes beachtet werden.

- ESXi unterstützt kein Multipathing, wenn Sie einen unabhängigen Hardwareadapter auf demselben Host mit Software-iSCSI- oder abhängigen iSCSI-Adaptoren kombinieren.
- Multipathing zwischen Software- und abhängigen Adaptoren auf demselben Host wird unterstützt.
- Sie können auf unterschiedlichen Hosts sowohl abhängige als auch unabhängige Adapter kombinieren.

Die folgende Abbildung zeigt Multipathing-Setups, die mit verschiedenen Typen von iSCSI-Initiatoren möglich sind.

**Abbildung 17-2. Hostbasiertes Pfad-Failover**



## Failover mit Hardware-iSCSI

Beim Hardware-iSCSI sind auf dem Host in der Regel mehrere Hardware-iSCSI-Adapter verfügbar, über die das Speichersystem mithilfe von einem oder mehreren Switches erreicht werden kann. Alternativ könnte das Setup auch einen Adapter und zwei Speicherprozessoren umfassen, sodass der Adapter einen anderen Pfad verwenden kann, um das Speichersystem zu erreichen.

In der Abbildung mit dem hostbasierten Pfad-Failover hat Host1 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 Mehrfachpfad-Plug-Ins den Pfad auf HBA2 wechseln.

## Failover mit Software-iSCSI

Mit Software-iSCSI können Sie, wie bei Host 2 der Abbildung „Hostbasiertes Pfad-Failover“ dargestellt, mehrere Netzwerkkarten verwenden, die Failover- und Lastausgleichsfunktionen für iSCSI-Verbindungen zwischen dem Host und Speichersystemen bieten.

Da Multipathing-Plug-Ins 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 Mehrfachpfad-Plug-Ins verwendet werden kann.

Informationen zur Konfiguration von Multipathing für das Software-iSCSI finden Sie unter [Einrichten des iSCSI-Netzwerks](#).

## Array-basiertes Failover mit iSCSI

Einige iSCSI-Speichersysteme verwalten die Pfadnutzung ihrer Ports automatisch und für ESXi transparent.

Wenn eines dieser Speichersysteme verwendet wird, erkennt der Host mehrere Ports im Speicher nicht und kann den Speicherport, mit dem er verbunden wird, nicht selbst wählen. Diese Systeme verfügen über eine einzelne virtuelle Portadresse, die der Host für die Anfangskommunikation nutzt. Während dieser Anfangskommunikation kann das Speichersystem den Host weiterleiten, sodass er mit einem anderen Port im Speichersystem kommuniziert. Die iSCSI-Initiatoren im Host befolgen diese Anforderung einer erneuten Verbindung und stellen dann eine Verbindung mit einem anderen Port im System her. Das Speichersystem nutzt diese Technik, um die Datenlast auf mehrere verfügbare Ports zu verteilen.

Falls der ESXi-Host die Verbindung zu einem dieser Ports verliert, versucht er automatisch, wieder eine Verbindung mit dem virtuellen Port des Speichersystems herzustellen und sollte an einen aktiven, nutzbaren Port weitergeleitet werden. Dieses Wiederverbinden und Umleiten erfolgt schnell und führt in der Regel nicht zu einer Unterbrechung bei der Ausführung der virtuellen Maschinen. Diese Speichersysteme können auch anfordern, dass iSCSI-Initiatoren wieder mit dem System verbunden werden, um den Speicherport zu ändern, mit dem sie verbunden sind. Dadurch wird eine möglichst effektive Nutzung mehrerer Ports gewährleistet.

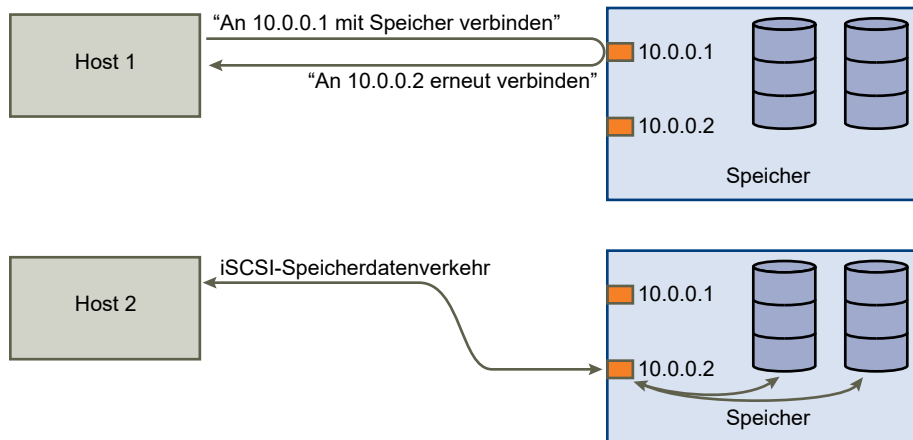
Die Abbildung „Portweiterleitung“ zeigt ein Beispiel für die Portweiterleitung. Der Host versucht, eine Verbindung zum virtuellen Port 10.0.0.1 herzustellen. Das Speichersystem leitet diese Anforderung an den Port 10.0.0.2 weiter. Der Host stellt eine Verbindung mit dem Port 10.0.0.2 her und verwendet diesen Port für die E/A-Kommunikation.

---

**Hinweis** Das Speichersystem leitet Verbindungen nicht immer weiter. Der Port 10.0.0.1 kann auch für Datenverkehr verwendet werden.

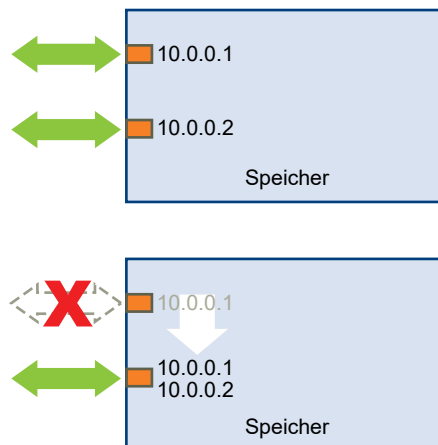
---

Abbildung 17-3. Portweiterleitung



Falls der Port im Speichersystem, der als virtueller Port fungiert, nicht mehr verfügbar ist, weist das Speichersystem die Adresse des virtuellen Ports einem anderen Port im System zu. Die Abbildung „Erneute Portzuweisung“ zeigt ein Beispiel für diese Art der erneuten Zuweisung von Ports. In diesem Fall ist der virtuelle Port 10.0.0.1 nicht mehr verfügbar, und das Speichersystem weist die IP-Adresse des virtuellen Ports einem anderen Port zu. Der zweite Port antwortet an beiden Adressen.

Abbildung 17-4. Erneute Portzuweisung



Bei dieser Art von Array-basiertem Failover sind nur dann mehrere Pfade zum Speicher möglich, wenn mehrere Ports im ESXi-Host verwendet werden. Dies sind Pfade vom Typ „Aktiv/Aktiv“. Weitere Informationen finden Sie unter [iSCSI-Sitzungsverwaltung](#).

## Pfad-Failover und virtuelle Maschinen

Das Pfad-Failover bezieht sich auf Situationen, in denen der aktive Pfad zu einer LUN in einen anderen Pfad geändert wird, üblicherweise weil eine SAN-Komponente ausgefallen ist, die den aktuellen Pfad verwendet.

Wenn ein Pfad ausfällt, wird Storage I/O für 30 bis 60 Sekunden angehalten, bis Ihr Host ermittelt hat, dass der Link nicht verfügbar ist, und das Failover abschließt. Beim Versuch, den Host, seine Speichergeräte oder seine Adapter anzuzeigen, hat es möglicherweise den Anschein, als sei der Vorgang angehalten worden. Es scheint, als ob virtuelle Maschinen mit ihren auf dem SAN installierten Festplatten nicht mehr reagieren. Nach dem Abschluss des Failovers wird die Ein-/Ausgabe normal fortgesetzt und die virtuellen Maschinen laufen wieder weiter.

Wenn Failover allerdings sehr lange benötigen, unterbricht eine virtuelle Windows-Maschine möglicherweise die Ein-/Ausgabe, was zu einem Ausfall führt. Um dies zu verhindern, legen Sie den Datenträger-Zeitüberschreitungswert für die virtuelle Windows-Maschine auf mindestens 60 Sekunden fest.

## Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen

Erhöhen Sie den standardmäßigen Zeitüberschreitungswert für Festplatten auf einem Windows-Gastbetriebssystem, um Unterbrechungen während eines Pfad-Failovers zu vermeiden.

Dieses Verfahren erläutert, wie der Zeitüberschreitungswert mithilfe der Windows-Registrierung geändert wird.

### Voraussetzungen

Sichern Sie die Windows-Registrierung.

### Verfahren

- 1 Wählen Sie **Start > Ausführen**.
- 2 Geben Sie **regedit.exe** ein und klicken Sie auf **OK**.
- 3 Doppelklicken Sie in der Hierarchieansicht auf der linken Seite auf **HKEY\_LOCAL\_MACHINE > System > CurrentControlSet > Services > Disk**.
- 4 Doppelklicken Sie auf **TimeoutValue**.
- 5 Setzen Sie den Datenwert auf 0x3c (hexadezimal) oder 60 (dezimal) und klicken Sie auf **OK**.

Nach dem Durchführen dieser Änderung wartet Windows mindestens 60 Sekunden darauf, dass die verzögerten Festplattenoperationen abgeschlossen werden, bevor ein Fehler generiert wird.

- 6 Starten Sie das Gastbetriebssystem neu, damit die Änderung wirksam wird.

## Verwalten mehrerer Pfade

Zur Verwaltung von Speicher-Multipathing verwendet ESXi eine Sammlung von Speicher-APIs, auch „Architektur des im Betrieb austauschbaren Speichers“ (Pluggable Storage Architecture, PSA) genannt. PSA stellt ein offenes, modulares Framework dar, das die gleichzeitige Ausführung von mehreren Multipathing-Plug-Ins (MPPs) koordiniert. Die Architektur des im Betrieb austauschbaren Speichers ermöglicht es Entwicklern, ihre eigenen Lastenausgleichstechniken und

Failover-Mechanismen für ein bestimmtes Speicher-Array zu entwerfen und den Code direkt in den ESXi-Speicher-E/A-Pfad einzufügen.

In den Themen zur Pfadverwaltung werden die folgenden Akronyme verwendet.

**Tabelle 17-1. Multipathing-Akronyme**

Akronym	Definition
PSA	Pluggable Storage Architecture (Architektur des im Betrieb austauschbaren Speichers)
NMP	Natives Multipathing-Plug-In. Allgemeines VMware-Multipathing-Modul.
PSP	Pfadauswahl-Plug-In, auch als Pfadauswahl-Richtlinie bezeichnet. Verarbeitet die Pfadauswahl für ein vorhandenes Gerät.
SATP	Speicher-Array-Typ-Plug-In, auch als Speicher-Array-Typ-Richtlinie bezeichnet. Verarbeitet Pfad-Failover für ein vorhandenes Speicher-Array.

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

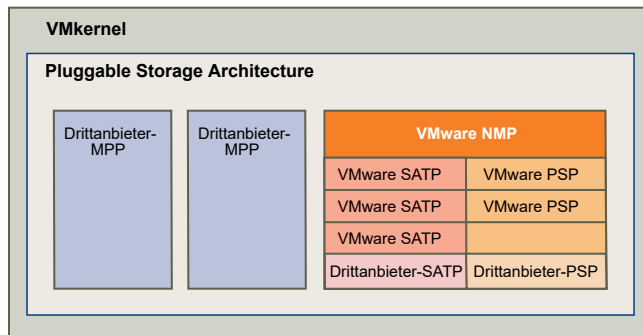
Wenn mehr Multipathing-Funktionen erforderlich sind, kann ein Drittanbieter MPP zusätzlich oder als Ersatz für das Standard-NMP bereitstellen.

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 in der Abbildung der Architektur des im Betrieb austauschbaren Speichers dargestellt, können mehrere Drittanbieter-MPPs parallel mit VMware NMP ausgeführt werden. Wenn sie installiert sind, ersetzen die Drittanbieter-MPPs das Verhalten des NMP und übernehmen die gesamte Steuerung des Pfad-Failovers und der Lastenausgleichs-Vorgänge für die angegebenen Speichergeräte.

**Abbildung 17-5. Pluggable Storage Architecture (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.
- Unterstützung der Erkennung und Behebung von nicht verfügbaren Pfaden.
- 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 Zurücksetzen von logischen Geräten.

## VMware Multipathing-Modul

Standardmäßig bietet ESXi ein erweiterbares Multipathing-Modul, das als NMP (Natives Multipathing-Plug-In) 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 Plug-In, PSP) verarbeitet. SATPs und PSPs sind Sub-Plug-Ins innerhalb des NMP-Moduls.

Mit ESXi wird automatisch das entsprechende SATP für ein von Ihnen verwendetes Array installiert. Sie müssen keine SATPs beschaffen oder herunterladen.

## VMware SATPs

Plug-Ins für Speicher-Array-Typen (SATPs) werden in Verbindung mit dem VMware NMP ausgeführt und übernehmen arrayspezifische Vorgänge.

ESXi bietet ein SATP für jeden von VMware unterstützten Array-Typ. Außerdem werden Standard-SATPs für nicht-spezifische Aktiv/Aktiv- und ALUA-Speicher-Arrays und das lokale SATP für direkt angeschlossene Geräte zur Verfügung gestellt. 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 selbst mit mehreren Speicher-Arrays arbeiten, ohne die Angaben zu den Speichergeräten zu kennen.

Nachdem das NMP ermittelt, welches SATP für ein bestimmtes Speichergerät verwendet 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 können für Aktiv/Passiv-Geräte passive Pfade aktiviert werden.

## VMware PSPs

Pfadauswahl-Plug-Ins (PSPs) sind Sub-Plug-Ins von VMware NMP und 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. Weitere Informationen hierzu finden Sie unter [Prüfen und Beanspruchen von Pfaden](#).

Standardmäßig unterstützt VMware NMP die folgenden PSPs:

### VMW\_PSP\_MRU

Der Host wählt den Pfad aus, den er zuletzt verwendet hat. 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 die meisten Aktiv/Passiv-Speichergeräte.

Aufgrund der Möglichkeit des VMW\_PSP\_MRU zur Einstufung können Sie einzelnen Pfaden Ränge zuweisen. Um den Rang einzelner Pfade festzulegen, verwenden Sie den Befehl `esxcli storage nmp psp generic pathconfig set`. Einzelheiten dazu finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2003468>.

Die Richtlinie wird im Client als Pfadauswahlrichtlinie „Zuletzt verwendet (VMware)“ angezeigt.

### VMW\_PSP\_FIXED

Der Host verwendet den festgelegten bevorzugten Pfad, falls dieser konfiguriert wurde. Anderenfalls wird der erste funktionierende Pfad ausgewählt, der beim Systemstart ermittelt wird. Wenn Sie möchten, dass der Host einen bestimmten bevorzugten Pfad verwendet, geben Sie diesen manuell an. Die Standardrichtlinie für die meisten Aktiv/Aktiv-Speichergeräte ist „Fest“.

---

**Hinweis** Wenn der Host einen bevorzugten Standardpfad verwendet und sich der Status des Pfads in „Ausgefallen“ ändert, wird ein neuer Pfad als bevorzugt ausgewählt. Wenn Sie den bevorzugten Pfad allerdings explizit auswählen, bleibt er auch dann bevorzugt, wenn auf ihn nicht zugegriffen werden kann.

---

Wird im Client als Pfadauswahlrichtlinie „Fest (VMware)“ angezeigt.

### VMW\_PSP\_RR

Der Host verwendet einen automatischen Pfadauswahlalgorithmus, bei dem beim Verbinden mit Aktiv/Passiv-Arrays eine Rotation unter Berücksichtigung aller aktiven Pfade bzw. aller verfügbaren Pfade stattfindet. „RR“ ist der Standardwert für mehrere Arrays. Dieser Wert kann mit Aktiv/Aktiv- und Aktiv/Passiv-Arrays verwendet werden, um den Lastausgleich zwischen Pfaden für verschiedene LUNs zu implementieren.

Wird im Client als Pfadauswahlrichtlinie „Round Robin (VMware)“ angezeigt.

## 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 Das NMP gibt die E/A-Anforderung auf dem vom PSP gewählten Pfad aus.
- 4 Wenn der E/A-Vorgang erfolgreich ist, meldet das NMP dessen Abschluss.
- 5 Wenn der E/A-Vorgang einen Fehler meldet, ruft das NMP das entsprechende SATP auf.
- 6 Das SATP interpretiert die E/A-Fehlercodes und aktiviert ggf. die inaktiven Pfade.
- 7 Das PSP wird aufgerufen, um einen neuen Pfad für das Senden der E/A zu wählen.

## 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. Der Host ermittelt auf Basis mehrerer Beanspruchungsregeln, welche Multipathing-Plug-Ins (MPP) die Pfade zu einem bestimmten Gerät beanspruchen sollten und somit für das Verwalten der Unterstützung von Multipathing für das Gerät verantwortlich sind.

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. Hierbei kann es sich um Drittanbieter-Multipathing-Plug-Ins oder das native Multipathing-Plug-In (NMP) handeln.

Für die durch das NMP-Modul verwalteten Pfade wird ein zweiter Satz von Beanspruchungsregeln angewendet. Diese Regeln legen fest, welches Speicher-Array-Typ-Plug-In (SATP) zum Verwalten der Pfade für einen bestimmten Array-Typ und welches Pfadauswahl-Plug-In (PSP) für die einzelnen Speichergeräte verwendet werden sollen.

Verwenden Sie den vSphere Web 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 Clients ändern. Zum Ändern des Standard-SATPs müssen Sie die Beanspruchungsregeln unter Verwendung der vSphere-CLI ändern.

Informationen zum Ändern von Beanspruchungsregeln finden Sie unter [Verwalten von Speicherpfaden und Multipathing-Plug-Ins](#).

Weitere Informationen zu den verfügbaren Befehlen zum Verwalten von PSA finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

Eine vollständige Liste der Speicher-Arrays und der entsprechenden SATPs und PSPs finden Sie in der SAN-Array-Modellreferenz von *vSphere-Kompatibilitätshandbuch*.

## Anzeigen der Pfadinformationen

Sie können die Speicher-Array-Typ-Richtlinie (SATP) und die Pfadauswahlrichtlinie (PSP), die der ESXi-Host für ein spezifisches Gerät verwendet, sowie den Status aller verfügbaren Pfade für dieses Speichergerät überprüfen. 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, eine Liste von Pfaden und der Status jedes einzelnen Pfads. 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.

### Standby

Falls aktive Pfade ausfallen, kann der Pfad schnell betriebsbereit sein und für E/A verwendet werden.

### Deaktiviert

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

### Ausgefallen

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.

Für jeden Pfad können Sie auch dessen Namen anzeigen. Der Name enthält Parameter, die den Pfad beschreiben: Adapter-ID, Ziel-ID und Geräte-ID. In der Regel hat der Pfadname in etwa folgendes Format:

```
fc.adapterID-fc.targetID-naa.deviceID
```

---

**Hinweis** Wenn Sie den Hostprofileditor zum Bearbeiten von Pfaden verwenden, müssen Sie alle drei für einen Pfad erforderlichen Parameter angeben: Adapter-ID, Ziel-ID und Geräte-ID.

---

## Anzeigen von Datenspeicherpfaden

Überprüfen Sie die Pfade, die eine Verbindung zu Speichergeräten herstellen, auf denen Ihre Datenspeicher gesichert werden.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf den Datenspeicher zum Anzeigen seiner Daten.
- 3 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 4 Klicken Sie auf **Konnektivität und Mehrfachpfad**.
- 5 Wenn der Datenspeicher gemeinsam genutzt wird, wählen Sie einen Host aus, um die Mehrfachpfad-Details der zugehörigen Geräte anzuzeigen.

- Überprüfen Sie unter Mehrfachpfad-Details die Multipathing-Richtlinien und Pfade für das Speichergerät, auf dem Ihr Datenspeicher gesichert wird.

## Anzeigen von Speichergerätepfaden

Zeigen Sie an, welche Mehrfachpfad-Richtlinien der Host für ein bestimmtes Speichergerät verwendet, und ermitteln Sie den Status aller verfügbaren Pfade für dieses Speichergerät.

### Verfahren

- Navigieren Sie zum Host im Navigator von vSphere Web Client.
- Klicken Sie auf die Registerkarte **Konfigurieren**.
- Klicken Sie auf **Speichergeräte**.
- Wählen Sie das Speichergerät, dessen Pfade Sie ansehen möchten.
- Klicken Sie auf die Registerkarte **Eigenschaften** und sehen Sie sich die Details unter „Mehrfachpfad-Richtlinien“ an.
- Klicken Sie auf die Registerkarte **Pfad**, um alle für das Speichergerät verfügbaren Pfade anzuzeigen.

## Festlegen einer Pfadauswahl-Richtlinie

Für jedes Speichergerät legt der ESXi-Host die Pfadauswahlrichtlinie basierend auf den 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 den festgelegten bevorzugten Pfad, falls dieser konfiguriert wurde. Anderenfalls wird der erste funktionierende Pfad ausgewählt, der beim Systemstart ermittelt wird. Wenn Sie möchten, dass der Host einen bestimmten bevorzugten Pfad verwendet, geben Sie diesen manuell an. Die Standardrichtlinie für die meisten Aktiv/Aktiv-Speichergeräte ist „Fest“.

---

**Hinweis** Wenn der Host einen bevorzugten Standardpfad verwendet und sich der Status des Pfads in „Ausgefallen“ ändert, wird ein neuer Pfad als bevorzugt ausgewählt. Wenn Sie den bevorzugten Pfad allerdings explizit auswählen, bleibt er auch dann bevorzugt, wenn auf ihn nicht zugegriffen werden kann.

---

### Zuletzt verwendet (VMware)

Der Host wählt den Pfad aus, den er zuletzt verwendet hat. 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 die meisten Aktiv/Passiv-Speichergeräte.

### Round-Robin (VMware)

Der Host verwendet einen automatischen Pfadauswahlalgorithmus, bei dem beim Verbinden mit Aktiv/Passiv-Arrays eine Rotation unter Berücksichtigung aller aktiven Pfade bzw. aller verfügbaren Pfade stattfindet. „RR“ ist der Standardwert für mehrere Arrays. Dieser Wert kann mit Aktiv/Aktiv- und Aktiv/Passiv-Arrays verwendet werden, um den Lastausgleich zwischen Pfaden für verschiedene LUNs zu implementieren.

## 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 **Mehrfachpfad-Richtlinien bearbeiten** eine Pfadauswahl-Richtlinie ändern und den bevorzugten Pfad für die Richtlinie „Fest“ angeben. Sie können in diesem Dialogfeld auch Multipathing für SCSI-basierte Protokollendpunkte ändern.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speichergeräte** oder **Protokollendpunkte**.
- 4 Wählen Sie das Element aus, dessen Pfade Sie ändern möchten, und klicken Sie auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie unter „Mehrfachpfad-Richtlinien“ auf **Mehrfachpfad bearbeiten**.
- 6 Wählen Sie eine Pfadrichtlinie 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)

- 7 Legen Sie für die feste Richtlinie den bevorzugten Pfad fest.
- 8 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

## Deaktivieren von Speicherpfaden

Pfade können zu Wartungszwecken oder aus anderen Gründen vorübergehend deaktiviert werden.

Sie deaktivieren einen Pfad mithilfe des Bereichs „Pfade“. Es gibt mehrere Methoden, um auf den Bereich „Pfade“ zuzugreifen: über einen Datenspeicher, ein Speichergerät oder eine Adapteransicht. Diese Aufgabe erklärt, wie Sie einen Pfad mithilfe der Ansicht für ein Speichergerät deaktivieren.

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Speichergeräte**.
- 4 Wählen Sie das Speichergerät aus, dessen Pfade Sie deaktivieren möchten, und klicken Sie auf die Registerkarte **Pfade**.
- 5 Wählen Sie den Pfad aus, der deaktiviert werden soll, und klicken Sie auf **Deaktivieren**.

## Verwalten von Speicherpfaden und Multipathing-Plug-Ins

Verwenden Sie die `esxcli`-Befehle, um die PSA-Multipathing-Plug-Ins und die ihnen zugewiesenen Speicherpfade zu verwalten.

Sie können alle auf Ihrem Host verfügbaren Multipathing-Plug-Ins anzeigen. Sie können alle Drittanbieter-MPPs sowie die NMP und SATPs Ihres Hosts auflisten und die Pfade überprüfen, die sie beanspruchen. Sie können ebenfalls neue Pfade festlegen und angeben, welches Multipathing-Plug-In die Pfade beansprucht.

Informationen zu weiteren Befehlen für die PSA-Verwaltung finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

## Überlegungen zu Multipathing

Beim Verwalten von Speicher-Multipathing-Plug-Ins und -Beanspruchungsregeln muss Folgendes beachtet werden.

Beachten Sie im Umgang mit Multipathing die folgenden Überlegungen:

- Wenn dem Gerät anhand der Beanspruchungsregeln kein SATP zugewiesen ist, lautet das Standard-SATP für iSCSI- oder FC-Geräte `VMW_SATP_DEFAULT_AA`. Das Standard-PSP lautet `VMW_PSP_FIXED`.
- Wenn das System die SATP-Regeln zur Ermittlung eines SATP für ein angegebenes Gerät durchsucht, werden zuerst die Treiberregeln durchsucht. Ist die Suche dort nicht erfolgreich, werden die Hersteller- bzw. Modellregeln und anschließend die Übertragungsregeln durchsucht. Wird keine übereinstimmende Regel gefunden, wählt NMP ein Standard-SATP für das Gerät aus.

- Wenn VMW\_SATP\_ALUA einem bestimmten Speichergerät zugewiesen ist, dieses Gerät ALUA jedoch nicht erkennt, gibt es für dieses Gerät keine Übereinstimmung der Beanspruchungsregeln. Das Gerät wird vom Standard-SATP gemäß dem Übertragungstyp des Geräts beansprucht.
- Das Standard-PSP für alle von VMW\_SATP\_ALUA beanspruchten Geräte lautet VMW\_PSP\_MRU. Das VMW\_PSP\_MRU wählt wie vom VMW\_SATP\_ALUA angegeben einen aktiven/optimierten Pfad oder einen aktiven/nicht optimierten Pfad aus, falls kein aktiver/optimierter Pfad vorhanden ist. Dieser Pfad wird so lange verwendet, bis ein besserer Pfad verfügbar ist (MRU). Wenn das VMW\_PSP\_MRU derzeit einen aktiven/nicht optimierten Pfad verwendet und ein aktiver/optimierter Pfad verfügbar wird, wechselt das VMW\_PSP\_MRU vom aktuellen Pfad zum aktiven/optimierten Pfad,
- Während VMW\_PSP\_MRU normalerweise standardmäßig für ALUA-Arrays gewählt wird, müssen gewisse ALUA-Speicher-Arrays VMW\_PSP\_FIXED verwenden. Informationen dazu, ob Ihr Speicher-Array VMW\_PSP\_FIXED benötigt, finden Sie im *VMware-Kompatibilitätshandbuch* oder wenden Sie sich an Ihren Speicheranbieter. Wenn Sie VMW\_PSP\_FIXED mit ALUA-Arrays verwenden, wählt der ESXi-Host den optimalen Arbeitspfad aus und legt ihn als bevorzugten Standardpfad fest, es sei denn, Sie geben explizit einen bevorzugten Pfad an. Ist der vom Host ausgewählte Pfad nicht mehr verfügbar, wählt der Host einen alternativen verfügbaren Pfad aus. Wenn Sie den bevorzugten Pfad allerdings explizit auswählen, bleibt er ungeachtet dessen Status der bevorzugte Pfad.
- Die PSA-Beanspruchungsregel 101 maskiert standardmäßig Pseudo-Array-Geräte von Dell. Löschen Sie diese Regel nur, wenn die Maskierung dieser Geräte aufgehoben werden soll.

## Auflisten von Multipathing-Beanspruchungsregeln für den Host

Verwenden Sie den `esxcli`-Befehl, um die verfügbaren Multipathing-Beanspruchungsregeln aufzulisten.

Beanspruchungsregeln geben an, welches Multipathing-Plug-In, NMP oder Drittanbieter-MPP einen vorhandenen physischen Pfad verwaltet. Jede Beanspruchungsregel gibt einen Satz an Pfaden basierend auf folgenden Parametern an:

- Hersteller-/Modellzeichenfolgen
- Übertragung wie zum Beispiel SATA, IDE, Fibre-Channel usw.
- Adapter, Ziel- oder LUN-Speicherort
- Gerätetreiber, zum Beispiel Mega-RAID

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.



## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den Befehl `esxcli --server=Servername storage core claimrule list --claimrule-class=MP` aus, um die Multipathing-Beanspruchungsregeln aufzulisten.

## Beispiel: Beispielausgabe des Befehls „esxcli storage core claimrule list“

Rule	Class	Rule	Class	Type	Plugin	Matches
MP		0	runtime	transport	NMP	transport=usb
MP		1	runtime	transport	NMP	transport=sata
MP		2	runtime	transport	NMP	transport=ide
MP		3	runtime	transport	NMP	transport=block
MP		4	runtime	transport	NMP	transport=unknown
MP		101	runtime	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		101	file	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		200	runtime	vendor	MPP_1	vendor=NewVend model=*
MP		200	file	vendor	MPP_1	vendor=NewVend model=*
MP		201	runtime	location	MPP_2	adapter=vmhba41 channel=* target=* lun=*
MP		201	file	location	MPP_2	adapter=vmhba41 channel=* target=* lun=*
MP		202	runtime	driver	MPP_3	driver=megaraid
MP		202	file	driver	MPP_3	driver=megaraid
MP		65535	runtime	vendor	NMP	vendor=* model=*

Dieses Beispiel zeigt Folgendes an:

- Das NMP beansprucht alle mit den Speichergeräten verbundenen Pfade, die USB-, SATA-, IDE- und Block SCSI-Übertragung verwenden.
- Sie können mit dem Modul MASK\_PATH nicht genutzte Geräte vor dem Host verbergen. Standardmäßig maskiert die PSA-Beanspruchungsregel 101 Dell-Array-Pseudogeräte mit der Anbieterzeichenfolge „DELL“ und der Modellzeichenfolge „Universal Xport“.
- Das MPP\_1-Modul beansprucht alle mit einem beliebigen Modell des NewVend-Speicher-Arrays verbundenen Pfade.
- Das MPP\_3-Modul beansprucht die Pfade zu Speichergeräten, die vom Mega-RAID-Gerätetreiber gesteuert werden.
- Alle nicht in den vorherigen Regeln beschriebenen Pfade werden von NMP beansprucht.
- Die Spalte „Rule Class“ der Ausgabe beschreibt die Kategorie einer Beanspruchungsregel. Sie kann MP (Multipathing-Plug-In), Filter oder VAAI sein.

- Die Class-Spalte zeigt, welche Regeln definiert und welche geladen sind. Der Parameter `file` in der Class-Spalte gibt an, dass die Regel definiert ist. Der Parameter `runtime` gibt an, dass die Regel in Ihr System geladen wurde. Damit eine benutzerdefinierte Regel aktiv wird, müssen zwei Zeilen in der selben Regelnummer enthalten sein. Eine Zeile für die Regel mit dem Parameter `file` und eine Zeile mit `runtime`. Einige Regeln mit niedrigen Nummern verfügen lediglich über eine Zeile mit der Class-Spalte `runtime`. Dies sind vom System festgelegte Beanspruchungsregeln, die nicht geändert werden können.

## Anzeigen von Multipathing-Modulen

Verwenden Sie den `esxcli`-Befehl, um alle im System geladenen Multipathing-Module aufzulisten. Multipathing-Module verwalten physische Pfade, die Ihren Host mit Speicher verbinden.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um die Multipathing-Module aufzulisten:

```
esxcli --server=Servername storage core plugin list --plugin-class=MP
```

### Ergebnisse

Mit diesem Befehl wird in der Regel das NMP und, falls geladen, das Attribut „MASK\_PATH“ angezeigt. Wenn Drittanbieter-MPPs geladen wurden, werden diese ebenfalls aufgelistet.

## Anzeigen von SATPs für den Host

Verwenden Sie den `esxcli`-Befehl, um in das System geladene VMware NMP SATPs aufzulisten. Zeigen Sie Informationen über die SATPs an.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um VMware SATPs aufzulisten:

```
esxcli --server=Servername storage nmp satp list
```

## Ergebnisse

Für jedes SATP zeigt die Ausgabe Informationen zum Typ des Speicher-Arrays oder Systems, das dieses SATP unterstützt, sowie zum Standard-PSP für alle LUNs an, die dieses SATP verwenden.

Platzhalter (Plug-In nicht geladen) gibt in der Spalte „Beschreibung“ an, dass das SATP nicht geladen ist.

## Anzeigen von NMP-Speichergeräten

Verwenden Sie den `esxcli`-Befehl, um alle von VMware NMP gesteuerten Speichergeräte aufzulisten und mit diesen Geräten verbundene SATP- und PSP-Informationen anzuzeigen.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den folgenden Befehl aus, um alle Speichergeräte aufzulisten:

```
esxcli --server=Servername storage nmp device list
```

Verwenden Sie die Option `--device | -d=Geräte-ID`, um die Ausgabe dieses Befehls zu filtern, so dass ein einzelnes Gerät angezeigt wird.

## Hinzufügen von Multipathing-Beanspruchungsregeln

Verwenden Sie die `esxcli`-Befehle, um eine neue Multipathing-PSA-Beanspruchungsregel zum Satz an Beanspruchungsregeln im System hinzuzufügen. Zur Aktivierung der neuen Beanspruchungsregeln müssen Sie diese zunächst definieren und in Ihr System laden.

Sie fügen eine neue PSA-Beanspruchungsregel beispielsweise hinzu, wenn Sie ein neues MPP (Multipathing-Plug-In) laden und festlegen müssen, welche Pfade dieses Modul beanspruchen soll. Möglicherweise müssen Sie eine Beanspruchungsregel erstellen, wenn Sie neue Pfade hinzufügen, die von einem vorhandenen MPP beansprucht werden sollen.

**Vorsicht** Vermeiden Sie beim Erstellen von neuen Beanspruchungsregeln Situationen, in denen verschiedene physische Pfade zu derselben LUN von verschiedenen MPPs beansprucht werden. Wenn es sich bei einem MPP nicht um MASK\_PATH MPP handelt, ruft diese Konfiguration Leistungsprobleme hervor.

In dem Vorgang wird der Zielserver durch `--server=Servername` angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Führen Sie zum Definieren einer neuen Beanspruchungsregel den folgenden Befehl aus:

```
esxcli --server=Servername storage core claimrule add
```

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
<code>-A --adapter=&lt;str&gt;</code>	Gibt den Adapter der Pfade an, der für diesen Vorgang verwendet werden soll.
<code>-u --autoassign</code>	Das System weist automatisch eine Regel-ID zu.
<code>-C --channel=&lt;long&gt;</code>	Gibt den Kanal der Pfade an, der für diesen Vorgang verwendet werden soll.
<code>-c --claimrule-class=&lt;str&gt;</code>	Gibt die Beanspruchungsregel-Klasse an, die für diesen Vorgang verwendet werden soll. Gültige Werte sind: MP, Filter, VAAI.
<code>-d --device=&lt;str&gt;</code>	Gibt die Geräte-UID an, die für diesen Vorgang verwendet werden soll.
<code>-D --driver=&lt;str&gt;</code>	Gibt den Treiber der Pfade an, der für diesen Vorgang verwendet werden soll.
<code>-f --force</code>	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
<code>--if-unset=&lt;str&gt;</code>	Führen Sie diesen Befehl aus, falls diese erweiterte Benutzervariable nicht auf 1 festgelegt ist.
<code>-i --iqn=&lt;str&gt;</code>	Gibt den iSCSI-qualifizierten Namen für das Ziel an, der in diesem Vorgang verwendet werden soll.

Option	Beschreibung
<b>-L --lun=&lt;long&gt;</b>	Gibt die LUN der Pfade an, die für diesen Vorgang verwendet werden soll.
<b>-M --model=&lt;str&gt;</b>	Gibt das Modell der Pfade an, das für diesen Vorgang verwendet werden soll.
<b>-P --plugin=&lt;str&gt;</b>	Gibt an, welches PSA-Plug-In für diesen Vorgang verwendet werden soll. (Erforderlich)
<b>-r --rule=&lt;long&gt;</b>	Gibt die Regel-ID an, die für diesen Vorgang verwendet werden soll.
<b>-T --target=&lt;long&gt;</b>	Gibt das Ziel der Pfade an, das für diesen Vorgang verwendet werden soll.
<b>-R --transport=&lt;str&gt;</b>	Gibt den Transport der Pfade an, der für diesen Vorgang verwendet werden soll. Gültige Werte sind: block, fc, iscsi, iscsivendor, ide, sas, sata, usb, parallel, unknown.
<b>-t --type=&lt;str&gt;</b>	Gibt an, welcher Abgleichstyp für „claim/unclaim“ oder „claimrule“ verwendet wird. Gültige Werte sind: vendor, location, driver, transport, device, target. (Erforderlich)
<b>-V --vendor=&lt;str&gt;</b>	Gibt den Hersteller der Pfade an, der für diesen Vorgang verwendet werden soll.
<b>--wwnn=&lt;str&gt;</b>	Gibt die World Wide Node Number (WWNN) für das Ziel an, die in diesem Vorgang verwendet werden soll.
<b>--wwpn=&lt;str&gt;</b>	Gibt die World Wide Port Number für das Ziel an, die in diesem Vorgang verwendet werden soll.

- 2 Führen Sie zum Laden der neuen Beanspruchungsregel in Ihr System den folgenden Befehl aus:

```
esxcli --server=Servername storage core claimrule load
```

Dieser Befehl lädt alle neu erstellten Multipathing-Beanspruchungsregeln aus der Konfigurationsdatei Ihres Systems.

## Beispiel: Definieren von Multipathing-Beanspruchungsregeln

Im folgenden Beispiel fügen Sie Regel Nr. 500 hinzu und laden diese, um alle Pfade mit der NewMod-Modellzeichenfolge und der NewVend-Anbieterzeichenfolge für das NMP-Plug-In zu beanspruchen.

```
# esxcli --server=Servername storage core claimrule add -r 500 -t vendor -V  
NewVend -M NewMod -P NMP
```

```
# esxcli --server=Servername storage core claimrule load
```

Nachdem Sie den Befehl **esxcli --server=Servername storage core claimrule list** ausgeführt haben, erscheint die neue Beanspruchungsregel in der Liste.

**Hinweis** Die beiden Zeilen für die Beanspruchungsregel mit der Klasse `runtime` und der Klasse `file` geben an, dass die neue Beanspruchungsregel in das System geladen wurde und aktiv ist.

Rule	Class	Rule	Class	Type	Plugin	Matches
MP		0	runtime	transport	NMP	transport=usb
MP		1	runtime	transport	NMP	transport=sata
MP		2	runtime	transport	NMP	transport=ide
MP		3	runtime	transport	NMP	transport=block
MP		4	runtime	transport	NMP	transport=unknown
MP		101	runtime	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		101	file	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		500	runtime	vendor	NMP	vendor=NewVend model=NewMod
MP		500	file	vendor	NMP	vendor=NewVend model=NewMod

## Löschen von Multipathing-Beanspruchungsregeln

Mithilfe des `esxcli`-Befehls können Sie eine Multipathing-PSA-Beanspruchungsregel aus dem Beanspruchungsregelsatz auf dem System entfernen.

In dem Vorgang wird der Zielsystem durch **--server=Servername** angegeben. Der angegebene Zielsystem fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Führen Sie zum Löschen einer Beanspruchungsregel aus dem Satz von Beanspruchungsregeln den folgenden Befehl aus.

```
esxcli --server=Servername storage core claimrule remove
```

**Hinweis** Die PSA-Beanspruchungsregel 101 maskiert standardmäßig Pseudo-Array-Geräte von Dell. Löschen Sie diese Regel nur, wenn die Maskierung dieser Geräte aufgehoben werden soll.

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
<code>-c --claimrule-class=&lt;str&gt;</code>	Gibt die Beanspruchungsregel-Klasse an, die für diesen Vorgang verwendet werden soll (MP, Filter, VAAI).
<code>-P --plugin=&lt;str&gt;</code>	Gibt das Plug-In an, das für diesen Vorgang verwendet werden soll.
<code>-r --rule=&lt;long&gt;</code>	Gibt die Regel-ID an, die für diesen Vorgang verwendet werden soll.

Mit diesem Schritt wird die Beanspruchungsregel aus der Klasse „File“ entfernt.

- 2 Löschen Sie die Beanspruchungsregel aus dem System.

```
esxcli --server=Servername storage core claimrule load
```

Mit diesem Schritt wird die Beanspruchungsregel aus der Klasse „Runtime“ entfernt.

## Maskieren von Pfaden

Sie können verhindern, dass der Host auf Speichergeräte oder LUNs zugreift oder einzelne Pfade zu einer LUN verwendet. Verwenden Sie die `esxcli`-Befehle, um die Pfade zu maskieren. Beim Maskieren von Pfaden können Sie Beanspruchungsregeln erstellen, die das MASK\_PATH-Plug-In bestimmten Pfaden zuordnen.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Prüfen Sie, welche die nächste verfügbare Regel-ID ist:

```
esxcli --server=Servername storage core claimrule list
```

Die zur Maskierung von Pfaden verwendeten Beanspruchungsregeln sollten über Regel-IDs im Bereich 101-200 verfügen. Wenn der Befehl zeigt, dass die Regeln 101 und 102 bereits vorhanden sind, können Sie festlegen, dass der Regel die Nummer 103 hinzugefügt wird.

- 2 Weisen Sie das MASK\_PATH-Plug-In einem Pfad zu, indem Sie eine neue Beanspruchungsregel für das Plug-In erstellen.

```
esxcli --server=Servername storage core claimrule add -P MASK_PATH
```

- 3 Laden Sie die MASK\_PATH-Beanspruchungsregel in Ihr System.

```
esxcli --server=Servername storage core claimrule load
```

- 4 Prüfen Sie, ob die MASK\_PATH-Beanspruchungsregel ordnungsgemäß hinzugefügt wurde.

```
esxcli --server=Servername storage core claimrule list
```

- 5 Falls für den maskierten Pfad eine Beanspruchungsregel vorhanden ist, entfernen Sie die Regel.

```
esxcli --server=Servername storage core claiming unclaim
```

- 6 Führen Sie die Pfadbeanspruchungsregeln aus.

```
esxcli --server=Servername storage core claimrule run
```

## Ergebnisse

Nach dem Zuweisen des MASK\_PATH-Plug-Ins zu einem Pfad verliert der Pfadstatus an Bedeutung und wird nicht länger vom Host verwaltet. Befehle, die Informationen zum maskierten Pfad bereitstellen, zeigen den Pfadstatus als nicht verfügbar (dead) an.

## Beispiel: Maskieren einer LUN

Im vorliegenden Beispiel wird die LUN 20 auf den Zielen T1 und T2 maskiert, auf die über die Speicheradapter vmhba2 und vmhba3 zugegriffen wird.

```
1 #esxcli --server=server_name storage core claimrule list

2 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 109 -t location -A
  vmhba2 -C 0 -T 1 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 110 -t location -A
  vmhba3 -C 0 -T 1 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 111 -t location -A
  vmhba2 -C 0 -T 2 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 112 -t location -A
  vmhba3 -C 0 -T 2 -L 20

3 #esxcli --server=server_name storage core claimrule load

4 #esxcli --server=server_name storage core claimrule list

5 #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba2
  #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba3

6 #esxcli --server=server_name storage core claimrule run
```

## Aufheben der Maskierung von Pfaden

Falls es erforderlich ist, dass der Host Zugriff auf das maskierte Speichergerät erhält, müssen Sie die Maskierung der Pfade zu diesem Gerät aufheben.



In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

---

**Hinweis** Wenn Sie die Beanspruchung einer Geräteeigenschaft, zum Beispiel Geräte-ID, Anbieter oder Modell, aufheben, wird die Beanspruchung der Pfade durch das MASK\_PATH-Plug-in nicht aufgehoben. Das MASK\_PATH-Plug-in verfolgt nicht die Geräteeigenschaft der Pfade, die es beansprucht.

---

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Löschen Sie die Beanspruchungsregel „MASK\_PATH“.

```
esxcli --server=Servername storage core claimrule remove -r rule#
```

- 2 Stellen Sie sicher, dass die Beanspruchungsregel ordnungsgemäß gelöscht wurde.

```
esxcli --server=Servername storage core claimrule list
```

- 3 Laden Sie die Pfadbeanspruchungsregeln aus der Konfigurationsdatei neu in den VMkernel.

```
esxcli --server=Servername storage core claimrule load
```

- 4 Führen Sie den Befehl `esxcli --server=Servername storage core claiming unclaim` für jeden Pfad auf das maskierte Speichergerät aus.

Beispiel:

```
esxcli --server=Servername storage core claiming unclaim -t location -A  
vmhba0 -C 0 -T 0 -L 149
```

- 5 Führen Sie die Pfadbeanspruchungsregeln aus.

```
esxcli --server=Servername storage core claimrule run
```

### Ergebnisse

Ihr Host hat jetzt Zugriff auf das zuvor maskierte Speichergerät.

## Definieren von NMP SATP-Regeln

Die NMP SATP-Beanspruchungsregeln geben an, welches SATP ein bestimmtes Speichergerät verwalten soll. Normalerweise ist es nicht erforderlich, NMP SATP-Regeln zu ändern. Falls doch, verwenden Sie die `esxcli`-Befehle, um eine Regel zu der Liste der Beanspruchungsregeln für das angegebene SATP hinzuzufügen.

Beim Installieren eines Drittanbieter-SATP für ein bestimmtes Speicher-Array müssen Sie unter Umständen eine SATP-Regel erstellen.

In dem Vorgang wird der Zielservers durch **--server=Servername** angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Führen Sie zum Hinzufügen einer Beanspruchungsregel für ein bestimmtes SATP den Befehl **esxcli --server=Servername storage nmp satp rule add** aus. Der Befehl verfügt über die folgenden Optionen.

Option	Beschreibung
<b>-b --boot</b>	Dies ist eine Standard-Systemregel, die zur Startzeit hinzugefügt wird. Ändern Sie die Datei „esx.conf“ nicht und fügen Sie sie nicht zum Hostprofil hinzu.
<b>-c --claim-option=Zeichenfolge</b>	Legt die Zeichenfolge der Beanspruchungsoption beim Hinzufügen einer SATP-Beanspruchungsregel fest.
<b>-e --description=Zeichenfolge</b>	Legt die Beschreibung der Beanspruchungsregel beim Hinzufügen einer SATP-Beanspruchungsregel fest.
<b>-d --device=Zeichenfolge</b>	Legt das Gerät beim Hinzufügen von SATP-Beanspruchungsregeln fest. Gerätereignisse und Anbieter/Modell- sowie Treiberregeln schließen sich gegenseitig aus.
<b>-D --driver=Zeichenfolge</b>	Legt die Treiberzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Treiberregeln und Anbieter/Modell-Regeln schließen sich gegenseitig aus.
<b>-f --force</b>	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
<b>-h --help</b>	Zeigt die Hilfenmeldung an.
<b>-M --model=Zeichenfolge</b>	Legt die Modellzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.
<b>-o --option=Zeichenfolge</b>	Legt die Optionszeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest.
<b>-P --psp=Zeichenfolge</b>	Legt das Standard-PSP für die SATP-Beanspruchungsregel fest.
<b>-O --psp-option=Zeichenfolge</b>	Legt die PSP-Optionen für die SATP-Beanspruchungsregel fest.
<b>-s --satp=Zeichenfolge</b>	Das SATP, für das eine neue Regel hinzugefügt wird.

Option	Beschreibung
<b>-R --transport= <i>Zeichenfolge</i></b>	Legt die Zeichenfolge für den Beanspruchungs-Transporttyp beim Hinzufügen einer SATP-Beanspruchungsregel fest.
<b>-t --type= <i>Zeichenfolge</i></b>	Legt den Beanspruchungstyp beim Hinzufügen einer SATP-Beanspruchungsregel fest.
<b>-V --vendor= <i>Zeichenfolge</i></b>	Legt die Herstellerzeichenfolge beim Hinzufügen von SATP-Beanspruchungsregeln fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.

**Hinweis** Beim Durchsuchen der SATP-Regeln zur Ermittlung eines SATP für ein vorhandenes Gerät werden zunächst die Treiberregeln vom NMP durchsucht. Ist die Suche dort nicht erfolgreich, werden die Hersteller- bzw. Modellregeln und anschließend die Übertragungsregeln durchsucht. Werden immer noch keine Ergebnisse angezeigt, wählt NMP ein Standard-SATP für das Gerät aus.

2 Starten Sie Ihren Host neu.

### Beispiel: Definieren einer NMP SATP-Regel

Der folgende Beispielbefehl ordnet das VMW\_SATP\_INV-Plug-In zu, um Speicher-Arrays mit der Herstellerzeichenfolge NewVend und der Modellzeichenfolge NewMod zu verwalten.

```
# esxcli --server=server_name storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

Wenn Sie den Befehl **esxcli --server=Servername storage nmp satp list -s VMW\_SATP\_INV** ausführen, können Sie die neue Regel sehen, die zur Liste der VMW\_SATP\_INV-Regeln hinzugefügt wurde.

## Planungswarteschlangen für VM-E/A

vSphere bietet standardmäßig einen Mechanismus zur Erstellung von Planungswarteschlangen für jede VM-Datei. Jede Datei, etwa „.vmdk“, erhält eine eigene Bandbreitenkontrolle.

Dieser Mechanismus gewährleistet, dass jede E/A einer VM-Datei, wie etwa .vmdk, eine eigene Warteschlange erhält und nicht mit anderen Datei-E/A kollidiert.

Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren müssen, passen Sie den Parameter `VMkernel.Boot.isPerFileSchedModelActive` in den erweiterten Systemeinstellungen entsprechend an.

### Bearbeiten der Pro-Datei-E/A-Planung

Mit dem erweiterten Parameter `VMkernel.Boot.isPerFileSchedModelActive` wird der Pro-Datei-E/A-Planungsmechanismus gesteuert. Der Mechanismus ist standardmäßig aktiviert.

#### Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Web Client.

- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie unter „Erweiterte Systemeinstellungen“ den Parameter **VMkernel.Boot.isPerFileSchedModelActive** aus und klicken Sie auf das Symbol **Bearbeiten**.
- 5 Wählen Sie eine der folgenden Optionen aus:

- Zum Deaktivieren des Pro-Datei-Planungsmechanismus ändern Sie den Wert auf **Nein**.

---

**Hinweis** Nach dem Ausschalten des Pro-Datei-E/A-Planungsmodells kehrt Ihr Host wieder zu einem älteren Planungsmechanismus zurück, der eine einzelne E/A-Warteschlange verwendet. Der Host wendet die einzelne E/A-Warteschlange für jede virtuelle Maschine und jedes Speichergerätepaar an. Alle E/A-Vorgänge zwischen der virtuellen Maschine und ihren virtuellen Festplatten auf dem Speichergerät werden in diese Warteschlange verschoben. Folglich wirken sich E/A-Vorgänge verschiedener virtueller Festplatten möglicherweise auf E/A-Vorgänge der anderen virtuellen Festplatten bei der gemeinsamen Nutzung der Bandbreite aus und beeinflussen möglicherweise die jeweilige Leistungsfähigkeit.

---

- Zum Neuaktivieren des Pro-Datei-Planungsmechanismus ändern Sie den Wert auf **Ja**.

- 6 Starten Sie den Host neu, damit die Änderungen wirksam werden.

## Verwenden von esxcli-Befehlen zur Aktivierung bzw. Deaktivierung der E/A-Planung nach Datei

Mithilfe der esxcli-Befehle können Sie auf die E/A-Planungsfunktion umstellen. Diese Funktion ist standardmäßig aktiviert.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie die folgenden Befehle aus, um die E/A-Planung nach Datei zu aktivieren bzw. zu deaktivieren:

Option	Beschreibung
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE</code>	E/A-Planung nach Datei deaktivieren
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE</code>	E/A-Planung nach Datei aktivieren

# Raw-Gerätezuordnung

# 18

Die Raw-Gerätezuordnung bietet virtuellen Maschinen einen Mechanismus für den direkten Zugriff auf eine LUN im physischen Speichersubsystem.

Die folgenden Themen enthalten Informationen über RDMs und bieten Anleitungen zum Erstellen und Verwalten von RDMs.

Dieses Kapitel enthält die folgenden Themen:

- [Wissenswertes zur Raw-Gerätezuordnung](#)
- [Raw-Gerätezuordnungseigenschaften](#)
- [Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen](#)
- [Verwalten von Pfaden in zugeordneten LUNs](#)

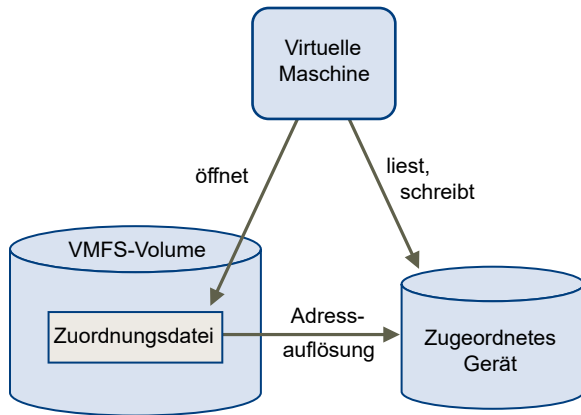
## Wissenswertes zur Raw-Gerätezuordnung

Eine Raw-Gerätezuordnung (RDM) ist eine Zuordnungsdatei in einem separaten VMFS-Volume, die als Proxy für ein physisches Speichergerät fungiert. Die RDM ermöglicht einer virtuellen Maschine den direkten Zugriff und die direkte Verwendung des Speichergeräts. 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 18-1. 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 virtuelle Festplatten auf einem freigegebenen VMFS.

Stellen Sie sich eine RDM als eine symbolische Verknüpfung zwischen einem VMFS-Volumen und einer Raw-LUN vor. Die Zuordnung zeigt die LUNs wie Dateien auf einem VMFS-Volumen 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 Web Client
- Verwenden von Dateisystemfunktionen wie verteilte Dateisperren, 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 Dateisperrung

Die Raw-Gerätezuordnung ermöglicht die Verwendung einer verteilten VMFS-Sperrung für Raw-SCSI-Geräte. Die verteilte Sperrung 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

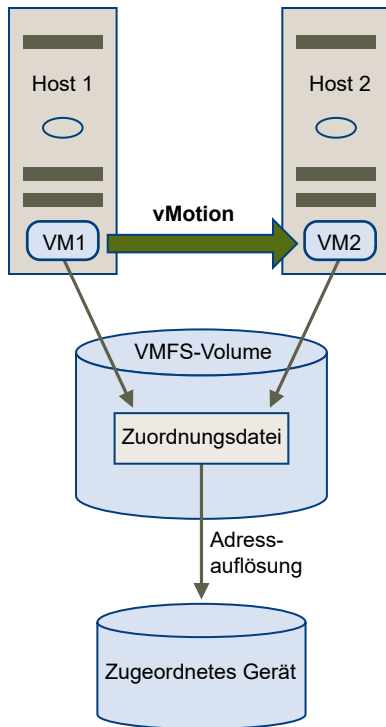
Die Raw-Gerätezuordnung ermöglicht die Verwendung von Snapshots virtueller Maschinen auf einem zugeordneten Volume. Snapshots stehen nicht zur Verfügung, wenn die Raw-Gerätezuordnung im Modus „Physische Kompatibilität“ verwendet wird.



## 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 18-2. 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 am besten zentral (nicht auf der ESXi-Maschine) ausgeführt, während andere problemlos 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 Anbieter der SAN-Verwaltungssoftware.

## RDM-Überlegungen und -Einschränkungen

Bei der Verwendung von Raw-Gerätezuordnungen gelten bestimmte Überlegungen und Einschränkungen.

- Die RDM steht für direkt verbundenen Blockgeräte oder gewisse RAID-Geräte nicht zur Verfügung. Die RDM verwendet eine SCSI-Seriennummer, um das zugeordnete Gerät zu identifizieren. Da Block- und bestimmte direkt angeschlossene RAID-Geräte Seriennummern nicht exportieren, können sie nicht in Raw-Gerätezuordnungen verwendet werden.
- Wenn Sie die RDM im physischen Kompatibilitätsmodus verwenden, können Sie keinen Snapshot mit der Festplatte verwenden. Im physischen Kompatibilitätsmodus kann die virtuelle Maschine eigene, speicherbasierte Snapshots oder Spiegelungsoperationen durchführen.

Snapshots virtueller Maschinen stehen für RDMs mit virtuellem Kompatibilitätsmodus zur Verfügung.

- Eine Festplattenpartition kann nicht zugeordnet werden. Für RDMs ist es erforderlich, dass das zugeordnete Gerät eine vollständige LUN ist.
- Wenn Sie vMotion zum Migrieren von virtuellen Maschinen mit RDMs verwenden, stellen Sie sicher, dass die LUN-IDs für RDMs auf allen teilnehmenden ESXi-Hosts konsistent bleiben.
- RDMs im physischen Kompatibilitätsmodus werden vom Flash-Lesecache nicht unterstützt. RDMs mit virtueller Kompatibilität werden vom Flash-Lesecache 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 sendet der VMkernel nur „Lesen“ und „Schreiben“ an das zugeordnete Gerät. Das Gastbetriebssystem erkennt 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 Dateispeicherung 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.

VMFS5 unterstützt Festplattengrößen von mehr als 2 TB für RDMs im virtuellen und physischen Modus. Sie können RDMs, die größer als 2 TB sind, nur in VMFS5-Datenspeicher verlagern.

## Dynamische Namensauflösung

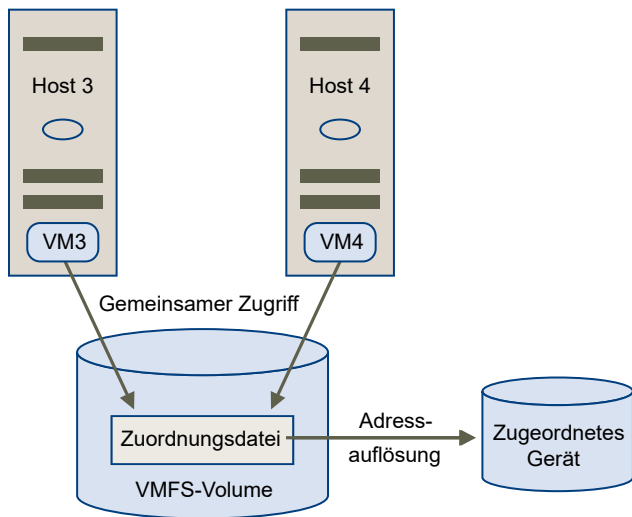
Die RDM-Datei unterstützt die dynamische Namensauflösung, wenn sich ein Pfad zu einem Raw-Device ändert.

Alle zugeordneten Speichergeräte werden durch VMFS eindeutig bezeichnet. Die Bezeichnung wird in den internen LUN-Datenstrukturen gespeichert. Alle Änderungen am Pfad zu einem Raw-Device, z. B. ein Fibre-Channel-Switchfehler oder das Hinzufügen eines neuen HBAs, können den Gerätenamen ändern. Die dynamische Namensauflösung löst diese Änderungen auf und verknüpft das ursprüngliche Gerät automatisch mit seinem neuen Namen.

## 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 18-3. 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 die folgende Tabelle einen Vergleich der Funktionen in den verschiedenen Modi.

Tabelle 18-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Gerätezuordnungen

ESXi-Funktionen	Virtuelle Festplattendatei	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

**Tabelle 18-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Gerätezuordnungen (Fortsetzung)**

ESXi-Funktionen	Virtuelle Festplattendatei	Raw-Gerätezuordnung – Virtueller Modus	Raw-Gerätezuordnung – Physischer Modus
Snapshots	Ja	Ja	Nein
Verteilte Sperrung	Ja	Ja	Ja
Clusterbildung	Nur systeminterne Cluster	Cluster-in-a-box Systemübergreifende Cluster	Physisch-zu-Virtuell-Clustering Systemübergreifende Cluster
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.

## Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen

Wenn Sie eine virtuelle Maschine mit einem Direktzugriff auf eine Raw-SAN-LUN versehen, erstellen Sie eine RDM-Festplatte, die sich in einem VMFS-Datenspeicher befindet und auf die LUN verweist. 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.

Wenngleich die RDM-Festplattendatei dieselbe `.vmdk`-Erweiterung wie eine herkömmliche virtuelle Festplattendatei hat, enthält die RDM nur Zuordnungsinformationen. Die eigentlichen virtuellen Festplattendaten werden direkt in der LUN gespeichert.

Bei diesem Verfahren wird vorausgesetzt, dass Sie eine neue virtuelle Maschine erstellen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

### Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datacenter, Ordner, Cluster, Ressourcenpool oder Host, und wählen Sie die Option **Neue virtuelle Maschine** aus.
- 2 Wählen Sie **Eine neue virtuelle Maschine erstellen** und klicken Sie auf **Weiter**.
- 3 Befolgen Sie sämtliche Anweisungen zum Erstellen einer virtuellen Maschine.
- 4 Klicken Sie auf der Seite „Hardware anpassen“ auf die Registerkarte **Virtuelle Hardware**.

- 5 (Optional) Um die virtuelle Standardfestplatte zu löschen, die vom System für ihre virtuelle Maschine erstellt wurde, bewegen Sie den Cursor über die Festplatte und klicken Sie auf das Symbol **Entfernen**.
- 6 Wählen Sie im Dropdown-Menü **Neu** unten auf der Seite die Option **RDM-Festplatte** aus und klicken Sie auf **Hinzufügen**.
- 7 Wählen Sie in der Liste der SAN-Geräte bzw. LUNs eine Raw-LUN aus, auf die die virtuelle Maschine direkt zugreifen soll, und klicken Sie auf **OK**.

Das System erstellt eine RDM-Festplatte, die Ihre virtuelle Maschine der Ziel-LUN zuordnet. Die RDM-Festplatte wird in der Liste der virtuellen Geräte als neue Festplatte angezeigt.

- 8 Klicken Sie auf das Dreieck **Neue Festplatte**, um die Eigenschaften für die RDM-Festplatte zu erweitern.
- 9 Wählen Sie einen Speicherort für die RDM-Festplatte aus.

Sie können die RDM im selben Datenspeicher ablegen, in dem sich die Konfigurationsdateien der virtuellen Maschine befinden, oder einen anderen Datenspeicher auswählen.

---

**Hinweis** Um vMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die RDM-Dateien und die Dateien der virtuellen Maschinen im selben Datenspeicher befinden. Sie können Storage vMotion nicht durchführen, wenn NPIV aktiviert ist.

---

- 10 Wählen Sie den Kompatibilitätsmodus aus.

Option	Beschreibung
<b>Physisch</b>	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.
<b>Virtuell</b>	Ermöglicht es der RDM, sich wie eine virtuelle Festplatte zu verhalten, sodass Sie Funktionen wie Snapshot-Erstellung, Klonen usw. verwenden können. Wenn Sie die Festplatte klonen oder eine Vorlage daraus erstellen, wird der Inhalt der LUN in eine virtuelle Festplattendatei <code>.vmdk</code> kopiert. Wenn Sie eine RDM im virtuellen Kompatibilitätsmodus migrieren, können Sie die Zuordnungsdatei migrieren oder den Inhalt der LUN in eine virtuelle Festplatte kopieren.

- 11 Wenn Sie den virtuellen Kompatibilitätsmodus ausgewählt haben, wählen Sie einen Festplattenmodus.

Festplattenmodi stehen für RDM-Festplatten mit physischem Kompatibilitätsmodus nicht zur Verfügung.

Option	Beschreibung
<b>Abhängig</b>	Abhängige Festplatten sind in Snapshots enthalten.
<b>Unabhängig – Dauerhaft</b>	Festplatten im dauerhaften Modus verhalten sich wie konventionelle Festplatten auf einem physischen Computer. Sämtliche Daten, die im dauerhaften Modus auf eine Festplatte geschrieben werden, werden permanent auf die Festplatte geschrieben.
<b>Unabhängig – Nicht dauerhaft</b>	Änderungen, die im nicht-dauerhaften Modus an Festplatten vorgenommen werden, werden beim Ausschalten oder Zurücksetzen der virtuellen Maschine verworfen. Der nicht-dauerhafte Modus sorgt dafür, dass sich die virtuelle Festplatte einer virtuellen Maschine bei jedem Neustart in demselben Zustand befindet. Änderungen an der Festplatte werden in eine Redo-Protokolldatei geschrieben und daraus gelesen. Diese Datei wird beim Ausschalten oder Zurücksetzen gelöscht.

- 12 Klicken Sie auf **OK**.

## Verwalten von Pfaden in zugeordneten LUNs

Wenn Sie virtuelle Maschinen mit RDMs verwenden, können Sie Pfade für zugeordnete Raw-LUNs verwalten.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Virtuelle Hardware** und dann auf **Festplatte**, um das Menü mit den Festplattenoptionen zu erweitern.
- 4 Klicken Sie auf **Pfade verwalten**.
- 5 Im Dialogfeld „Mehrfachpfad-Richtlinien bearbeiten“ 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 [Kapitel 17 Grundlegendes zu Multipathing und Failover](#).

Mit der Funktionalität für virtuelle Volumes wird bei der Speicherverwaltung nicht mehr der Speicherplatz innerhalb von Datenspeichern verwaltet, sondern es werden abstrakte, von Speicher-Arrays gehandhabte Speicherobjekte verwaltet. Mit virtuellen Volumes wird eine einzelne virtuelle Maschine anstelle des Datenspeichers zur Einheit für die Speicherverwaltung, und die Speicherhardware erhält vollständige Kontrolle über den Inhalt, das Layout und die Verwaltung virtueller Datenträger.

Früher wurde in der vSphere-Speicherverwaltung ein Ansatz verwendet, bei dem Datenspeicher im Mittelpunkt standen. Bei diesem Ansatz besprechen die Speicheradministratoren und die vSphere-Administratoren im Voraus die zugrunde liegenden Speicheranforderungen für virtuelle Maschinen. Der Speicheradministrator richtet dann LUNs oder NFS-Freigaben ein und stellt sie den ESXi-Hosts bereit. Der vSphere-Administrator erstellt Datenspeicher, die auf LUNs oder NFS basieren, und verwendet diese Datenspeicher als Speicher für virtuelle Maschinen. In der Regel ist aus der Speicherperspektive der Datenspeicher die niedrigste Granularitätsstufe, auf der die Datenverwaltung erfolgt. Ein einzelner Datenspeicher enthält jedoch mehrere virtuelle Maschinen, für die u. U. unterschiedliche Anforderungen gelten können. Mit dem traditionellen Ansatz ist eine Differenzierung auf der Ebene einzelner virtueller Maschinen schwierig.

Die Funktionalität der virtuellen Volumes trägt zur Verbesserung der Granularität bei und ermöglicht die Differenzierung von Diensten auf virtuellen Maschinen für einzelne Anwendungen. Sie bietet somit einen neuen Ansatz für die Speicherverwaltung. Anstatt den Speicher um Funktionen eines Speichersystems anzuordnen, wird der Speicher mit virtuellen Volumes entsprechend den Bedürfnissen einzelner virtueller Maschinen angeordnet, sodass im Mittelpunkt des Speichers die virtuellen Maschinen stehen.

Mit virtuellen Volumes werden virtuelle Datenträger und deren Derivate, Klone, Snapshots und Replikate direkt Objekten, den so genannten virtuellen Volumes, in einem Speichersystem zugewiesen. Mit dieser Zuordnung kann vSphere intensive Speichervorgänge wie Snapshots, Klonerstellung und Replikation an das Speichersystem übertragen.

Indem Sie ein Volume für jeden virtuellen Datenträger erstellen, können Sie Richtlinien auf der optimalen Ebene einrichten. Sie können im Voraus über die Speicheranforderungen einer Anwendung entscheiden und diese Anforderungen an das Speichersystem weitergeben. Dieses erstellt dann einen passenden virtuellen Datenträger, der auf diesen Anforderungen basiert.



Wenn Ihre virtuelle Maschine beispielsweise ein Aktiv-Aktiv-Speicherarray benötigt, ist es nicht mehr erforderlich, einen Datenspeicher auszuwählen, der das Aktiv-Aktiv-Modell unterstützt. Stattdessen erstellen Sie ein einzelnes virtuelles Volume, das automatisch in das Aktiv-Aktiv-Array platziert wird.

Dieses Kapitel enthält die folgenden Themen:

- [Konzepte zu Virtual Volumes](#)
- [Richtlinien bei der Verwendung von virtuellen Volumes](#)
- [Virtuelle Volumes und Speicherprotokolle](#)
- [Architektur von Virtual Volumes](#)
- [Virtuelle Volumes und VMware Certificate Authority](#)
- [Schritte vor der Aktivierung virtueller Volumes](#)
- [Konfigurieren virtueller Volumes](#)
- [Bereitstellen von virtuellen Maschinen auf virtuellen Datenspeichern](#)

## Konzepte zu Virtual Volumes

Mit Virtual Volumes ersetzen abstrakte Speichercontainer traditionelle Speichervolumes basierend auf LUNs oder NFS-Anteilen. In vCenter Server werden die Speichercontainer durch virtuelle Datenspeicher dargestellt. Virtuelle Datenspeicher heben künstliche Grenzen traditioneller Datenspeicher auf und werden zum Speichern von virtuellen Volumes verwendet. Hierbei handelt es sich um Objekte, die Dateien der virtuellen Maschine enthalten.

Weitere Informationen zu den verschiedenen Komponenten der Funktionalität für Virtual Volumes erhalten Sie im entsprechenden Video.



Virtual Volumes, Teil 1: Konzepte

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_jvj5idt3/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_jvj5idt3/uiConfId/49694343/))

- [Virtuelle Volumes](#)  
Virtuelle Volumes sind Verkapselungen der Dateien und virtuellen Festplatten von virtuellen Maschinen sowie deren Derivate.
- [Virtuelle Volumes und Speicheranbieter](#)  
Ein Speicheranbieter von virtuellen Volumes, auch VASA-Anbieter genannt, ist eine Softwarekomponente, die für vSphere die Aufgaben eines Storage-Awareness-Diensts übernimmt. Der Anbieter ermöglicht die Out-of-Band-Kommunikation zwischen vCenter Server und ESXi-Hosts auf einer Seite und einem Speichersystem auf der anderen.

## ■ Speichercontainer

Im Unterschied zu traditionellem LUN- und NFS-basiertem vSphere-Speicher sind für die Funktionalität virtueller Volumes keine vorkonfigurierten Volumes auf Speicherseite erforderlich. Stattdessen verwenden virtuelle Volumes einen Speichercontainer, d. h. einen Pool von Rohspeicherkapazität bzw. eine Zusammenfassung von Speicherfunktionen, die ein Speichersystem für virtuelle Volumes bereitstellen kann.

## ■ Protokollendpunkte

Obwohl Speichersysteme alle Aspekte von virtuellen Volumes verwalten, haben ESXi-Hosts keinen Direktzugriff auf virtuelle Volumes auf der Speicherseite. Stattdessen verwenden ESXi-Hosts einen logischen E/A-Proxy, den so genannten Protokollendpunkt, zum Kommunizieren mit virtuellen Volumes und virtuellen Festplattendateien, die virtuelle Volumes enthalten. ESXi verwendet Protokollendpunkte zum Einrichten eines Datenpfads auf Anforderung von virtuellen Maschinen zu ihren jeweiligen virtuellen Volumes.

## ■ Virtuelle Datenspeicher

Ein virtueller Datenspeicher stellt einen Speichercontainer in vCenter Server und im vSphere Web Client dar.

## ■ Virtuelle Volumes und VM-Speicherrichtlinien

Für eine virtuelle Maschine, die auf einem virtuellen Datenspeicher ausgeführt wird, ist eine VM-Speicherrichtlinie erforderlich.

# Virtuelle Volumes

Virtuelle Volumes sind Verkapselungen der Dateien und virtuellen Festplatten von virtuellen Maschinen sowie deren Derivate.

Virtuelle Volumes werden systemseitig in einem Speichersystem gespeichert, das über Ethernet oder SAN verbunden ist. Sie werden als Objekte von einem kompatiblen Speichersystem exportiert und vollständig von der Hardware auf Speicherseite verwaltet. In der Regel wird ein virtuelles Volume von einer eindeutigen GUID identifiziert. Virtuelle Volumes werden nicht im Voraus bereitgestellt, sondern automatisch erstellt, wenn Sie Verwaltungsvorgänge an virtuellen Maschinen durchführen. Zu diesen Vorgängen zählen die VM-Erstellung, das Klonen und das Erstellen von Snapshots. +ESXi und vCenter Server ordnen einen oder mehrere virtuelle Volumes einer virtuellen Maschine zu. Das System erstellt die folgenden Typen virtueller Volumes für die Kernelemente einer virtuellen Maschine:

- Ein virtuelles Daten-Volume, das direkt jeder `.vmdk`-Datei der virtuellen Festplatte entspricht. Wie virtuelle Festplattendateien in herkömmlichen Datenspeichern werden virtuelle Volumes den virtuellen Maschinen als SCSI-Festplatten angezeigt.
- Ein virtuelles Konfigurations-Volume bzw. Stammverzeichnis stellt ein kleines Verzeichnis mit Metadatendateien für eine virtuelle Maschine dar. Die Datei umfasst eine `.vmx`-Datei, Deskriptordateien für virtuelle Festplatten, Protokolldateien usw. Das virtuelle Konfigurations-

Volume wird mit einem Dateisystem formatiert. Wenn ESXi das SCSI-Protokoll für die Verbindung mit dem Speicher verwendet, werden virtuelle Konfigurations-Volumes mit VMFS konfiguriert. Beim NFS-Protokoll werden virtuelle Konfigurations-Volumes als NFS-Verzeichnis angezeigt.

Zusätzliche virtuelle Volumes können für andere Komponenten der virtuellen Maschinen und Derivate der virtuellen Festplatten erstellt werden, z. B. Klons, Snapshots und Replikate. Diese virtuellen Volumes umfassen ein virtuelles Swap-Volume für die Swap-Dateien der virtuellen Maschine und ein virtuelles Speicher-Volume für den Inhalt des Arbeitsspeichers der virtuellen Maschine für einen Snapshot.

Indem Sie unterschiedliche virtuelle Volumes für verschiedene VM-Komponenten verwenden, können Sie Speicherrichtlinien auf der feinsten Granularitätsstufe anwenden und handhaben. Beispiel: Ein virtuelles Volume, das eine virtuelle Festplatte enthält, kann mehr Datendienste und Leistungsstufen enthalten als das virtuelle Volume für das VM-Startlaufwerk. Ebenso kann ein virtuelles Snapshot-Volume eine andere Speicherebene als das aktuelle virtuelle Volume verwenden.

## Virtuelle Volumes und Speicheranbieter

Ein Speicheranbieter von virtuellen Volumes, auch VASA-Anbieter genannt, ist eine Softwarekomponente, die für vSphere die Aufgaben eines Storage-Awareness-Diensts übernimmt. Der Anbieter ermöglicht die Out-of-Band-Kommunikation zwischen vCenter Server und ESXi-Hosts auf einer Seite und einem Speichersystem auf der anderen.

Der Speicheranbieter wird über VMware APIs für Storage Awareness (VASA) implementiert und verwaltet alle Aspekte der Speicherung auf virtuellen Volumes. Bei der Kommunikation mit vCenter Server und ESXi-Hosts arbeitet er eng mit dem im Lieferumfang von vSphere enthaltenen Speicherüberwachungsdienst (Storage Monitoring Service, SMS) zusammen.

Der Speicheranbieter übermittelt Informationen aus dem zugrunde liegenden Speicher – bzw. Speichercontainer, im Falle von virtuellen Volumes –, sodass die Funktionen des Speichercontainers in vCenter Server und dem vSphere Web Client angezeigt werden. Anschließend übermittelt er die Speicheranforderungen der virtuellen Maschine, die Sie in Form einer Speicherrichtlinie definieren können, an die Speicherebene. Der Integrationsprozess stellt sicher, dass ein in der Speicherebene erstelltes virtuelles Volume die Anforderungen in der Richtlinie erfüllt.

Speicheranbieter, die in vSphere integriert werden können und virtuelle Volumes unterstützen, werden üblicherweise von externen Herstellern bezogen. Jeder Speicheranbieter muss von VMware zertifiziert sein und ordnungsgemäß bereitgestellt werden. Weitere Informationen zur Bereitstellung eines Speicheranbieters für virtuelle Volumes erhalten Sie von Ihrem Speicherhersteller.

Nach der Bereitstellung des Speicheranbieters müssen Sie ihn in vCenter Server registrieren, damit er über den SMS mit vSphere kommunizieren kann.

## Speichercontainer

Im Unterschied zu traditionellem LUN- und NFS-basiertem vSphere-Speicher sind für die Funktionalität virtueller Volumes keine vorkonfigurierten Volumes auf Speicherseite erforderlich. Stattdessen verwenden virtuelle Volumes einen Speichercontainer, d. h. einen Pool von Rohspeicherkapazität bzw. eine Zusammenfassung von Speicherfunktionen, die ein Speichersystem für virtuelle Volumes bereitstellen kann.

Ein Speichercontainer ist ein Teil der logischen Speicher-Fabric und eine logische Einheit der zugrunde liegenden Hardware. Der Speichercontainer gruppiert virtuelle Volumes logisch basierend auf den Verwaltungs- und Administratoranforderungen. Der Speichercontainer kann zum Beispiel alle virtuellen Volumes enthalten, die für einen Mandanten in einer Mehrmandantenbereitstellung oder eine Abteilung in einer Unternehmensbereitstellung erstellt wurden. Jeder Speichercontainer dient als Speicher für virtuelle Volumes, und virtuelle Volumes werden entsprechend der Kapazität des Speichercontainers zugeteilt.

In der Regel definiert ein Speicheradministrator auf der Speicherseite Speichercontainer. Die Anzahl der Speichercontainer, ihre Kapazität und Größe hängen von einer anbieterspezifischen Implementierung ab, aber mindestens ein Container pro Speichersystem ist erforderlich.

---

**Hinweis** Ein einzelner Speichercontainer kann sich nicht über verschiedene physische Arrays erstrecken.

---

Nach dem Registrieren eines mit dem Speichersystem verknüpften Speicheranbieters erkennt vCenter Server alle konfigurierten Speichercontainer zusammen mit ihren Speicherfunktionsprofilen, Protokollendpunkten und anderen Attributen. Ein einzelner Speichercontainer kann mehrere Funktionsprofile exportieren. Deshalb können virtuelle Maschinen mit verschiedenen Anforderungen und verschiedenen Speicherrichtlinieneinstellungen Teil desselben Speichercontainers sein.

Anfangs ist keiner der erkannten Speichercontainer mit einem bestimmten Host verbunden, und sie werden im vSphere Web Client nicht angezeigt. Zum Mounten eines Speichercontainers müssen Sie diesen einem virtuellen Datenspeicher zuordnen.

## Protokollendpunkte

Obwohl Speichersysteme alle Aspekte von virtuellen Volumes verwalten, haben ESXi-Hosts keinen Direktzugriff auf virtuelle Volumes auf der Speicherseite. Stattdessen verwenden ESXi-Hosts einen logischen E/A-Proxy, den so genannten Protokollendpunkt, zum Kommunizieren mit virtuellen Volumes und virtuellen Festplattendateien, die virtuelle Volumes enthalten. ESXi verwendet Protokollendpunkte zum Einrichten eines Datenpfads auf Anforderung von virtuellen Maschinen zu ihren jeweiligen virtuellen Volumes.

Jedes virtuelle Volume ist an einen speziellen Protokollendpunkt gebunden. Wenn eine virtuelle Maschine auf dem Host einen E/A-Vorgang ausführt, leitet der Protokollendpunkt die E/A zum entsprechenden virtuellen Volume. In der Regel erfordert ein Speichersystem nur sehr wenig Protokollendpunkte. Ein einzelner Protokollendpunkt kann mit Hunderten oder Tausenden von virtuellen Volumes verbunden werden.

Auf der Speicherseite konfiguriert ein Speicheradministrator Protokollendpunkte, einen oder mehrere pro Speichercontainer. Protokollendpunkte sind Teil des physischen Speicher-Fabrics und werden zusammen mit verknüpften Speichercontainern vom Speichersystem durch einen Speicheranbieter exportiert. Nachdem Sie einen Speichercontainer einem virtuellen Datenspeicher zugeordnet haben, werden Protokollendpunkte durch ESXi erkannt und im vSphere Web Client sichtbar. Protokollendpunkte können auch während der Neuprüfung eines Speichers erkannt werden.

Im vSphere Web Client sieht die Liste verfügbarer Protokollendpunkte ähnlich wie die Liste der Hostspeichergeräte aus. Sie können verschiedene Speichertransporte verwenden, um Protokollendpunkte für ESXi offenzulegen. Wenn der SCSI-basierte Transport verwendet wird, stellt der Protokollendpunkt eine durch eine T10-basierte LUN WWN definierte Proxy-LUN dar. Für das NFS-Protokoll ist der Protokollendpunkt ein Mount-Punkt, wie zum Beispiel IP-Adresse und ein Freigabename. Sie können Mehrfachpfade auf einem SCSI-basierten Protokollendpunkt, aber nicht auf einem NFS-basierten Protokollendpunkt konfigurieren. Unabhängig vom verwendeten Protokoll kann ein Speicherarray allerdings mehrere Protokollendpunkte zu Verfügbarkeitszwecken bereitstellen.

## Virtuelle Datenspeicher

Ein virtueller Datenspeicher stellt einen Speichercontainer in vCenter Server und im vSphere Web Client dar.

Nachdem vCenter Server durch Speichersysteme exportierte Speichercontainer erkannt hat, müssen Sie sie mounten, um sie verwenden zu können. Mit dem Assistenten zum Erstellen von Datenspeichern im vSphere Web Client ordnen Sie einen Speichercontainer einem virtuellen Datenspeicher zu. Der virtuelle Datenspeicher, den Sie erstellen, entspricht direkt dem speziellen Speichercontainer; er repräsentiert den Container in vCenter Server und im vSphere Web Client.

Vom Standpunkt eines vSphere-Administrators aus ähnelt der virtuelle Datenspeicher jedem beliebigen anderen Datenspeicher und wird als Behälter für virtuelle Maschinen verwendet. Wie andere Datenspeicher kann der virtuelle Datenspeicher durchsucht werden; dabei werden virtuelle Volumes nach dem Namen der virtuellen Maschine aufgelistet. Wie traditionelle Datenspeicher unterstützt der virtuelle Datenspeicher Unmounten und Mounten. Bestimmte Vorgänge wie beispielsweise Aktualisieren oder Vergrößern/Verkleinern sind allerdings nicht auf den virtuellen Datenspeicher anwendbar. Die Kapazität des virtuellen Datenspeichers kann vom Speicheradministrator außerhalb von vSphere konfiguriert werden.

Sie können virtuelle Datenspeicher mit traditionellen VMFS- und NFS-Datenspeichern und mit Virtual SAN verwenden.

---

**Hinweis** Die Größe eines virtuellen Volumes muss ein Vielfaches von 1 MB bei einer Mindestgröße von 1 MB sein. Die Größe aller virtuellen Festplatten, die Sie auf einem virtuellen Datenspeicher bereitstellen oder von einem beliebigen nicht virtuellen Datenspeicher migrieren, sollte deshalb ein gerades Vielfaches von 1 MB sein. Wenn die Kapazität der virtuellen Festplatte, die Sie in den virtuellen Datenspeicher migrieren, kein gerades Vielfaches von 1 MB ist, erweitern Sie den Datenträger manuell auf das nächste gerade Vielfache von 1 MB.

---

## Virtuelle Volumes und VM-Speicherrichtlinien

Für eine virtuelle Maschine, die auf einem virtuellen Datenspeicher ausgeführt wird, ist eine VM-Speicherrichtlinie erforderlich.

VM-Speicherrichtlinien sind Regelsätze, die die Platzierungs- und Dienstqualitätsanforderungen für eine virtuelle Maschine beschreiben. Die Richtlinie setzt die geeignete Platzierung der virtuellen Maschine im Speicher der virtuellen Volumes durch und sorgt dafür, dass der Speicher die Anforderungen der virtuellen Maschine erfüllen kann.

Mithilfe der Schnittstelle für VM-Speicherrichtlinien können Sie eine Speicherrichtlinie für virtuelle Volumes erstellen. Wenn Sie der virtuellen Maschine die neue Richtlinie zuweisen, bewirkt diese, dass der Speicher für virtuelle Volumes die Anforderungen erfüllt.

Wenn Sie keine VM-Speicherrichtlinie erstellen, die kompatibel zum virtuellen Datenspeicher ist, verwendet das System die Standardrichtlinie „Keine Anforderungen“. Die Richtlinie „Keine Anforderungen“ ist eine allgemeine Richtlinie für virtuelle Volumes ohne Regeln und Speicherspezifikationen. Mithilfe der Richtlinie können Speicher-Arrays für virtuelle Volumes die geeignetste Platzierung für die VM-Objekte bestimmen.

## Richtlinien bei der Verwendung von virtuellen Volumes

Die Funktionalität der virtuellen Volumes bietet mehrere Nutzen und Vorteile. Beim Arbeiten mit virtuellen Volumes sind bestimmte Richtlinien zu befolgen.

Virtuelle Volumes verfügen über die folgenden Eigenschaften:

- Virtuelle Volumes unterstützen das Auslagern einer Reihe von Vorgängen an Speicherhardware. Zu diesen Vorgängen gehören Snapshots, Klone und Storage DRS.
- Mit virtuellen Volumes können Sie erweiterte Speicherdienste wie Replikation, Verschlüsselung, Deduplizierung und Komprimierung auf einzelnen virtuellen Festplatten verwenden.
- Virtuelle Volumes unterstützen vSphere-Funktionen wie vMotion, Storage vMotion, Snapshots, verknüpfte Klone, Flash Read Cache und DRS.
- Mit virtuellen Volumes können Speicheranbieter systemeigene Snapshot-Funktionen zum Verbessern der Leistung von vSphere-Snapshots verwenden.
- Virtuelle Volumes können zusammen mit Speicher-Arrays verwendet werden, die vSphere APIs for Array Integration (VAAI) unterstützen.
- Virtuelle Volumes unterstützen Sicherungssoftware, die vSphere APIs for Data Protection (VADP) verwendet.

## Richtlinien und Beschränkungen für virtuelle Volumes

Befolgen Sie bei der Verwendung von virtuellen Volumes die folgenden Richtlinien.

- Da für die Umgebung der virtuellen Volumes vCenter Server erforderlich ist, können Sie virtuelle Volumes nicht mit einem eigenständigen Host verwenden.

- Virtuelle Volumes unterstützen keine RDMS.
- Ein Speichercontainer für virtuelle Volumes kann keine unterschiedlichen physischen Arrays umfassen.
- Hostprofile, die virtuelle Datenspeicher enthalten, sind vCenter Server-spezifisch. Nachdem Sie diesen Hostprofiltyp extrahiert haben, können Sie ihn nur an Hosts oder Cluster anbinden, die vom gleichen vCenter Server wie der Referenzhost verwaltet werden.

## Virtuelle Volumes und Speicherprotokolle

Die Funktionalität für virtuelle Volumes unterstützt Fibre-Channel, FCoE, iSCSI und NFS. Bei Speichertransporten werden Protokollendpunkte für ESXi-Hosts offengelegt.

Wenn das SCSI-basierte Protokoll verwendet wird, stellt der Protokollendpunkt eine durch eine T10-basierte LUN WWN definierte LUN dar. Für das NFS-Protokoll ist der Protokollendpunkt ein Mount-Punkt, wie zum Beispiel eine IP-Adresse oder ein DNS-Name und ein Freigabename.

Unabhängig vom verwendeten Speicherprotokoll wird ein virtuelles Volume, wie z. B. Dateien auf anderen traditionellen Datenspeichern, einer virtuellen Maschine als SCSI-Datenträger dargestellt. Virtuelle Volumes auf Festplatten-Arrays unterstützen denselben Satz von SCSI-Befehlen wie VMFS und verwenden ATS als Sperrmechanismus.

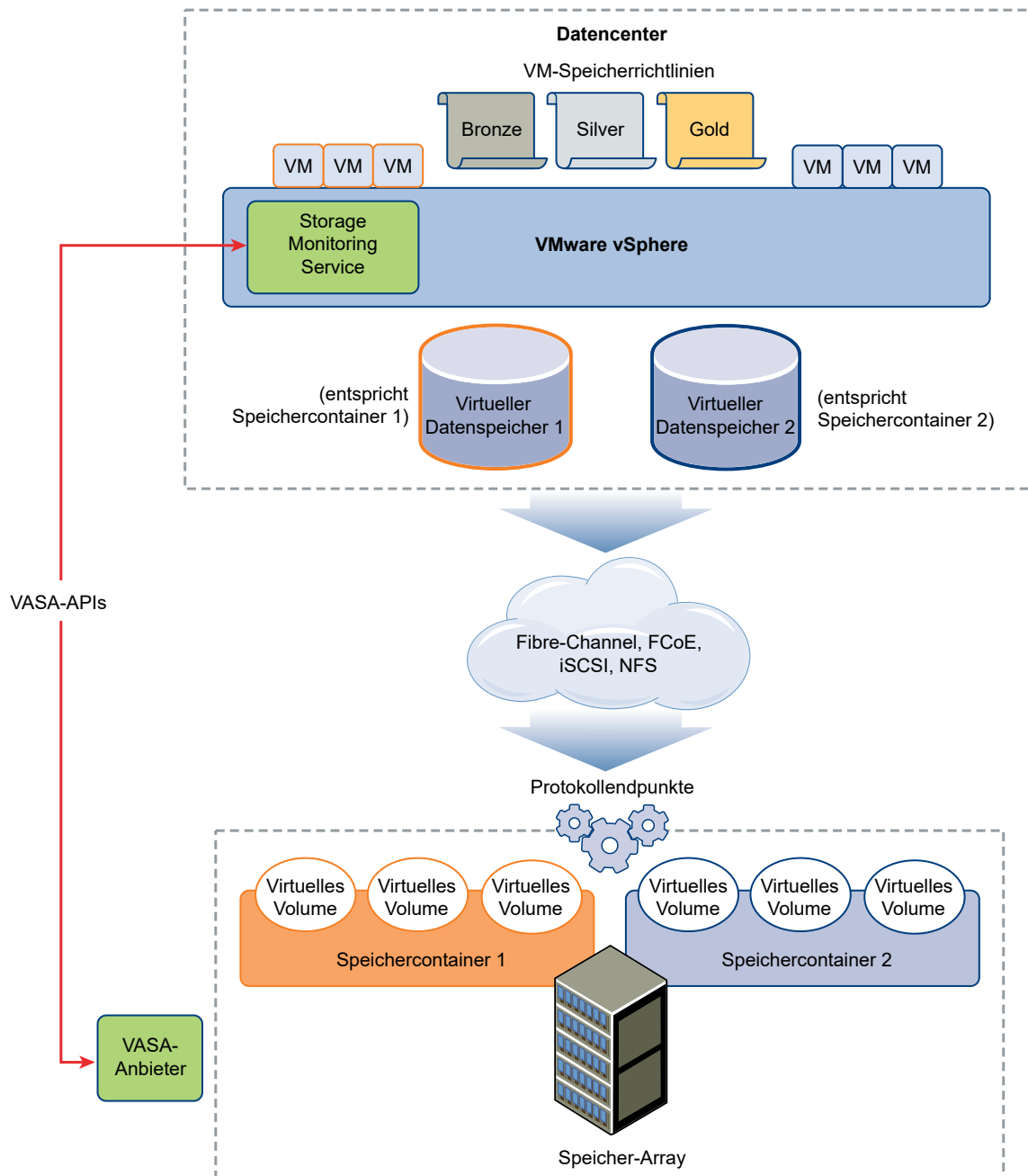
Virtuelle Volumes auf NAS-Geräten unterstützen dieselben NFS-RPCs (Remote Procedure Calls), die von ESXi-Hosts zum Verbinden mit NFS-Mount-Punkten benötigt werden.

Die folgenden Überlegungen und Richtlinien gelten, wenn Sie unterschiedliche Speicherprotokolle verwenden:

- Mit NFS können Sie Version 3 verwenden. Virtuelle Volumes unterstützen NFS 4.1 nicht.
- Das IPv6-Format wird nicht unterstützt.
- Für iSCSI müssen Sie den Software-iSCSI-Adapter aktivieren. Konfigurieren Sie die dynamische Erkennung und geben Sie die IP-Adresse des VVols-Speicheranbieters ein. Siehe [Konfigurieren des Software-iSCSI-Adapters](#).
- Sie können Mehrfachpfade auf einem SCSI-basierten Protokollendpunkt, aber nicht auf einem NFS-basierten Protokollendpunkt konfigurieren. Unabhängig vom verwendeten Protokoll kann ein Speicherarray mehrere Protokollendpunkte zu Verfügbarkeitszwecken bereitstellen.

## Architektur von Virtual Volumes

Ein architektonisches Diagramm bietet eine Übersicht darüber, wie alle Komponenten der Funktionalität für Virtual Volumes miteinander interagieren.



Virtuelle Volumes sind Objekte, die von einem kompatiblen Speichersystem exportiert wurden, und entsprechen gewöhnlich 1:1 einer Festplatte einer virtuellen Maschine und anderen Dateien im Zusammenhang mit virtuellen Maschinen. Ein virtuelles Volume wird durch einen VASA-Anbieter out-of-band und nicht im Datenpfad erstellt und manipuliert.

Ein VASA-Anbieter bzw. ein Speicheranbieter wird durch vSphere-APIs für Storage Awareness entwickelt. Der Speicheranbieter ermöglicht die Kommunikation zwischen dem vSphere-Stack – ESXi-Hosts, vCenter Server und vSphere Web Client – und dem Speichersystem. Der VASA-Anbieter wird auf der Speicherseite ausgeführt und ist auf den vSphere-



Speicherüberwachungsdienst (SMS) zum Verwalten aller Aspekte des Speichers für Virtual Volumes abgestimmt. Der VASA-Anbieter ordnet Objekte virtueller Festplatten und deren Ableitungen, wie Klone, Snapshots und Repliken, direkt den virtuellen Volumes auf dem Speichersystem zu.

ESXi-Hosts haben keinen Direktzugriff auf den Speicher für virtuelle Volumes. Stattdessen greifen die Hosts durch eine Zwischenstelle im Datenpfad, den so genannten Protokollendpunkt, auf virtuelle Volumes zu. Protokollendpunkte richten bei Bedarf einen Datenpfad von virtuellen Maschinen zu deren virtuellen Volumes ein und dienen als Gateway für direkte In-Band-E/A zwischen ESXi-Hosts und dem Speichersystem. ESXi kann Fibre-Channel-, FCoE-, iSCSI- und NFS-Protokolle für In-Band-Datenaustausch verwenden.

Virtuelle Volumes befinden sich in Speichercontainern, die logisch einen Pool physischer Festplatten im Speichersystem darstellen. Im vSphere-Stack werden Speichercontainer als virtuelle Datenspeicher dargestellt. Ein einzelner Speichercontainer kann mehrere Speicherfunktionssätze exportieren. Wenn Sie eine virtuelle Maschine auf dem virtuellen Datenspeicher erstellen, können Sie deshalb verschiedene Speicherrichtlinien zum Platzieren virtueller Volumes im selben Speichercontainer so verwenden, dass unterschiedliche Speicherbedürfnisse einer virtuellen Maschine erfüllt werden.

Informationen zur Architektur von Virtual Volumes erhalten Sie im entsprechenden Video.



Virtual Volumes, Teil 2: Architektur

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_9e6fnx3m/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_9e6fnx3m/uiConfId/49694343/))

## Virtuelle Volumes und VMware Certificate Authority

Im Lieferumfang von vSphere 6.0.x ist VMware Certificate Authority (VMCA) enthalten. VMCA generiert standardmäßig alle internen Zertifikate, die in der vSphere-Umgebung verwendet werden. Hierzu zählen auch Zertifikate für neu hinzugefügte ESXi-Hosts und VASA-Speicheranbieter, die VVOL-Speichersysteme verwalten oder repräsentieren.

Die Kommunikation mit dem VASA-Anbieter wird durch SSL-Zertifikate geschützt. Diese Zertifikate können vom VASA-Anbieter oder von VMCA stammen.

- Zertifikate können direkt vom VASA-Anbieter für die langfristige Verwendung bereitgestellt werden und können entweder selbstgeneriert und selbstsigniert sein oder aber von einer externen Zertifizierungsstelle stammen.
- Zertifikate können von VMCA für die Verwendung durch den VASA-Anbieter generiert werden.

Wenn ein Host oder VASA-Anbieter registriert ist, führt VMCA diese Schritte automatisch aus, ohne dass der vSphere-Administrator eingreifen muss.

- 1 Wenn ein VASA-Anbieter erstmalig zum Speicherverwaltungsdienst (Storage Management Service, SMS) von vCenter Server hinzugefügt wird, wird ein selbstsigniertes Zertifikat erstellt.

- 2 Nach der Überprüfung des Zertifikats fordert der Speicherverwaltungsdienst eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) vom VASA-Anbieter an.
- 3 Nach dem Empfang und der Überprüfung der CSR wird sie vom Speicherverwaltungsdienst im Namen des VASA-Anbieters gegenüber VMCA präsentiert und es wird ein von der Zertifizierungsstelle signiertes Zertifikat angefordert.

VMCA kann als eigenständige Zertifizierungsstelle oder als untergeordnete Zertifizierungsstelle für eine Unternehmenszertifizierungsstelle konfiguriert werden. Wenn Sie VMCA als untergeordnete Zertifizierungsstelle einrichten, signiert VMCA die CSR mit der vollständigen Zertifizierungskette.

- 4 Das signierte Zertifikat wird zusammen mit dem Rootzertifikat an den VASA-Anbieter übergeben, um damit alle zukünftigen sicheren Verbindungen, die vom Speicherverwaltungsdienst ausgehen, in vCenter Server und auf ESXi-Hosts authentifizieren zu können.

## Schritte vor der Aktivierung virtueller Volumes

Für die Arbeit mit virtuellen Volumes müssen Sie sicherstellen, dass Ihre Speicherumgebung und Ihre vSphere-Umgebung korrekt eingerichtet sind.

Befolgen Sie diese Richtlinien, um Ihre Speichersystemumgebung für virtuelle Volumes vorzubereiten. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

- Das verwendete Speichersystem oder Speicherarray muss in der Lage sein, virtuelle Volumes zu unterstützen und über vSphere-APIs für Storage Awareness (VASA) in vSphere integriert zu werden.
- Ein VVols-Speicheranbieter muss bereitgestellt werden.
- Speicherseitig müssen Protokollendpunkte, Speichercontainer und Speicherprofile konfiguriert sein.

Bereiten Sie Ihre vSphere-Umgebung vor.

- Befolgen Sie die Setup-Richtlinien für den verwendeten Speichertyp: Fibre Channel, FCoE, iSCSI oder NFS. Falls erforderlich, installieren und konfigurieren Sie Speicheradapter auf Ihren ESXi-Hosts.

Bei Verwendung von iSCSI aktivieren Sie die Software-iSCSI-Adapter auf Ihren ESXi-Hosts. Konfigurieren Sie die dynamische Erkennung und geben Sie die IP-Adresse Ihres VVols-Speichersystems ein.

- Synchronisieren Sie alle Komponenten im Speicherarray mit vCenter Server und allen ESXi-Hosts. Verwenden Sie dazu das Network Time Protocol (NTP).

## Synchronisieren der vSphere Storage-Umgebung mit einem NTP-Server

Stellen Sie vor der Bereitstellung von Virtual Volumes sicher, dass auf allen Maschinen im vSphere-Netzwerk die Systemuhren synchronisiert sind.

### Verfahren

- 1 Wählen Sie den Host in der vSphere-Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie im Abschnitt „System“ die Option **Uhrzeitkonfiguration** aus.
- 4 Klicken Sie auf **Bearbeiten** und richten Sie den NTP-Server ein.
  - a Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.
  - b Legen Sie die Startrichtlinie für den NTP-Dienst fest.
  - c Geben Sie die IP-Adressen der NTP-Server ein, mit denen synchronisiert werden soll.
  - d Klicken Sie im Abschnitt „NTP-Dienststatus“ auf **Starten** oder **Neu starten**.

- 5 Klicken Sie auf **OK**.

Der Host wird mit dem NTP-Server synchronisiert.

## Konfigurieren virtueller Volumes

Zum Konfigurieren der Umgebung Ihrer virtuellen Volumes müssen Sie mehrere Schritte ausführen.

### Voraussetzungen

Befolgen Sie die Anweisungen in [Schritte vor der Aktivierung virtueller Volumes](#).

### Verfahren

- 1 [Registrieren von Speicheranbietern für virtuelle Volumes](#)

Ihre Umgebung mit virtuellen Volumes muss Speicheranbieter umfassen, auch als VASA-Anbieter bezeichnet. In der Regel entwickeln Drittanbieter Speicheranbieter über die VMware APIs for Storage Awareness (VASA). Speicheranbieter ermöglichen die Kommunikation zwischen vSphere und dem Speicher. Sie müssen den Speicheranbieter in vCenter Server registrieren, um mit virtuellen Volumes arbeiten zu können.

- 2 [Erstellen eines virtuellen Datenspeichers](#)

Neue Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

### 3 Prüfen und Verwalten von Protokoll-Endpoints

ESXi-Hosts verwenden einen logischen E/A-Proxy, Protokollendpunkt genannt, um mit virtuellen Volumes und den Dateien auf virtuellen Festplatten zu kommunizieren. Protokollendpunkte werden vom Speichersystem über einen Speicheranbieter gemeinsam mit den zugehörigen Speichercontainern exportiert. Protokollendpunkte werden im vSphere Web Client nach der Zuordnung eines Speichercontainers zu einem virtuellen Datenspeicher angezeigt. Sie können die Eigenschaften von Protokollendpunkten prüfen und einzelne Einstellungen ändern.

### 4 (Optional) Ändern der Pfadauswahlrichtlinie für einen Protokoll-Endpoint

Wenn Ihr ESXi-Host SCSI-basierten Transport zur Kommunikation mit den Protokollendpunkten eines Speicherarrays verwendet, können Sie die standardmäßigen Mehrfachpfad-Richtlinien ändern, die den Protokollendpunkten zugewiesen sind. Die Pfadauswahlrichtlinie ändern Sie im Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten**.

#### Nächste Schritte

Sie können jetzt virtuelle Maschinen auf dem virtuellen Datenspeicher bereitstellen. Informationen zum Erstellen virtueller Maschinen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Informationen zur Fehlerbehebung finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

## Registrieren von Speicheranbietern für virtuelle Volumes

Ihre Umgebung mit virtuellen Volumes muss Speicheranbieter umfassen, auch als VASA-Anbieter bezeichnet. In der Regel entwickeln Drittanbieter Speicheranbieter über die VMware APIs for Storage Awareness (VASA). Speicheranbieter ermöglichen die Kommunikation zwischen vSphere und dem Speicher. Sie müssen den Speicheranbieter in vCenter Server registrieren, um mit virtuellen Volumes arbeiten zu können.

Nach der Registrierung kommuniziert der Anbieter virtueller Volumes mit vCenter Server und meldet Merkmale des zugrunde liegenden Speichers. Die Merkmale werden auf der Schnittstelle für VM-Speicherrichtlinien angezeigt und können verwendet werden, um eine VM-Speicherrichtlinie zu erstellen, die mit dem virtuellen Datenspeicher kompatibel ist. Nachdem Sie diese Speicherrichtlinie auf eine virtuelle Maschine angewandt haben, wird die Richtlinie an den Speicher der virtuellen Volumes übertragen. Die Richtlinie setzt die optimale Platzierung der virtuellen Maschine im Speicher der virtuellen Volumes durch und sorgt dafür, dass der Speicher die Anforderungen der virtuellen Maschine erfüllen kann.

#### Voraussetzungen

Stellen Sie sicher, dass die Speicheranbieter-Komponente auf der Speicherseite installiert ist, und fragen Sie Ihren Speicheradministrator nach den Anmeldedaten. Weitere Informationen erhalten Sie von Ihrem Anbieter.

#### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.

- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Klicken Sie auf das Symbol **Neuen Speicheranbieter registrieren**.
- 4 (Optional) Um vCenter Server zum Speicheranbieterzertifikat zu leiten, wählen Sie die Option **Zertifikat des Speicheranbieters verwenden** aus und geben den Speicherort des Zertifikats an.

Wenn Sie diese Option nicht auswählen, wird ein Fingerabdruck des Zertifikats angezeigt. Sie können den Fingerabdruck überprüfen und ihn genehmigen.

- 5 Klicken Sie auf **OK**, um die Registrierung abzuschließen.

### Ergebnisse

vCenter Server erkennt und registriert den Speicheranbieter für virtuelle Volumes.

## Erstellen eines virtuellen Datenspeichers

Neue Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf das Symbol **Neuer Datenspeicher**.
- 3 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.  
  
Achten Sie darauf, für jeden Datenspeicher in Ihrer Datenspeicherumgebung einen eindeutigen Namen zu vergeben.  
  
Beim Mounten eines virtuellen Datenspeichers auf mehreren Hosts muss der Datenspeichername auf allen Hosts gleich sein.
- 4 Wählen Sie **VVOL** als Datenspeichertyp.
- 5 Wählen Sie aus der Liste der Speichercontainer einen Backing-Speichercontainer aus.
- 6 Wählen Sie die Hosts aus, die Zugriff auf den Datenspeicher benötigen.
- 7 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

### Nächste Schritte

Nach der Erstellung des virtuellen Datenspeichers können Sie ihn umbenennen, Datenspeicherdateien durchsuchen, den Datenspeicher unmounten und weitere Datenspeicheraktionen ausführen.

Sie können den Datenspeicher nicht einem Datenspeicher-Cluster hinzufügen.

## Prüfen und Verwalten von Protokoll-Endpoints

ESXi-Hosts verwenden einen logischen E/A-Proxy, Protokollendpunkt genannt, um mit virtuellen Volumes und den Dateien auf virtuellen Festplatten zu kommunizieren. Protokollendpunkte

werden vom Speichersystem über einen Speicheranbieter gemeinsam mit den zugehörigen Speichercontainern exportiert. Protokollendpunkte werden im vSphere Web Client nach der Zuordnung eines Speichercontainers zu einem virtuellen Datenspeicher angezeigt. Sie können die Eigenschaften von Protokollendpunkten prüfen und einzelne Einstellungen ändern.

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Protokollendpunkte**.
- 4 Um Details eines bestimmten Elements anzuzeigen, wählen Sie das Element aus der Liste aus.
- 5 Auf den Registerkarten unter „Details zu Protokollendpunkten“ finden Sie weitere Informationen und können die Eigenschaften des ausgewählten Endpunkts ändern.

Registerkarte	Beschreibung
<b>Eigenschaften</b>	Zeigen Sie die Eigenschaften und Merkmale des Elements an. Bei SCSI-(Block-)Elementen können Sie die Mehrfachpfad-Richtlinien anzeigen und bearbeiten.
<b>Pfade (nur SCSI-Protokollendpunkte)</b>	Anzeigen der für den Protokollendpunkt verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads. Ändern der Pfadauswahl-Richtlinie.
<b>Datenspeicher</b>	Anzeigen eines entsprechenden virtuellen Datenspeichers. Ausführen von Vorgängen zur Datenspeicherverwaltung.

## Ändern der Pfadauswahlrichtlinie für einen Protokoll-Endpoint

Wenn Ihr ESXi-Host SCSI-basierten Transport zur Kommunikation mit den Protokollendpunkten eines Speicherarrays verwendet, können Sie die standardmäßigen Mehrfachpfad-Richtlinien ändern, die den Protokollendpunkten zugewiesen sind. Die Pfadauswahlrichtlinie ändern Sie im Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten**.

#### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie auf **Protokollendpunkte**.
- 4 Wählen Sie den Protokollendpunkt aus, dessen Pfade Sie ändern möchten, und klicken Sie auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie unter „Mehrfachpfad-Richtlinien“ auf **Mehrfachpfad bearbeiten**.
- 6 Wählen Sie eine Pfadrichtlinie aus.
  - Fest (VMware)
  - Zuletzt verwendet (VMware)

- Round-Robin (VMware)

- 7 Legen Sie für die feste Richtlinie den bevorzugten Pfad fest.
- 8 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

## Bereitstellen von virtuellen Maschinen auf virtuellen Datenspeichern

Sie können virtuelle Maschinen auf einem virtuellen Datenspeicher bereitstellen.

---

**Hinweis** Die Kapazität aller virtuellen Festplatten, die Sie auf einem virtuellen Datenspeicher bereitstellen, sollte ein gerades Vielfaches von 1 MB sein.

---

Für eine virtuelle Maschine, die auf einem virtuellen Datenspeicher ausgeführt wird, ist eine geeignete VM-Speicherrichtlinie erforderlich.

Nach der Bereitstellung der virtuellen Maschine können Sie typische Verwaltungsaufgaben für die virtuelle Maschine ausführen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Informationen zur Fehlerbehebung finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

### Verfahren

#### 1 Definieren einer VM-Speicherrichtlinie für Virtual Volumes

Sie können eine VM-Speicherrichtlinie erstellen, die mit einem virtuellen Datenspeicher kompatibel ist.

#### 2 Zuweisen der Speicherrichtlinie für virtuelle Volumes zu virtuellen Maschinen

Um zu gewährleisten, dass der virtuelle Datenspeicher beim Zuordnen einer virtuellen Maschine die spezifischen Datenspeicheranforderungen erfüllt, weisen Sie die VVols-Speicherrichtlinie der virtuellen Maschine zu.

#### 3 Ändern der Standardspeicherrichtlinie für einen virtuellen Datenspeicher

Für virtuelle Maschinen, die auf virtuellen Datenspeichern bereitgestellt sind, stellt VMware eine Standardrichtlinie ohne Anforderungen bereit. Diese Richtlinie kann nicht bearbeitet werden; Sie können jedoch eine neu erstellte Richtlinie als Standard bereitstellen.

## Definieren einer VM-Speicherrichtlinie für Virtual Volumes

Sie können eine VM-Speicherrichtlinie erstellen, die mit einem virtuellen Datenspeicher kompatibel ist.

### Voraussetzungen

Vergewissern Sie sich, dass der Speicheranbieter für Virtual Volumes verfügbar und aktiv ist. Weitere Informationen hierzu finden Sie unter [Registrieren von Speicheranbietern für virtuelle Volumes](#).

## Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen**.
- 3 Wählen Sie die vCenter Server-Instanz aus.
- 4 Geben Sie einen Namen und eine Beschreibung für die Speicherrichtlinie ein und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Regelsätze“ aus dem Dropdown-Menü **Regeln basierend auf Datendiensten** den gewünschten Speicheranbieter für Virtual Volumes.

Die Seite wird erweitert und zeigt die vom Virtual Volumes-Speicherelement bereitgestellten Datendienste an.

- 6 Wählen Sie einen Datendienst aus und geben Sie dessen Werte an.

Achten Sie darauf, dass die eingegebenen Werte innerhalb des vom Profil des Datenspeichers für Virtual Volumes angegebenen Wertebereichs liegen.

Basierend auf Ihrer Eingabe berechnet die Speicherbelegung den für die virtuelle Festplatte im virtuellen Datenspeicher erforderlichen Speicherplatz.

- 7 Schließen Sie die Erstellung der Speicherrichtlinie ab und klicken Sie auf **Beenden**.

## Ergebnisse

Die neue Virtual Volumes-kompatible Speicherrichtlinie wird in der Liste angezeigt.

## Nächste Schritte

Sie können diese Richtlinie nun einer virtuellen Maschine zuweisen oder als Standard festlegen.

## Zuweisen der Speicherrichtlinie für virtuelle Volumes zu virtuellen Maschinen

Um zu gewährleisten, dass der virtuelle Datenspeicher beim Zuordnen einer virtuellen Maschine die spezifischen Datenspeicheranforderungen erfüllt, weisen Sie die VVols-Speicherrichtlinie der virtuellen Maschine zu.

Sie können die VVols-Speicherrichtlinie bei der anfänglichen Bereitstellung einer virtuellen Maschine oder im Zuge sonstiger VM-Vorgänge zuweisen, etwa beim Klonen oder Migrieren. Dieses Thema beschreibt die Zuweisung der VVols-Speicherrichtlinie bei der Erstellung einer neuen virtuellen Maschine. Informationen zu anderen VM-Bereitstellungsmethoden finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Sie können dieselbe Speicherrichtlinie auf die Konfigurationsdatei der virtuellen Maschine und alle ihre virtuellen Festplatten anwenden. Wenn Sie unterschiedliche Speicheranforderungen an die Konfigurationsdatei und die virtuellen Festplatten haben, können sie ihnen auch eigene Speicherrichtlinien zuweisen.



## Verfahren

- 1 Starten Sie im vSphere Web Client den Vorgang zur Bereitstellung von virtuellen Maschinen und befolgen Sie die entsprechenden Schritte.
- 2 Weisen Sie allen VM-Dateien und Festplatten dieselbe Speicherrichtlinie zu.
  - a Wählen Sie auf der Seite „Speicher auswählen“ im Dropdown-Menü **VM-Speicherrichtlinie** eine mit virtuellen Festplatten kompatible Speicherrichtlinie aus, etwa VVols Silver.
  - b Wählen Sie aus der Liste der verfügbaren Datenspeicher den gewünschten virtuellen Datenspeicher aus und klicken Sie auf **Weiter**.

Der Datenspeicher wird zum Zielspeicherelement für die VM-Konfigurationsdatei und alle virtuellen Festplatten.

- 3 Ändern Sie die Speicherrichtlinie für virtuelle Festplatten.

Verwenden Sie diese Option, wenn Sie für virtuelle Festplatten andere Anforderungen bezüglich der Speicherplatzierung haben.

- a Erweitern Sie auf der Seite „Hardware anpassen“ den Bereich „Neue Festplatte“.
- b Wählen Sie im Dropdown-Menü **VM-Speicherrichtlinie** die Speicherrichtlinie aus (etwa VVols Gold), die Sie der virtuellen Festplatte zuweisen möchten.

- 4 Schließen Sie die Bereitstellung der virtuellen Maschine ab.

## Ergebnisse

Nach der Erstellung der virtuellen Maschine zeigt die Registerkarte **Übersicht** die zugewiesenen Speicherrichtlinien und deren Übereinstimmungsstatus an.

## Nächste Schritte

Wenn sich die Speicherplatzierungsanforderungen für die Konfigurationsdatei oder die virtuellen Festplatten zu einem späteren Zeitpunkt ändern sollten, können Sie die Zuweisung der VM-Richtlinie entsprechend anpassen. Siehe [Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten](#).

## Ändern der Standardspeicherrichtlinie für einen virtuellen Datenspeicher

Für virtuelle Maschinen, die auf virtuellen Datenspeichern bereitgestellt sind, stellt VMware eine Standardrichtlinie ohne Anforderungen bereit. Diese Richtlinie kann nicht bearbeitet werden; Sie können jedoch eine neu erstellte Richtlinie als Standard bereitstellen.

## Voraussetzungen

Erstellen Sie eine Speicherrichtlinie, die mit virtuellen Volumes kompatibel ist.

## Verfahren

- 1 Navigieren Sie zu dem virtuellen Datenspeicher, dessen Standardspeicherrichtlinie Sie ändern möchten.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie auf **Allgemein** und dann im Bereich „Standardspeicherrichtlinie“ auf **Bearbeiten**.
- 4 Wählen Sie aus der Liste der verfügbaren Speicherrichtlinien eine Richtlinie aus, die Sie als Standard zuweisen möchten, und klicken Sie auf **OK**.

## Ergebnisse

Die ausgewählte Speicherrichtlinie wird die Standardspeicherrichtlinie für den virtuellen Datenspeicher. vSphere weist diese Richtlinie allen Objekten für virtuelle Maschinen zu, die Sie auf dem virtuellen Datenspeicher bereitstellen, es sei denn, es wird ausdrücklich eine andere Richtlinie ausgewählt.

VM-Speicherrichtlinien sind entscheidend für die Bereitstellung von virtuellen Maschinen. Mit diesen Richtlinien können Sie die Speicheranforderungen für die virtuelle Maschine festlegen und bestimmen, welche Art von Speicher für die virtuelle Maschine bereitgestellt wird, wie die virtuelle Maschine innerhalb des Speichers platziert wird und welche Datendienste der virtuellen Maschine zur Verfügung gestellt werden.

Wenn Sie eine Speicherrichtlinie definieren, geben Sie die Speicheranforderungen für Anwendungen an, die auf virtuellen Maschinen ausgeführt werden. Nachdem Sie die Speicherrichtlinie auf eine virtuelle Maschine angewendet haben, wird die virtuelle Maschine in einem spezifischen Datenspeicher untergebracht, der die Speicheranforderungen erfüllt. In softwaredefinierten Speicherumgebungen wie Virtual SAN und virtuellen Volumes bestimmt die Speicherrichtlinie auch, wie die Speicherobjekte der virtuellen Maschine bereitgestellt und innerhalb der Speicherressource zugeordnet werden, um den erforderlichen Service-Level zu gewährleisten. In Umgebungen mit installierten Drittanbieter-E/A-Filtern können Sie mithilfe von Speicherrichtlinien eine zusätzliche Ebene von Datendiensten, wie beispielsweise Zwischenspeicherung und Replizierung, für virtuelle Festplatten aktivieren.

Dieses Kapitel enthält die folgenden Themen:

- [Upgrade von Legacy Storage Profiles](#)
- [Grundlegende Informationen zu VM-Speicherrichtlinien](#)
- [Arbeiten mit VM-Speicherrichtlinien](#)
- [Erstellen und Verwalten von VM-Speicherrichtlinien](#)
- [Speicherrichtlinien und virtuelle Maschinen](#)

## Upgrade von Legacy Storage Profiles

In vSphere 5.x wurden VM-Speicherrichtlinien als Storage Profiles bezeichnet und wiesen ein anderes Format auf. Beim Upgrade der vSphere-Umgebung von der Version 5.x auf vSphere 6.x werden in früheren Versionen erstellte Storage Profiles in Speicherrichtlinien konvertiert.

Alle Komponenten von Legacy Storage Profiles werden in neue Formate oder Objekte konvertiert. Alle systemdefinierten Storage Capabilities werden in auf Metadaten basierte speicherspezifische Datendienste konvertiert. Benutzerdefinierte Funktionen werden zu Datenspeicher-Tags.

Tabelle 20-1. Altes und neues Format von Speicherrichtlinien

vSphere 5.x	vSphere 6.x
VM Storage Profile	VM-Speicherrichtlinie
Systemdefinierte Funktionen	Speicherspezifische Datendienste
Benutzerdefinierte Funktionen	Datenspeicher-Tags
N/A	Gemeinsame Datendienste

## Grundlegende Informationen zu VM-Speicherrichtlinien

Speicherrichtlinien für virtuelle Maschinen erfassen Speichermerkmale, die von den Home-Dateien der virtuellen Maschine und virtuellen Festplatten zum Ausführen von Anwendungen in der VM benötigt werden. Sie können mehrere Speicherrichtlinien erstellen, um die Typen und Klassen von Speicheranforderungen zu definieren.

Eine Speicherrichtlinie stellt nicht nur Einschränkungen dar, die gleichzeitig angewendet werden. Eine einzelne Richtlinie kann alternative Unterrichtlinien (Regelsätze) enthalten, die datenspeicherspezifisch sind und gleichermaßen akzeptable Speicheranforderungen darstellen. Wenn Sie vSphere APIs für E/A-Filter verwenden, kann die Speicherrichtlinie Regeln enthalten, die für alle Speichertypen gelten. Die Richtlinie kann nur gemeinsame Regeln und/oder nur datenspezifische Regelsätze enthalten.

Wenn Sie eine virtuelle Maschine erstellen, klonen oder migrieren, können Sie die Speicherrichtlinie auf die virtuelle Maschine anwenden. Sie können die virtuelle Maschine in einem Datenspeicher platzieren, der mit den Richtlinienanforderungen übereinstimmt. Für den Abgleich der Richtlinienanforderungen muss der Datenspeicher folgende Voraussetzungen erfüllen:

- Wenn die E/A-Filterung und gemeinsame Regeln nicht verfügbar sind, muss der Datenspeicher alle Regeln mindestens eines datenspeicherspezifischen Regelsatzes erfüllen.
- Wenn gemeinsame Regeln aktiviert sind, muss der Datenspeicher alle gemeinsamen Regeln und alle Regeln mindestens eines Regelsatzes erfüllen.

Die Home-Dateien der virtuellen Maschine (.vmtx, .vmsd, .nvram, .log usw.) und die virtuellen Festplatten (.vmdk) können separate Speicherrichtlinien aufweisen.

Tabelle 20-2. Beispiel einer Speicherrichtlinie für eine virtuelle Maschine

Beispiel-VM-Dateien	Beispiel für eine Speicherrichtlinie	Beispiel für einen Datenspeicher, der mit der Speicherrichtlinie übereinstimmt
<code>windows_2008r2_test.vmx</code>	Speicherrichtlinie 2	datastore02, datastore05, datastore10
<code>windows_2008r2_test.vmx</code>		
<code>windows_2008r2_test.log</code>		
<code>windows_2008r2_test.nvram</code>		

Tabelle 20-2. Beispiel einer Speicherrichtlinie für eine virtuelle Maschine (Fortsetzung)

Beispiel-VM-Dateien	Beispiel für eine Speicherrichtlinie	Beispiel für einen Datenspeicher, der mit der Speicherrichtlinie übereinstimmt
<i>windows_2008r2_test.vmem</i>		
<i>windows_2008r2_test.vmsd</i>		
<i>windows_2008r2_test.vmdk</i>	Speicherrichtlinie 3	datastore05
<i>windows_2008r2_test_1.vmdk</i>	Speicherrichtlinie 5	datastore10
k		

## Speicherrichtlinien und Regeln

Regeln, die Sie in eine Speicherrichtlinie aufnehmen, können auf speicherspezifischen Datendiensten und Tags basieren, oder es kann sich um gemeinsame Regeln handeln.

### ■ Gemeinsame Regeln

Gemeinsame Regeln basieren auf Datendiensten, die allen Speichertypen gemeinsam sind und nicht von einem bestimmten Datenspeicher abhängig sind. Diese zusätzlichen Dienste werden in der Schnittstelle für VM-Speicherrichtlinien bei der Installation von E/A-Filtern von Drittanbietern verfügbar, die über vSphere APIs für E/A-Filter entwickelt werden. Auf diese Datendienste kann in einer VM-Speicherrichtlinie verwiesen werden.

### ■ Regeln basierend auf speicherspezifischen Datendiensten

Diese Regeln basieren auf Datendiensten, die von Speicherelementen wie Virtual SAN und virtuellen Volumes angekündigt werden.

### ■ Regeln basierend auf Tags

Auf Tags basierende Regeln verweisen auf Datenspeicher-Tags, die Sie mit bestimmten Datenspeichern verknüpfen. Sie können mehr als einen Tag auf einen Datenspeicher anwenden.

## Gemeinsame Regeln

Gemeinsame Regeln basieren auf Datendiensten, die allen Speichertypen gemeinsam sind und nicht von einem bestimmten Datenspeicher abhängig sind. Diese zusätzlichen Dienste werden in der Schnittstelle für VM-Speicherrichtlinien bei der Installation von E/A-Filtern von Drittanbietern verfügbar, die über vSphere APIs für E/A-Filter entwickelt werden. Auf diese Datendienste kann in einer VM-Speicherrichtlinie verwiesen werden.

Im Gegensatz zu speicherspezifischen Regeln werden mit gemeinsamen Regeln nicht die Speicherplatzierung und die Speicheranforderungen für eine virtuelle Maschine definiert, aber sie stellen sicher, dass zusätzliche Dienste wie z. B. E/A-Filter für die virtuelle Maschine aktiviert werden. Unabhängig davon, auf welcher virtuellen Maschine der Datenspeicher ausgeführt wird, können die aktivierten Filter die folgenden Dienste anbieten:

- **Zwischenspeicherung.** Konfiguriert einen Cache für virtuelle Festplattendaten. Der Filter kann mit einem lokalen Cache oder einem Flash-Speichergerät die Daten zwischenspeichern und die E/A-Vorgänge pro Sekunde und die Hardwarenutzungsraten für die virtuelle Festplatte erhöhen.
- **Replizierung.** Repliziert die virtuelle Maschine oder virtuelle Festplatten in externen Zielen wie beispielsweise auf einem anderen Host oder Cluster.

Weitere Informationen zu E/A-Filtern finden Sie unter [Kapitel 21 Filtern der E/A einer virtuellen Maschine](#).

## Regeln basierend auf speicherspezifischen Datendiensten

Diese Regeln basieren auf Datendiensten, die von Speicherelementen wie Virtual SAN und virtuellen Volumes angekündigt werden.

Um vCenter Server Informationen über zugrunde liegenden Speicher zu übermitteln, verwenden Virtual SAN und virtuelle Volumes Speicheranbieter, auch VASA-Anbieter genannt. Speicherinformationen und Datenspeichermerkmale erscheinen unter den VM-Speicherrichtlinien im vSphere Web Client als Datendienste, die vom betreffenden Datenspeichertyp angeboten werden.

Ein Datenspeicher kann mehrere Dienste anbieten. Diese Datendienste werden in einem Datenspeicherprofil zusammengefasst, das die Dienstqualität angibt, die der Datenspeicher bieten kann.

Beim Erstellen von Regeln für eine VM-Speicherrichtlinie verweisen Sie auf die Datendienste, die von einem bestimmten Datenspeicher angekündigt werden. Der Datenspeicher garantiert der virtuellen Maschine, die diese Richtlinie verwendet, dass er ihre Speicheranforderungen erfüllt. Der Datenspeicher kann der virtuellen Maschine auch einen spezifischen Satz von Merkmalen für Kapazität, Leistung, Verfügbarkeit, Redundanz usw. zur Verfügung stellen.

Weitere Informationen zu Speicheranbietern finden Sie unter [Kapitel 25 Verwenden von Speicheranbietern](#).

## Regeln basierend auf Tags

Auf Tags basierende Regeln verweisen auf Datenspeicher-Tags, die Sie mit bestimmten Datenspeichern verknüpfen. Sie können mehr als einen Tag auf einen Datenspeicher anwenden.

In der Regel dienen Tags den folgenden Zwecken:

- **Anfügen einer umfassenden Speicherebenendefinition zu Datenspeichern,** die von keinem Speicheranbieter repräsentiert werden, z. B. VMFS- und NFS-Datenspeicher

- Codieren von richtlinienrelevanten Informationen, die nicht über vSphere API for Storage Awareness (VASA) angekündigt werden, wie der geografische Standort oder die Administratorengruppe

Ähnlich wie speicherspezifische Dienste werden auch alle mit Datenspeichern verbundenen Tags unter den VM-Speicherrichtlinien angezeigt. Sie können die Tags zum Erstellen von Speicherrichtlinien verwenden.

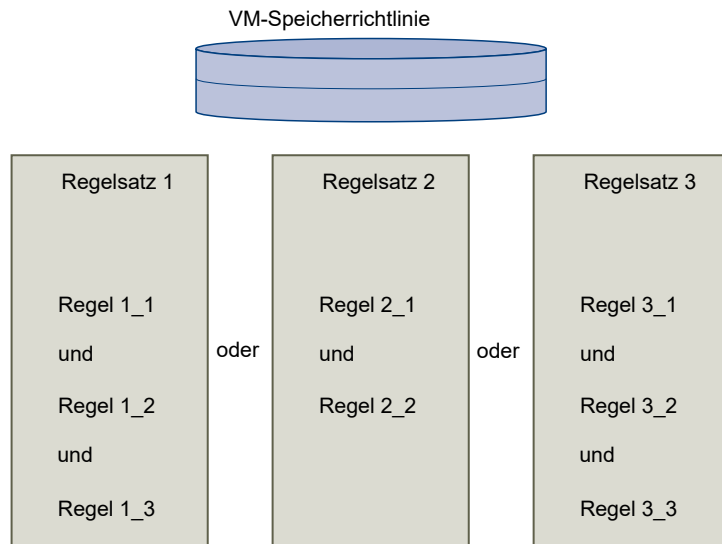
## Informationen zu datenspeicherspezifischen und gemeinsamen Regelsätzen

Eine Speicherrichtlinie kann einen oder mehrere Regelsätze enthalten, die Anforderungen für die Speicherressourcen der virtuellen Maschinen beschreiben. Sie kann auch gemeinsame Regeln enthalten.

Falls gemeinsame Regeln in Ihrer Umgebung nicht verfügbar sind oder nicht definiert sind, können Sie eine Richtlinie erstellen, die datenspeicherspezifische Regelsätze enthält. Zum Definieren einer Richtlinie ist nur ein einziger Regelsatz erforderlich. Zusätzliche Regelsätze sind optional. Mehrere Regelsätze ermöglichen eine einzelne Richtlinie, die alternative Auswahlparameter definiert, oft von mehreren Speicheranbietern.

Ein einzelner Regelsatz enthält eine oder mehrere Regeln. Jede Regel kann auf einem einzigen zugrunde liegenden Datendienst basieren, der von einem Speicherelement garantiert wird. Die Regel beschreibt eine bestimmte Qualität oder Quantität, die von einer Speicherressource bereitgestellt werden muss. Sie können in den Regeln auch auf benutzerdefinierte Datenspeicher-Tags verweisen. Ein datenspeicherspezifischer Regelsatz kann mehrere Regeln von nur einem Speicherelement enthalten.

Die Beziehung zwischen allen Regelsätzen innerhalb einer Richtlinie wird durch den booleschen Operator ODER definiert, während die Beziehung zwischen allen Regeln innerhalb eines Regelsatzes durch den booleschen Operator UND definiert wird. Die Einhaltung aller Regeln eines bestimmten Regelsatzes reicht aus, um die gesamte Richtlinie zu erfüllen. Jeder Regelsatz stellt einen gleichermaßen akzeptablen Einschränkungssatz dar.



Falls gemeinsame Regeln aktiviert sind, ist die Richtlinie erforderlich, um gemeinsame Regeln oder mindestens einen datenspeicherspezifischen Regelsatz einzubeziehen. Wenn Sie sowohl gemeinsame Regeln als auch datenspeicherspezifische Regeln definieren, stimmt die Speicherrichtlinie mit Datenspeichern überein, die alle gemeinsamen Regeln und alle Regeln in mindestens einem der Regelsätze erfüllen.

## Arbeiten mit VM-Speicherrichtlinien

Der Vorgang zum Erstellen und Verwalten von Speicherrichtlinien umfasst üblicherweise mehrere Schritte. Ob die einzelnen Schritte ausgeführt müssen, hängt möglicherweise vom Speichertyp oder den Datendiensten in Ihrer Umgebung ab.

- 1 Wenn Sie Speicherrichtlinien mit Speicheranbietern verwenden, überprüfen Sie, ob der betreffende Speicheranbieter registriert ist. Zu den Elementen, für die Speicheranbieter erforderlich sind, zählen Virtual SAN, Virtual Volumes und E/A-Filter, die für virtuelle Maschinen zusätzliche Softwaredatendienste bereitstellen.

Weitere Informationen hierzu finden Sie unter [Kapitel 25 Verwenden von Speicheranbietern](#).

- 2 Wenden Sie Speicher-Tags auf Datenspeicher an. Weitere Informationen hierzu finden Sie unter [Zuweisen von Tags zu Datenspeichern](#).
- 3 Erstellen Sie Speicherrichtlinien, indem Sie Anforderungen für Anwendungen definieren, die auf einer virtuellen Maschine ausgeführt werden. Weitere Informationen hierzu finden Sie unter [Definieren einer Speicherrichtlinie für eine virtuelle Maschine](#).
- 4 Wenden Sie die VM-Speicherrichtlinie auf eine virtuelle Maschine an. Sie können die Speicherrichtlinie anwenden, wenn Sie die virtuelle Maschine bereitstellen oder deren virtuelle Festplatten konfigurieren. Weitere Informationen hierzu finden Sie unter [Zuweisen von Speicherrichtlinien zu virtuellen Maschinen](#).



- 5 Ändern Sie die Speicherrichtlinie für die Home-Dateien der virtuellen Maschine oder für virtuelle Festplatten. Weitere Informationen hierzu finden Sie unter [Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten](#).
- 6 Stellen Sie sicher, dass virtuelle Maschinen und virtuelle Festplatten Datenspeicher verwenden, die der ihnen zugewiesenen Speicherrichtlinie entsprechen. Weitere Informationen hierzu finden Sie unter [Prüfen der Übereinstimmung für eine VM-Speicherrichtlinie](#).

## Erstellen und Verwalten von VM-Speicherrichtlinien

Zum Aktivieren, Erstellen und Verwalten von Speicherrichtlinien für virtuelle Maschinen verwenden Sie in der Regel die Schnittstelle für VM-Speicherrichtlinien des vSphere Web Client.

Wenn Sie Speicherrichtlinien mit Virtual SAN, virtuellen Volumes oder E/A-Filtern verwenden, finden Sie in der folgenden Dokumentation weitere Informationen:

- *Verwalten von VMware Virtual SAN*
- [Kapitel 19 Arbeiten mit virtuellen Volumes](#)
- [Kapitel 21 Filtern der E/A einer virtuellen Maschine](#)

## Zuweisen von Tags zu Datenspeichern

Wenn Ihr Datenspeicher nicht durch einen Speicheranbieter repräsentiert wird und nicht seine Funktionen und Datendienste auf der Benutzeroberfläche „VM-Speicherrichtlinien“ anzeigt, verwenden Sie Tags, um Informationen über den Datenspeicher zu kodieren. Sie können beim Definieren einer Speicherrichtlinie für eine virtuelle Maschine auf diese Tags verweisen.

Sie können ein neues Tag anwenden, das Speicherinformationen zu einem Datenspeicher enthält. Informationen über Tags, deren Kategorien und über das Verwalten von Tags finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

### Verfahren

- 1 Gehen Sie zu einem Datenspeicher im vSphere Web Client-Navigator.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und klicken Sie auf **Tags**.
- 3 Klicken Sie auf das Symbol **Neues Tag**.
- 4 Wählen Sie im Dropdown-Menü **vCenter Server** die vCenter Server-Instanz aus, für die Sie dieses Tag erstellen möchten.
- 5 Geben Sie einen Namen und eine Beschreibung für das Tag ein.

Sie können beispielsweise eine umfassende Speicherebenenendefinition, wie Gold Storage, angeben oder eine Eigenschaft festlegen, die nicht über den Speicheranbieter übertragen wird, wie den geografischen Standort oder die Administratorengruppe.

Tag-Eigenschaft	Beispiel
Name	Fault Tolerance
Beschreibung	Speicher, der eine Kapazität von mehr als 2 TB aufweist und fehlertolerant ist

- 6 Wählen Sie im Dropdown-Menü **Kategorie** eine vorhandene Kategorie aus oder erstellen Sie eine Kategorie.
- 7 (Optional) Erstellen Sie eine Kategorie:
  - a Wählen Sie **Neue Kategorie** aus.
  - b Geben Sie die Kategorieoptionen an.

Kategorieeigenschaften	Beispiel
Kategorienname	Speicherkategorie
Beschreibung	Kategorie für Tags, die mit dem Speicher zusammenhängen
Kardinalität	<b>Viele Tags pro Objekt</b>
Zuweisbare Objekttypen	<b>Datenspeicher</b> und <b>Datenspeicher-Cluster</b>

- 8 Klicken Sie auf **OK**.

### Ergebnisse

Das neue Tag wird dem Datenspeicher zugewiesen und auf der Registerkarte **Übersicht** des Datenspeichers im Fenster „Tags“ eingeblendet.

### Nächste Schritte

Sie können beim Hinzufügen tagbasierter Regeln zur Speicherrichtlinie auf das Tag verweisen. Siehe [Hinzufügen oder Bearbeiten Tag-basierter Regeln](#). Der Datenspeicher wird in einer Liste kompatibler Speicherressourcen für virtuelle Maschinen angezeigt, die die Richtlinie verwenden.

## Definieren einer Speicherrichtlinie für eine virtuelle Maschine

Beim Definieren von Speicherrichtlinien für virtuelle Maschinen geben Sie die Speicheranforderungen für die Anwendungen an, die auf den virtuellen Maschinen ausgeführt werden.

Speicherrichtlinien können auf von Speicherelementen angekündigten Datendiensten oder auf Datenspeicher-Tags basieren. Die Richtlinie kann auch auf gemeinsame Datendienste verweisen, die vom E/A-Filter-Framework bereitgestellt werden.

### Voraussetzungen

- Bei der Verwendung von VM-Speicherrichtlinien zusammen mit Speicheranbietern müssen Sie sicherstellen, dass ein geeigneter Speicheranbieter registriert ist. Weitere Informationen hierzu finden Sie unter [Kapitel 25 Verwenden von Speicheranbietern](#).

- Erforderliche Berechtigungen: **VM-Speicherrichtlinien.Aktualisieren** und **VM-Speicherrichtlinien.Anzeigen**.

## Verfahren

### 1 Starten des Erstellungsvorgangs für eine VM-Speicherrichtlinie

Verwenden Sie zum Definieren einer VM-Speicherrichtlinie den Assistenten **Neue VM-Speicherrichtlinie erstellen**.

### 2 Definieren gemeinsamer Regeln für eine VM-Speicherrichtlinie

Gemeinsame Regeln basieren auf Datendiensten, die allen Speichertypen gemeinsam sind und nicht von einem bestimmten Datenspeicher abhängig sind. Diese Datendienste werden in der Schnittstelle für VM-Speicherrichtlinien bei der Installation von E/A-Filtern von Drittanbietern verfügbar, die über vSphere APIs für E/A-Filter entwickelt werden. Auf diese Datendienste kann in einer Speicherrichtlinie verwiesen werden.

### 3 Erstellen speicherspezifischer Regeln für eine VM-Speicherrichtlinie

Datenspeicherspezifische Regeln basieren auf Datendiensten, die Speicherelemente wie Virtual SAN und virtuelle Volumes anbieten. Der Datenspeicher garantiert der virtuellen Maschine, die diese Richtlinie verwendet, dass er ihre Speicheranforderungen erfüllt. Der Datenspeicher sorgt auch dafür, dass bestimmte Merkmale für Kapazität, Leistung, Verfügbarkeit, Redundanz usw. bereitgestellt werden können.

### 4 Hinzufügen oder Bearbeiten Tag-basierter Regeln

Wenn Sie eine Speicherrichtlinie für virtuelle Maschinen definieren oder bearbeiten, können Sie eine Regel erstellen oder ändern, die Tags für bestimmte Datenspeicher referenziert. Die Datenspeicher werden mit diesem Speicherrichtlinientyp kompatibel.

### 5 Beenden der Erstellung einer VM-Speicherrichtlinie

Sie können die Liste der mit der VM-Speicherrichtlinie kompatiblen Datenspeicher prüfen und gewünschte Speicherrichtlinieneinstellungen ändern.

## Nächste Schritte

Diese Speicherrichtlinien können auf virtuelle Maschinen angewendet werden. Bei objektbasierter Speicherung wie Virtual SAN und virtuellen Volumes können Sie eine Speicherrichtlinie dieser Art als Standard festlegen.

## Starten des Erstellungsvorgangs für eine VM-Speicherrichtlinie

Verwenden Sie zum Definieren einer VM-Speicherrichtlinie den Assistenten **Neue VM-Speicherrichtlinie erstellen**.

## Verfahren

### 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.

### 2 Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen**.

- 3 Wählen Sie die vCenter Server-Instanz aus.
- 4 Geben Sie einen Namen und eine Beschreibung für die Speicherrichtlinie ein.

## Definieren gemeinsamer Regeln für eine VM-Speicherrichtlinie

Gemeinsame Regeln basieren auf Datendiensten, die allen Speichertypen gemeinsam sind und nicht von einem bestimmten Datenspeicher abhängig sind. Diese Datendienste werden in der Schnittstelle für VM-Speicherrichtlinien bei der Installation von E/A-Filtern von Drittanbietern verfügbar, die über vSphere APIs für E/A-Filter entwickelt werden. Auf diese Datendienste kann in einer Speicherrichtlinie verwiesen werden.

### Verfahren

- 1 Wählen Sie auf der Seite „Gemeinsame Regeln“ die Option **Gemeinsame Regeln in der VM-Speicherrichtlinie verwenden** aus, um gemeinsame Regeln zu aktivieren.
- 2 Wählen Sie im Dropdown-Menü **Regel hinzufügen** einen Datendienst aus, der in die Regel einbezogen werden soll.
- 3 Wählen Sie einen Anbieter für den Datendienst aus.  
  
Wenn ein bestimmter Datendienst, wie z. B. die Replizierung, von verschiedenen Anbietern bereitgestellt wird, können Sie nur eine Regel hinzufügen, die sich auf diesen Datendienst bezieht.
- 4 Geben Sie Werte für die Regel an und klicken Sie auf **Weiter**.

## Erstellen speicherspezifischer Regeln für eine VM-Speicherrichtlinie

Datenspeicherspezifische Regeln basieren auf Datendiensten, die Speicherelemente wie Virtual SAN und virtuelle Volumes anbieten. Der Datenspeicher garantiert der virtuellen Maschine, die diese Richtlinie verwendet, dass er ihre Speicheranforderungen erfüllt. Der Datenspeicher sorgt auch dafür, dass bestimmte Merkmale für Kapazität, Leistung, Verfügbarkeit, Redundanz usw. bereitgestellt werden können.

Ein datenspeicherspezifischer Regelsatz kann mehrere Regeln von nur einem Speicherelement enthalten.

### Voraussetzungen

Wenn Ihre Umgebung Speicherelemente wie Virtual SAN oder virtuelle Volumes enthält, prüfen Sie diese Funktionen. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware Virtual SAN* und unter [Kapitel 19 Arbeiten mit virtuellen Volumes](#).

### Verfahren

- 1 Wählen Sie auf der Seite „Regelsatz“ im Dropdown-Menü **Regeln basierend auf Datendiensten** einen Speicheranbieter, zum Beispiel Virtual SAN oder virtuelle Volumes, aus.  
  
Die Seite wird um die von der Speicherressource bereitgestellten Datendienste erweitert.

- 2 Wählen Sie einen Datendienst aus und geben Sie dessen Werte an.

Stellen Sie sicher, dass die eingegebenen Werte innerhalb des vom Datendienstprofil der Speicherressource angegebenen Wertebereichs liegen.

Anhand Ihrer Eingabe berechnet der Speicherbelegungsmechanismus den Speicherplatz, der für eine virtuelle Festplatte erforderlich ist, die sich auf diesem Speicherelement befindet.

- 3 (Optional) Fügen Sie Tag-basierte Regeln hinzu.

- 4 Klicken Sie auf **Weiter**.

## Hinzufügen oder Bearbeiten Tag-basierter Regeln

Wenn Sie eine Speicherrichtlinie für virtuelle Maschinen definieren oder bearbeiten, können Sie eine Regel erstellen oder ändern, die Tags für bestimmte Datenspeicher referenziert. Die Datenspeicher werden mit diesem Speicherrichtlinientyp kompatibel.

Sie können einem Regelsatz, der speicherspezifische Regeln enthält, Tag-basierte Regeln hinzufügen oder einen separaten Regelsatz mit nur Tag-basierten Regeln erstellen. Wenn Sie Tags in den Richtlinien verwenden, befolgen Sie die folgenden Leitlinien:

- Wenn der Regelsatz andere speicherspezifische Regeln enthält, muss der Datenspeicher mit dem zugewiesenen Tag alle Regeln im Regelsatz erfüllen.
- Wenn Sie mehrere Tags aus der gleichen Kategorie innerhalb der gleichen Regel hinzufügen, werden die Tags als alternative Einschränkungen behandelt. Es kann ein beliebiger der Tags erfüllt werden.
- Wenn Sie die Tags in getrennten Regeln im gleichen Regelsatz hinzufügen, müssen alle Tags erfüllt werden.

### Voraussetzungen

Erstellen Sie Speicher-Tags und wenden Sie sie auf Datenspeicher an. Weitere Informationen hierzu finden Sie unter [Zuweisen von Tags zu Datenspeichern](#).

### Verfahren

- 1 Verwenden Sie die Seite „Regelsatz“ zum Hinzufügen oder Bearbeiten einer Tag-basierten Regel:
  - Um eine Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Tag-basierte Regel hinzufügen**.
  - Um eine vorhandene Regel zu ändern, wählen Sie die Regel aus und klicken Sie auf das Symbol **Regel ändern**.
- 2 Geben Sie eine Kategorie an.
- 3 Nehmen Sie eine Tag-Auswahl vor oder bearbeiten Sie eine vorhandene Auswahl.

### Ergebnisse

Datenspeicher, die die ausgewählten Tags verwenden, sind mit der Speicherrichtlinie kompatibel.

## Beenden der Erstellung einer VM-Speicherrichtlinie

Sie können die Liste der mit der VM-Speicherrichtlinie kompatiblen Datenspeicher prüfen und gewünschte Speicherrichtlinieneinstellungen ändern.

### Verfahren

- 1 Überprüfen Sie auf der Seite „Speicherkompatibilität“ die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen, und klicken Sie auf **Weiter**.

Um kompatibel zu sein, muss der Datenspeicher mindestens einen Regelsatz sowie alle Regeln in diesem Regelsatz erfüllen.

- 2 Überprüfen Sie die Speicherrichtlinieneinstellungen und nehmen Sie Änderungen vor, indem Sie über **Zurück** auf die betreffende Seite zurückkehren.
- 3 Klicken Sie auf **Beenden**.

### Ergebnisse

Die VM-Speicherrichtlinie wird in der Liste angezeigt.

## Löschen einer VM-Speicherrichtlinie

Sie können eine Speicherrichtlinie löschen, die Sie nicht für virtuelle Maschinen oder virtuelle Festplatten verwenden.

### Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Wählen Sie auf der Benutzeroberfläche „VM-Speicherrichtlinien“ eine Richtlinie aus, die Sie löschen möchten, und klicken Sie auf das Symbol **VM-Speicherrichtlinie löschen (X)**.
- 3 Klicken Sie auf **Ja**.

### Ergebnisse

Die Richtlinie wird aus der Bestandsliste entfernt.

## Bearbeiten oder Klonen einer VM-Speicherrichtlinie

Wenn sich die Speicheranforderungen für virtuelle Maschinen und virtuelle Festplatten ändern, können Sie die Speicherrichtlinie bearbeiten. Außerdem können Sie durch Klonen eine Kopie der bestehenden VM-Speicherrichtlinie erstellen. Beim Klonen können Sie optional wählen, ob die zugrunde liegende Speicherrichtlinie angepasst werden soll.

### Voraussetzungen

Erforderliche Berechtigung: **StorageProfile.View**

## Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Wählen Sie eine Speicherrichtlinie aus und klicken Sie auf eines der folgenden Symbole:
  - **VM-Speicherrichtlinie bearbeiten**
  - **VM-Speicherrichtlinie klonen**
- 3 (Optional) Ändern Sie die Richtlinie und klicken Sie auf **OK**.
- 4 Wenn die Speicherrichtlinie, die Sie bearbeiten, von einer virtuellen Maschine verwendet wird, wenden Sie die Richtlinie erneut auf die virtuelle Maschine an.

Option	Beschreibung
Manuell später	Wenn Sie diese Option auswählen, wird der Übereinstimmungsstatus für alle virtuellen Festplatten und für alle Home-Objekte der virtuellen Maschine, die der Speicherrichtlinie zugeordnet sind, in „Veraltet“ geändert. Um die Konfiguration und die Übereinstimmung zu aktualisieren, wenden Sie die Speicherrichtlinie manuell erneut auf alle verknüpften Elemente an. Weitere Informationen hierzu finden Sie unter <a href="#">Erneutes Anwenden der VM-Speicherrichtlinien</a> .
Jetzt	Aktualisieren Sie die virtuelle Maschine und den Übereinstimmungsstatus unmittelbar nach der Bearbeitung der Speicherrichtlinie.

## Speicherrichtlinien und virtuelle Maschinen

Nach dem Definieren einer VM-Speicherrichtlinie können Sie sie auf eine virtuelle Maschine anwenden. Die Speicherrichtlinie wird angewendet, wenn Sie die virtuelle Maschine bereitstellen oder deren virtuelle Festplatten konfigurieren. Abhängig von Typ und Konfiguration kann die Richtlinie unterschiedlichen Zwecken dienen. Sie kann den am besten geeigneten Datenspeicher für die virtuelle Maschine auswählen und die erforderliche Dienstebene durchsetzen oder spezifische Datendienste für die virtuelle Maschine und deren Festplatten aktivieren.

Wenn Sie die Speicherrichtlinie nicht angeben, verwendet das System die Standardspeicherrichtlinie des Datenspeichers. Wenn sich Ihre Speicheranforderungen für die Anwendungen auf der virtuellen Maschine ändern, können Sie die ursprünglich zugewiesene Speicherrichtlinie entsprechend bearbeiten.

### Standardspeicherrichtlinien

Wenn Sie eine virtuelle Maschine auf einem objektbasierten Datenspeicher wie z. B. Virtual SAN oder virtuellen Volumes bereitstellen, müssen Sie der virtuellen Maschine eine entsprechende Speicherrichtlinie für virtuelle Maschinen zuweisen, die mit dem Datenspeicher kompatibel ist. Diese Zuweisung gewährleistet die optimale Platzierung für Objekte virtueller Maschinen innerhalb des objektbasierten Speichers. Wenn Sie der virtuellen Maschine nicht ausdrücklich eine Speicherrichtlinie zuweisen, verwendet das System eine Standardspeicherrichtlinie, die dem

Datenspeicher zugeordnet ist. Die Standardrichtlinie wird auch verwendet, wenn die zugewiesene Richtlinie keine spezifischen Regeln für virtuelle Volumes oder Virtual SAN enthält.

Die Standardspeicherrichtlinien für Virtual SAN und virtuelle Volumes können von VMware bereitgestellt werden oder benutzerdefiniert sein. VMFS- und NFS-Datenspeicher haben keine Standardspeicherrichtlinien.

## Von VMware bereitgestellte Standardrichtlinien

VMware bietet Standardspeicherrichtlinien für Virtual SAN und virtuelle Datenspeicher.

### Standardspeicherrichtlinie für Virtual SAN

Die von VMware angebotene Standardspeicherrichtlinie wird auf alle VM-Objekte angewendet, die auf einem Datenspeicher für Virtual SAN bereitgestellt sind, wenn Sie keine andere Richtlinie für Virtual SAN auswählen.

Die von VMware angebotene Richtlinie weist die folgenden Eigenschaften auf:

- Sie können die Richtlinie nicht löschen.
- Die Richtlinie lässt sich bearbeiten. Zum Bearbeiten der Richtlinie müssen Sie über die Speicherrichtlinienberechtigungen verfügen, die das Anzeigen und Aktualisieren zulassen.
- Beim Bearbeiten der Richtlinie können Sie den Namen der Richtlinie oder die Spezifikation des Speicheranbieters für Virtual SAN nicht ändern. Alle anderen Parameter einschließlich der Regeln sind bearbeitbar.
- Sie können die Standardrichtlinie klonen und als Vorlage zum Erstellen einer Speicherrichtlinie verwenden.
- Die Standardrichtlinie für Virtual SAN ist nur zu Datenspeichern für Virtual SAN kompatibel.
- Sie können eine VM-Speicherrichtlinie für Virtual SAN erstellen und als Standard festlegen.

### Standardspeicherrichtlinie für virtuelle Volumes

Für virtuelle Volumes bietet VMware eine Standardspeicherrichtlinie, die keine Regeln oder Speicheranforderungen enthält. Wie bei Virtual SAN wird diese Richtlinie auf VM-Objekte angewendet, wenn Sie keine andere Richtlinie für die virtuelle Maschine festlegen, die Sie auf dem virtuellen Datenspeicher platzieren. Mit der Richtlinie „Keine Anforderungen“ können Speicher-Arrays die optimale Platzierung für die VM-Objekte bestimmen.

Die von VMware angebotene Standardrichtlinie für virtuelle Volumes weist die folgenden Eigenschaften auf:

- Sie können diese Richtlinie nicht löschen, bearbeiten oder klonen.
- Die Standardrichtlinie für virtuelle Volumes ist nur zu virtuellen Datenspeichern kompatibel.
- Sie können eine VM-Speicherrichtlinie für virtuelle Volumes erstellen und als Standard festlegen.



## Benutzerdefinierte Standardrichtlinien für VM-Speicher

Sie können eine mit Virtual SAN oder virtuellen Volumes kompatible VM-Speicherrichtlinie erstellen und als Standardrichtlinie für Virtual SAN und virtuelle Datenspeicher festlegen. Die benutzerdefinierte Speicherrichtlinie ersetzt die Standardspeicherrichtlinie von VMware.

Jedes Virtual SAN und jeder Datenspeicher können nur jeweils eine Standardrichtlinie aufweisen. Sie können allerdings eine VM-Speicherrichtlinie erstellen, die mit mehreren Virtual SAN- oder Virtual Volume-Datenspeichern kompatibel ist, und diese als Standardrichtlinie für alle Datenspeicher festlegen.

Wenn die VM-Speicherrichtlinie zur Standardrichtlinie eines Datenspeichers wird, können Sie sie nur dann löschen, wenn Sie sie vom Datenspeicher abtrennen.

## Ändern der Standardspeicherrichtlinie für einen Datenspeicher

Für virtuelle Volumes und Datenspeicher für Virtual SAN bietet VMware Speicherrichtlinien, die beim Bereitstellen von virtuellen Maschinen als Standard verwendet werden. Sie können die Standardspeicherrichtlinie für ausgewählte virtuelle Volumes oder einen Datenspeicher für Virtual SAN ändern.

### Voraussetzungen

Erstellen Sie eine Speicherrichtlinie, die kompatibel mit virtuellen Volumes oder Virtual SAN ist. Sie können eine Richtlinie erstellen, die für beide Speicherarten geeignet ist.

### Verfahren

- 1 Wählen Sie im vSphere Web Client-Navigator **Globale Bestandslisten > Datenspeicher** aus.
- 2 Klicken Sie auf den Datenspeicher.
- 3 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 4 Klicken Sie auf **Allgemein** und dann im Bereich „Standardspeicherrichtlinie“ auf **Bearbeiten**.
- 5 Wählen Sie in der Liste der verfügbaren Speicherrichtlinien eine Richtlinie aus, die als Standard verwendet werden soll, und klicken Sie auf **OK**.

### Ergebnisse

Die ausgewählte Speicherrichtlinie wird zur Standardrichtlinie für den Datenspeicher. vSphere weist diese Richtlinie jedem VM-Objekt zu, das Sie im Datenspeicher bereitstellen, wenn keine andere Richtlinie ausgewählt ist.

## Zuweisen von Speicherrichtlinien zu virtuellen Maschinen

Sie können eine VM-Speicherrichtlinie beim anfänglichen Bereitstellen einer virtuellen Maschine oder beim Durchführen anderer VM-Vorgänge, wie Klonen oder Migrieren, zuweisen.

Bei diesem Thema wird beschrieben, wie Sie die VM-Speicherrichtlinie beim Erstellen einer virtuellen Maschine zuweisen. Informationen zu anderen Bereitstellungsmethoden, wie Klonen, Bereitstellung über eine Vorlage usw., finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Sie können dieselbe Speicherrichtlinie auf die Konfigurationsdatei der virtuellen Maschine und alle ihre virtuellen Festplatten anwenden. Wenn Sie unterschiedliche Speicheranforderungen an die Konfigurationsdatei und die virtuellen Festplatten haben, können sie ihnen auch eigene Speicherrichtlinien zuweisen.

## Verfahren

- 1 Starten Sie im vSphere Web Client den Bereitstellungsvorgang für die virtuelle Maschine und führen Sie die entsprechenden Schritte aus.
- 2 Weisen Sie allen VM-Dateien und Festplatten dieselbe Speicherrichtlinie zu.
  - a Wählen Sie auf der Seite „Speicher auswählen“ eine Speicherrichtlinie aus dem Dropdown-Menü **VM-Speicherrichtlinie** aus.

Je nach ihrer Konfiguration teilt die Speicherrichtlinie alle Datenspeicher in kompatible und inkompatible Sätze auf. Wenn die Richtlinie auf Datendienste verweist, die von einem speziellen Speicherelement, wie zum Beispiel virtuellen Volumes, angeboten werden, enthält die kompatible Liste Datenspeicher, die nur diesen Speichertyp darstellen.

- b Wählen Sie einen geeigneten Datenspeicher in der Liste kompatibler Datenspeicher aus und klicken Sie auf **Weiter**.

Der Datenspeicher wird zum Zielspeicherelement für die VM-Konfigurationsdatei und alle virtuellen Festplatten.

- 3 Ändern Sie die VM-Speicherrichtlinie für den virtuellen Datenträger.

Verwenden Sie diese Option, wenn Sie für virtuelle Festplatten andere Anforderungen bezüglich der Speicherplatzierung haben. Sie können diese Option auch verwenden, wenn Sie Software-Datendienste, wie beispielsweise Zwischenspeichern oder Replizierung, für Ihre virtuellen Festplatten aktivieren müssen.

- a Erweitern Sie auf der Seite „Hardware anpassen“ den Ansichtsbereich **Neue Festplatte**.
  - b Wählen Sie im Dropdown-Menü **VM-Speicherrichtlinie** die der virtuellen Festplatte zuzuweisende Speicherrichtlinie aus.
  - c (Optional) Ändern Sie den Speicherort der virtuellen Festplatte.

Verwenden Sie diese Option zum Speichern des virtuellen Datenträgers auf einem anderen Datenspeicher als demjenigen, auf dem sich die VM-Konfigurationsdatei befindet.

- 4 Schließen Sie die Bereitstellung der virtuellen Maschine ab.

## Ergebnisse

Nach der Erstellung der virtuellen Maschine zeigt die Registerkarte **Übersicht** die zugewiesenen Speicherrichtlinien und deren Übereinstimmungsstatus an.

## Nächste Schritte

Wenn sich die Speicherplatzierungsanforderungen für die Konfigurationsdatei oder die virtuellen Festplatten zu einem späteren Zeitpunkt ändern sollten, können Sie die Zuweisung der VM-Richtlinie entsprechend anpassen.

## Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten

Wenn Ihre Speicheranforderungen für die Anwendungen auf der virtuellen Maschine sich ändern, können Sie die Speicherrichtlinie bearbeiten, die ursprünglich auf die virtuelle Maschine angewendet wurde.

Sie können die Speicherrichtlinie für eine ausgeschaltete oder eingeschaltete virtuelle Maschine bearbeiten.

Beim Ändern der VM-Speicherrichtlinienzuweisung können Sie dieselbe Speicherrichtlinie auf die Konfigurationsdatei der virtuellen Maschine und alle ihre virtuellen Festplatten anwenden. Wenn Sie unterschiedliche Speicheranforderungen an die Konfigurationsdatei und die virtuellen Festplatten haben, können Sie ihnen auch eigene Speicherrichtlinien zuweisen.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf **Richtlinien**.
- 3 Klicken Sie auf **Speicher**.
- 4 Klicken Sie auf **VM-Speicherrichtlinie bearbeiten**.
- 5 Legen Sie die VM-Speicherrichtlinie für Ihre virtuelle Maschine fest.

Option	Beschreibung
<b>Wenden Sie dieselbe Speicherrichtlinie auf alle VM-Objekte an.</b>	a Wählen Sie die Richtlinie aus dem Dropdown-Menü <b>VM-Speicherrichtlinie</b> aus.
	b Klicken Sie auf <b>Auf alle anwenden</b> .
<b>Wenden Sie auf das VM-Home-Objekt und virtuelle Festplatten unterschiedliche Speicherrichtlinien an.</b>	a Markieren Sie das Objekt.
	b Wählen Sie die Richtlinie aus dem Dropdown-Menü <b>VM-Speicherrichtlinie</b> für das Objekt aus.

- 6 Klicken Sie auf **OK**.

### Ergebnisse

Die Speicherrichtlinie wird der virtuellen Maschine und ihren Festplatten zugeordnet.

## Überwachen der Speicherübereinstimmung für virtuelle Maschinen

Wenn Sie eine Richtlinie Objekten von virtuellen Maschinen zuordnen und die Datenspeicher auswählen, auf denen die virtuellen Maschinen und die virtuellen Festplatten ausgeführt werden,

können Sie prüfen, ob die virtuellen Maschinen und die virtuellen Festplatten Datenspeicher verwenden, die mit der Richtlinie übereinstimmen.

Wenn Sie die Übereinstimmung einer virtuellen Maschine prüfen, bei deren Host oder Cluster Speicherrichtlinien deaktiviert sind, wird als Ergebnis der Prüfung „Keine Übereinstimmung“ ausgegeben, da die Funktion deaktiviert ist.

### Voraussetzungen

Zum Durchführen einer Übereinstimmungsprüfung für eine Speicherrichtlinie ordnen Sie die Richtlinie mindestens einer virtuellen Maschine oder virtuellen Festplatte zu.

### Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Doppelklicken Sie auf eine Speicherrichtlinie.
- 3 Klicken Sie auf die Registerkarte **Überwachen** und dann auf **VMs und virtuelle Festplatten**.
- 4 Klicken Sie auf **Überprüfung der Einhaltung von VM-Speicherrichtlinien auslösen**.

In der Spalte „Übereinstimmungsstatus“ wird der Übereinstimmungsstatus des Speichers für virtuelle Maschinen und deren Richtlinien angezeigt.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, der von der virtuellen Maschine oder virtuellen Festplatte verwendet wird, hat die Speicherfunktionen, die die Richtlinie erfordert.
Nicht übereinstimmend	Der Datenspeicher unterstützt festgelegte Speichieranforderungen, kann jedoch zurzeit nicht die Speicherrichtlinie der virtuellen Maschine erfüllen. Der Status kann z. B. in „Keine Übereinstimmung“ wechseln, wenn physische Ressourcen, auf denen der Datenspeicher gesichert wird, nicht verfügbar oder erschöpft sind. Sie können die Übereinstimmung des Datenspeichers wiederherstellen, indem Sie Änderungen an der physischen Konfiguration vornehmen, beispielsweise indem Sie Hosts oder Festplatten zum Cluster hinzufügen. Wenn weitere Ressourcen die Speicherrichtlinie der virtuellen Maschine erfüllen, ändert sich der Status in „Übereinstimmung“.
Veraltet	Der Status gibt an, dass die Richtlinie bearbeitet wurde, aber die neuen Anforderungen wurden nicht an den Datenspeicher weitergegeben, in dem sich die Objekte der virtuellen Maschine befinden. Um die Änderungen zu kommunizieren, wenden Sie die Richtlinie erneut auf die veralteten Objekte an.
Nicht anwendbar	Diese Speicherrichtlinie verweist auf Datenspeicherfunktionen, die vom Datenspeicher, in dem sich die virtuelle Maschine befindet, nicht unterstützt werden.

### Nächste Schritte

Wenn Sie für den Datenspeicher mit dem Status „Keine Übereinstimmung“ die Übereinstimmung nicht wiederherstellen können, migrieren Sie die Dateien oder virtuellen Festplatten in einen kompatiblen Datenspeicher. Weitere Informationen hierzu finden Sie unter [Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine](#).

Wenn der Status „Veraltet“ lautet, wenden Sie die Richtlinie erneut auf die Objekte an. Weitere Informationen hierzu finden Sie unter [Erneutes Anwenden der VM-Speicherrichtlinien](#).

## Prüfen der Übereinstimmung für eine VM-Speicherrichtlinie

Sie können prüfen, ob der Datenspeicher einer virtuellen Maschine mit den in der VM-Speicherrichtlinie festgelegten Speicheranforderungen kompatibel ist.

### Voraussetzungen

Stellen Sie sicher, dass der virtuellen Maschine eine Speicherrichtlinie zugeordnet ist.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option **VM-Richtlinien > Einhaltung der VM-Speicherrichtlinien prüfen**.

Das System verifiziert die Übereinstimmung.

- 3 Klicken Sie auf die Registerkarte **Übersicht** für die virtuelle Maschine.
- 4 Prüfen Sie den Übereinstimmungsstatus im Bereich „VM-Speicherrichtlinien“ an.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, der von der virtuellen Maschine oder virtuellen Festplatte verwendet wird, hat die Speicherfunktionen, die die Richtlinie erfordert.
Nicht übereinstimmend	Der Datenspeicher unterstützt festgelegte Speicheranforderungen, kann jedoch zurzeit nicht die Speicherrichtlinie der virtuellen Maschine erfüllen. Der Status kann z. B. in „Keine Übereinstimmung“ wechseln, wenn physische Ressourcen, auf denen der Datenspeicher gesichert wird, nicht verfügbar oder erschöpft sind. Sie können die Übereinstimmung des Datenspeichers wiederherstellen, indem Sie Änderungen an der physischen Konfiguration vornehmen, beispielsweise indem Sie Hosts oder Festplatten zum Cluster hinzufügen. Wenn weitere Ressourcen die Speicherrichtlinie der virtuellen Maschine erfüllen, ändert sich der Status in „Übereinstimmung“.
Veraltet	Der Status gibt an, dass die Richtlinie bearbeitet wurde, aber die neuen Anforderungen wurden nicht an den Datenspeicher weitergegeben, in dem sich die Objekte der virtuellen Maschine befinden. Um die Änderungen zu kommunizieren, wenden Sie die Richtlinie erneut auf die veralteten Objekte an.
Nicht anwendbar	Diese Speicherrichtlinie verweist auf Datenspeicherfunktionen, die vom Datenspeicher, in dem sich die virtuelle Maschine befindet, nicht unterstützt werden.

### Nächste Schritte

Wenn Sie für den Datenspeicher mit dem Status „Keine Übereinstimmung“ die Übereinstimmung nicht wiederherstellen können, migrieren Sie die Dateien oder virtuellen Festplatten in einen kompatiblen Datenspeicher. Weitere Informationen hierzu finden Sie unter [Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine](#).

Wenn der Status „Veraltet“ lautet, wenden Sie die Richtlinie erneut auf die Objekte an. Weitere Informationen hierzu finden Sie unter [Erneutes Anwenden der VM-Speicherrichtlinien](#).

## Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine

Ermitteln Sie, welcher Datenspeicher mit der Speicherrichtlinie Ihrer virtuellen Maschine kompatibel ist.

Es kann vorkommen, dass eine einer virtuellen Maschine zugewiesene Speicherrichtlinie den Status „Keine Übereinstimmung“ aufweist. Dieser Status ist ein Hinweis darauf, dass die virtuelle Maschine oder deren Festplatten Datenspeicher verwenden, die nicht mit der Richtlinie kompatibel sind. Sie können die Dateien der virtuellen Maschine und die virtuellen Festplatten in kompatible Datenspeicher migrieren.

Bestimmen Sie mithilfe dieser Aufgabe, welche Datenspeicher die Anforderungen der Richtlinie erfüllen.

### Voraussetzungen

Stellen Sie sicher, dass das Feld **VM-Speicherrichtlinieneinhaltung** auf der Registerkarte **Übersicht** der virtuellen Maschine der Status „Keine Übereinstimmung“ angezeigt wird.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie auf die Registerkarte **Übersicht (Summary)**.  
Im Bereich „VM-Speicherrichtlinien“ wird im Bereich „VM-Speicherrichtlinieneinhaltung“ der Status „Keine Übereinstimmung“ angezeigt.
- 3 Klicken Sie im Bereich **VM-Speicherrichtlinien** auf den Link zur Richtlinie.
- 4 Klicken Sie auf die Registerkarte **Überwachen** und anschließend auf **VMs und virtuelle Festplatten**, um festzustellen, welche Dateien der virtuellen Maschine nicht übereinstimmen.
- 5 Klicken Sie auf **Speicherkompatibilität**.  
Die Liste der Datenspeicher, die den Anforderungen der Richtlinie entsprechen, wird angezeigt.

### Nächste Schritte

Sie können die virtuelle Maschine oder deren Datenträger in einen Datenspeicher aus der Liste migrieren.

## Erneutes Anwenden der VM-Speicherrichtlinien

Nachdem Sie eine Speicherrichtlinie bearbeitet haben, die bereits einem VM-Objekt zugeordnet ist, müssen Sie die Richtlinie erneut anwenden. Durch die erneute Anwendung der Richtlinie teilen Sie dem Datenspeicher, in dem sich das VM-Objekt befindet, neue Speicheranforderungen mit.

## Voraussetzungen

Der Übereinstimmungsstatus für eine virtuelle Maschine lautet „Veraltet“. Der Status gibt an, dass die Richtlinie bearbeitet wurde, aber die neuen Anforderungen wurden nicht an den Datenspeicher weitergegeben.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf **Richtlinien**.
- 3 Vergewissern Sie sich, dass als Übereinstimmungsstatus „Veraltet“ angezeigt wird.
- 4 Klicken Sie auf das Symbol **VM-Speicherrichtlinie erneut anwenden**.
- 5 Prüfen Sie den Übereinstimmungsstatus im Bereich „VM-Speicherrichtlinien“ an.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, der von der virtuellen Maschine oder virtuellen Festplatte verwendet wird, hat die Speicherfunktionen, die die Richtlinie erfordert.
Nicht übereinstimmend	<p>Der Datenspeicher, der von der virtuellen Maschine oder virtuellen Festplatte verwendet wird, hat nicht die Speicherfunktionen, die die Richtlinie erfordert. Sie können anschließend die Dateien der virtuellen Maschine und die virtuellen Festplatten in übereinstimmende Datenspeicher migrieren.</p> <p>Wenn Sie für den Datenspeicher mit dem Status „Keine Übereinstimmung“ die Übereinstimmung nicht wiederherstellen können, migrieren Sie die Dateien oder virtuellen Festplatten in einen kompatiblen Datenspeicher. Siehe <a href="#">Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine</a>.</p>
Nicht anwendbar	Dieser Service-Level für Speicher verweist auf Datenspeicherfunktionen, die von dem Datenspeicher, in dem sich die virtuelle Maschine befindet, nicht unterstützt werden.

# Filtern der E/A einer virtuellen Maschine

# 21

vSphere APIs für E/A-Filter (VAIO) liefern ein Framework, mit dessen Hilfe Drittanbieter als E/A-Filter bezeichnete Softwarekomponenten erstellen können.

Die Filter können auf ESXi-Hosts installiert werden und können virtuellen Maschinen zusätzliche Datendienste anbieten, indem E/A-Anforderungen zwischen dem Gastbetriebssystem einer virtuellen Maschine und virtuellen Festplatten verarbeitet werden.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu E/A-Filtern](#)
- [Verwenden von Flash-Speichergeräten mit Cache-E/A-Filtern](#)
- [Bereitstellen und Konfigurieren von E/A-Filtern in der vSphere-Umgebung](#)
- [Verwalten von E/A-Filtern](#)
- [Richtlinien und empfohlene Vorgehensweisen für E/A-Filter](#)

## Grundlegendes zu E/A-Filtern

E/A-Filter, die virtuellen Festplatten zugeordnet sind, haben direkten Zugriff auf den E/A-Pfad der virtuellen Maschine, und zwar unabhängig von der zugrunde liegenden Speichertopologie.

Die E/A-Filter werden von Drittanbietern erstellt und als Pakete vertrieben, die ein Installationsprogramm zum Bereitstellen von Filterkomponenten auf vCenter Server und ESXi-Hostclustern enthalten.

Nach der Installation des E/A-Filters und der Bereitstellung der zugehörigen Komponenten auf dem ESXi-Cluster konfiguriert und registriert vCenter Server automatisch einen E/A-Filter-Speicheranbieter (wird auch als VASA-Anbieter bezeichnet) für jeden Host im Cluster. Die Speicheranbieter kommunizieren mit vCenter Server und vom E/A-Filter angebotene Datendienste werden in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Beim Erstellen gemeinsamer Regeln für eine VM-Richtlinie können Sie auf diese Datendienste zurückgreifen. Nachdem Sie diese Richtlinie virtuellen Festplatten zugeordnet haben, werden die E/A-Filter auf den virtuellen Festplatten aktiviert.



## E/A-Filtertypen

In der Regel werden E/A-Filter von VMware-Partnern über das vSphere APIs für E/A-Filter (VAIO)-Entwicklerprogramm erstellt. Drittanbieter können E/A-Filter für verschiedene Verwendungszwecke entwickeln.

In dieser Version werden die folgenden Filtertypen unterstützt:

- **Zwischenspeicherung.** Implementiert einen Cache für virtuelle Festplattendaten. Der Filter kann mit einem lokalen Flash-Speichergerät die Daten zwischenspeichern und die E/A-Vorgänge pro Sekunde (IOPS) und die Hardwarenutzungsraten für die virtuelle Festplatte erhöhen. Bei Verwendung des Cache-Filters müssen Sie möglicherweise eine vFlash-Ressource konfigurieren.
- **Replizierung.** Repliziert alle E/A-Schreibvorgänge in einem externen Zielspeicherort, wie beispielsweise auf einem anderen Host oder Cluster.

---

**Hinweis** Sie können mehrere Filter aus derselben Kategorie (z. B. „Zwischenspeicherung“) auf Ihrem ESXi-Host installieren. Pro virtueller Festplatte ist jedoch nur ein Filter aus derselben Kategorie möglich.

---

## E/A-Filterkomponenten

Mehrere Komponenten sind an der E/A-Filterung beteiligt.

Es gibt die folgenden E/A-Filterkomponenten:

### VAIO-Filter-Framework

Eine von ESXi bereitgestellte Kombination aus Benutzer-World und VMkernel-Infrastruktur, mit der VMware-Partner Filter-Plug-Ins zum E/A-Pfad zu und von virtuellen Festplatten hinzufügen können.

### E/A-Filter-Plug-In

Eine von VMware-Partnern entwickelte Softwarekomponente, die E/A-Daten, die zwischen virtuellen Festplatten und Gastbetriebssystemen übertragen werden, abfängt und filtert.

### CIM-Anbieter

Eine von VMware-Partnern entwickelte optionale Komponente, mit der E/A-Filter-Plug-Ins konfiguriert und verwaltet werden.

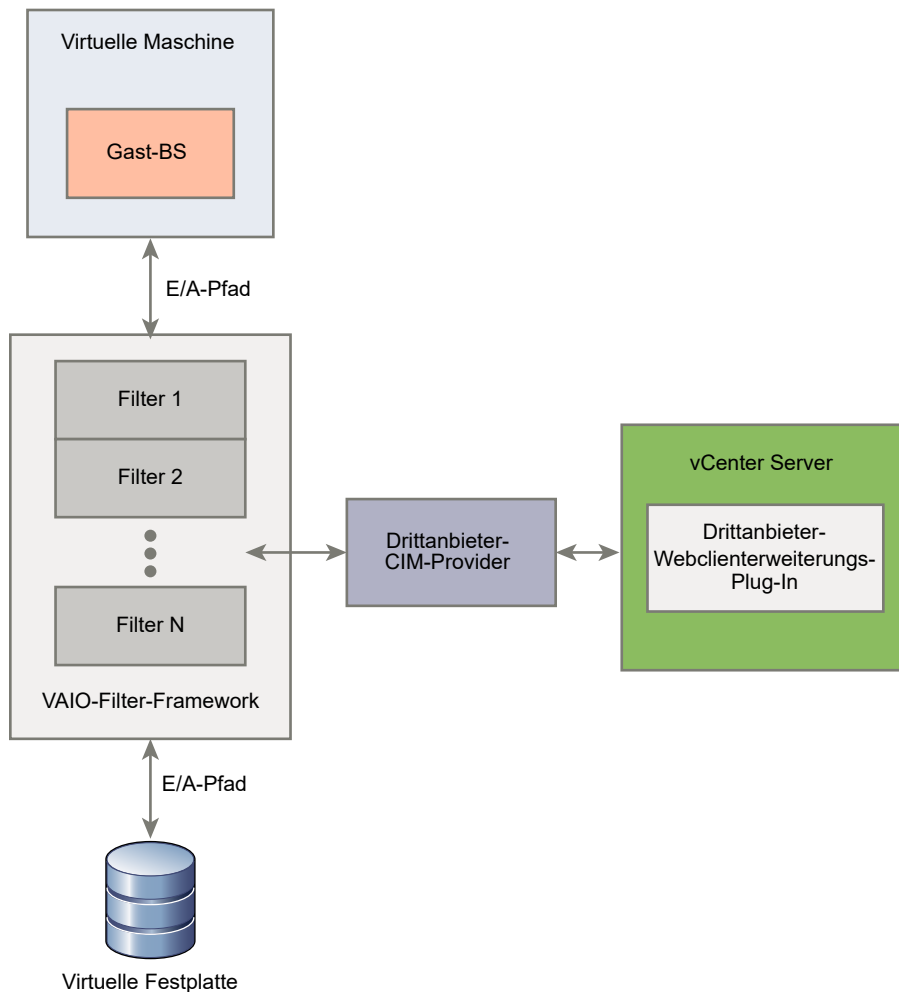
### vSphere Web Client-Plug-In

Eine von VMware-Partnern entwickelte optionale Komponente. Sie liefert vSphere-Administratoren Methoden für die Kommunikation mit einem E/A-Filter-CIM-Anbieter, um Überwachungsinformationen zum E/A-Filterstatus zu empfangen sowie Konfigurationsbefehle an den CIM-Anbieter zum Konfigurieren der E/A-Filter zu senden.

### E/A-Filter-Daemon

Eine von VMware-Partnern entwickelte optionale Komponente. Sie kann als zusätzlicher Dienst verwendet werden, der mit den einzelnen Filterinstanzen, die auf einem Host ausgeführt werden, interagiert. Dieser Dienst kann hostübergreifende Netzwerk-Kommunikationskanäle einrichten.

Die folgende Abbildung veranschaulicht die Komponenten der E/A-Filterung und den E/A-Workflow zwischen dem Gastbetriebssystem und der virtuellen Festplatte.



Jede VMX-Komponente (Virtual Machine Executable) einer virtuellen Maschine enthält ein Filter-Framework, mit dem die mit der virtuellen Festplatte verbundenen E/A-Filter-Plug-Ins verwaltet werden. Das Filter-Framework ruft Filter auf, wenn E/A-Anforderungen zwischen dem Gastbetriebssystem und der virtuellen Festplatte übertragen werden. Darüber hinaus wird jeder E/A-Zugriff auf die virtuelle Festplatte, der außerhalb einer ausgeführten virtuellen Maschine erfolgt, von dem Filter abgefangen.

Die Filter werden nacheinander in der angegebenen Reihenfolge ausgeführt. Beispielsweise wird ein Replizierungsfilter vor einem Cache-Filter ausgeführt. Mehrere Filter können die virtuelle Festplatte filtern, aber pro Kategorie ist nur ein Filter möglich.

Nachdem die E/A-Anforderung von allen Filtern für die betreffende Festplatte gefiltert wurde, wird die E/A-Anforderung an das Ziel übertragen, also entweder die virtuelle Maschine oder die virtuelle Festplatte.

Da die Filter im Benutzerspeicherplatz ausgeführt werden, betreffen etwaige Filterfehler nur die virtuelle Maschine, jedoch nicht den ESXi-Host.

## Speicheranbieter für VAIO-Filter

Nach der Installation und Bereitstellung von E/A-Filtern auf ESXi-Hosts konfiguriert und registriert das E/A-Filter-Framework einen Speicheranbieter (wird auch als VASA-Anbieter bezeichnet) für jeden Host im Cluster.

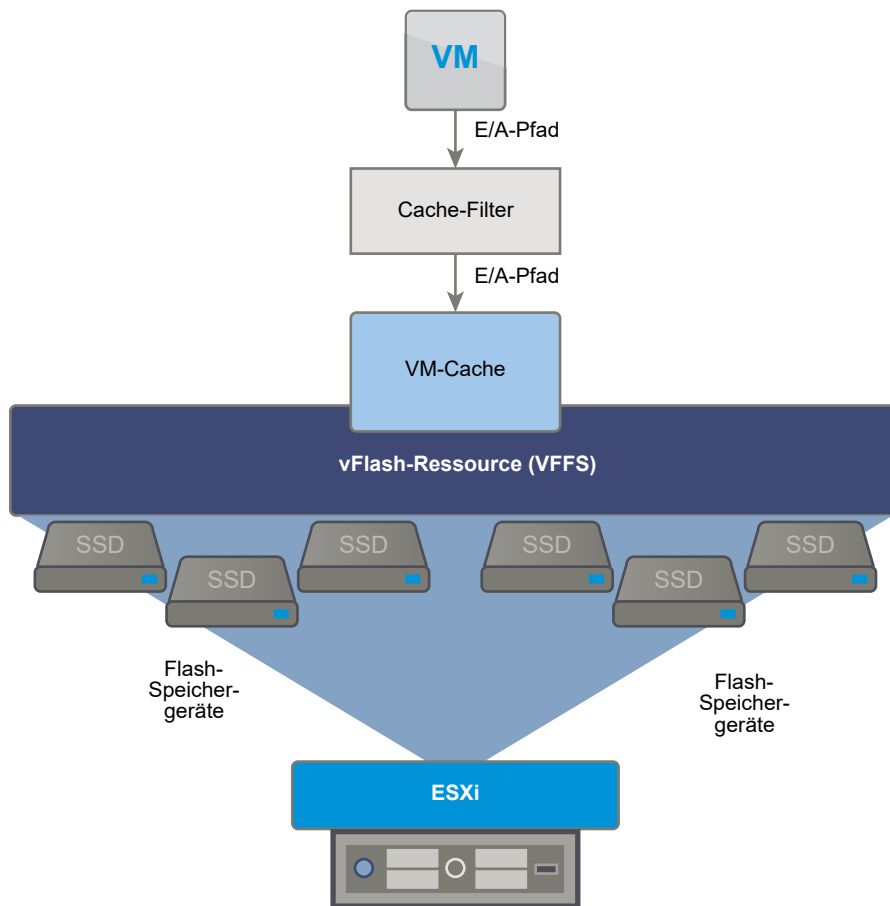
Speicheranbieter für die E/A-Filterung sind von vSphere angebotene Softwarekomponenten. Sie werden mit E/A-Filtern und Bericht-Datendienstfunktionen, die von E/A-Filtern unterstützt werden, in vCenter Server integriert.

Diese Datendienste werden in der Schnittstelle für VM-Speicherrichtlinien angezeigt und können in einer VM-Richtlinie verwendet werden. Anschließend können Sie diese Richtlinie auf virtuelle Festplatten anwenden, damit die E/A für die Festplatten mithilfe der Filter verarbeitet werden kann.

## Verwenden von Flash-Speichergeräten mit Cache-E/A-Filtern

Ein Cache-E/A-Filter kann ein lokales Flash-Gerät zum Zwischenspeichern von Daten virtueller Maschinen verwenden.

Wenn Ihr Cache-E/A-Filter lokale Flash-Geräte verwendet, müssen Sie vor dem Aktivieren des Filters eine virtuelle Flash-Ressource bzw. vFlash-Ressource, die auch als VFFS-Volume bezeichnet wird, auf Ihrem ESXi-Host konfigurieren. Bei der Verarbeitung der E/A-Lesevorgänge der virtuellen Maschine erstellt der Filter einen VM-Cache und platziert ihn auf dem VFFS-Volume.



Zum Einrichten einer vFlash-Ressource verwenden Sie Flash-Geräte, die mit dem Host verbunden sind. Wenn Sie die Kapazität der vFlash-Ressource erhöhen möchten, können Sie weitere Flash-Geräte hinzufügen. Ein einzelnes Flash-Laufwerk muss einer vFlash-Ressource exklusiv zugeteilt werden und kann nicht gemeinsam mit einem anderen vSphere-Dienst (z. B. Virtual SAN oder VMFS) genutzt werden.

Flash Read Cache und Cache-E/A-Filter schließen sich gegenseitig aus, da beide Funktionen die vFlash-Ressource auf dem Host verwenden. Flash Read Cache kann nicht auf einer virtuellen Festplatte mit den Cache-E/A-Filtern aktiviert werden. Entsprechend kann eine virtuelle Maschine mit konfiguriertem Flash Read Cache die Cache-E/A-Filter nicht verwenden.

## Bereitstellen und Konfigurieren von E/A-Filtern in der vSphere-Umgebung

Sie können die E/A-Filter in Ihrer vSphere-Umgebung installieren und dann von den Filtern bereitgestellte Datendienste auf Ihren virtuellen Maschinen aktivieren.

## Voraussetzungen

VMware-Partner erstellen E/A-Filter über das vSphere APIs für E/A-Filter (VAIO)-Entwicklerprogramm und verteilen sie als Filterpakete. Zu den als vSphere-Installationspaketen (vSphere Installation Bundles, VIBs) angebotenen Paketen zählen E/A-Filter-Daemons, CIM-Anbieter und andere zugehörige Komponenten. Weitere Informationen erhalten Sie von Ihrem Anbieter oder Ihrem VMware-Repräsentanten.

## Verfahren

### 1 Installieren von E/A-Filtern in einem Cluster

Für die Installation von E/A-Filtern in einem ESXi-Hostcluster führen Sie die von den Anbietern bereitgestellten Installationsprogramme aus.

### 2 Anzeigen der Speicheranbieter von E/A-Filtern

Nach der Bereitstellung von E/A-Filtern wird automatisch ein Speicheranbieter (wird auch als VASA-Anbieter bezeichnet) für jeden ESXi-Host im Cluster registriert. Sie können überprüfen, ob die E/A-Filter-Speicheranbieter erwartungsgemäß angezeigt werden und aktiv sind.

### 3 Prüfen von E/A-Filterfunktionen

Nach der Installation eines E/A-Filters in Ihrer vSphere-Umgebung werden Funktionen und Datendienste des Filters registriert und in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Sie können diese Dienste und Funktionen und deren Standardwerte prüfen.

### 4 Konfigurieren der vFlash-Ressource für die Zwischenspeicherung von E/A-Filtern

Wenn Ihr Cache-E/A-Filter lokale Flash-Geräte verwendet, müssen Sie vor dem Aktivieren des Filters eine virtuelle Flash-Ressource bzw. vFlash-Ressource, die auch als VFFS-Volume bezeichnet wird, auf Ihrem ESXi-Host konfigurieren.

### 5 Aktivieren von E/A-Filter-Datendiensten auf virtuellen Festplatten

Die Aktivierung der von E/A-Filtern bereitgestellten Datendienste erfolgt in zwei Schritten: Sie erstellen eine Richtlinie für virtuelle Maschinen basierend auf den von E/A-Filtern bereitgestellten Datendiensten und fügen dann diese Richtlinie an eine virtuelle Maschine an.

## Nächste Schritte

Weitere Informationen zur Fehlerbehebung von E/A-Filtern finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

## Installieren von E/A-Filtern in einem Cluster

Für die Installation von E/A-Filtern in einem ESXi-Hostcluster führen Sie die von den Anbietern bereitgestellten Installationsprogramme aus.

## Voraussetzungen

- Erforderliche Rechte: **Host.Configuration.Query-Patch**.

- Stellen Sie sicher, dass die E/A-Filterlösung mit vSphere ESX Agent Manager integriert wird und von VMware zertifiziert ist.
- Stellen Sie sicher, dass Ihr Cluster ESXi 6.0 Update 1-Hosts enthält.
- Aktivieren Sie DRS auf dem Cluster.

#### Verfahren

- 1 Führen Sie das vom Anbieter bereitgestellte Installationsprogramm aus.

Das Installationsprogramm installiert die entsprechende E/A-Filtererweiterung auf vCenter Server und stellt die Filterkomponenten auf allen Hosts in einem Cluster bereit. Der Filter kann nicht auf bestimmten Hosts installiert werden.

- 2 Stellen Sie sicher, dass die E/A-Filterkomponenten auf Ihren ESXi-Hosts ordnungsgemäß installiert wurden:

```
esxcli --server=server_name software vib list
```

Der Filter wird in der Liste der VIB-Pakete angezeigt.

## Anzeigen der Speicheranbieter von E/A-Filtern

Nach der Bereitstellung von E/A-Filtern wird automatisch ein Speicheranbieter (wird auch als VASA-Anbieter bezeichnet) für jeden ESXi-Host im Cluster registriert. Sie können überprüfen, ob die E/A-Filter-Speicheranbieter erwartungsgemäß angezeigt werden und aktiv sind.

Die erfolgreiche automatische Registrierung des E/A-Filter-Speicheranbieters löst ein Ereignis auf der Hostebene aus. Falls der Speicheranbieter nicht automatisch registriert werden kann, löst das System einen Alarm auf dem Host aus.

#### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Prüfen Sie die Speicheranbieter für E/A-Filter.

## Prüfen von E/A-Filterfunktionen

Nach der Installation eines E/A-Filters in Ihrer vSphere-Umgebung werden Funktionen und Datendienste des Filters registriert und in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Sie können diese Dienste und Funktionen und deren Standardwerte prüfen.

#### Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen**.
- 3 Wählen Sie die vCenter Server-Instanz aus.

- 4 Geben Sie einen Namen, wie beispielsweise „Cache-E/A-Filter“, und eine Beschreibung für die Richtlinie ein und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Gemeinsame Regeln“ die Option **Gemeinsame Regeln in der VM-Speicherrichtlinie verwenden** aus.
- 6 Wählen Sie im Dropdown-Menü **Regel hinzufügen** eine E/A-Filterkategorie wie beispielsweise „Cache“ aus.
- 7 Wählen Sie im Dropdown-Menü **Wert auswählen** den Filter aus, dessen Funktionen Sie prüfen möchten.

Im Fensterbereich werden nun die Datendienste des E/A-Filters und die entsprechenden Standardwerte angezeigt.

## Konfigurieren der vFlash-Ressource für die Zwischenspeicherung von E/A-Filtern

Wenn Ihr Cache-E/A-Filter lokale Flash-Geräte verwendet, müssen Sie vor dem Aktivieren des Filters eine virtuelle Flash-Ressource bzw. vFlash-Ressource, die auch als VFFS-Volume bezeichnet wird, auf Ihrem ESXi-Host konfigurieren.

### Voraussetzungen

Von Ihrem E/A-Filter-Anbieter erfahren Sie, ob die vFlash-Ressource aktiviert werden muss.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie unter „Virtueller Flash“ die Option **vFlash-Ressourcenverwaltung** und klicken Sie auf **Kapazität hinzufügen**.
- 4 Wählen Sie aus der Liste der verfügbaren Flash-Laufwerke eines oder mehrere Flash-Laufwerke zur Verwendung durch die vFlash-Ressource aus und klicken Sie auf **OK**.

### Ergebnisse

Die vFlash-Ressource wird erstellt. Im Bereich „Geräte-Backing“ werden alle Laufwerke aufgelistet, die für die vFlash-Ressource verwendet werden.

## Aktivieren von E/A-Filter-Datendiensten auf virtuellen Festplatten

Die Aktivierung der von E/A-Filtern bereitgestellten Datendienste erfolgt in zwei Schritten: Sie erstellen eine Richtlinie für virtuelle Maschinen basierend auf den von E/A-Filtern bereitgestellten Datendiensten und fügen dann diese Richtlinie an eine virtuelle Maschine an.

## Voraussetzungen

Für Cache-E/A-Filter konfigurieren Sie die vFlash-Ressource auf Ihrem ESXi-Host.

## Verfahren

### 1 Definieren einer VM-Richtlinie basierend auf E/A-Filterfunktionen

Wenn Sie E/A-Filter für virtuelle Maschinen aktivieren möchten, müssen Sie zunächst eine Richtlinie für virtuelle Maschinen erstellen, die die von den E/A-Filtern bereitgestellten Datendienstfunktionen auflistet.

### 2 Zuweisen der E/A-Filterrichtlinie zu virtuellen Maschinen

Zum Aktivieren der von E/A-Filtern bereitgestellten Datendienste ordnen Sie die E/A-Filterrichtlinien virtuellen Festplatten zu. Die Richtlinie können Sie beim Erstellen oder Bearbeiten einer virtuellen Maschine zuweisen.

## Definieren einer VM-Richtlinie basierend auf E/A-Filterfunktionen

Wenn Sie E/A-Filter für virtuelle Maschinen aktivieren möchten, müssen Sie zunächst eine Richtlinie für virtuelle Maschinen erstellen, die die von den E/A-Filtern bereitgestellten Datendienstfunktionen auflistet.

Die E/A-Filterfunktionen werden auf der Seite „Gemeinsame Regeln“ des Assistenten für VM-Speicherrichtlinien angezeigt.

## Voraussetzungen

- Vergewissern Sie sich, dass der E/A-Filter-Speicheranbieter verfügbar und aktiv ist. Siehe [Anzeigen der Speicheranbieter von E/A-Filtern](#).

## Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile > VM-Speicherrichtlinien**.
- 2 Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen**.
- 3 Wählen Sie die vCenter Server-Instanz aus.
- 4 Geben Sie einen Namen, wie beispielsweise „E/A-Filter“, und eine Beschreibung für die VM-Richtlinie ein und klicken Sie auf **Weiter**.
- 5 Geben Sie auf der Seite „Gemeinsame Regeln“ die E/A-Filterdienste an, die für die virtuelle Maschine aktiviert werden sollen.

E/A-Filter aus verschiedenen Kategorien, wie beispielsweise Zwischenspeicherung und Replizierung, können in einer einzigen Speicherrichtlinie kombiniert werden. Sie können aber auch für jede Kategorie unterschiedliche Richtlinien erstellen. Pro Speicherrichtlinie können Sie nur einen Filter aus derselben Kategorie (z. B. Zwischenspeicherung) verwenden.



- a Wählen Sie **Gemeinsame Regeln in der VM-Speicherrichtlinie verwenden** aus.
- b Wählen Sie im Dropdown-Menü **Regel hinzufügen** eine E/A-Filterkategorie aus.

Option	Beschreibung
<b>Replizierung</b>	Repliziert alle E/A-Schreibvorgänge zwischen dem Gastbetriebssystem einer virtuellen Maschine und virtuellen Festplatten in einem externen Zielspeicherort, wie beispielsweise auf einem anderen Host oder Cluster.
<b>Zwischenspeicherung</b>	Konfiguriert einen Cache für virtuelle Festplattendaten. Verwendet ein lokales Flash-Speichergerät, um die Daten zwischenspeichern und die E/A-Vorgänge pro Sekunde (IOPS) und die Hardwarenutzungsraten für die virtuelle Festplatte zu erhöhen.

- c Wählen Sie im Dropdown-Menü **Wert auswählen** den Filter aus.  
Auf der Seite werden nun die von diesem Filter unterstützten Datendienstfunktionen und Standardwerte angezeigt.
  - d Geben Sie Werte für die Regel an und klicken Sie auf **Weiter**.
- 6 Geben Sie auf der Seite „Regelsatz“ Speicherplatzierungsanforderungen an und klicken Sie auf **Weiter**.

**Hinweis** Wenn Sie die virtuelle Maschine mit E/A-Filtern zwischen verschiedenen Datenspeichertypen migrieren möchten, wie beispielsweise zwischen VMFS und virtuellen Volumes, müssen Sie darauf achten, dass die VM-Speicherrichtlinie Regelsätze für jeden Datenspeichertyp enthält, den Sie verwenden möchten. Wenn Sie beispielsweise Ihre virtuelle Maschine zwischen einem VMFS-Datenspeicher und einem Datenspeicher für virtuelle Volumes migrieren, sollten Sie eine gemischte VM-Speicherrichtlinie erstellen, die Tag-basierte Regeln für den VMFS-Datenspeicher sowie Regeln für den Datenspeicher für virtuelle Volumes beinhaltet.

- 7 Überprüfen Sie auf der Seite „Speicherkompatibilität“ die Liste der verfügbaren Datenspeicher und klicken Sie auf **Weiter**.

Für die Kompatibilität mit der E/A-Filterrichtlinie müssen Datenspeicher mit einem Host mit installierten E/A-Filtern verbunden sein und die Speichieranforderungen der Richtlinie erfüllen.

- 8 Schließen Sie die Erstellung der Speicherrichtlinie ab und klicken Sie auf **Beenden**.

### Ergebnisse

Die neue Richtlinie wird zur Liste hinzugefügt.

## Zuweisen der E/A-Filterrichtlinie zu virtuellen Maschinen

Zum Aktivieren der von E/A-Filtern bereitgestellten Datendienste ordnen Sie die E/A-Filterrichtlinien virtuellen Festplatten zu. Die Richtlinie können Sie beim Erstellen oder Bearbeiten einer virtuellen Maschine zuweisen.

Die E/A-Filterrichtlinie kann bei der anfänglichen Bereitstellung einer virtuellen Maschine zugewiesen werden. In diesem Thema wird beschrieben, wie Sie die Richtlinie beim Erstellen einer neuen virtuellen Maschine zuweisen. Informationen zu anderen Bereitstellungsmethoden finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

---

**Hinweis** Die E/A-Filterrichtlinie kann beim Migrieren oder Klonen einer virtuellen Maschine nicht geändert oder zugewiesen werden.

---

### Voraussetzungen

Stellen Sie sicher, dass der E/A-Filter auf dem ESXi-Host installiert ist, auf dem die virtuelle Maschine ausgeführt wird.

### Verfahren

- 1 Starten Sie im vSphere Web Client den Bereitstellungsvorgang für die virtuelle Maschine und führen Sie die entsprechenden Schritte aus.
- 2 Wählen Sie auf der Seite „Speicher auswählen“ eine E/A-Filterrichtlinie aus dem Dropdown-Menü **VM-Speicherrichtlinie** aus.
- 3 Wählen Sie aus der Liste der verfügbaren Datenspeicher den gewünschten Datenspeicher aus und klicken Sie auf **Weiter**.

Der Datenspeicher wird zum Zielspeicherelement für die VM-Konfigurationsdatei und alle virtuellen Festplatten. Diese Richtlinie aktiviert auch E/A-Filterdienste für die virtuellen Festplatten.

- 4 Schließen Sie die Bereitstellung der virtuellen Maschine ab.

### Ergebnisse

Nach der Erstellung der virtuellen Maschine zeigt die Registerkarte **Übersicht** die zugewiesenen Speicherrichtlinien und deren Übereinstimmungsstatus an.

## Nächste Schritte

Die Zuweisung der VM-Richtlinie kann später geändert werden. Siehe [Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten](#).

## Verwalten von E/A-Filtern

Sie können das von Ihrem Anbieter bereitgestellte Installationsprogramm ausführen, um E/A-Filter zu installieren, deinstallieren oder aktualisieren.

Bei Verwendung von E/A-Filtern sollten Sie Folgendes beachten:

- vCenter Server verwendet ESX Agent Manager (EAM) zum Installieren und Deinstallieren von E/A-Filtern. Als Administrator sollten Sie niemals EAM-APIs direkt für EAM-Agencys aufrufen, die von vCenter Server erstellt oder verwendet werden. Alle Vorgänge im Zusammenhang mit E/A-Filtern müssen über VIM-APIs durchgeführt werden. Falls Sie versehentlich eine von vCenter Server erstellte EAM-Agency ändern, müssen Sie die Änderungen rückgängig machen. Falls Sie versehentlich eine von E/A-Filtern verwendete EAM-Agency löschen, müssen Sie `Vim.IoFilterManager#uninstallIoFilter` aufrufen, um die betroffenen E/A-Filter zu deinstallieren. Führen Sie nach der Deinstallation eine Neuinstallation durch.
- Wenn ein neuer Host einem Cluster beitrifft, der E/A-Filter aufweist, werden die auf dem Cluster installierten Filter auf dem Host bereitgestellt. vCenter Server registriert den E/A-Filter-Speicheranbieter für den Host. Clusteränderungen werden in der Schnittstelle für VM-Speicherrichtlinien des vSphere Web Client angezeigt.
- Wenn Sie einen Host aus einem Cluster verschieben oder aus vCenter Server entfernen, werden die E/A-Filter auf dem Host deinstalliert. vCenter Server hebt die Registrierung des E/A-Filter-Speicheranbieters des Hosts nach der Deinstallation der Filter auf.
- Wenn Sie einen statusfreien ESXi-Host verwenden, gehen möglicherweise während eines Neustarts dessen E/A-Filter-VIBs verloren. vCenter Server überprüft die auf dem Host installierten Pakete nach dem Neustart und verschiebt die E/A-Filter-VIBs ggf. auf den Host.

## Deinstallieren von E/A-Filtern in einem Cluster

In einem ESXi-Hostcluster bereitgestellte E/A-Filter können deinstalliert werden.

### Voraussetzungen

- Erforderliche Berechtigungen: **Host.Config.Patch**.

### Verfahren

- 1 Deinstallieren Sie den E/A-Filter durch Ausführen des Installationsprogramms Ihres Anbieters.

Während der Deinstallation versetzt vSphere ESX Agent Manager die Hosts automatisch in den Wartungsmodus.

Falls die Deinstallation erfolgreich ist, werden der Filter und alle zugehörigen Komponenten von den Hosts entfernt.

- 2 Stellen Sie sicher, dass die E/A-Filterkomponenten auf Ihren ESXi-Hosts ordnungsgemäß deinstalliert wurden:

```
esxcli --server=Servername software vib list
```

Der deinstallierte Filter wird nicht mehr aufgeführt.

## Aktualisieren von E/A-Filtern in einem Cluster

Verwenden Sie die von den E/A-Filteranbietern bereitgestellten Installationsprogramme für das Upgrade der in einem ESXi-Hostcluster bereitgestellten E/A-Filter.

Ein Upgrade besteht aus dem Deinstallieren der alten Filterkomponenten und dem Ersetzen durch die neuen Filterkomponenten. Um festzustellen, ob es sich bei einer Installation um ein Upgrade handelt, prüft vCenter Server die Namen und Versionen vorhandener Filter. Falls die Namen der vorhandenen Filter mit den Namen der neuen Filter übereinstimmen, aber unterschiedliche Versionen aufweisen, gilt die Installation als Upgrade.

### Voraussetzungen

- Erforderliche Rechte: **Host.Config.Patch**.

### Verfahren

- 1 Führen Sie das vom Anbieter bereitgestellte Installationsprogramm aus, um ein Upgrade des Filters durchzuführen.

Während des Upgrades versetzt vSphere ESX Agent Manager die Hosts automatisch in den Wartungsmodus.

Das Installationsprogramm identifiziert vorhandene Filterkomponenten und entfernt sie vor der Installation der neuen Filterkomponenten.

- 2 Stellen Sie sicher, dass die E/A-Filterkomponenten auf Ihren ESXi-Hosts ordnungsgemäß deinstalliert wurden:

```
esxcli --server=Servername software vib list
```

### Ergebnisse

Nach dem Upgrade versetzt vSphere ESX Agent Manager die Hosts wieder in den Betriebsmodus.

## Richtlinien und empfohlene Vorgehensweisen für E/A-Filter

Halten Sie sich bei der Verwendung von E/A-Filtern in Ihrer Umgebung an spezielle Richtlinien und empfohlene Vorgehensweisen.

- RDMS im physischen Kompatibilitätsmodus werden von E/A-Filtern nicht unterstützt.
- Flash Read Cache und Cache-E/A-Filter schließen sich gegenseitig aus, da beide Funktionen die vFlash-Ressource auf dem Host verwenden. Flash Read Cache kann nicht auf einer virtuellen Festplatte mit den Cache-E/A-Filtern aktiviert werden. Entsprechend kann eine virtuelle Maschine mit konfiguriertem Flash Read Cache die Cache-E/A-Filter nicht verwenden.

- Die E/A-Filtrerrichtlinie kann beim Migrieren oder Klonen einer virtuellen Maschine nicht geändert oder zugewiesen werden.
- Für das Klonen oder Migrieren einer virtuellen Maschine mit einer E/A-Filtrerrichtlinie zwischen Hosts muss für den Zielhost ein kompatibler Filter installiert sein. Diese Anforderung gilt für Migrationen, die von einem Administrator oder mit Funktionen wie HA oder DRS gestartet werden.
- Wenn Sie eine Vorlage in eine virtuelle Maschine konvertieren und für die Vorlage eine E/A-Filtrerrichtlinie konfiguriert ist, muss für den Zielhost der kompatible E/A-Filter installiert sein.
- Wenn Sie mit vCenter Site Recovery Manager virtuelle Festplatten replizieren, weisen die daraus resultierenden Festplatten auf der Wiederherstellungs-Site keine E/A-Filtrerrichtlinien auf. Sie müssen E/A-Filtrerrichtlinien für die Wiederherstellungs-Site erstellen und erneut zu den replizierten Festplatten hinzufügen.
- Falls der virtuellen Maschine eine Snapshot-Struktur zugeordnet wurde, können Sie die E/A-Filtrerrichtlinie für die virtuelle Maschine nicht hinzufügen, ändern oder entfernen.

Weitere Informationen zur Fehlerbehebung von E/A-Filtern finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

## Migrieren von virtuellen Maschinen mit E/A-Filtern

Bei der Migration einer virtuellen Maschine mit E/A-Filtern gelten spezielle Anforderungen.

Wenn Sie Storage vMotion zum Migrieren einer virtuellen Maschine mit E/A-Filtern verwenden, muss ein Zieldatenspeicher mit Hosts mit installierten kompatiblen E/A-Filtern verbunden sein.

Möglicherweise müssen Sie eine virtuelle Maschine mit E/A-Filtern zwischen verschiedenen Datenspeichertypen migrieren, wie beispielsweise zwischen VMFS und virtuellen Volumes, zwischen VMFS und Virtual SAN usw. Achten Sie in diesem Fall darauf, dass die VM-Speicherrichtlinie neben gemeinsamen Regeln zur Beschreibung der E/A-Filtrerrichtlinie auch Regelsätze für jeden Datenspeichertyp enthält, den Sie verwenden möchten. Wenn Sie beispielsweise Ihre virtuelle Maschine zwischen einem VMFS-Datenspeicher und einem Datenspeicher für virtuelle Volumes migrieren, sollten Sie eine gemischte VM-Speicherrichtlinie erstellen, die Folgendes beinhaltet:

- Gemeinsame Regeln für die E/A-Filter
- Regelsatz 1 für den VMFS-Datenspeicher. Da das speicherrichtlinienbasierte Management keine explizite VMFS-Richtlinie bietet, muss der Regelsatz Tag-basierte Regeln für den VMFS-Datenspeicher enthalten.
- Regelsatz 2 für den Datenspeicher für virtuelle Volumes.

Wenn die virtuelle Maschine mit Storage vMotion migriert wird, wird der entsprechende Regelsatz für den Zieldatenspeicher ausgewählt. Die E/A-Filterregeln bleiben unverändert.

Falls Sie keine Regeln für Datenspeicher angeben und nur gemeinsame Regeln für die E/A-Filter definieren, werden Standardspeicherrichtlinien für Virtual SAN-Datenspeicher, für Datenspeicher für virtuelle Volumes und für VMFS/NFS-Datenspeicher ausgewählt.

Der VMkernel ist ein äußerst leistungsfähiges Betriebssystem, das direkt auf dem ESXi-Host ausgeführt wird. Der VMkernel verwaltet die meisten physischen Ressourcen auf der Hardware, einschließlich Arbeitsspeichern, physischen Prozessoren, Datenspeichern und Netzwerkcontrollern.

Zum Verwalten von Speicher verfügt der VMkernel über ein Speichersubsystem, das mehrere Hostbusadapter (HBAs) unterstützt, einschließlich paralleles SCSI, SAS, Fibre-Channel, FCoE und iSCSI. Diese HBAs verbinden eine Vielfalt an aktiv/aktiv-, aktiv/passiv- und ALUA-Speicher-Arrays, die für die Verwendung mit dem VMkernel zertifiziert sind. Siehe die Dokumentation zu *vSphere-Kompatibilitätshandbuch*. Dort finden Sie eine Liste der unterstützten HBAs und Speicher-Arrays.

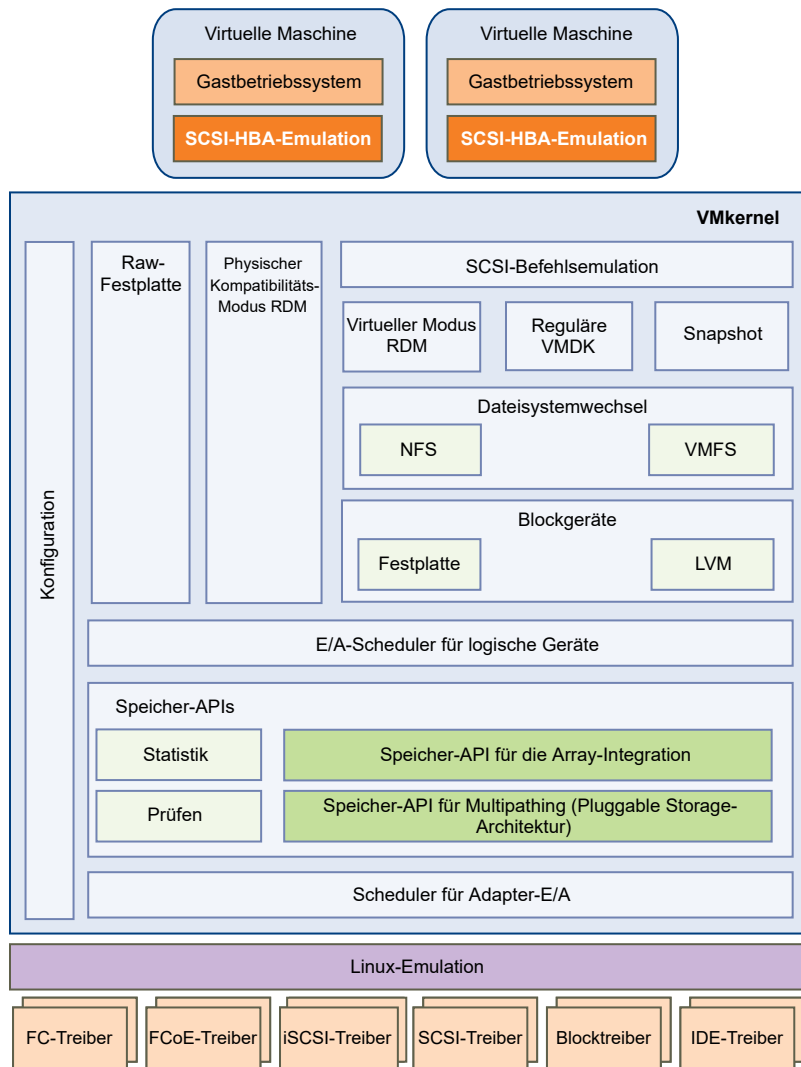
Das primäre Dateisystem, das der VMkernel verwendet, ist das VMware Virtual Machine File System (VMFS). VMFS ist ein Cluster-Dateisystem, das entworfen und optimiert wurde, um große Dateien, wie z. B. virtuelle Festplatten und Auslagerungsdateien, zu unterstützen. Der VMkernel unterstützt zudem das Speichern von virtuellen Festplatten auf NFS-Dateisystemen.

Der Speicher-E/A-Pfad bietet virtuellen Maschinen Zugriff auf Speichergeräte über eine Geräteemulation. Durch diese Geräteemulation kann eine virtuelle Maschine so auf Dateien auf einem VMFS- oder NFS-Dateisystem zugreifen, als ob sie SCSI-Geräte wären. Der VMkernel bietet Speichervirtualisierungsfunktionen, wie z. B. das Planen von E/A-Anforderungen von mehreren virtuellen Maschinen sowie Multipathing.

Außerdem bietet der VMkernel mehrere Speicher-APIs, anhand derer Speicherpartner ihre Produkte für vSphere integrieren und optimieren können.

Die folgende Darstellung illustriert die grundlegenden Elemente des VMkernel-Kerns unter besonderer Berücksichtigung des Speicher-Stacks. Speicherbezogene Module befinden sich zwischen den Ebenen des E/A-Schedulers für logische Geräte und des Adapter-E/A-Schedulers.

Abbildung 22-1. VMkernel und Speicher



Dieses Kapitel enthält die folgenden Themen:

- **Speicher-APIs**

## Speicher-APIs

Speicher-APIs sind APIs, die von Drittanbieterhardware, -software und Speicheranbietern verwendet werden, um Komponenten zu entwickeln, die vSphere-Funktionen und -Lösungen erweitern.

Diese Dokumentation beschreibt die folgenden Speicher-APIs und erläutert, welchen Beitrag diese in Ihrer Speicherumgebung leisten. Informationen zu anderen APIs dieser Familie, z. B. „Storage API - Data Protection“ und „Storage API - Site Recovery Manager“, finden Sie auf der VMware-Website.

- „Storage APIs - Multipathing“, auch bekannt als die Architektur des im Betrieb austauschbaren Speichers (Pluggable Storage Architecture, PSA). PSA ist eine Sammlung von VMkernel-APIs, mit deren Hilfe Speicherpartner ihre Arrays asynchron zu den Zeitplänen für die Freigabe von ESXi-Versionen aktivieren und zertifizieren sowie leistungssteigerndes, Multipathing- und Lastausgleichs-Verhalten bieten können, die für jedes Array optimiert sind. Weitere Informationen finden Sie unter [Verwalten mehrerer Pfade](#).
- „Storage APIs - Array Integration“, früher auch als VAAI bezeichnet, enthalten die folgenden APIs:
  - Hardwarebeschleunigungs-APIs. Ermöglicht Arrays die Integration mit vSphere zur transparenten Auslagerung bestimmter Speichervorgänge auf das Array. Diese Integration sorgt für eine wesentliche Reduzierung des CPU-Overheads auf dem Host. Weitere Informationen hierzu finden Sie unter [Kapitel 23 Speicherhardware-Beschleunigung](#).
  - Array-Thin-Provisioning-APIs. Unterstützt das Überwachen der Speicherplatznutzung auf Thin-bereitgestellten Speicher-Arrays, um Speicherplatzengpässe zu verhindern und Speicherplatzrückgewinnung durchzuführen. Weitere Informationen hierzu finden Sie unter [Array-Thin Provisioning und VMFS-Datenspeicher](#).
- Storage APIs - Storage Awareness. Diese vCenter Server-basierten APIs ermöglichen es den Speicher-Arrays, vCenter Server über ihre Konfiguration, ihre Funktionen sowie Speicherstatus und -ereignisse zu informieren. Weitere Informationen hierzu finden Sie unter [Kapitel 25 Verwenden von Speicheranbietern](#).



Die Hardwarebeschleunigungsfunktion ermöglicht dem ESXi-Host die Integration mit konformen Speicher-Arrays und die Auslagerung bestimmter VM- und Speicherverwaltungsvorgänge in Speicherhardware. Mit der Speicherhardware-Unterstützung führt Ihr Host diese Vorgänge schneller aus und verbraucht weniger CPU, Arbeitsspeicher und Speicher-Fabric-Bandbreite.

Die Hardwarebeschleunigung wird von Blockspeichergeräten, Fibre-Channel und iSCSI sowie NAS-Geräten unterstützt.

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1021976>.

Dieses Kapitel enthält die folgenden Themen:

- Vorteile der Hardwarebeschleunigung
- Anforderungen der Hardwarebeschleunigung
- Status der Hardwarebeschleunigungs-Unterstützung
- Hardwarebeschleunigung für Blockspeichergeräte
- Hardwarebeschleunigung auf NAS-Geräten
- Überlegungen bei der Hardwarebeschleunigung

## Vorteile der Hardwarebeschleunigung

Wenn die Hardwarebeschleunigungs-Funktion unterstützt wird, kann der Host Hardwareunterstützung erhalten und etliche Aufgaben schneller und effizienter ausführen:

Der Host kann Unterstützung bei den folgenden Aktivitäten erhalten:

- Migrieren von virtuellen Maschinen mit Storage vMotion
- Bereitstellen von virtuellen Maschinen anhand von Vorlagen
- Klonen virtueller Maschinen oder Vorlagen
- VMFS Clustered Locking und Metadatenvorgänge für Dateien virtueller Maschinen
- Bereitstellen von virtuellen Festplatten mit Thick Provisioning
- Erstellen von fehlertoleranten virtuellen Maschinen

- Erstellen und Klonen von Thick-Festplatten auf NFS-Datenspeichern

## Anforderungen der Hardwarebeschleunigung

Die Hardwarebeschleunigungs-Funktion kann nur mit einer geeigneten Kombination aus Host und Speicher-Array verwendet werden.

**Tabelle 23-1. Speicheranforderungen der Hardwarebeschleunigung**

ESXi	Blockspeichergeräte	NAS-Geräte
ESXi Version 6.0	Unterstützen T10 SCSI Standard- oder Blockspeicher-Plug-Ins für die Array-Integration (VAAI)	Unterstützen NAS-Plug-Ins für die Array-Integration  <b>Hinweis</b> NFS 4.1 bietet keine Unterstützung für Hardwarebeschleunigung.

**Hinweis** Wenn Ihr SAN- oder NAS-Speicher-Fabric vor dem die Hardwarebeschleunigung unterstützenden Speichersystem eine dazwischenliegende Appliance verwendet, muss die dazwischenliegende Appliance die Hardwarebeschleunigung ebenfalls unterstützen und ordnungsgemäß zertifiziert sein. Bei der dazwischenliegenden Appliance kann es sich um eine Speichervirtualisierungs-Appliance, eine E/A-Beschleunigungs-Appliance, eine Verschlüsselungs-Appliance usw. handeln.

## Status der Hardwarebeschleunigungs-Unterstützung

Der vSphere Web Client zeigt den Status der Hardwarebeschleunigungs-Unterstützung für jedes Speichergerät und jeden Datenspeicher an.

Die Statuswerte lauten „Unbekannt“, „Unterstützt“ und „Nicht unterstützt“. Der Anfangswert ist „Unbekannt“.

Bei Blockgeräten ändert sich der Status in „Unterstützt“, wenn der Host den Auslagerungsvorgang erfolgreich ausgeführt hat. Wenn der Auslagerungsvorgang fehlschlägt, ändert sich der Status in „Nicht unterstützt“. Der Status bleibt „Unbekannt“, wenn das Gerät die Hardwarebeschleunigung nur teilweise unterstützt.

Bei NAS ist der Status „Unterstützt“, wenn der Speicher mindestens einen Hardwareablagerungsvorgang durchführen kann.

Wenn Speichergeräte die Hostvorgänge nicht oder nur teilweise unterstützen, kehrt der Host für die Ausführung nicht unterstützter Vorgänge zu seinen nativen Methoden zurück.

## Hardwarebeschleunigung für Blockspeichergeräte

Mithilfe der Hardwarebeschleunigung kann der Host mit Blockspeichergeräten, Fibre-Channel oder iSCSI integriert werden und bestimmte Speicher-Array-Vorgänge verwenden.

Die ESXi-Hardwarebeschleunigung unterstützt die folgenden Array-Vorgänge:

- „Full Copy“ (wird auch als „Clone Blocks“ oder „Copy Offload“ bezeichnet). Ermöglicht den Speicher-Arrays, vollständige Kopien von Daten innerhalb des Arrays zu erstellen, ohne dass der Host die Daten lesen und schreiben muss. Dieser Vorgang reduziert die Zeit und die Netzwerkauslastung beim Klonen von virtuellen Maschinen, beim Bereitstellen einer Vorlage oder beim Migrieren mit vMotion.
- „Block zeroing“ (wird auch als „write same“ bezeichnet). Ermöglicht den Speicher-Arrays, eine große Anzahl von Blöcken mit Nullbyte zu füllen, um neu zugeteilten Speicher, der keine bereits geschriebenen Daten enthält, bereitzustellen. Dieser Vorgang reduziert die Zeit und die Netzwerkauslastung beim Erstellen von virtuellen Maschinen und beim Formatieren von virtuellen Festplatten.
- „Hardware assisted locking“ (wird auch als „atomic test and set [ATS]“ bezeichnet). Unterstützt das Sperren einer virtuellen Maschine, ohne SCSI-Reservierungen verwenden zu müssen. Diese Operation erlaubt das Sperren von Festplatten auf Sektorbasis anstatt der gesamten LUN (wie bei der Verwendung von SCSI-Reservierungen).

Wenden Sie sich hinsichtlich der Unterstützung der Hardwarebeschleunigung an Ihren Anbieter. Für bestimmte Speicher-Arrays ist es erforderlich, dass Sie die Unterstützung auf der Speicherseite aktivieren.

Auf Ihrem Host ist die Hardwarebeschleunigung standardmäßig aktiviert. Falls Ihr Speicher die Hardwarebeschleunigung nicht unterstützt, können Sie sie deaktivieren.

Neben der Unterstützung der Hardwarebeschleunigung bietet ESXi auch Unterstützung für das Thin Provisioning. Weitere Informationen hierzu finden Sie unter [Array-Thin Provisioning und VMFS-Datenspeicher](#).

## Deaktivieren der Hardwarebeschleunigung für Blockspeichergeräte

Auf Ihrem Host ist die Hardwarebeschleunigung für Blockspeichergeräte standardmäßig aktiviert. Sie können die erweiterten Einstellungen des vSphere Web Client verwenden, um die Hardwarebeschleunigungsvorgänge zu deaktivieren.

Wenden Sie sich, wie bei allen erweiterten Einstellungen, an den VMware-Support, bevor Sie die Hardwarebeschleunigung deaktivieren.

### Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
- 4 Ändern Sie den Wert für eine beliebige Option auf 0 (deaktiviert):
  - VMFS3.HardwareAcceleratedLocking
  - DataMover.HardwareAcceleratedMove

- DataMover.HardwareAcceleratedInit

## Verwalten der Hardwarebeschleunigung auf Blockspeichergeräten

Um eine Integration mit den Blockspeicher-Arrays zu ermöglichen und von den Array-Hardwarevorgängen zu profitieren, nutzt vSphere die ESXi-Erweiterungen, die als „Storage APIs - Array Integration“ bezeichnet werden (früher VAAI).

In vSphere 5.x und höher werden diese Erweiterungen als T10 SCSI-basierte Befehle implementiert. Folglich kann der ESXi-Host direkt mit den Geräten, die den T10 SCSI-Standard unterstützen, kommunizieren, d. h., die VAAI-Plug-Ins sind nicht erforderlich.

Wenn das Gerät T10 SCSI nicht oder nur teilweise unterstützt, kehrt ESXi zur Verwendung der auf dem Host installierten VAAI-Plug-Ins zurück oder verwendet eine Kombination aus T10 SCSI-Befehlen und Plug-Ins. Die VAAI-Plug-Ins sind anbieterspezifisch und können entweder von VMware oder von Partnern entwickelt worden sein. Zum Verwalten des VAAI-fähigen Geräts hängt der Host den VAAI-Filter und das anbieterspezifische VAAI-Plug-In an das Gerät an.

Informationen darüber, ob Ihr Speicher VAAI Plug-Ins benötigt oder die Hardwarebeschleunigung über T10 SCSI-Befehle unterstützt, finden Sie im *VMware-Kompatibilitätshandbuch* oder kontaktieren Sie Ihren Speicheranbieter.

Sie können mehrere `esxcli`-Befehle verwenden, um Speichergeräte nach den Informationen zur Unterstützung der Hardwarebeschleunigung abzufragen. Geräten, die VAAI-Plug-Ins benötigen, stehen zudem die Beanspruchungsregeln zur Verfügung. Weitere Informationen zu `esxcli`-Befehlen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Anzeigen der Hardwarebeschleunigungs-Plug-Ins und des Hardwarebeschleunigungsfilters

Zur Kommunikation mit den Geräten, die die T10 SCSI-Norm nicht unterstützen, verwendet der Host eine Kombination aus einem einzigen VAAI-Filter und einem herstellerspezifischen VAAI-Plug-In. Verwenden Sie den Befehl `esxcli`, um den Hardwarebeschleunigungsfilter und die Plug-Ins anzuzeigen, die derzeit im System geladen sind.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den Befehl **esxcli --server=Servername storage core plugin list --plugin-class=Wert** aus.

Geben Sie für *Wert* eine der folgenden Optionen ein:

- Geben Sie **VAAI** ein, um die Plug-Ins anzuzeigen.

Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
#esxcli --server=server_name storage core plugin list --plugin-class=VAAI
Plugin name      Plugin class
VMW_VAAIP_EQL    VAAI
VMW_VAAIP_NETAPP VAAI
VMW_VAAIP_CX     VAAI
```

- Geben Sie **Filter** ein, um den Filter anzuzeigen.

Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
esxcli --server=server_name storage core plugin list --plugin-class=Filter
Plugin name  Plugin class
VAAI_FILTER  Filter
```

## Verifizieren des Status der Hardwarebeschleunigungs-Unterstützung

Verwenden Sie den **esxcli**-Befehl, um den Hardwarebeschleunigungs-Unterstützungsstatus eines bestimmten Speichergeräts zu überprüfen.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den Befehl **esxcli --server=Servername storage core device list -d=Geräte-ID** aus.

Die Ausgabe zeigt den Hardwarebeschleunigung- oder VAAI-Status an, der „Unbekannt“, „Unterstützt“ oder „Nicht unterstützt“ lauten kann.

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
XXXXXXXXXXXXXXX
Attached Filters: VAAI_FILTER
VAAI Status: supported
XXXXXXXXXXXXXXX
```

## Verifizieren der Details der Hardwarebeschleunigungs-Unterstützung

Verwenden Sie den Befehl **esxcli**, um die vom Blockspeichergerät unterstützte Hardwarebeschleunigung zu ermitteln.

In dem Vorgang wird der Zielservers durch **--server=Servername** angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den Befehl **esxcli --server=Servername storage core device vaa1 status get -d=Geräte-ID** aus.

Wenn das Gerät von einem VAAI-Plug-In verwaltet wird, wird bei der Ausgabe der Name des Plug-Ins angezeigt, der dem Gerät zugewiesen ist. Die Ausgabe zeigt zudem den Unterstützungsstatus für jedes T10 SCSI-basierte einfache Plug-In an, falls verfügbar. Dies ist ein Beispiel für eine Ausgabe:

```
# esxcli --server=server_name storage core device vaa1 status get -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
VAAI Plugin Name: VMW_VAAIP_SYMM
ATS Status: supported
Clone Status: supported
Zero Status: supported
Delete Status: unsupported
```

## Auflisten der Hardwarebeschleunigungs-Beanspruchungsregeln

Jedes von einem VAAI Plug-In verwaltete Blockspeichergerät benötigt zwei Beanspruchungsregeln: Eine Regel, die den Hardwarebeschleunigungsfilter festlegt, und eine Regel, die das Hardwarebeschleunigungs-Plug-In für das Gerät festlegt. Sie können die Beanspruchungsregeln für den Hardwarebeschleunigungsfilter und das Hardwarebeschleunigungs-Plug-In mithilfe der **esxcli**-Befehle auflisten.

## Verfahren

- 1 Führen Sie zum Auflisten der Filterbeanspruchungsregeln den Befehl **esxcli --server=Servername storage core claimrule list --claimrule-class=Filter** aus.

In diesem Beispiel geben die Filter-Beanspruchungsregeln Geräte an, die durch den Filter VAAI\_FILTER beansprucht werden sollten.

```
# esxcli --server=server_name storage core claimrule list --claimrule-class=Filter
Rule Class   Rule   Class   Type   Plugin      Matches
Filter       65430  runtime vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter       65430  file    vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter       65431  runtime vendor VAAI_FILTER vendor=DGC model=*
Filter       65431  file    vendor VAAI_FILTER vendor=DGC model=*
```

- 2 Führen Sie zum Auflisten der VAAI-Plug-In-Beanspruchungsregeln den Befehl **esxcli --server=Servername storage core claimrule list --claimrule-class=VAAI** aus.

In diesem Beispiel geben die VAAI-Beanspruchungsregeln Geräte an, die durch ein bestimmtes VAAI-Plug-In beansprucht werden sollten.

```
esxcli --server=server_name storage core claimrule list --claimrule-class=VAAI
Rule Class   Rule   Class   Type   Plugin      Matches
```

VAAI	65430	runtime	vendor	VMW_VAAIP_SYMM	vendor=EMC	model=SYMMETRIX
VAAI	65430	file	vendor	VMW_VAAIP_SYMM	vendor=EMC	model=SYMMETRIX
VAAI	65431	runtime	vendor	VMW_VAAIP_CX	vendor=DGC	model=*
VAAI	65431	file	vendor	VMW_VAAIP_CX	vendor=DGC	model=*

## Hinzufügen von Hardwarebeschleunigungs-Beanspruchungsregeln

Um die Hardwarebeschleunigung für ein neues Array zu konfigurieren, müssen Sie zwei Beanspruchungsregeln hinzufügen, eine für den VAAI-Filter und eine weitere für das VAAI-Plug-In. Damit die neuen Beanspruchungsregeln aktiv sind, definieren Sie zuerst die Regeln und laden Sie sie anschließend in Ihr System.

Dieses Verfahren ist für diejenigen Blockspeichergeräte geeignet, die keine T10-SCSI-Befehle unterstützen und stattdessen VAAI-Plug-Ins verwenden.

In dem Vorgang wird der Zielservers durch **--server=Servername** angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Definieren Sie eine neue Beanspruchungsregel für den VAAI-Filter, indem Sie den Befehl **esxcli --server=Servername storage core claimrule add --claimrule-class=Filter --plugin=VAAI\_FILTER** ausführen.
- 2 Definieren Sie eine neue Beanspruchungsregel für das VAAI-Plug-In, indem Sie den Befehl **esxcli --server=Servername storage core claimrule add --claimrule-class=VAAI** ausführen.
- 3 Laden Sie beide Beanspruchungsregeln, indem Sie die folgenden Befehle ausführen:  
**esxcli --server=Servername storage core claimrule load --claimrule-class=Filter**  
**esxcli --server=Servername storage core claimrule load --claimrule-class=VAAI**



- 4 Führen Sie die VAAI-Filter-Beanspruchungsregel aus, indem Sie den Befehl **esxcli --server=Servername storage core claimrule run --claimrule-class=Filter** ausführen.

---

**Hinweis** Es müssen nur die Regeln der Klasse „Filter“ ausgeführt werden. Wenn der VAAI-Filter ein Gerät beansprucht, findet er automatisch das richtige VAAI-Plug-In, das angehängt werden muss.

---

### Beispiel: Definieren von Hardwarebeschleunigungs-Beanspruchungsregeln

Dieses Beispiel zeigt, wie Sie die Hardwarebeschleunigung für IBM-Arrays mithilfe des Plug-Ins „VMW\_VAAIP\_T10“ konfigurieren. Verwenden Sie die folgende Befehlsfolge. Weitere Informationen zu den Befehlsoptionen finden Sie unter [Hinzufügen von Multipathing-Beanspruchungsregeln](#).

```
# esxcli --server=Servername storage core claimrule add --claimrule-
class=Filter --plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign

# esxcli --server=Servername storage core claimrule add --claimrule-
class=VAAI --plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign

# esxcli --server=Servername storage core claimrule load --claimrule-
class=Filter

# esxcli --server=Servername storage core claimrule load --claimrule-
class=VAAI

# esxcli --server=Servername storage core claimrule run --claimrule-
class=Filter
```

### Löschen von Hardwarebeschleunigungs-Beanspruchungsregeln

Mithilfe des **esxcli**-Befehls können Sie vorhandene Hardwarebeschleunigungs-Beanspruchungsregeln löschen.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

#### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie die folgenden Befehle aus:

```
esxcli --server=Servername storage core claimrule remove -r claimrule_ID
--claimrule-class=Filter
```

```
esxcli --server=Servername storage core claimrule remove -r claimrule_ID
--claimrule-class=VAAI
```

## Hardwarebeschleunigung auf NAS-Geräten

Mithilfe der Hardwarebeschleunigung können ESXi-Hosts auf NAS-Geräte abgestimmt werden und mehrere vom NAS-Speicher bereitgestellte Hardwarevorgänge nutzen. Die Hardwarebeschleunigung verwendet VMware vSphere Speicher-APIs für die Array-Integration (VAAI) für den Datenaustausch zwischen den Hosts und Speichergeräten.

Die APIs definieren einen Satz von Speicherprimitiven, mit denen der Host bestimmte Speichervorgänge auf das Array auslagern kann. In der folgenden Liste werden die unterstützten NAS-Vorgänge aufgeführt:

- Vollständiges Klonen von Dateien. Ermöglicht NAS-Geräten das Klonen virtueller Festplattendateien. Dieser Vorgang ähnelt dem VMFS-Blockklonen mit der Ausnahme, dass NAS-Geräte ganze Dateien anstatt Dateisegmente klonen.
- Speicherplatz reservieren. Mithilfe dieses Vorgangs können Speicher-Arrays Speicherplatz für die Datei einer virtuellen Festplatte im Thick-Format zuteilen.

In der Regel legt der NAS-Server die Zuweisungsrichtlinie fest, wenn Sie eine virtuelle Festplatte auf einem NFS-Datenspeicher erstellen. Die Standardzuweisungsrichtlinie auf den meisten NAS-Servern ist „Thin“ und garantiert keinen Backing-Speicher für die Datei. Allerdings kann der Vorgang „Speicherplatz reservieren“ das NAS-Gerät anweisen, anbieterspezifische Mechanismen zu verwenden, um Speicherplatz für eine virtuelle Festplatte zu reservieren. Als Folge davon können Sie auf dem NFS-Datenspeicher virtuelle Festplatten im Thick-Format erstellen.

- Systemeigene Snapshot-Unterstützung. Ermöglicht die Erstellung von Snapshots einer virtuellen Maschine, die auf das Array ausgelagert werden können.
- Erweiterte Statistik. Ermöglicht Sichtbarkeit in Bezug auf Speicherplatznutzung auf NAS-Geräten und ist für das Bereitstellungsformat „Thin“ nützlich.

Bei NAS-Speichergeräten wird die Integration der Hardwarebeschleunigung über anbieterspezifische NAS-Plug-Ins implementiert. Diese Plug-Ins werden in der Regel von den Anbietern erstellt und als VIB-Pakete über eine Webseite vertrieben. Die NAS-Plug-Ins funktionieren ohne Beanspruchungsregeln.

Es gibt mehrere Tools zum Installieren und Aktualisieren von VIB-Paketen. Dazu gehören die `esxcli`-Befehle und vSphere Update Manager. Weitere Informationen finden Sie unter *vSphere-Upgrade* und *Installieren und Verwalten von VMware vSphere Update Manager*.

## Installieren des NAS-Plug-Ins

Installieren Sie vom Anbieter vertriebene Hardwarebeschleunigungs-NAS-Plug-Ins auf Ihrem Host.

Dieses Thema bietet ein Beispiel für eine VIB-Paketinstallation mithilfe des Befehls `esxcli`. Weitere Informationen finden Sie unter *vSphere-Upgrade*.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

1 Versetzen Sie den Host in den Wartungsmodus.

2 Legen Sie die Hostakzeptanzebene fest:

```
esxcli --server=Servername software acceptance set --level=Wert
```

Der Befehl legt fest, welches VIB-Paket auf dem Host zulässig ist. *Wert* kann sein:

- VMwareCertified
- VMwareAccepted
- PartnerSupported
- CommunitySupported

3 Installieren Sie das VIB-Paket:

```
esxcli --server=Servername software vib install -v|--viburl=URL
```

*URL* gibt die URL des zu installierenden VIB-Pakets an. Die Protokolle http:, https:, ftp: und file: werden unterstützt.

4 Stellen Sie sicher, dass das Plug-In installiert ist:

```
esxcli --server=Servername software vib list
```

5 Starten Sie den Host neu, damit die Installation wirksam wird.

## Deinstallieren von NAS-Plug-Ins

Entfernen Sie zum Deinstallieren eines NAS-Plug-Ins das VIB-Paket von Ihrem Host.

Dieses Thema behandelt das Deinstallieren eines VIB-Pakets unter Verwendung des `esxcli`-Befehls. Weitere Informationen finden Sie unter *vSphere-Upgrade*.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Deinstallieren Sie das Plug-In:

```
esxcli --server=Servername software vib remove -n|--vibname=Name
```

*Name* ist der Name des zu entfernenden VIB-Pakets.

- 2 Stellen Sie sicher, dass das Plug-In entfernt wird:

```
esxcli --server=Servername software vib list
```

- 3 Starten Sie den Host neu, damit die Änderung wirksam wird.

## Update von NAS-Plug-Ins

Aktualisieren Sie Hardwarebeschleunigungs-NAS-Plug-Ins auf Ihrem Host, wenn ein Speicheranbieter eine neue Plug-In-Version freigibt.

In dem Vorgang wird der Zielserver durch **--server=Servername** angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Dieses Thema behandelt das Durchführen von Updates eines VIB-Pakets unter Verwendung des **esxcli**-Befehls. Weitere Informationen finden Sie in der Dokumentation *vSphere-Upgrade*.

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung **esxcli**-Befehle in der ESXi Shell aus.

### Verfahren

- 1 Upgrade auf eine neue Plug-In-Version:

```
esxcli --server=Servername software vib update -v|--viburl=URL
```

*URL* gibt die URL des zu installierenden VIB-Pakets an. Die Protokolle http:, https:, ftp: und file: werden unterstützt.

- 2 Stellen Sie sicher, dass die korrekte Version installiert ist:

```
esxcli --server=Servername software vib list
```

- 3 Starten Sie den Host neu.

## Verifizieren des Status der Hardwarebeschleunigung für NAS

Zusätzlich zum Client können Sie unter Verwendung des `esxcli`-Befehls den Hardwarebeschleunigungs-Status des NAS-Geräts verifizieren.

In dem Vorgang wird der Zielserver durch `--server=Servername` angegeben. Der angegebene Zielserver fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Verfahren

- ◆ Führen Sie den Befehl `esxcli --server=Servername storage nfs list` aus.

In der Spalte „Hardwarebeschleunigung“ der Ausgabe wird der Status angezeigt.

## Überlegungen bei der Hardwarebeschleunigung

Wenn Sie die Funktionalität der Hardwarebeschleunigung nutzen, muss Folgendes beachtet werden.

Es gibt mehrere mögliche Gründe für das Fehlschlagen eines hardwarebeschleunigten Vorgangs.

Für jedes Primitiv, das das Array nicht implementiert, gibt das Array einen Fehler zurück. Der Fehler sorgt dafür, dass der ESXi-Host versucht, den Vorgang unter Verwendung seiner nativen Methoden durchzuführen.

Der VMFS Data Mover nutzt keine Hardware-Offloads. Stattdessen werden in den folgenden Fällen Software-Datenverschiebungen verwendet:

- Die Quell- und Ziel-VMFS-Datenspeicher haben unterschiedliche Blockgrößen.
- Der Typ der Quelldatei ist RDM und der Typ der Zieldatei ist Nicht-RDM (normale Datei).
- Der VMDK-Typ der Quelle ist „eagerzeroedthick“ und der VMDK-Typ des Ziels ist „thin“.
- Das Format der Quell- oder Ziel-VMDK ist „sparse“ oder „hosted“.
- Die virtuelle Quellmaschine hat einen Snapshot.

- Die logische Adresse und die Übertragungslänge des angeforderten Vorgangs sind nicht auf die vom Speichergerät erforderliche Mindestausrichtung ausgerichtet. Alle mit dem vSphere Web Client erstellten Datenspeicher werden automatisch ausgerichtet.
- Das VMFS hat mehrere LUNs oder Erweiterungen und sie befinden sich auf unterschiedlichen Arrays.

Das Klonen von Hardware zwischen Arrays, auch innerhalb desselben VMFS-Datenspeichers, funktioniert nicht.

# Bereitstellung im Format „Thick“ bzw. „Thin“ beim Speicher

# 24

vSphere unterstützt zwei Formate der Bereitstellung von Speicher, Thick und Thin.

## Bereitstellungsformat „Thick“

Hierbei handelt es sich um das traditionelle Format der Speicherbereitstellung. Beim Thick Provisioning wird eine große Menge an Speicherplatz im Voraus in Erwartung zukünftiger Speicheranforderungen bereitgestellt. Möglicherweise bleibt der Speicherplatz jedoch ungenutzt, was dazu führen kann, dass die Speicherkapazität nicht voll ausgenutzt wird.

## Thin Provisioning

Bei dieser Methode können Sie im Unterschied zum Format „Thick“ Probleme mit zu geringer Auslastung des Speichers beseitigen, indem Speicherplatz auf flexible Weise nach Bedarf zugeteilt wird. Mit ESXi können Sie zwei Modelle des Thin Provisioning verwenden: Thin Provisioning auf Array-Ebene und Thin Provisioning auf der Ebene der virtuellen Festplatte.

Dieses Kapitel enthält die folgenden Themen:

- [Datenspeicher-Überbuchung](#)
- [Thin Provisioning virtueller Festplatten](#)
- [Array-Thin Provisioning und VMFS-Datenspeicher](#)

## Datenspeicher-Überbuchung

Thin Provisioning ermöglicht Ihnen, eine größere Menge an virtuellem Speicherplatz zu melden als die echte physische Kapazität. Diese Diskrepanz kann zu einer Datenspeicher-Überbuchung führen, die auch als Überbelegung bezeichnet wird.

Wenn Sie Thin Provisioning verwenden, sollten Sie die tatsächliche Speichernutzung überwachen, um eine Knappheit des physischen Speicherplatzes zu verhindern.

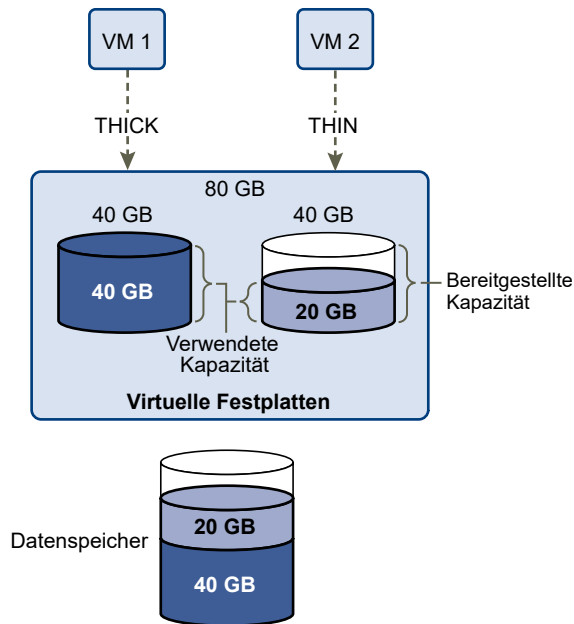
## Thin Provisioning virtueller Festplatten

Wenn Sie eine virtuelle Maschine erstellen, wird ein bestimmter Teil des Speicherplatzes auf einem Datenspeicher für die virtuellen Festplattendateien bereitgestellt.

Standardmäßig bietet ESXi eine herkömmliche Speicherbereitstellungsmethode für virtuelle Maschinen. Mit dieser Methode schätzen Sie zuerst, wie viel Speicher die virtuelle Maschine für den gesamten Lebenszyklus benötigt. Sie stellen dann im Voraus eine feste Menge an Speicherplatz für ihre virtuelle Festplatte bereit, beispielsweise 40 GB, und ordnen den gesamten bereitgestellten Speicherplatz der virtuellen Festplatte zu. Eine virtuelle Festplatte, die sofort den gesamten bereitgestellten Speicherplatz belegt, ist eine Thick-Festplatte.

ESXi unterstützt Thin Provisioning für virtuelle Festplatten. Die Thin Provisioning-Funktion auf Festplattenebene ermöglicht Ihnen das Erstellen von virtuellen Festplatten in einem Thin-Format. ESXi teilt einer virtuellen Festplatte im Thin-Format den gesamten für aktuelle und zukünftige Aktionen erforderlichen Speicherplatz zu, beispielsweise 40 GB. Allerdings verwendet die Thin-Festplatte nur so viel Speicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. In diesem Beispiel belegt die Thin-bereitgestellte Festplatte nur 20 GB an Speicherplatz. Wenn die Festplatte mehr Speicherplatz benötigt, kann sie bis auf die 40 GB an bereitgestelltem Speicherplatz anwachsen.

**Abbildung 24-1. Virtuelle Thick- und Thin-Festplatten**



## Grundlegendes zu Bereitstellungsrichtlinien für virtuelle Festplatten

Wenn Sie bestimmte Vorgänge für die Verwaltung virtueller Maschinen ausführen, z. B. Erstellen einer virtuellen Festplatte, Klonen einer virtuellen Maschine in eine Vorlage oder Migrieren einer virtuellen Maschine, können Sie eine Bereitstellungsrichtlinie für die Datei der virtuellen Festplatte festlegen.

NFS-Datenspeicher mit Hardwarebeschleunigung und VMFS-Datenspeicher unterstützen die folgenden Festplattenbereitstellungsrichtlinien. Auf NFS-Datenspeichern, die die Hardwarebeschleunigung nicht unterstützen, steht nur das Thin-Format zur Verfügung.



Mithilfe von Storage vMotion oder Cross-Host Storage vMotion können Sie virtuelle Laufwerke von einem Format in ein anderes umwandeln.

### Thick-Provision Lazy-Zeroed

Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird zugeteilt, wenn die Festplatte erstellt wird. Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens gelöscht, sondern sie werden bei Bedarf zu einem späteren Zeitpunkt beim ersten Schreiben von der virtuellen Maschine durch Nullbyte ersetzt. Virtuelle Maschinen lesen keine veralteten Daten vom physischen Gerät.

### Thick-Provision Eager-Zeroed

Ein Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Thick-Provision Lazy-Zeroed-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von virtuellen Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen.

### Thin Provision

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 Größe der virtuellen Festplatte eingeben. Die Festplatte besitzt jedoch zunächst nur eine geringe Größe und verwendet nur so viel Datenspeicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. Wenn die Festplatte später mehr Speicherplatz benötigt, kann sie auf ihre maximale Kapazität anwachsen und den gesamten für sie bereitgestellten Datenspeicherplatz in Anspruch nehmen.

Thin Provisioning stellt die schnellste Methode zum Erstellen einer virtuellen Festplatte dar, da lediglich eine Festplatte nur mit den Header-Informationen erstellt wird. Speicherblöcke werden nicht zugewiesen oder auf Null gesetzt. Speicherblöcke werden bei ihrem ersten Zugriff zugewiesen oder auf Null gesetzt.

---

**Hinweis** Wenn eine virtuelle Festplatte Clusterlösungen wie z. B. Fault Tolerance unterstützt, verwenden Sie für die Festplatte nicht das Format „Thin“.

---

Sie können die Thin-Festplatte manuell vergrößern, sodass sie den gesamten bereitgestellten Speicherplatz belegt. Wenn der Speicherplatz des physischen Speichers aufgebraucht ist und die Thin-bereitgestellte Festplatte nicht vergrößert werden kann, kann die virtuelle Maschine nicht mehr genutzt werden.

## Erstellen von virtuellen Thin-bereitgestellten Festplatten

Um Speicherplatz zu sparen, 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. Sie können Thin-Festplatten nur auf Datenspeichern erstellen, die Thin Provisioning auf Festplattenebene unterstützen.

Bei diesem Verfahren wird vorausgesetzt, dass Sie eine neue virtuelle Maschine erstellen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

## Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datacenter, Ordner, Cluster, Ressourcenpool oder Host, und wählen Sie die Option **Neue virtuelle Maschine** aus.
- 2 Wählen Sie **Eine neue virtuelle Maschine erstellen** und klicken Sie auf **Weiter**.
- 3 Befolgen Sie sämtliche Anweisungen zum Erstellen einer virtuellen Maschine.
- 4 Klicken Sie auf der Seite „Hardware anpassen“ auf die Registerkarte **Virtuelle Hardware**.
- 5 Klicken Sie auf das Dreieck **Neue Festplatte**, um die Festplattenoptionen zu erweitern.
- 6 (Optional) Passen Sie die Standardfestplattengröße an.

Mit einer virtuellen Thin-Festplatte zeigt der Wert für die Datenträgergröße an, wie viel Speicher auf der Festplatte bereitgestellt und garantiert wird. Anfänglich verwendet die virtuelle Festplatte möglicherweise nicht den gesamten bereitgestellten Speicher und der aktuelle Wert für die Speicherverwendung kann die Größe der virtuellen Festplatte unterschreiten.

- 7 Wählen Sie **Thin Provision** für Festplattenbereitstellung aus.
- 8 Schließen Sie die Erstellung einer virtuellen Maschine ab.

## Ergebnisse

Sie haben eine virtuelle Maschine mit einer Festplatte im Thin-Format erstellt.

## Nächste Schritte

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.

Die Anzeige der Speicherbelegung zeigt den Datenspeicherplatz, der 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.

Für virtuelle Maschinen mit Thin-Festplatten kann der tatsächliche Speichernutzungswert geringer als die Größe der virtuellen Festplatte sein.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Doppelklicken Sie auf die virtuelle Maschine, und klicken Sie auf die Registerkarte **Übersicht**.
- 3 Prüfen Sie die Informationen über die Speicherbelegung rechts oben auf der Registerkarte **Übersicht**.

## Festlegen des Festplattenformats für eine virtuelle Maschine

Sie können festlegen, ob Ihre virtuelle Festplatte im Thick- oder im Schnell-Format vorliegen soll.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Virtuelle Hardware**.
- 4 Klicken Sie auf das Dreieck **Festplatte**, um die Festplattenoptionen zu erweitern.

Im Textfeld **Typ** wird das Format Ihrer virtuellen Festplatte angezeigt.

### Nächste Schritte

Wenn die virtuelle Festplatte das Format „Schnell“ aufweist, können Sie sie auf ihre volle Größe vergrößern.

## Vergrößern virtueller Thin-Festplatten

Wenn Sie eine virtuelle Festplatte im Format „Thin-Bereitstellung“ erstellt haben, können Sie die Thin-Festplatte in das Format „Thick-Provision“ konvertieren.

Sie können mit dem Datenspeicherbrowser die virtuelle Festplatte vergrößern.

### Voraussetzungen

- Stellen Sie sicher, dass der Datenspeicher, in dem sich die virtuelle Maschine befindet, über ausreichend Speicherplatz verfügt.
- Stellen Sie zudem sicher, dass die virtuelle Festplatte das Thin-Format aufweist.
- Entfernen Sie Snapshots.
- Schalten Sie die virtuelle Maschine aus.

### Verfahren

- 1 Wechseln Sie zu dem Ordner der virtuellen Festplatte, die Sie vergrößern möchten.
  - a Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
  - b Doppelklicken Sie auf die virtuelle Maschine zum Anzeigen ihrer Informationen.


- c Klicken Sie auf der Registerkarte **Verwandte Objekte** und klicken Sie auf **Datenspeicher**.

Der Datenspeicher, in dem die Dateien der virtuellen Maschine gespeichert sind, wird angezeigt.

- d Wählen Sie den Datenspeicher aus und klicken Sie auf das Symbol **Navigieren zum Datei-Browser des Datenspeichers**.

Der Datenspeicherbrowser zeigt den Inhalt des Datenspeichers an.

- 2 Öffnen Sie den Ordner der virtuellen Maschine und navigieren Sie zu der virtuellen Festplattendatei, die Sie konvertieren möchten.

Die Datei hat die Erweiterung `.vmdk` und ist durch das Symbol für virtuelle Festplatten () gekennzeichnet.

- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Festplattendatei und wählen Sie **Vergrößern**.

---

**Hinweis** Die Option ist möglicherweise nicht verfügbar, wenn die virtuelle Festplatte das Thick-Format aufweist oder wenn die virtuelle Maschine ausgeführt wird.

---

## Ergebnisse

Die vergrößerte virtuelle Festplatte belegt den ganzen Datenspeicherplatz, der ursprünglich für sie 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.

Informationen zum Einstellen von Alarmen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

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.

Weitere Informationen hierzu finden Sie unter [Erhöhen der VMFS-Datenspeicherkapazität](#).

## Array-Thin Provisioning und VMFS-Datenspeicher

Sie können Thin-bereitgestellte Speicher-Arrays mit ESXi verwenden.

Herkömmliche LUNs, die Arrays dem ESXi-Host präsentieren, sind Thick-bereitgestellt. Der gesamte physische Speicherplatz, der zum Stützen einer jeden LUN benötigt wird, wird im Voraus zugeteilt.

ESXi unterstützt auch Thin-bereitgestellte LUNs. Wenn eine LUN Thin-bereitgestellt ist, meldet das Speicher-Array die logische Größe der LUN, die möglicherweise größer als die echte physische Kapazität ist, die diese LUN stützt.

Ein VMFS-Datenspeicher, den Sie auf der Thin-bereitgestellten LUN bereitstellen, kann nur die logische Größe der LUN erkennen. Wenn das Array beispielsweise 2 TB Speicherkapazität meldet, während in Wirklichkeit das Array nur 1 TB Speicherkapazität bereitstellt, geht der Datenspeicher davon aus, dass die Größe der LUN 2 TB beträgt. Während der Datenspeicher anwächst, kann er nicht feststellen, ob die tatsächliche Menge des physischen Speichers noch ausreicht.

Wenn Sie jedoch „Storage APIs - Array Integration“ verwenden, kann sich der Host mit dem physischen Speicher integrieren und somit die zugrunde liegenden Thin-bereitgestellten LUNs und deren Speichernutzung erkennen.

Mithilfe der Thin-Provision-Integration kann der Host diese Aufgaben durchführen:

- Überwachen der Nutzung des Speicherplatzes auf Thin-bereitgestellten LUNs, um zu verhindern, dass der physische Speicherplatz aufgebraucht wird. Während der Datenspeicher anwächst oder wenn Sie Storage vMotion zum Migrieren von virtuellen Maschinen auf eine Thin-bereitgestellte LUN verwenden, kommuniziert der Host mit der LUN und warnt Sie vor Verletzungen des physischen Speicherplatzes und vor Speicherplatzknappheit.
- Informieren des Arrays über den Speicherplatz des Datenspeichers, der freigegeben wird, wenn Storage vMotion Dateien löscht oder aus dem Datenspeicher entfernt. Das Array kann dann die freigegebenen Speicherblöcke zurückgewinnen.

---

**Hinweis** ESXi unterstützt das Aktivieren und Deaktivieren von Thin Provisioning auf einem Speichergerät nicht.

---

## Anforderungen

Zur Verwendung der Thin Provisioning-Berichtsfunktion müssen der Host und das Speicher-Array die folgenden Anforderungen erfüllen:

- ESXi Version 5.0 oder höher.
- Das Speicher-Array verfügt über die entsprechende Firmware, die T10-basierte „Storage-APIs - Array Integration“ (Thin Provisioning) unterstützt. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter oder sehen Sie in der Hardwarekompatibilitätsliste nach.

## Überwachen der Speicherplatznutzung

Die Funktion für die Thin Provisioning-Integration hilft Ihnen, die Speicherplatznutzung auf Thin-bereitgestellten LUNs zu überwachen und zu vermeiden, dass kein Speicherplatz mehr zur Verfügung steht.

Das folgende Datenflussbeispiel zeigt, wie der ESXi-Host und das Speicher-Array interagieren, um Warnungen hinsichtlich Speicherplatzverletzungen und Speicherplatzknappheit für einen Datenspeicher mit zugrunde liegender Thin-bereitgestellter LUN zu generieren. Derselbe Mechanismus wird angewendet, wenn Sie Storage vMotion zum Migrieren von virtuellen Maschinen auf die Thin-bereitgestellte LUN verwenden.

- 1 Mithilfe von speicherspezifischen Tools stellt Ihr Speicheradministrator eine Thin-LUN bereit und legt einen Soft-Schwellenwert fest, bei dessen Erreichen ein Alarm ausgelöst wird. Dieser Schritt ist anbieterspezifisch.
- 2 Mithilfe des vSphere Web Client erstellen Sie einen VMFS-Datenspeicher auf der Thin-bereitgestellten LUN. Der Datenspeicher umfasst die gesamte logische Größe, die die LUN meldet.
- 3 Wenn die vom Datenspeicher verwendete Speicherplatzmenge ansteigt und den angegebenen Soft-Schwellenwert erreicht, finden die folgenden Aktionen statt:
  - a Das Speicher-Array meldet die Verletzung Ihrem Host.
  - b Ihr Host löst einen Warnungsalarm für den Datenspeicher aus.

Sie können sich an den Speicheradministrator wenden, um mehr physischen Speicherplatz anzufordern, oder Storage vMotion verwenden, um Ihre virtuellen Maschinen zu entfernen, bevor die LUN keine Kapazität mehr hat.
- 4 Wenn kein Speicherplatz mehr zur Verfügung steht, der der Thin-bereitgestellten LUN zugeteilt werden kann, finden die folgenden Aktionen statt:
  - a Das Speicher-Array meldet dem Host, dass kein freier Speicherplatz verfügbar ist.

---

**Vorsicht** In einigen Fällen, wenn eine LUN voll wird, kann es offline gehen oder die Zuordnung vom Host entfernen.

---

- b Der Host hält virtuelle Maschinen an und generiert einen Speicherplatzknappheits-Alarm.
- Sie können das dauerhafte Problem der Speicherplatzknappheit beheben, indem Sie vom Speicheradministrator mehr physischen Speicherplatz anfordern.

## Identifizieren von Thin-bereitgestellten Speichergeräten

Verwenden Sie den Befehl `esxcli`, um festzustellen, ob ein bestimmtes Speichergerät Thin-bereitgestellt ist.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Führen Sie den Befehl `esxcli --server=Servername storage core device list -d=Geräte-ID` aus.

## Ergebnisse

Der folgende Thin Provisioning-Status gibt an, dass das Speichergerät Thin-bereitgestellt ist.

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c
  Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXX4c)
  Size: 20480
  Device Type: Direct-Access
  Multipath Plugin: NMP
  -----
  Thin Provisioning Status: yes
  Attached Filters: VAAI_FILTER
  VAAI Status: supported
  -----
```

Ein unbekannter Status gibt an, dass ein Speichergerät Thick ist.

---

**Hinweis** Einige Speichersysteme präsentieren alle Geräte als Thin-bereitgestellt, egal ob die Geräte Thin oder Thick sind. Ihr Thin Provisioning-Status ist immer Ja. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

---

## Zurückgewinnen von angesammeltem Speicherplatz

Wenn sich VMFS-Datenspeicher auf in Thin-bereitgestellten LUNs befinden, können Sie mit dem Befehl `esxcli` nicht verwendete Speicherblöcke zurückzugewinnen.

In dem Vorgang wird der Zielservers durch `--server=Servername` angegeben. Der angegebene Zielservers fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

## Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

## Verfahren

- ◆ Gewinnen Sie nicht verwendete Speicherblöcke im VMFS5-Datenspeicher für das Thin-bereitgestellte Gerät zurück, indem Sie den folgenden Befehl ausführen:

```
esxcli --server=Servername storage vmfs unmap --volume-label=Volume-Bezeichnung|--volume-uuid=Volume-UUID --reclaim-unit=Anzahl
```

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
<b>-l --volume-label=Volume-Bezeichnung</b>	Die Bezeichnung des VMFS-Volumes, dessen Zuordnung aufgehoben werden soll. Dies ist ein erforderliches Argument. Verwenden Sie bei Angabe dieses Arguments nicht <b>-u --volume-uuid=Volume-UUID</b> .
<b>-u --volume-uuid=Volume-UUID</b>	Die UUID des VMFS-Volumes, dessen Zuordnung aufgehoben werden soll. Dies ist ein erforderliches Argument. Verwenden Sie bei Angabe dieses Arguments nicht <b>-l --volume-label=Volume-Bezeichnung</b> .
<b>-n --reclaim-unit=Anzahl</b>	Die Anzahl der VMFS-Blöcke, deren Zuordnung pro Iteration aufgehoben werden soll. Dies ist ein optionales Argument. Wenn es nicht angegeben wird, verwendet der Befehl den Standardwert 200.

## Nächste Schritte

**Wichtig** Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2014849>.



# Verwenden von Speicheranbietern

# 25

Ein Speicheranbieter ist eine Softwarekomponente, die entweder von vSphere angeboten oder von einem Drittanbieter über die vSphere-APIs für Storage Awareness (VASA) entwickelt wurde. Speicheranbieter sind auf verschiedene Speicherelemente abgestimmt, darunter externe physische Speicher und Speicherabstraktionen, wie Virtual SAN und virtuelle Volumes. Speicheranbieter können auch Softwarelösungen unterstützen, wie beispielsweise über vSphere APIs für E/A-Filter entwickelte E/A-Filter.

Im Allgemeinen verwendet vSphere Speicheranbieter zum Abrufen von Informationen zur Speichertopologie, zum Status und zu Speicherdatendiensten, die in Ihrer Umgebung angeboten werden. Diese Informationen werden im vSphere Web Client angezeigt. Mit diesen Informationen können Sie leichter die richtige Entscheidung in Bezug auf die Platzierung der virtuellen Maschine treffen und Ihre Speicherumgebung überwachen.

In der Regel wird der externe Speicheranbieter auf der Speicherseite installiert und dient als Storage Awareness-Dienst in der vSphere-Umgebung.

Um zu erfahren, ob Ihr Speicher die Speicheranbieter-Plug-Ins unterstützt, wenden Sie sich an Ihren Speicheranbieter. Sofern Ihr Speicher externe Speicheranbieter unterstützt, verwenden Sie den vSphere Web Client zum Registrieren und Verwalten der Speicheranbieter-Komponenten.

Integrierte Speicheranbieter werden üblicherweise auf den ESXi-Hosts ausgeführt und müssen nicht registriert werden. Der Speicheranbieter, der Virtual SAN unterstützt, wird beispielsweise bei der Aktivierung des Virtual SAN automatisch registriert. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware Virtual SAN*.

Dieses Kapitel enthält die folgenden Themen:

- [Speicheranbieter und Darstellung von Speicherdaten](#)
- [Anforderungen und Überlegungen hinsichtlich Speicheranbietern](#)
- [Speicherstatusberichte](#)
- [Registrieren von Speicheranbietern](#)
- [Absichern der Kommunikation mit Speicheranbietern](#)
- [Anzeigen von Speicheranbieterinformationen](#)
- [Aufheben der Registrierung von Speicheranbietern](#)
- [Aktualisieren von Speicheranbietern](#)

## Speicheranbieter und Darstellung von Speicherdaten

vCenter Server und ESXi kommunizieren mit dem Speicheranbieter, um Informationen zu erhalten, die der Speicheranbieter von zugrunde liegenden physischen und softwaredefinierten Speichern oder von verfügbaren E/A-Filtern erfasst. vCenter Server kann dann die Speicherdaten in vSphere Web Client anzeigen.

Die vom Speicheranbieter bereitgestellten Informationen können in die folgenden Kategorien aufgeteilt werden:

- **Speicherdatendienste und -funktionen.** Diese Art von Informationen sind maßgeblich für Funktionen wie Virtual SAN, virtuelle Volumes und E/A-Filter. Der Speicheranbieter erfasst Informationen über die Datendienste, die von den zugrunde liegenden Speicherelementen oder verfügbaren E/A-Filtern angeboten werden.

Sie beziehen sich auf diese Datendienste, wenn Sie Speicheranforderungen für virtuelle Maschinen und virtuelle Festplatten in einer Speicherrichtlinie definieren. Die Speicherrichtlinie gewährleistet den für Ihre Umgebung geeigneten Speicherort einer virtuellen Maschine oder aktiviert spezifische Datendienste für virtuelle Festplatten. Weitere Informationen finden Sie unter [Grundlegende Informationen zu VM-Speicherrichtlinien](#).

- **Speicherstatus.** Diese Kategorie enthält Berichte zum Status verschiedener Speicherelemente. Sie enthält zudem Alarme und Ereignisse zum Senden von Benachrichtigungen über Konfigurationsänderungen.

Diese Informationen sind nützlich beim Beheben von Fehlern bei der Speicherverbindung und von Leistungsproblemen. Sie sind zudem hilfreich, um Array-generierte Ereignisse und Alarme mit den entsprechenden Leistungs- und Laständerungen am Array zu korrelieren.

- **Informationen über Storage DRS.** Für Distributed Resource Scheduling (DRS) in Blockgeräten oder Dateisystemen. Speicheranbieter liefern zusätzliche Daten über das Speichersystem, sodass die Verfahren von Storage DRS mit den Verfahren der Ressourcenverwaltung innerhalb der Speichersysteme kompatibel sind.

## Anforderungen und Überlegungen hinsichtlich Speicheranbietern

Wenn Sie die Speicheranbieter-Funktionalität verwenden, sind bestimmte Anforderungen und Überlegungen zu berücksichtigen.

In der Regel stellen die Lieferanten Speicheranbieter zur Verfügung, die mit vSphere verwendet werden können. Speicheranbieter werden über VMware-APIs für Storage Awareness (VASA) implementiert. Die VASA-Architektur erweitert den Speicherüberwachungsdienst (SMS), der bei vSphere enthalten ist, und definiert einen Satz von Funktionen, die vCenter Server und ESXi-Hosts zur Kommunikation mit VASA-Anbietern verwenden können.

Um Speicheranbieter zu verwenden, müssen diese Anforderungen erfüllt sein:

- Stellen Sie sicher, dass jeder Speicheranbieter, den Sie verwenden, durch VMware zertifiziert und ordnungsgemäß bereitgestellt ist. Informationen zum Bereitstellen der Speicheranbieter erhalten Sie vom Lieferanten Ihres Speichers oder im *VMware-Kompatibilitätshandbuch*.
- Stellen Sie sicher, dass der Speicheranbieter kompatibel mit der vSphere-Version ist. Siehe *VMware-Kompatibilitätshandbuch*.

Wenn Sie Speicheranbieter verwenden, ist Folgendes zu beachten:

- Sowohl Blockspeichergeräte als auch Dateisystem-Speichergeräte können Speicheranbieter verwenden.
- Speicheranbieter können überall ausgeführt werden, ausgenommen auf vCenter Server. In der Regel wird ein Dritt-Speicheranbieter auf dem Speicherarray-Dienstprozessor oder auf einem eigenständigen Host ausgeführt.
- Mehrere vCenter Server können gleichzeitig mit einer einzelnen Instanz eines Speicheranbieters verbunden werden.
- Ein einzelner vCenter Server kann gleichzeitig mit mehreren unterschiedlichen Speicheranbietern verbunden werden. Es ist möglich, für jeden Typ des physischen Speichergeräts, der Ihrem Host zur Verfügung steht, einen unterschiedlichen Speicheranbieter zu verwenden.

## Speicherstatusberichte

Wenn Sie Speicheranbieter verwenden, kann vCenter Server Statureigenschaften für physische Speichergeräte sammeln und diese Informationen im vSphere Web Client anzeigen.

Die Statusinformationen umfassen Ereignisse und Alarme.

- Ereignisse geben wichtige Änderungen an der Speicherkonfiguration an. Zu solchen Änderungen können die Erstellung und Löschung einer LUN gehören, oder dass auf eine LUN aufgrund der LUN-Maskierung nicht mehr zugegriffen werden kann.
- Alarme weisen auf eine Änderung der Speichersystemverfügbarkeit hin. Wenn Sie beispielsweise die profilbasierte Speicherverwaltung verwenden, können Sie Speicheranforderungen für virtuelle Maschinen angeben. Wenn Änderungen am zugrunde liegenden Speicher erfolgen, die möglicherweise gegen die Speicheranforderungen der virtuellen Maschine verstoßen, wird ein Alarm ausgelöst.

Weitere Informationen zu Ereignissen und Alarmen finden Sie in der Dokumentation zu *vSphere-Überwachung und -Leistung*.

Für Thin-bereitgestellte LUNs bestehen spezielle Anforderungen hinsichtlich der Berichterstellung. Informationen zur Speicherplatzüberwachung auf Thin-bereitgestellten LUNs finden Sie unter [Array-Thin Provisioning und VMFS-Datenspeicher](#).

## Registrieren von Speicheranbietern

Sie müssen zum Herstellen einer Verbindung zwischen vCenter Server und einem Speicheranbieter den Speicheranbieter registrieren. Stellen Sie sicher, dass Sie einen separaten Speicheranbieter für jeden Host in einem Cluster registrieren.

---

**Hinweis** Wenn Sie Virtual SAN verwenden, werden die Speicheranbieter für Virtual SAN registriert und automatisch in der Liste der Speicheranbieter angezeigt. Virtual SAN unterstützt keine manuelle Registrierung von Speicheranbietern. Informationen finden Sie in der Dokumentation *Verwalten von VMware Virtual SAN*.

---

### Voraussetzungen

Stellen Sie sicher, dass die Speicheranbieter-Komponente auf der Speicherseite installiert ist, und fragen Sie Ihren Speicheradministrator nach den Anmeldedaten.

### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Klicken Sie auf das Symbol **Neuen Speicheranbieter registrieren**.
- 4 Geben Sie die Verbindungsinformationen für den Speicheranbieter ein, einschließlich des Namens, der URL und der Anmeldedaten.
- 5 (Optional) Um vCenter Server zum Speicheranbieterzertifikat zu leiten, wählen Sie die Option **Zertifikat des Speicheranbieters verwenden** aus und geben den Speicherort des Zertifikats an.  
  
Wenn Sie diese Option nicht auswählen, wird ein Fingerabdruck des Zertifikats angezeigt. Sie können den Fingerabdruck überprüfen und ihn genehmigen.
- 6 Klicken Sie auf **OK**, um die Registrierung abzuschließen.

### Ergebnisse

vCenter Server hat den Speicheranbieter registriert und eine sichere SSL-Verbindung mit ihm hergestellt.

### Nächste Schritte

Falls der Speicheranbieter nicht registriert werden kann, lesen Sie den VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2079087>. Informationen zu Problemen bei der Registrierung von Virtual SAN-Speicheranbietern finden Sie unter <http://kb.vmware.com/kb/2105018>.

## Absichern der Kommunikation mit Speicheranbietern

Für die Kommunikation mit einem Speicheranbieter verwendet der vCenter Server eine sichere SSL-Verbindung. Der SSL-Authentifizierungsmechanismus erfordert, dass beide Parteien, der

vCenter Server und der Speicheranbieter, SSL-Zertifikate austauschen und sie zu ihren Truststores hinzufügen.

Der vCenter Server kann das Speicheranbieterzertifikat im Rahmen der Speicheranbieterinstallation zu seinem Truststore hinzufügen. Falls das Zertifikat nicht während der Installation hinzugefügt wird, verwenden Sie eine der folgenden Methoden, um es beim Registrieren des Speicheranbieters hinzuzufügen:

- Navigieren Sie in vCenter Server zum Zertifikat des Speicheranbieters. Wählen Sie im Dialogfeld **Neuer Speicheranbieter** die Option **Zertifikat des Speicheranbieters verwenden** aus und geben Sie den Speicherort des Zertifikats an.
- Verwenden Sie einen Fingerabdruck des Speicheranbieterzertifikats. Wenn Sie vCenter Server nicht verlassen, das Anbieter-Zertifikat zu verwenden, wird der Fingerabdruck des Zertifikats angezeigt. Sie können den Fingerabdruck überprüfen und ihn genehmigen. Der vCenter Server fügt das Zertifikat zum Truststore hinzu und fährt mit dem Herstellen der Verbindung fort.

Der Speicheranbieter fügt das vCenter Server-Zertifikat zu seinem Truststore hinzu, wenn der vCenter Server zum ersten Mal eine Verbindung zum Anbieter herstellt.

## Anzeigen von Speicheranbieterinformationen

Nachdem Sie eine Speicheranbieterkomponente mit dem vCenter Server registriert haben, erscheint der Speicheranbieter auf der Liste der Speicheranbieter.

Zeigen Sie die allgemeinen Informationen zum Speicheranbieter und die Details für jede Speicherkomponente an.

### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Zeigen Sie in der Liste „Speicheranbieter“ die mit dem vCenter Server registrierten Speicheranbieterkomponenten an.

Die Liste enthält allgemeine Anbieterinformationen, wie den Namen, die URL sowie den Zeitpunkt der letzten Ansichtsaktualisierung.

- 4 Wenn Sie weitere Details ansehen möchten, wählen Sie einen bestimmten Speicheranbieter aus der Liste aus.

Zu den Detailinformationen gehören Speicher-Array-Anbieter sowie die vom Anbieter unterstützten Array-Modelle.

---

**Hinweis** Ein einzelner Speicheranbieter kann Speicher-Arrays vieler verschiedener Anbieter unterstützen.

---

## Aufheben der Registrierung von Speicheranbietern

Heben Sie die Registrierung für nicht benötigte Speicheranbieter auf.

---

**Vorsicht** Die Registrierung von Speicheranbietern, die von VMware geliefert werden, wie zum Beispiel Speicheranbieter für Virtual SAN, kann nicht manuell aufgehoben werden.

---

### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Wählen Sie aus der Liste der Speicheranbieter denjenigen aus, für den Sie die Registrierung aufheben möchten, und klicken Sie auf **Registrierung des Speicheranbieters aufheben**.

### Ergebnisse

vCenter Server beendet die Verbindung und entfernt den Speicheranbieter aus seiner Konfiguration.

## Aktualisieren von Speicheranbietern

vCenter Server aktualisiert die Speicherdaten in seiner Datenbank in regelmäßigen Abständen. Die Updates sind unvollständig und spiegeln nur die Speicheränderungen wider, die Speicheranbieter an den vCenter Server übertragen. Bei Bedarf können Sie eine vollständige Datenbanksynchronisierung für den ausgewählten Speicheranbieter durchführen.

### Verfahren

- 1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
- 3 Wählen Sie aus der Liste den Speicheranbieter aus, mit dem Sie synchronisieren möchten, und klicken Sie auf das Symbol **Speicheranbieter erneut prüfen**.

### Ergebnisse

Der vSphere Web Client aktualisiert die Speicherdaten für den Anbieter.

# Verwenden von „vmkfstools“

# 26

`vmkfstools` ist einer der ESXi-Shell-Befehle zum Verwalten von VMFS-Volumes und virtuellen Festplatten. Mit dem `vmkfstools`-Befehl können Sie viele Speichervorgänge durchführen. Beispielsweise können Sie VMFS-Datenspeicher auf einer physischen Partition erstellen und verwalten oder virtuelle Festplattendateien bearbeiten, die auf VMFS- oder NFS-Datenspeichern abgelegt sind.

---

**Hinweis** Nachdem Sie mit `vmkfstools` eine Änderung vorgenommen haben, wird der vSphere Web Client möglicherweise nicht sofort aktualisiert. Sie müssen vom Client aus eine Aktualisierung oder eine erneute Prüfung vornehmen.

---

Weitere Informationen zur ESXi-Shell finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Dieses Kapitel enthält die folgenden Themen:

- [vmkfstools-Befehlssyntax](#)
- [vmkfstools-Optionen](#)

## vmkfstools-Befehlssyntax

Im Allgemeinen müssen Sie sich nicht als Root-Benutzer anmelden, um die `vmkfstools`-Befehle auszuführen. Einige Befehle, z. B. Dateisystembefehle, erfordern jedoch eine Root-Anmeldung.

Der Befehl `vmkfstools` hat die folgende Befehlssyntax:

`vmkfstools` *Verbindungsoptionen* *Optionen* *Ziel*.

*Ziel* gibt eine Partition, ein Gerät oder einen Pfad an, auf den die Befehlsoption angewendet werden soll.

Tabelle 26-1. `vmkfstools`-Befehlsargumente

Argument	Beschreibung
Optionen	<p>Eine oder mehrere Befehlszeilenoptionen und die zugehörigen Argumente, mit denen Sie die Aktivität angeben können, die <code>vmkfstools</code> ausführen soll. Hierzu gehört beispielsweise die Auswahl des Festplattenformats beim Erstellen einer neuen virtuellen Festplatte.</p> <p>Geben Sie nach der Eingabe der Option ein Ziel für den Vorgang an. Ziel kann eine Partition, ein Gerät oder ein Pfad sein.</p>
Partition	<p>Bezeichnet die Festplattenpartitionen. Dieses Argument verwendet das Format <i>Festplatten-ID:P</i>, wobei es sich bei <i>Festplatten-ID</i> um die vom Speicher-Array zurückgegebene Geräte-ID und bei <i>P</i> um eine Ganzzahl handelt, die die Partitionsnummer angibt. Diese Zahl der Partition muss größer als Null (0) sein und einer gültigen VMFS-Partition entsprechen.</p>
Gerät	<p>Gibt die Geräte oder logischen Volumes an. Dieses Argument verwendet einen Pfadnamen im ESXi-Gerätedateisystem. Der Pfadname beginnt mit <code>/vmfs/</code> Geräte, wobei es sich um den Mount-Punkt des Gerätedateisystems handelt. Verwenden Sie zur Angabe der verschiedenen Gerätetypen die folgenden Formate:</p> <ul style="list-style-type: none"> <li>■ <code>/vmfs/Geräte/Festplatten</code> für lokale oder SAN-basierte Festplatten.</li> <li>■ <code>/vmfs/devices/lvm</code> für logische ESXi-Volumes.</li> <li>■ <code>/vmfs/Geräte/generisch</code> für generische SCSI-Geräte.</li> </ul>
Pfad	<p>Bezeichnet ein VMFS-Dateisystem oder eine Datei. Bei diesem Argument handelt es sich um einen absoluten oder relativen Pfad, der einen symbolischen Link zu einem Verzeichnis, einer Raw-Gerätezuordnung oder einer Datei unter <code>/vmfs</code> aufführt.</p> <ul style="list-style-type: none"> <li>■ Um ein VMFS-Dateisystem anzugeben, verwenden Sie dieses Format: <pre>/vmfs/volumes/file_system_UUID</pre> <p>oder</p> <pre>/vmfs/volumes/file_system_label</pre> </li> <li>■ Verwenden Sie dieses Format, um eine Datei auf einem VMFS-Datenspeicher anzugeben: <pre>/vmfs/volumes/file_system_label file_system_UUID/[dir]/myDisk.vmdk</pre> <p>Sie brauchen nicht den gesamten Pfad anzugeben, wenn das aktuelle Arbeitsverzeichnis gleichzeitig das übergeordnete Verzeichnis von <code>myDisk.vmdk</code> ist.</p> </li> </ul>

## vmkfstools-Optionen

Der Befehl `vmkfstools` enthält mehrere Optionen. Einige der Optionen sollten nur von erfahrenen Benutzern verwendet werden.



Die Lang- und Kurzformen (mit einem Buchstaben) der Optionen sind gleichwertig. So sind zum Beispiel die folgenden Befehle identisch.

```
vmkfstools --createfs vmfs5 --blocksize 1m disk_ID:P
vmkfstools -C vmfs5 -b 1m disk_ID:P
```

## Unteroption -v

Die Unteroption `-v` bestimmt die Ausführlichkeit der Meldungen in der Befehlsausgabe.

Das Format für diese Unteroption lautet wie folgt:

```
-v --verbose number
```

Der Wert *Zahl* wird als ganze Zahl von 1 bis 10 angegeben.

Sie können die Unteroption `-v` für alle `vmkfstools`-Optionen verwenden. Wenn die Unteroption `-v` für die Ausgabe einer Option nicht vorgesehen ist, ignoriert `vmkfstools` den Teil `-v` der Befehlszeile.

---

**Hinweis** Da Sie die Unteroption `-v` in jeder `vmkfstools`-Befehlszeile verwenden können, wird sie in den Beschreibungen der einzelnen Optionen nicht als Unteroption verwendet.

---

## Dateisystemoptionen

Mithilfe von Dateisystemoptionen können Sie einen VMFS-Datenspeicher erstellen und verwalten. Diese Optionen gelten nicht für NFS. Sie können viele dieser Aufgaben auch über den vSphere Web Client ausführen.

### Auflisten der Attribute eines VMFS-Volumes

Verwenden Sie zum Auflisten der Attribute eines VMFS-Volumes den Befehl `vmkfstools`.

```
-P --queryfs
    -h --humanreadable
```

Diese Option listet die Attribute des angegebenen Volumes auf, wenn Sie sie auf eine Datei oder ein Verzeichnis auf einem VMFS-Volume anwenden. Zu den aufgelisteten Attributen gehören die Dateisystembezeichnung, falls vorhanden, die Anzahl an Erweiterungen, aus denen das angegebene VMFS-Volume besteht, die UUID und eine Liste der Namen der Geräte, auf denen sich die einzelnen Erweiterungen befinden.

---

**Hinweis** Wenn ein Gerät zur Sicherung des VMFS-Dateisystems offline geschaltet wird, ändert sich die Anzahl der Erweiterungen und des verfügbaren Speichers entsprechend.

---

Sie können die Unteroption `-h` für die Option `-P` verwenden. In diesem Fall listet `vmkfstools` die Kapazität des Volumes in verständlicherer Form auf, z. B. 5 k, 12.1 M oder 2.1 G.

## Erstellen eines VMFS-Datenspeichers

Verwenden Sie zum Erstellen eines VMFS-Datenspeichers den Befehl `vmkfstools`.

```
-C --createfs [vmfs5]
-S --setfsname datastore
```

Mit dieser Option wird ein VMFS5-Datenspeicher auf der angegebenen SCSI-Partition erstellt, z. B. `disk_ID:P`. Diese Partition wird die vorgelagerte Partition des Dateisystems.

---

**Hinweis** Sie können vorhandene VMFS3-Datenspeicher weiterhin verwenden, aber keine neuen VMFS3-Datenspeicher erstellen. Aktualisieren Sie Ihre VMFS3-Datenspeicher auf VMFS5.

---

Für die Option `-c` können Sie folgende Unteroptionen angeben:

- `-S --setfsname` – Definieren Sie die Volume-Bezeichnung des VMFS-Datenspeichers, den Sie erstellen. Für die Option `-c` können Sie folgende Unteroptionen angeben. Die Bezeichnung kann bis zu 128 Zeichen lang sein und darf keine Leerstellen am Anfang oder Ende enthalten.

---

**Hinweis** vCenter Server unterstützt die Längenbeschränkung von 80 Zeichen für alle Einträge. Wenn ein Datenspeichername diese Länge überschreitet, wird der Name beim Hinzufügen dieses Datenspeichers zu vCenter Server gekürzt.

---

Nachdem Sie die Volume-Bezeichnung festgelegt haben, können Sie sie bei der Angabe des VMFS-Datenspeichers im Befehl `vmkfstools` verwenden. Die Volume-Bezeichnung erscheint auch in den Auflistungen, die mit dem Linux-Befehl `ls -l` generiert werden, und als symbolische Verknüpfung zum VMFS-Volume im Verzeichnis `/vmfs/volumes`.

Verwenden Sie den Befehl `ln -sf`, wenn Sie die VMFS-Volume-Bezeichnung ändern möchten. Beispiel:

```
ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
```

*Datenspeicher* ist die neue Volume-Bezeichnung, die für das VMFS mit der *UUID* zu verwenden ist.

---

**Hinweis** Wenn der Host bei vCenter Server registriert ist, werden alle Änderungen, die Sie an der VMFS-Volume-Bezeichnung vornehmen, von vCenter Server überschrieben. Dies sorgt dafür, dass die VMFS-Bezeichnung über alle vCenter Server-Hosts hinweg einheitlich ist.

---

## Erstellen eines VMFS-Dateisystems – Beispiel

Dieses Beispiel veranschaulicht die Erstellung eines neuen VMFS5-Datenspeichers mit dem Namen „my\_vmfs“ auf der Partition `naa.ID:1`. Die Blockgröße dieser Datei ist 1 MB.

```
vmkfstools -C vmfs5 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

## Erweitern eines bestehenden VMFS-Volumes

Verwenden Sie zum Hinzufügen einer Erweiterung zu einem VMFS-Volume den Befehl `vmkfstools`.

```
-Z --spanfs span_partitionhead_partition
```

Mithilfe dieser Option wird das VMFS-Dateisystem mit der angegebenen Head-Partition erweitert, indem es sich über die durch `span_partition` angegebene Partition erstreckt. Sie müssen den vollständigen Pfadnamen eingeben, z. B. `/vmfs/devices/disks/disk_ID:1`. Bei jeder Verwendung dieser Option wird das VMFS-Volume um eine neue Erweiterung vergrößert, sodass das Volume mehrere Partitionen umfasst.

**Vorsicht** Wenn Sie diese Option ausführen, gehen alle Daten verloren, die auf dem SCSI-Gerät, das unter `span_partition` angegeben wird, gespeichert sind.

## Beispiel für die Erweiterung eines VMFS-Volumes

In diesem Beispiel erweitern Sie das logische Dateisystem, indem Sie zulassen, dass es eine neue Partition umfasst.

```
vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

Das erweiterte Dateisystem erstreckt sich über zwei Partitionen: `naa.disk_ID_1:1` und `naa.disk_ID_2:1`. In diesem Beispiel ist `naa.disk_ID_1:1` der Name der Head-Partition.

## Vergrößern einer vorhandenen Erweiterung

Anstatt einem VMFS-Datenspeicher eine neue Erweiterung hinzuzufügen, können Sie mithilfe des Befehls `vmkfstools -G` eine vorhandene Erweiterung vergrößern.

Verwenden Sie die folgende Option, um die Größe eines VMFS-Datenspeichers zu vergrößern, nachdem die Kapazität des zugrunde liegenden Speichers erhöht wurde.

```
-G --growfs devicedevice
```

Mithilfe dieser Option kann ein vorhandener VMFS-Datenspeicher oder seine Erweiterung vergrößert werden. Beispiel:

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

## Upgrade eines VMFS-Datenspeichers

Wenn Sie einen VMFS3-Datenspeicher verwenden, müssen Sie ein Upgrade auf VMFS5 durchführen.

**Vorsicht** Das Upgrade ist ein Prozess, der nur in eine Richtung ausgeführt werden kann. Nachdem Sie einen VMFS3-Datenspeicher in einen VMFS5-Datenspeicher konvertiert haben, können Sie diese Konvertierung nicht rückgängig machen.

Verwenden Sie zum Upgrade des Datenspeichers den folgenden Befehl: `vmkfstools -T|--upgrademfs /vmfs/volumes/UUID`

---

**Hinweis** Alle Hosts, die auf den Datenspeicher zugreifen, müssen VMFS5 unterstützen. Wenn ein ESX/ESXi-Host der Version 4.x oder früher den VMFS3-Datenspeicher verwendet, schlägt das Upgrade fehl und die MAC-Adresse des Hosts, der den Datenspeicher aktiv verwendet, wird angezeigt.

---

## Optionen für virtuelle Festplatten

Mithilfe von Optionen für virtuelle Festplatten können Sie in VMFS- und NFS-Dateisystemen gespeicherte virtuelle Festplatten einrichten, migrieren und verwalten. Sie können die meisten dieser Aufgaben auch über den vSphere Web Client ausführen.

### Unterstützte Festplattenformate

Beim Erstellen oder Klonen einer virtuellen Festplatte können Sie mit der Unteroption `-d --diskformat` das Format der Festplatte angeben.

Wählen Sie eines der folgenden Formate aus:

- `zeroedthick` (Standard) – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Alle Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt während der ersten Schreibvorgänge der virtuellen Maschine gelöscht. Die virtuelle Maschine liest keine veralteten Daten von der Festplatte.
- `eagerzeroedthick` – Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum `zeroedthick`-Format werden die verbleibenden Daten auf dem physischen Gerät während des Anlegens gelöscht. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.
- `thin` – Thin-bereitgestellte virtuelle Festplatte. Im Gegensatz zum `Thick`-Format wird der erforderliche Speicher für die virtuelle Festplatte nicht während des Anlegens bereitgestellt, sondern später in gelöschter Form und nach Bedarf.
- `rdm: Gerät` – Virtueller Kompatibilitätsmodus für die Raw-Festplattenzuordnung.
- `rdmp: Gerät` – Physischer Kompatibilitätsmodus (Pass-Through) für die Raw-Festplattenzuordnung.
- `2gbsparse` – Eine Ersatzfestplatte mit höchstens 2 GB Erweiterungsgröße. Festplatten in diesem Format können mit gehosteten VMware-Produkten verwendet werden, wie z. B. VMware Fusion, Player, Server oder Workstation. Sie können jedoch Ersatzfestplatten auf einem ESXi-Host erst einschalten, nachdem Sie die Festplatte mithilfe von `vmkfstools` in einem kompatiblen Format, wie z. B. `thick` oder `thin`, erneut importiert haben.

Weitere Informationen hierzu finden Sie unter [Migrieren von virtuellen Maschinen zwischen verschiedenen VMware-Produkten](#).

## NFS-Festplattenformate

Die einzigen Festplattenformate, die für NFS verwendet werden können, sind `thin`, `thick`, `zeroedthick` und `2gbsparse`.

Die Formate `Thick`, `zeroedthick` und `thin` weisen in der Regel dasselbe Verhalten auf, da der NFS-Server und nicht der ESXi-Host die Zuteilungsrichtlinie festlegt. Die Standardzuordnungsrichtlinie auf den meisten NFS-Servern ist `thin`. Auf NFS-Servern, die „Storage APIs - Array-Integration“ unterstützen, können Sie virtuelle Festplatten im `zeroedthick`-Format erstellen. Der Vorgang „Speicherplatz reservieren“ ermöglicht NFS-Servern das Zuteilen und Garantieren von Speicherplatz.

Weitere Informationen zu den APIs für die Array-Integration finden Sie unter [Kapitel 23 Speicherhardware-Beschleunigung](#).

## Erstellen eines virtuellen Laufwerks

Verwenden Sie zum Erstellen einer virtuellen Festplatte den Befehl `vmkfstools`.

```
-c --createvirtualdisk size[kK|mM|gG]
-a --adaportertype [buslogic|lsilogic|ide|lsisas|pvscsi] srcfile
-d --diskformat [thin|zeroedthick|eagerzeroedthick]
-W --objecttype [file|vsan|vvol]
--policyFile fileName
```

Diese Option erstellt eine virtuelle Festplatte im angegebenen Pfad auf einem Datenspeicher. Legen Sie die Größe der virtuellen Festplatte fest. Wenn Sie einen Wert für die *Größe* angeben, können Sie die Einheit festlegen, indem Sie entweder das Suffix `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) angeben. Bei der Größeneinheit wird die Groß-/Kleinschreibung nicht berücksichtigt. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Byte.

Für die Option `-c` können Sie folgende Unteroptionen angeben.

- `-a` gibt den Controller an, den eine virtuelle Maschine für die Kommunikation mit den virtuellen Festplatten verwendet. Sie können zwischen BusLogic, LSI Logic, IDE, LSI Logic SAS und VMware Paravirtual SCSI wählen.
- `-d` bezeichnet die Festplattenformate.
- `-w` gibt an, ob es sich bei der virtuellen Festplatte um eine Datei in einem VMFS- oder NFS-Datenspeicher oder aber um ein Objekt in einem Virtual SAN- oder VVOL-Datenspeicher handelt.
- `--policyFile fileName` gibt die VM-Speicherrichtlinie für die Festplatte an.

## Beispiel der Erstellung einer virtuellen Festplatte

Dieses Beispiel zeigt die Erstellung einer virtuellen Festplattendatei mit 2 GB und dem Namen `rh6.2.vmdk` im VMFS-Dateisystem mit dem Namen `myVMFS`. Diese Datei stellt eine leere virtuelle Festplatte dar, auf die virtuelle Maschinen zugreifen können.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

## Initialisieren einer virtuellen Festplatte

Verwenden Sie zum Initialisieren einer virtuellen Festplatte den Befehl `vmkfstools`.

```
-w --writezeros
```

Mit dieser Option wird die virtuelle Festplatte bereinigt, indem die gesamten Daten mit Nullen überschrieben werden. In Abhängigkeit der Größe Ihrer virtuellen Festplatte und der E/A-Bandbreite des Geräts, das als Host der virtuellen Festplatte dient, kann die Ausführung dieses Befehls lange dauern.

---

**Vorsicht** Bei der Ausführung dieses Befehls werden alle vorhandenen Daten auf der virtuellen Festplatte gelöscht.

---

## Vergrößern einer virtuellen Festplatte im Thin-Format

Verwenden Sie zum Vergrößern einer virtuellen Thin-Festplatte den Befehl `vmkfstools`.

```
-j --inflatedisk
```

Mit dieser Option wird eine virtuelle Festplatte vom Typ `thin` in den Typ `eagerzeroedthick` konvertiert, wobei alle bestehenden Daten erhalten bleiben. Alle Blöcke, die nicht bereits nicht zugewiesen wurden, werden zugewiesen und gelöscht.

## Entfernen von mit Nullen aufgefüllten Blöcken

Verwenden Sie den Befehl `vmkfstools`, um eine virtuelle Festplatte des Typs „schnell bereitgestellt“, „zeroedthick“ oder „eagerzeroedthick“ in eine schnell bereitgestellte Festplatte zu konvertieren, bei der die mit Nullen aufgefüllten Blöcke entfernt wurden.

```
-K --punchzero
```

Diese Option hebt die Zuweisung aller mit Nullen aufgefüllten Blöcke auf und belässt nur die Blöcke, die zuvor zugewiesen wurden und gültige Daten enthalten. Die Festplatte, die bei dem Vorgang erstellt wird, besitzt das Format „schnell bereitgestellt“.

## Konvertieren einer virtuellen „zeroedthick“-Festplatte in eine „eagerzeroedthick“-Festplatte

Verwenden Sie den Befehl `vmkfstools`, um eine virtuelle Festplatte des Typs „zeroedthick“ in eine Festplatte des Typs „eagerzeroedthick“ zu konvertieren.

```
-k --eagerzero
```

Mit dieser Option werden alle Daten auf der virtuellen Festplatte während der Durchführung der Konvertierung beibehalten.

## Löschen einer virtuellen Festplatte

Mit dieser Option wird eine virtuelle Festplattendatei im angegebenen Pfad des VMFS-Volumes gelöscht.

```
-U --deletevirtualdisk
```

## Umbenennen eines virtuellen Laufwerks

Mit dieser Option wird eine virtuelle Festplattendatei im angegebenen Pfad des VMFS-Volumes umbenannt.

Sie können den ursprünglichen Dateinamen oder -pfad für *alter Name* und den neuen Dateinamen oder -pfad für *neuer Name* angeben.

```
-E --renamevirtualdisk oldName newName
```

## Klonen oder Konvertieren einer virtuellen Festplatte oder einer RDM-Festplatte

Mit dem `vmkfstools`-Befehl können Sie eine Kopie einer von Ihnen angegebenen virtuellen Festplatte oder Rohfestplatte erstellen.

Nur Root-Benutzer dürfen eine virtuelle Festplatte oder eine RDM klonen. Sie müssen den ursprünglichen Dateinamen oder Dateipfad *oldName* und den neuen Dateinamen oder Dateipfad *newName* angeben.

```
-i|--clonevirtualdisk oldName newName
-d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device]
-W|--objecttype [file|vsan|vvol]
--policyFile fileName
-N|--avoidnativeclone
```

Mit den folgenden Unteroptionen können Sie die entsprechenden Parameter für die von Ihnen erstellte Kopie ändern.

- `-d|--diskformat` bezeichnet die Festplattenformate.
- `-W|--objecttype` gibt an, ob es sich bei der virtuellen Festplatte um eine Datei in einem VMFS- oder NFS-Datenspeicher oder um ein Objekt in einem Virtual SAN- oder Virtual Volumes-Datenspeicher handelt.

- `--policyFile fileName` gibt die VM-Speicherrichtlinie für die Festplatte an.

Standardmäßig verwendet ESXi die nativen Methoden zur Ausführung der Klonvorgänge. Wenn das Array die Klontechnologien unterstützt, können Sie die Vorgänge an das Array auslagern. Geben Sie die Option `-N|--avoidnativeclone` an, um natives ESXi-Klonen zu vermeiden.

### Beispiel: Beispiel für das Klonen oder Konvertieren einer virtuellen Festplatte

In diesem Beispiel wird das Klonen der Inhalte einer virtuellen Gold-Festplatte aus dem Repository `templates` in eine virtuelle Festplattendatei mit der Bezeichnung `myOS.vmdk` im Dateisystem `myVMFS` veranschaulicht.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Sie können eine virtuelle Maschine für die Verwendung dieser virtuellen Festplatte konfigurieren, indem Sie der Konfigurationsdatei der virtuellen Maschine Zeilen hinzufügen, wie im folgenden Beispiel gezeigt:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Wenn Sie das Format der Festplatte konvertieren möchten, verwenden Sie hierfür die Unteroption `-d|--diskformat`.

Diese Unteroption ist nützlich, wenn Sie virtuelle Festplatten in einem Format importieren möchten, das nicht mit ESXi kompatibel ist, wie beispielsweise das `2gbsparse`-Format. Nachdem die Festplatte konvertiert wurde, können Sie diese Festplatte einer neuen virtuellen Maschine hinzufügen, die Sie in ESXi erstellen.

Beispiel:

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk -d thin
```

## Migrieren von virtuellen Maschinen zwischen verschiedenen VMware-Produkten

In der Regel verwenden Sie VMware Converter, um virtuelle Maschinen von anderen VMware-Produkten auf Ihr ESXi-System zu migrieren. Sie können jedoch den Befehl `vmkfstools -i` dazu verwenden, virtuelle Festplatten im `2gbsparse`-Format in ESXi zu importieren und anschließend diese Festplatte einer neuen virtuellen Maschine hinzufügen, die Sie in ESXi erstellen.

Sie müssen zuerst die virtuelle Festplatte importieren, da Sie keine Festplatten im `2gbsparse`-Format auf dem ESXi-Host einschalten können.

### Verfahren

- 1 Sie importieren eine Festplatte im `2gbsparse`-Format auf den ESXi-Host, indem Sie den folgenden Befehl ausführen. Achten Sie darauf, dass Sie das Festplattenformat wählen, das mit ESXi kompatibel ist.

```
vmkfstools -i <Eingabe> <Ausgabe> -d <Format>
```



- 2 Verwenden Sie den vSphere Web Client, um die Festplatte hinzuzufügen, die Sie in ESXi in eine virtuelle Maschine importiert haben.

Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

## Erweitern einer virtuellen Festplatte

Diese Option erweitert die Größe einer Festplatte, die einer virtuellen Maschine zugewiesen wurde, nachdem die virtuelle Maschine erstellt wurde.

```
-X --extendvirtualdisk newSize [kK|mM|gG]
```

Die virtuelle Maschine, die diese Festplattendatei verwendet, muss bei Eingabe dieses Befehls ausgeschaltet sein. Außerdem muss das Gastbetriebssystem in der Lage sein, die neue Festplattengröße zu erkennen und zu verwenden, damit es z. B. das Dateisystem auf der Festplatte aktualisieren kann, sodass der zusätzliche Speicherplatz auch genutzt wird.

---

**Hinweis** Sie können keine virtuellen SATA-Festplatten im laufenden Betrieb erweitern, oder irgendeine virtuelle Festplatte, wenn die Kapazität nach der Erweiterung größer oder gleich 2 TB ist.

---

Sie geben den Parameter `Neue Größe` in Kilobyte, Megabyte oder Gigabyte an, indem Sie das Suffix `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) hinzufügen. Bei der Größeneinheit wird die Groß-/Kleinschreibung nicht berücksichtigt. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Kilobyte.

Der Parameter `Neue Größe` beschreibt die gesamte neue Größe und nicht nur die beabsichtigte Erweiterung der Festplatte.

Um beispielsweise eine virtuelle Festplatte mit 4GB um 1GB zu erweitern, geben Sie Folgendes an: `vmkfstools -X 5g Festplattenname`.

Mithilfe der Option `-d eagerzeroedthick` können Sie die virtuelle Festplatte auf das Format „eagerzeroedthick“ erweitern.

---

**Hinweis** Erweitern Sie nicht die Basisfestplatte einer virtuellen Maschine, der Snapshots zugeordnet sind. Falls doch, können Sie den Snapshot nicht länger übergeben oder die Basisfestplatte auf ihre ursprüngliche Größe zurücksetzen.

---

## Aktualisieren virtueller Festplatten

Diese Option konvertiert die angegebene virtuelle Festplattendatei vom Format ESX Server 2 ins Format ESXi.

```
-M --migratevirtualdisk
```

## Anlegen einer Raw-Gerätezuordnung im virtuellen Kompatibilitätsmodus

RDM- (Raw Device Mapping-)Datei auf einem VMFS-Volume angelegt und dieser Datei eine Raw-LUN zugeordnet. Nach Herstellung dieser Zuordnung können Sie auf die LUN wie auf normale virtuelle VMFS-Festplatten zugreifen. Die Dateigröße der Zuordnung entspricht der Größe der Raw-LUN, auf die sie verweist.

```
-r --createrdm device
```

Verwenden Sie beim Festlegen des *Geräte*-Parameters das folgende Format:

```
/vmfs/devices/disks/disk_ID:P
```

## Beispiel der Erstellung einer Raw-Gerätezuordnung im virtuellen Kompatibilitätsmodus

Im vorliegenden Beispiel erstellen Sie eine RDM-Datei namens *my\_rdm.vmdk* und ordnen dieser Datei die Raw-Festplatte *disk\_ID* zu.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

Sie können eine virtuelle Maschine so konfigurieren, dass sie die Zuordnungsdatei *my\_rdm.vmdk* verwendet, indem Sie die Konfigurationsdatei der virtuellen Maschine um die folgenden Zeilen ergänzen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

## Anlegen einer Raw-Gerätezuordnung im physischen Kompatibilitätsmodus

Mit dieser Option können Sie einer Datei auf einem VMFS Volume ein Pass-Through-Raw-Gerät zuordnen. Bei dieser Zuordnung kann eine virtuelle Maschine die ESXi-SCSI-Befehlsfilterung umgehen, wenn sie auf ihre virtuelle Festplatte zugreift. Diese Art der Zuordnung eignet sich dann, wenn die virtuelle Maschine systeminhärente SCSI-Befehle versenden muss, wie beispielsweise dann, wenn SAN-gestützte Software auf der virtuellen Maschine ausgeführt wird.

```
-z --createrdmpassthru device
```

Nachdem Sie diese Art der Zuordnung aktiviert haben, können Sie damit auf die Raw-Festplatte wie auf jede andere virtuelle Festplatte zugreifen.

Verwenden Sie beim Festlegen des *Geräte*-Parameters das folgende Format:

```
/vmfs/devices/disks/disk_ID
```

## Aufführen der Attribute einer RDM

Mit dieser Option können Sie die Attribute einer Raw-Festplattenzuordnung auflisten.

```
-q --queryrdm
```

Diese Option druckt den Namen der Raw-Festplatte „RDM“. Die Option druckt ferner weitere Identifikationsdaten wie die Festplatten-ID der Raw-Festplatte.

## Anzeigen der Architektur der virtuellen Festplatte

Mit dieser Option werden Informationen zur Architektur einer virtuellen Festplatte angezeigt.

```
-g --geometry
```

Die Ausgabe erfolgt in dieser Form: `Architekturinformationen C/H/S`, wobei `C` die Anzahl der Zylinder, `H` die Anzahl der Köpfe und `S` die Anzahl der Sektoren angibt.

**Hinweis** Wenn Sie virtuelle Festplatten aus gehosteten VMware-Produkten auf den ESXi-Host importieren, kann es zu Fehlermeldungen bezüglich Diskrepanzen in der Festplattenarchitektur kommen. Eine Diskrepanz in der Festplattenarchitektur kann auch die Ursache von Problemen beim Laden eines Gastbetriebssystems oder bei der Ausführung einer neu erstellten virtuellen Maschine sein.

## Prüfen und Reparieren virtueller Festplatten

Verwenden Sie diese Option, um eine virtuelle Festplatte im Fall eines nicht ordnungsgemäßen Herunterfahrens zu prüfen oder zu reparieren.

```
-x , --fix [check|repair]
```

## Prüfen der Festplattenkette auf Konsistenz

Mithilfe dieser Option können Sie die gesamte Festplattenkette prüfen. Sie können feststellen, ob Glieder in der Kette beschädigt sind oder ungültige hierarchische Beziehungen bestehen.

```
-e --chainConsistent
```

## Speichergerätoptionen

Geräteoptionen ermöglichen Ihnen die Ausführung von Verwaltungsaufgaben für physische Speichergeräte.

## Verwalten der SCSI-Reservierungen von LUNs

Mit der Option `-L` können Sie eine SCSI-LUN für die ausschließliche Verwendung durch einen ESXi-Host reservieren, eine Reservierung aufheben, sodass andere Hosts auf die LUN zugreifen können, und eine Reservierung zurücksetzen, wodurch alle Reservierungen eines Ziels aufgehoben werden.

```
-L --lock [reserve|release|lunreset|targetreset|busreset] device
```

**Vorsicht** Eine Verwendung der Option `-L` kann den Betrieb der anderen Server in einem SAN beeinträchtigen. Verwenden Sie die Option `-L` nur zur Fehlerbehebung bei der Einrichtung von Clustern.

Wenden Sie diese Option nie auf eine LUN mit einem VMFS-Volume an, es sei denn, VMware empfiehlt Ihnen ausdrücklich das Gegenteil.

Sie können die Option `-L` auf verschiedene Arten anwenden:

- `-L reserve` – Reserviert die angegebene LUN. Nach der Reservierung kann nur der Server, der diese LUN reserviert hatte, darauf zugreifen. Wenn andere Server versuchen, auf diese LUN zuzugreifen, erhalten Sie einen Reservierungsfehler.
- `-L release` – Hebt die Reservierung der angegebenen LUN auf. Andere Server können wieder auf die LUN zugreifen.
- `-L lunreset` – Setzt die angegebene LUN zurück, indem jede Reservierung der LUN zurückgesetzt und die LUN den anderen Servern wieder zur Verfügung gestellt wird. Dies beeinflusst die anderen LUNs auf dem Gerät nicht. Wenn eine andere LUN auf dem Gerät reserviert wurde, bleibt sie reserviert.
- `-L targetreset` – Setzt das gesamte Ziel zurück. Dadurch werden die Reservierungen für alle LUNs, die dem Ziel zugeordnet sind, aufgehoben. Die entsprechenden LUNs stehen wieder allen Servern zur Verfügung.
- `-L busreset` – Setzt alle zugänglichen Ziele auf dem Bus zurück. Dadurch werden die Reservierungen für alle LUNs, auf die durch den Bus zugegriffen werden kann, aufgehoben und die entsprechenden LUNs stehen wieder allen Servern zur Verfügung.

Verwenden Sie für den Parameter *Gerät* folgendes Format:

```
/vmfs/devices/disks/disk_ID:P
```

## Durchbrechen von Gerätesperren

Mithilfe der Option `-B` können Sie die Gerätesperre einer bestimmten Partition durchbrechen.

```
-B --breaklock device
```

Verwenden Sie für den Parameter *Gerät* folgendes Format:

```
/vmfs/devices/disks/disk_ID:P
```

Sie können diesen Befehl verwenden, wenn mitten in einem Datenspeichervorgang, z. B. beim Vergrößern bzw. Hinzufügen einer Erweiterung oder bei der Neusignierung, ein Host ausfällt. Wenn Sie diesen Befehl ausführen, stellen Sie sicher, dass kein anderer Host die Sperre hält.