

vSphere-Verwaltung mit dem vSphere Client

VMware vSphere 6.0
vCenter Server 6.0
VMware ESXi 6.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter

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

DE-001606-03

vmware®

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

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

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

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

docfeedback@vmware.com

Copyright © 2009 – 2017 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken](#).

VMware, Inc.

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

VMware Global, Inc.

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

Inhalt

vSphere-Verwaltung mit dem vSphere Client	9
Aktualisierte Informationen	11
1 Verwenden des vSphere-Clients	13
Starten und Anmelden des vSphere Clients	14
Beenden und Abmelden des vSphere Clients	14
Statusleiste und kürzlich bearbeitete Aufgaben	15
Registerkarten „Erste Schritte“	15
Anzeigen der VM-Konsole	16
Verwenden von Listen	16
Speichern von vSphere Clientdaten	17
Fensterbereiche	17
Durchsuchen der vSphere Clientbestandsliste	17
Benutzerdefinierte Attribute	19
Auswählen der Objekte	21
vCenter Server-Plug-Ins verwalten	21
Arbeiten mit aktiven Sitzungen	22
2 Konfigurieren von ESXi-Hosts und vCenter Server im vSphere Client	25
Konfigurieren von ESXi-Hosts	25
Konfigurieren von vCenter Server im vSphere Client	28
Konfigurieren der Kommunikation zwischen ESXi , vCenter Server und vSphere-Client	35
Neustarten oder Herunterfahren eines ESXi -Hosts	35
3 Organisieren Ihrer Bestandsliste	37
Datencenter erstellen	38
Hosts hinzufügen	39
Cluster erstellen	40
Erstellen von Ressourcenpools	41
Datenspeicher erstellen	41
Hostweite Netzwerke erstellen	42
Datencenterweite Netzwerke erstellen	43
4 Verwalten von Lizenzschlüsseln im vSphere Client	49
Lizenzierungseinschränkungen im vSphere Client	49
Verwalten von Lizenzschlüsseln auf ESXi -Hosts	49
Verwalten von Lizenzschlüsseln auf vCenter Server	51
5 Verwalten von Aufgaben	55
Anzeigen von Aufgaben	55

	Abbrechen einer Aufgabe	57
	Planen von Aufgaben	58
	Richtlinienregeln für Aufgaben	62
6	Absichern der Verwaltungsschnittstelle	63
	Sichern der ESXi -Hosts	63
	Sichern von virtuellen Maschinen	67
7	ESXi -Authentifizierung und Benutzerverwaltung	73
	Verwalten von Benutzern mit dem vSphere Client	73
	Zuweisen der Berechtigungen für ESXi	76
	Verwalten von ESXi -Rollen	78
	Verwenden von Active Directory zum Verwalten von ESXi-Benutzern	80
	Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne	82
	Anpassen der Suchliste in großen Domänen	83
8	Verwalten von Hosts in vCenter Server	85
	Trennen und Herstellen einer Hostverbindung	85
	Entfernen eines Hosts aus einem Cluster	86
	Entfernen eines verwalteten Hosts aus vCenter Server	87
9	Verwenden von vCenter-Zuordnungen	89
	Festlegen der maximalen Anzahl an Map-Objekten	90
	Anzeigen von vCenter-Zuordnungen	90
	Drucken von vCenter-Zuordnungen	90
	Exportieren von vCenter-Zuordnungen	90
10	Erstellen einer virtuellen Maschine im vSphere-Client	93
	Starten des Erstellungsvorgangs der virtuellen Maschine im vSphere-Client	94
	Auswählen einer Konfigurationsoption für die neue virtuelle Maschine im vSphere-Client	95
	Eingeben eines Namens und Speicherorts für die virtuelle Maschine im vSphere Client	96
	Auswählen eines Hosts oder Clusters im vSphere Client	96
	Auswählen eines Ressourcenpools im vSphere-Client	97
	Auswählen eines Datenspeichers im vSphere Client	97
	Auswählen einer Version für die virtuelle Maschine im vSphere Client	97
	Auswählen eines Betriebssystems im vSphere Client	98
	Auswählen der Anzahl der virtuellen CPUs im vSphere Client	99
	Konfigurieren des virtuellen Arbeitsspeichers im vSphere Client	99
	Konfigurieren von Netzwerken im vSphere-Client	100
	Auswählen eines SCSI-Controllers im vSphere Client	101
	Auswählen des Typs der virtuellen Festplatte	102
	Abschließen der Erstellung virtueller Maschinen im vSphere-Client	106
11	Arbeiten mit Vorlagen und Klonen im vSphere-Client	107
	Klonen einer virtuellen Maschine im vSphere Client	108
	Erstellen einer geplanten Aufgabe zum Klonen einer virtuellen Maschine im vSphere Client	110
	Erstellen einer Vorlage im vSphere-Client	111
	Bereitstellen einer virtuellen Maschine anhand einer Vorlage im vSphere-Client	114

Ändern des Vorlagennamens im vSphere-Client	117
Löschen von Vorlagen	117
Konvertieren einer Vorlage in eine virtuelle Maschine im vSphere-Client	119
12 Anpassen von Gastbetriebssystemen	121
Anforderungen für die Anpassung des Gastbetriebssystems	121
Konfigurieren eines Skripts für die Generierung von Computernamen und IP-Adressen bei der Anpassung des Gastbetriebssystems im vSphere-Client	122
Anpassen von Windows beim Klonen oder Bereitstellen im vSphere Client	123
Anpassen von Linux beim Klonen oder Bereitstellen im vSphere Client	126
Verwalten der Anpassungsspezifikationen im vSphere-Client	127
13 Migrieren von virtuellen Maschinen im vSphere Client	135
Migrieren einer eingeschalteten virtuellen Maschine mit vMotion im vSphere Client	136
Migrieren einer virtuellen Maschine mit Storage vMotion im vSphere Client	137
Migrieren einer ausgeschalteten oder angehaltenen virtuellen Maschine im vSphere Client	138
CPU-Kompatibilität und EVC	140
14 Bereitstellen von OVF-Vorlagen	147
Bereitstellen einer OVF-Vorlage im vSphere Client	147
Export einer OVF-Vorlage	149
15 Konfigurieren virtueller Maschinen im vSphere Client	151
VM-Einschränkungen im vSphere Client	152
VM-Hardwareversionen	153
Ermitteln der Hardwareversion einer virtuellen Maschine im vSphere-Client	154
Ändern des Namens der virtuellen Maschine im vSphere Client	155
Anzeigen des Speicherorts der Konfigurationsdatei der virtuellen Maschine im vSphere-Client	155
Bearbeiten der Parameter der Konfigurationsdatei im vSphere-Client	156
Ändern des konfigurierten Gastbetriebssystems in vSphere-Client	156
Konfigurieren von virtuellen Maschinen zum automatischen Aktualisieren der VMware Tools	157
Konfiguration virtueller CPUs	158
Konfigurieren von virtuellem Arbeitsspeicher	165
Netzwerkkonfiguration virtueller Maschinen	169
Konfiguration der parallelen und seriellen Schnittstelle	171
Konfiguration der virtuellen Festplatte	177
SCSI- und SATA-Speicher-Controller – Bedingungen, Einschränkungen und Kompatibilität	182
Weitere Gerätekonfigurationen für die virtuelle Maschine	186
Konfigurieren von vServices	192
USB-Konfiguration von einem ESXi -Host zu einer virtuellen Maschine	194
USB-Konfiguration von einem Clientcomputer zu einer virtuellen Maschine im vSphere-Client	198
Verwalten von Energieverwaltungseinstellungen für eine virtuelle Maschine	201
Konfigurieren der Betriebszustände der virtuellen Maschine	202
Verzögern der Startsequenz in vSphere-Client	204
Aktivieren der Protokollierung im vSphere Client	204
Deaktivieren der Beschleunigung im vSphere Client	205
Konfigurieren des Debuggings und der Statistiken im vSphere Client	205

- 16 Verwalten von virtuelle Maschinen 207**
 - Bearbeiten der Einstellungen zum Starten/Herunterfahren der virtuellen Maschine 207
 - Öffnen einer Konsole für eine virtuelle Maschine 208
 - Hinzufügen und Entfernen von virtuellen Maschinen 209
 - Verwenden von Snapshots zum Verwalten virtueller Maschinen 210

- 17 Verwalten von Multi-Tier-Anwendungen mit vSphere vApp im vSphere-Client 221**
 - Erstellen einer vApp 222
 - Einschalten einer vApp im vSphere-Client 223
 - vApp klonen 224
 - Ausschalten einer vApp im vSphere-Client 224
 - Anhalten einer vApp im vSphere-Client 225
 - Fortsetzen einer vApp im vSphere-Client 225
 - Auffüllen der vApp 225
 - Bearbeiten der vApp-Einstellungen im vSphere-Client 226
 - Konfigurieren von IP-Pools 231
 - Bearbeiten einer vApp-Anmerkung im vSphere-Client 233

- 18 Überwachen von Lösungen mit vCenter Solutions Manager 235**
 - Anzeigen von Lösungen 236
 - Überwachungsagenten 236
 - Überwachen von vServices 237

- 19 Verwenden von Hostprofilen im vSphere-Client 239**
 - Modell für die Verwendung von Hostprofilen 239
 - Zugreifen auf die Ansicht „Hostprofile“ 240
 - Erstellen eines Hostprofils 241
 - Exportieren eines Hostprofils 242
 - Importieren eines Hostprofils 242
 - Klonen eines Hostprofils 243
 - Bearbeiten eines Hostprofils 243
 - Verwalten von Profilen 246
 - Prüfen der Übereinstimmung 250
 - Hostprofile und vSphere Auto Deploy 251

- 20 Netzwerke beim vSphere Client 255**
 - Netzwerkeinschränkungen im vSphere Client 255
 - Anzeigen der Netzwerkinformationen im vSphere-Client 256
 - Anzeigen der Netzwerkadapterinformationen auf dem vSphere Client 256
 - Einrichten von Netzwerken mit vSphere Standard-Switches 257
 - Einrichten von Netzwerken mit vSphere Distributed Switches 261

- 21 Verwalten von Netzwerkressourcen 279**
 - vSphere Network I/O Control 279
 - TCP-Segmentierungs-Offload und Jumbo-Frames 282
 - DirectPath I/O 284
 - Single Root I/O Virtualization (SR-IOV) 286

22	Netzwerkrichtlinien	291
	Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch	291
	Teaming- und Failover-Richtlinie	293
	VLAN-Richtlinie	302
	Sicherheitsrichtlinie	305
	Traffic-Shaping-Richtlinie	309
	Ressourcenzuteilungsrichtlinie	313
	Überwachungsrichtlinie	314
	Portblockierungsrichtlinien	315
	Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch	316
23	Erweiterte Netzwerkthemen	321
	Unterstützung für Internet Protocol Version 6 (IPv6)	321
	VLAN-Konfiguration	322
	Arbeiten mit der Portspiegelung	322
	Konfigurieren der NetFlow-Einstellungen	329
	Switch-Discovery-Protokoll	330
	Ändern der DNS- und Routing-Konfiguration	332
	Verwaltung von MAC-Adressen	333
24	Verwalten des Speichers im vSphere Client	335
	Speichereinschränkungen im vSphere Client	336
	Anzeigen von Speichergeräten für einen Host im vSphere Client	336
	Anzeigen von Speichergeräten für einen Adapter im vSphere Client	337
	Anzeigen von Informationen zu Speicheradaptern im vSphere Client	337
	Überprüfen der Informationen zu Datenspeichern im vSphere Client	337
	Zuweisen von WWNs zu virtuellen Maschinen	338
	Ändern von WWN-Zuweisungen	339
	Einrichten des Netzwerks für Software-FCoE	339
	Hinzufügen von Software-FCoE-Adaptern	340
	Deaktivieren der automatischen Hostregistrierung	341
	Einrichten von unabhängigen Hardware-iSCSI-Adaptern	341
	Konfigurieren von abhängigen Hardware-iSCSI-Adaptern	343
	Konfigurieren von Software-iSCSI-Adaptern	345
	Einrichten des iSCSI-Netzwerks	347
	Verwenden von Jumbo-Frames mit iSCSI	352
	Konfigurieren von Erkennungsadressen für iSCSI-Adapter	353
	Konfigurieren von CHAP-Parametern für iSCSI-Adapter	355
	Konfigurieren erweiterter Parameter für iSCSI im vSphere Client	359
	Verwalten von Speichergeräten	359
	Arbeiten mit Datenspeichern	361
	Raw-Gerätezuordnung	372
	Grundlegendes zu Multipathing und Failover	374
	Speicherhardware-Beschleunigung	377
	Thin Provisioning von Speicher	377
	Verwenden von Speicher-Anbieter-Providern	380

25	Ressourcenverwaltung für Einzelhosts	383
	Konfigurieren von Einstellungen für die Ressourcenzuteilung	383
	Verwalten von CPU-Ressourcen	385
	Verwalten von Arbeitsspeicherressourcen	388
	Verwalten von Speicher-E/A-Ressourcen	393
	Verwalten von Ressourcenpools	397
	Verwenden des DRS-Clusters zur Ressourcenverwaltung	401
	Erstellen eines Datenspeicher-Clusters	415
	Verwenden des Datenspeicher-Clusters zur Verwaltung von Speicherressourcen	419
	Verwenden von NUMA-Systemen mit ESXi	428
	Erweiterte Attribute	430
26	Erstellen und Verwenden von vSphere HA-Clustern	433
	vSphere HA-Checkliste	433
	Erstellen und Konfigurieren eines vSphere HA-Clusters	434
	Anpassen einer einzelnen virtuellen Maschine im vSphere Web Client	439
27	Aktivieren der Fault Tolerance für virtuelle Maschinen	441
	Beispiele für die Nutzen der Fault Tolerance	441
	Fault Tolerance-Checkliste	442
	Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance	443
	Verwenden von Fault Tolerance	447
	Anzeigen von Daten über fehlertolerante virtuelle Maschinen im vSphere-Client	450
	Best Practices für Fault Tolerance	451
28	Überwachen eines einzelnen Hosts mit dem vSphere Client	455
	Diagramme anzeigen	455
	Arbeiten mit erweiterten und benutzerdefinierten Diagrammen	456
	Überwachen des Serversystemstatus	459
	Überwachen von Ereignissen, Alarmen und automatisierten Aktionen	461
	Anzeigen von Lösungen	476
	Konfigurieren von SNMP-Einstellungen für vCenter Server	477
	Systemprotokolldateien	478
	Index	483

vSphere-Verwaltung mit dem vSphere Client

Die Dokumentation zur vSphere-Administration mit vSphere Client enthält Informationen zur Verwaltung eines einzelnen ESXi-Hosts oder vCenter Server -Systems über eine Direktverbindung von vSphere Client. Mithilfe dieser Aufgaben können Sie Hosts verwalten, die nicht mit einem vCenter Server-System verbunden sind, oder Probleme bei Hosts beheben bzw. Hosts verwalten, die vom vCenter Server-System getrennt wurden, von dem sie verwaltet wurden.

Diese Dokumentation enthält in erster Linie eine Beschreibung der Aufgaben, die Sie ausführen können, wenn Sie mit dem vSphere Client eine direkte Verbindung mit einem Host oder vCenter Server herstellen. Ausführliche Informationen zu vSphere-Netzwerken, Speicher, Sicherheit, Verwaltung virtueller Maschinen und sonstigen Themen finden Sie in der entsprechenden vSphere-Dokumentation.

Zielgruppe

Diese Informationen sind für alle Benutzer gedacht, die einen einzelnen ESXi-Host bzw. ein einzelnes vCenter Server-System verwalten möchten, indem sie mit dem vSphere Client eine direkte Verbindung herstellen. Sie sind für erfahrene Windows-Systemadministratoren bestimmt, die mit VM-Technologie und Datacenteroperationen vertraut sind.

Aktualisierte Informationen

Diese Dokumentation zur *vSphere-Administration mit dem vSphere Client* wird mit jeder Version des Produkts oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf der Dokumentation zur *vSphere-Administration mit dem vSphere Client*.

Revision	Beschreibung
DE-001606-03	■ Die standardmäßigen Sicherheitsrichtlinien für verteilte Portgruppen unter „ Bearbeiten der Sicherheitsrichtlinie für eine verteilte Portgruppe “, auf Seite 307 wurden korrigiert.
DE-001606-02	■ Informationen zu vSphere Storage Appliance wurden entfernt. Diese Funktion wird in vSphere 6.0 nicht mehr unterstützt. ■ In Kapitel 1, „Verwenden des vSphere-Clients“ , auf Seite 13 wurde ein Hinweis zur Aktivierung von einem Active Directory-Benutzer hinzugefügt.
DE-001606-01	■ Informationen zu Speicheransichten und Speicherberichten wurden entfernt. Diese Funktion wird in vSphere 6.0 nicht mehr unterstützt. ■ Die Anzahl der LUN-IDs wurde in „ Ändern der Anzahl gescannter Speichergeräte “, auf Seite 360 aktualisiert. ■ Das Thema „ Lizenzierungseinschränkungen im vSphere Client “, auf Seite 49 zu Lizenzierungseinschränkungen wurde hinzugefügt.
DE-001606-00	Erstversion.

Verwenden des vSphere-Clients

Der vSphere Client ist eine Schnittstelle zum Verwalten von vCenter Server und ESXi.

Die Konfiguration der Benutzerschnittstelle des vSphere Clients beruht auf dem Server, mit dem er verbunden ist:

- Wenn der Server ein vCenter Server-System ist, zeigt der vSphere Client alle für die vSphere-Umgebung verfügbaren Optionen an. Dies erfolgt auf Grundlage der konfigurierten Lizenzierung und der Berechtigungen des Benutzers.
- Ist der Server ein ESXi-Host, zeigt der vSphere Client nur die Optionen für die Verwaltung eines einzelnen Hosts an.

HINWEIS Wenn Sie einem Active Directory-Benutzer die Anmeldung bei einer vCenter Server-Instanz unter Verwendung des vSphere Client mit SSPI ermöglichen möchten, müssen Sie die vCenter Server-Instanz zur Active Directory-Domäne hinzufügen. Weitere Informationen zum Hinzufügen einer vCenter Server Appli-ance mit einem externen Platform Services Controller zu einer Active Directory-Domäne finden Sie in dem VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2118543>.

Bei der Erstanmeldung beim vSphere Client wird eine Homepage mit Symbolen angezeigt, die den Zugriff auf Funktionen des vSphere Clients ermöglichen. Wenn Sie sich beim vSphere Client abmelden, wird in der Clientanwendung gespeichert, welche Ansicht beim Schließen der Anwendung angezeigt wurde, und Sie kehren bei Ihrer nächsten Anmeldung zu dieser Ansicht zurück.

Viele Verwaltungsfunktionen führen Sie von der Bestandslistenansicht aus, die aus einem einzelnen Fenster mit einer Menüleiste, einer Navigationsleiste, einer Symbolleiste, einer Statusleiste, einem Fensterabschnitt und Kontextmenüs besteht.

Dieses Kapitel behandelt die folgenden Themen:

- „Starten und Anmelden des vSphere Clients“, auf Seite 14
- „Beenden und Abmelden des vSphere Clients“, auf Seite 14
- „Statusleiste und kürzlich bearbeitete Aufgaben“, auf Seite 15
- „Registerkarten „Erste Schritte““, auf Seite 15
- „Anzeigen der VM-Konsole“, auf Seite 16
- „Verwenden von Listen“, auf Seite 16
- „Speichern von vSphere Clientdaten“, auf Seite 17
- „Fensterbereiche“, auf Seite 17
- „Durchsuchen der vSphere Clientbestandsliste“, auf Seite 17
- „Benutzerdefinierte Attribute“, auf Seite 19

- „Auswählen der Objekte“, auf Seite 21
- „vCenter Server-Plug-Ins verwalten“, auf Seite 21
- „Arbeiten mit aktiven Sitzungen“, auf Seite 22

Starten und Anmelden des vSphere Clients

Der vSphere Client ist eine grafische Benutzeroberfläche für die Verwaltung von ESXi-Host und vCenter Server.

Ein Anmeldebildschirm wird angezeigt, wenn Sie den vSphere-Client starten. Nachdem Sie sich angemeldet haben, zeigt der Client die entsprechenden Objekte und Funktionen für den Server, auf den Sie zugreifen, sowie die Berechtigungen des angemeldeten Benutzer an.

Vorgehensweise

- 1 Melden Sie sich am Windows-System an.

Wenn Sie den vSphere-Client das erste Mal starten, melden Sie sich als Administrator an.

- Wenn es sich bei dem verwalteten Host nicht um einen Domänencontroller handelt, melden Sie sich entweder als **Name_des_lokalen_Hosts\Benutzer** oder als *Benutzer* an, wobei *Benutzer* ein Mitglied der lokalen Administratorengruppe ist.
- Wenn der verwaltete Server ein Domänencontroller ist, müssen Sie sich als **Domäne\Benutzer**, anmelden, wobei *Domäne* für den Namen der Domäne steht, für den der Host als Domänencontroller fungiert, und *Benutzer* ein Mitglied der Gruppe der Domänenadministratoren für die betreffende Domäne ist. Die Ausführung auf einem Domänencontroller wird nicht empfohlen.

- 2 Doppelklicken Sie auf eine Verknüpfung oder wählen Sie den vSphere Client über **Start > Programme > VMware > VMware vSphere Client** aus.
- 3 Geben Sie IP-Adresse oder Servernamen, Ihren Benutzernamen und Ihr Kennwort ein.
- 4 Klicken Sie zum Fortfahren auf **Anmelden (Login)**.

Sie sind jetzt mit dem Host verbunden.

HINWEIS Wenn Sie sich mit einem ESXi-Host verbunden haben, der derzeit von einem vCenter Server-System verwaltet wird, erhalten Sie eine Warnmeldung und Änderungen am Host werden im vCenter Server-System nicht übernommen.

Beenden und Abmelden des vSphere Clients

Wenn Sie die ausgeführten Aktivitäten des ESXi-Hosts oder vCenter Server-Systems nicht mehr überwachen oder bearbeiten müssen, melden Sie sich vom vSphere Client ab.

HINWEIS Durch das Schließen einer vSphere Clientsitzung wird das Hostsystem nicht beendet.

Vorgehensweise

- ◆ Klicken Sie auf das Feld zum Schließen (X) oder wählen Sie **Datei > Beenden**.

Der vSphere-Client wird heruntergefahren. Der vSphere Client wird vom ESXi-Host oder vCenter Server-System abgemeldet. Die normalen Aktivitäten des Host werden weiterhin im Hintergrund ausgeführt.

Statusleiste und kürzlich bearbeitete Aufgaben

In der Statusleiste sehen Sie Informationen über kürzlich abgeschlossene oder derzeit aktive Aufgaben.

Die Statusleiste wird im unteren Fensterbereich angezeigt. Sie enthält alle derzeit aktiven oder kürzlich abgeschlossenen Aufgaben. Außerdem wird ein Fortschrittsbalken angezeigt, der angibt, zu welchem Prozentsatz eine Aufgabe abgeschlossen wurde.

Registerkarten „Erste Schritte“

Wenn ESXi oder vCenter Server neu installiert wird und keine Bestandslistenobjekte hinzugefügt wurden, fungieren die Registerkarten „Erste Schritte“ als Einrichtungsassistent, der den Benutzer durch das Hinzufügen von Elementen zur Bestandsliste und die Einrichtung der virtuellen Umgebung führt.

- [Deaktivieren der Registerkarten „Erste Schritte“](#) auf Seite 15
Falls Sie die Registerkarten „Erste Schritte“ nicht anzeigen möchten, können Sie sie deaktivieren.
- [Wiederherstellen der Registerkarten „Erste Schritte“](#) auf Seite 15
Wenn Sie die Anzeige der Registerkarten „Erste Schritte“ ausgeschaltet haben, können Sie die Einstellungen wiederherstellen, damit sie für alle Bestandslistenobjekte angezeigt werden.

Deaktivieren der Registerkarten „Erste Schritte“

Falls Sie die Registerkarten „Erste Schritte“ nicht anzeigen möchten, können Sie sie deaktivieren.

Sie können die Registerkarten folgendermaßen deaktivieren.

Vorgehensweise

- Um die Registerkarten Erste Schritte (Getting Started) für den ausgewählten Objekttyp zu deaktivieren, klicken Sie auf den Link **Registerkarte schließen (Close Tab)**.
- Ändern Sie die vSphere-Client-Einstellungen, sodass alle Registerkarten „Erste Schritte“ ausgeblendet werden.
 - a Wählen Sie **Bearbeiten > Clienteneinstellungen**.
 - b Wählen Sie die Registerkarte **Allgemein**.
 - c Deaktivieren Sie das Kontrollkästchen **Registerkarten 'Erste Schritte' anzeigen** und klicken Sie auf **OK**.

Wiederherstellen der Registerkarten „Erste Schritte“

Wenn Sie die Anzeige der Registerkarten „Erste Schritte“ ausgeschaltet haben, können Sie die Einstellungen wiederherstellen, damit sie für alle Bestandslistenobjekte angezeigt werden.

Vorgehensweise

- 1 Wählen Sie **Bearbeiten > Clienteneinstellungen**.
- 2 Klicken Sie auf die Registerkarte **Allgemein**.
- 3 Wählen Sie **Registerkarten 'Erste Schritte' anzeigen** und klicken Sie auf **OK**.

Anzeigen der VM-Konsole

Die Konsole einer eingeschalteten virtuellen Maschine ist über einen verbundenen Server verfügbar. Allen Konsolenverbindungen mit der virtuellen Maschine werden dieselben Informationen angezeigt. In der Meldungszeile wird die Anzahl der aktiven Verbindungen mit der virtuellen Maschine angegeben.

Vorgehensweise

- 1 Wählen Sie eine eingeschaltete virtuelle Maschine aus.
- 2 Klicken Sie im Informationsfenster auf die Registerkarte **Konsole**.
- 3 (Optional) Klicken Sie zum Anzeigen der Konsole der virtuellen Maschine in einem eigenen Fenster auf das Ausklappsymbol in der Navigationsleiste.
- 4 (Optional) Drücken Sie STRG+ALT+EINGABE, um den Vollbildmodus zu aktivieren bzw. zu beenden.

Verwenden von Listen

Viele vSphere-Client-Bestandslistenregisterkarten führen Listen von Informationen.

Die Registerkarte **Virtuelle Maschinen** bietet z. B. eine Liste aller virtuellen Maschinen, die einem Host oder Cluster zugewiesen sind. Sie können alle Listen im vSphere-Client sortieren, indem Sie auf die Spaltenkopfbezeichnung klicken. Ein Dreieck im Spaltenkopf gibt an, ob aufsteigend oder absteigend sortiert wurde.

Sie können eine Liste auch filtern, indem Sie sie sortieren und nur bestimmte Elemente einschließen. Ein Filter wird mithilfe eines Schlüsselworts sortiert. Wählen Sie die Spalten aus, die in die Suche nach dem Schlüsselwort einbezogen werden sollen.

Filtern einer Listenansicht

Sie können eine Liste filtern, wenn sie zu lang ist oder um in der Liste nach bestimmten Elementen zu suchen. Sie können beispielsweise eine Liste von Alarmen nach Alarmen filtern, die mit dem Wort „Datenspeicher“ beginnen. Sie können das Filterfeld mithilfe der Option **Filtern** im Menü **Ansicht** anzeigen und ausblenden.

Die Listenansicht wird abhängig davon aktualisiert, ob das Filtern aktiviert oder deaktiviert ist. Wenn Sie beispielsweise auf der Registerkarte **Virtuelle Maschinen** arbeiten und der gefilterte Text „eingeschaltet“ lautet, sehen Sie nur virtuelle Maschinen, deren Status auf „Eingeschaltet“ gesetzt ist. Wenn sich der Status einer virtuellen Maschine ändert, wird die virtuelle Maschine aus der Liste entfernt. Virtuelle Maschinen, die zur Liste hinzugefügt werden, werden ebenfalls gefiltert.

Vorgehensweise

- 1 Klicken Sie auf den Pfeil neben dem Filterfeld rechts oben in einem Bestandslistenbereich, in dem eine Liste angezeigt wird.
- 2 Wählen Sie die Attribute aus, die gefiltert werden sollen.
- 3 Geben Sie Suchkriterien in das Filterfeld ein.

Die Suche startet nach einer Pause von mehr als einer Sekunde automatisch. Boolesche Ausdrücke und Sonderzeichen werden nicht unterstützt. Beim Filtern wird die Groß-/Kleinschreibung nicht berücksichtigt.

- 4 (Optional) Klicken Sie auf **Löschen**, um das Filterfeld zu leeren.

Exportieren einer Liste

Sie können eine Liste im vSphere Client in eine Datei exportieren. Wenn Sie die Datei lokal speichern, sind mehrere Dateitypen verfügbar.

Vorgehensweise

- 1 Navigieren Sie im vSphere Client zu einer Listenansicht. Klicken Sie zum Beispiel beim Anzeigen eines Hosts auf die Registerkarte **Virtuelle Maschinen**.
- 2 Wählen Sie **Datei > Exportieren > Liste exportieren**.
- 3 Geben Sie einen Dateinamen ein und wählen Sie einen Dateityp aus.
- 4 Klicken Sie auf **Speichern**.

Speichern von vSphere Clientdaten

Die Benutzerschnittstelle des vSphere-Clients ähnelt einem Browser. Die meisten Benutzeraktionen sind in den angezeigten Daten für ESXi-Host und vCenter Server-Center dauerhaft. In der Regel müssen Sie die Daten nicht speichern.

Vorgehensweise

- ◆ Sie können die Clientdaten speichern, indem Sie entweder eine Kopie des Fensters drucken oder die Serverdaten exportieren.

Option	Beschreibung
Fenster kopieren	Verwenden Sie die Microsoft Windows-Option Druck , um eine Kopie des vSphere-Clientfensters auszudrucken.
Serverdaten exportieren	Wählen Sie Datei > Exportieren und wählen Sie ein Format, in dem die Daten gespeichert werden sollen. Öffnen Sie die Daten in einer entsprechenden Anwendung und drucken Sie sie von dieser Anwendung aus.

Fensterbereiche

Der Hauptbereich der vSphere-Client-Seite enthält einen Fensterbereich. In den meisten Ansichten gibt es einen linken und einen rechten Fensterbereich: das Bestandslistenfenster und das Informationsfenster.

Die Größe dieser Fenster kann angepasst werden.

Bestandslistenfenster	Zeigt eine hierarchische Liste der vSphere-Objekte an, wenn eine Bestandslisten- oder Zuordnungsansicht erscheint.
Informationsfenster	In diesem Fenster werden Listen und Diagramme angezeigt. Je nach ausgewählten Navigationselementen oder Bestandslistenelement wird das Informationsfenster in Registerkarten unterteilt.

Durchsuchen der vSphere Clientbestandsliste

Wenn Sie über den vSphere Client mit einem vCenter Server-System verbunden sind, können Sie in Ihrer vSphere-Bestandsliste nach virtuellen Maschinen, Hosts, Datenspeichern, Netzwerken oder Ordner suchen, die angegebenen Kriterien entsprechen.

Wenn der vSphere Client mit einem vCenter Server-System verbunden ist, das zu einer verbundenen Gruppe im verknüpften Modus von vCenter gehört, können Sie die Bestandslisten aller vCenter Server-Systeme dieser Gruppe durchsuchen. Sie können nur nach solchen Bestandslistenobjekten suchen und diese anzeigen, für die Sie über die Berechtigung zum Anzeigen verfügen. Weil der Suchdienst Active Directory Infor-

mationen über Benutzerberechtigungen abfragt, müssen Sie bei einem Domänenkonto angemeldet sein, um alle vCenter Server-Systeme im verknüpften Modus durchsuchen zu können. Wenn Sie sich unter Verwendung eines lokalen Kontos anmelden, werden auch dann nur Suchergebnisse für das lokale vCenter Server-System zurückgegeben, wenn der Server mit anderen Servern im verknüpften Modus verbunden ist.

HINWEIS Falls sich Ihre Berechtigungen ändern, während Sie angemeldet sind, erkennt der Suchdienst diese Änderungen möglicherweise nicht sofort. Melden Sie sich von allen geöffneten Sitzungen ab und melden Sie sich dann erneut an, um sicherzustellen, dass Ihre Suche mit den aktuellen Berechtigungen ausgeführt wird.

Durchführen einer einfachen Suche

Bei einer einfachen Suche werden alle Eigenschaften der angegebenen Objekttypen nach dem eingegebenen Suchbegriff durchsucht.

Vorgehensweise

- 1 Klicken Sie oben rechts im vSphere Clientfenster auf das Symbol im Suchfeld und wählen Sie den Bestandslistenelementtyp aus, nach dem Sie suchen möchten.
 - **Virtuelle Maschinen**
 - **Hosts**
 - **Ordner**
 - **Datenspeicher**
 - **Netzwerke**
 - **Bestandsliste** findet Übereinstimmungen mit den Suchkriterien bei allen verfügbaren Typen von verwalteten Objekten.
- 2 Geben Sie einen oder mehrere Suchbegriffe in das Suchfeld ein und drücken Sie die Eingabetaste.
- 3 (Optional) Wenn mehr Elemente gefunden werden, als im Ergebnisfenster angezeigt werden können, klicken Sie auf **Alle anzeigen**.

Weiter

Wenn die Ergebnisse der einfachen Suche nicht Ihren Erwartungen entsprechen, führen Sie eine erweiterte Suche durch.

Ausführen einer erweiterten Suche

Mithilfe der erweiterten Suche können Sie nach verwalteten Objekten suchen, die mehreren Kriterien entsprechen. Beispielsweise können Sie nach virtuellen Maschinen suchen, die mit einem bestimmten Suchbegriff übereinstimmen und sich auf Hosts befinden, deren Namen mit einem zweiten Suchbegriff übereinstimmen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server -System.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die Option **Ansicht > Bestandsliste > Suchen**, um die Seite für die erweiterte Suche anzuzeigen.
- 2 Klicken Sie auf das Symbol im Suchtextfeld und wählen Sie den Objekttyp aus, nach dem Sie suchen möchten.
- 3 Geben Sie einen oder mehrere Suchbegriffe in das Suchtextfeld ein.

- 4 (Optional) Verfeinern Sie die Suche basierend auf zusätzlichen Eigenschaften.
 - a Klicken Sie auf **Optionen anzeigen**.
 - b Wählen Sie im Dropdown-Menü die zusätzliche Eigenschaft aus, die Sie zum Eingrenzen der Suchergebnisse verwenden möchten. Welche Eigenschaften verfügbar sind, hängt von dem Objekttyp ab, nach dem Sie suchen.
 - c Wählen Sie die entsprechenden Optionen für die von Ihnen ausgewählte Eigenschaft aus oder geben Sie sie ein.
 - d Wenn Sie weitere Eigenschaften hinzufügen möchten, klicken Sie auf **Hinzufügen** und wiederholen Sie die Schritte a bis c.

Eine erweiterte Suche findet immer Objekte, die allen Eigenschaften in der Liste entsprechen.

- 5 Klicken Sie auf **Suchen**.

Die Suchergebnisse werden unter den Angaben für die Suche angezeigt.

Benutzerdefinierte Attribute

Mit benutzerdefinierten Attributen können Sie benutzerspezifische Metainformationen virtuellen Maschinen und verwalteten Servern zuordnen.

Attribute sind die Ressourcen, die auf allen verwalteten Hosts und virtuellen Maschinen Ihrer vSphere-Umgebung überwacht und verwaltet werden. Der Status und Zustand der Attribute wird in den Bestandslistenbereichen angezeigt.

Wenn Sie Attribute erstellt haben, legen Sie den Wert des Attributs auf jeder virtuellen Maschine bzw. jedem verwalteten Server fest. Dieser Wert wird in vCenter Server und nicht auf der virtuellen Maschine oder auf dem verwalteten Host gespeichert. Mit dem neuen Attribut können Sie Informationen zu den virtuellen Maschinen und verwalteten Hosts filtern. Wenn Sie das benutzerdefinierte Attribut nicht mehr benötigen, entfernen Sie es. Bei einem benutzerdefinierten Attribut handelt es sich immer um eine Zeichenfolge.

Angenommen, Ihnen liegt eine Liste von Produkten vor, die Sie nach Außendienstmitarbeitern sortieren möchten. Erstellen Sie ein benutzerdefiniertes Attribut für den Namen des Außendienstmitarbeiters (Name). Fügen Sie das benutzerdefinierte Attribut „Name“ als Spalte in einer der Listenansichten hinzu. Fügen Sie jedem Produkt den entsprechenden Namen hinzu. Klicken Sie auf die Spaltenüberschrift „Name“, um die Einträge alphabetisch zu sortieren.

Benutzerdefinierte Attribute sind nur dann verfügbar, wenn eine Verbindung mit einem vCenter Server-System besteht.

- [Hinzufügen von benutzerdefinierten Attributen](#) auf Seite 20

Sie können benutzerdefinierte Attribute erstellen und diese virtuellen Maschinen oder verwalteten Hosts zuweisen.

- [Bearbeiten eines benutzerdefinierten Attributs](#) auf Seite 20

Sie können über die Registerkarte Übersicht für das Objekt benutzerdefinierte Attribute bearbeiten und Anmerkungen für eine virtuelle Maschine oder einen Host hinzufügen. Anmerkungen können dazu verwendet werden, zusätzlichen beschreibenden Text oder Kommentare für ein Objekt bereitzustellen.

Hinzufügen von benutzerdefinierten Attributen

Sie können benutzerdefinierte Attribute erstellen und diese virtuellen Maschinen oder verwalteten Hosts zuweisen.

Vorgehensweise

- 1 Wählen Sie **Verwaltung > Benutzerdefinierte Attribute**.
Diese Option ist nicht verfügbar, wenn nur eine Verbindung mit einem ESXi-Host besteht.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Geben Sie die Werte für das benutzerdefinierte Attribut ein.
 - a Geben Sie den Namen des Attributs im Textfeld **Name** ein.
 - b Wählen Sie in der Dropdown-Liste **Typ** den Attributtyp aus: **Virtuelle Maschine**, **Host** oder **Global**.
 - c Geben Sie im Textfeld **Wert (Value)** den Wert ein, den das Attribut für das ausgewählte Objekt erhalten soll.
 - d Klicken Sie auf **OK**.
Nachdem Sie ein Attribut für eine einzelne virtuelle Maschine oder einen Host definiert haben, steht es für alle Objekte dieses Typs in der Bestandsliste zur Verfügung. Der angewendete Wert gilt jedoch nur für das ausgewählte Objekt.
- 4 (Optional) Klicken Sie zum Ändern des Attributnamens in das Feld **Name**, und geben Sie dann den gewünschten Namen für das Attribut ein.
- 5 Klicken Sie auf **OK**.

Bearbeiten eines benutzerdefinierten Attributs

Sie können über die Registerkarte **Übersicht** für das Objekt benutzerdefinierte Attribute bearbeiten und Anmerkungen für eine virtuelle Maschine oder einen Host hinzufügen. Anmerkungen können dazu verwendet werden, zusätzlichen beschreibenden Text oder Kommentare für ein Objekt bereitzustellen.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine oder den Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Übersicht** für die virtuelle Maschine oder den Host.
- 3 Klicken Sie im Feld Anmerkungen auf den Link **Bearbeiten**.
Das Dialogfeld „Benutzerdefinierte Attribute bearbeiten“ wird angezeigt.
- 4 Um den Wert eines bereits definierten Attributs zu bearbeiten, doppelklicken Sie auf das Feld **Wert (Value)** für das Attribut, und geben Sie einen neuen Wert ein.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Auswählen der Objekte

Zu den vCenter Server-Objekten zählen Datacenter, Ressourcenpools, Cluster, Netzwerke, Datenspeicher, Vorlagen, Hosts und virtuelle Maschinen. Die Auswahl eines Objekts ermöglicht Ihnen die Anzeige des Objektstatus und aktiviert die Menüs, sodass Sie Aktionen für das Objekt auswählen können.

Vorgehensweise

- ◆ Zeigen Sie das Objekt in der Bestandsliste an oder führen Sie eine Suche nach dem Objekt durch.
 - Klicken Sie auf der Homepage des vSphere-Clients auf das Symbol für die entsprechende Bestandslistenansicht und durchsuchen Sie die Bestandslistenhierarchie, um das Objekt auszuwählen.
 - Führen Sie eine Suche nach dem Objekt durch und doppelklicken Sie darauf in den Suchergebnissen.

vCenter Server-Plug-Ins verwalten

Nachdem Sie die Serverkomponente eines Plug-Ins installiert und beim vCenter Server registriert haben, steht die zugehörige Clientkomponente auf den vSphere-Clients zur Verfügung. Die Installation und Aktivierung von Clientkomponenten werden über das Dialogfeld Plug-In-Manager verwaltet.

Der Plug-In-Manager ermöglicht Ihnen die Ausführung der folgenden Aktionen:

- Anzeigen der verfügbaren Plug-Ins, die derzeit nicht auf dem Client installiert sind.
- Anzeigen der installierten Plug-Ins
- Herunterladen und Installieren verfügbarer Plug-Ins
- Aktivieren und Deaktivieren installierter Plug-Ins

Installieren von Plug-Ins

Sie können Plug-Ins mithilfe des Plug-In-Managers installieren.

Vorgehensweise

- 1 Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.
- 2 Wählen Sie **Plug-ins > Plug-ins verwalten**.
- 3 Wählen Sie im Dialogfeld „Plug-In-Manager“ die Registerkarte **Verfügbare Plug-Ins**.
- 4 Klicken Sie für das gewünschte Plug-In auf **Herunterladen und installieren**.
- 5 Folgen Sie den Anweisungen des Installations-Assistenten.
- 6 Überprüfen Sie nach Abschluss der Installation, ob das Plug-In auf der Registerkarte **Installierte Plug-Ins** angezeigt wird und aktiviert ist.

Möglicherweise erscheinen die Plug-Ins nach dem Abschluss der Installation erst mit einer geringen Verzögerung in der Liste der installierten Plug-Ins.

Deaktivieren und Aktivieren von Plug-Ins

Sie können Plug-Ins mithilfe des Plug-In-Managers deaktivieren und aktivieren.

Durch das Deaktivieren von Plug-In wird es nicht vom Client entfernt. Sie müssen ein Plug-In deinstallieren, um es zu entfernen.

Vorgehensweise

- 1 Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.
- 2 Wählen Sie **Plug-ins > Plug-ins verwalten**.
- 3 Wählen Sie die Registerkarte **Installiert** des Dialogfelds „Plug-In-Manager“ aus.
- 4 Klicken Sie mit der rechten Maustaste auf ein Plug-in und wählen Sie **Aktivieren** oder **Deaktivieren**.

Entfernen von Plug-Ins

Plug-Ins können über die Systemsteuerung des Betriebssystems entfernt werden.

Vorgehensweise

- ◆ Anweisungen zur Verwendung des Applets „Software“ in der Systemsteuerung finden Sie in der Dokumentation zu Ihrem Betriebssystem.

vCenter Server -Plug-Ins - Fehlerbehebung

Wenn vCenter Server-Plug-Ins nicht funktionieren, verfügen Sie über mehrere Optionen, um das Problem zu beheben.

vCenter Server-Plug-Ins, die auf dem Tomcat-Server ausgeführt werden, besitzen Dateien namens `extension.xml`, die die URL enthalten, unter der auf die entsprechende Webanwendung zugegriffen werden kann. Diese Dateien befinden sich im Ordner `C:\Programme\VMware\Infrastructure\VirtualCenter Server\extensions`. Erweiterungsinstallationsprogramme fügen diesen XML-Dateien DNS-Namen für die Maschine hinzu.

Beispiel aus der `extension.xml`-Datei: `<url>https://SPULOV-XP-VM12.vmware.com:8443/statsreport/vicr.do</url>`.

vCenter Server, Plug-In-Server und die Clients, die die Server verwenden, müssen sich auf Systemen in derselben Domäne befinden. Wenn sie sich nicht in derselben Domäne befinden oder das DNS des Plug-In-Servers geändert wird, können die Plug-In-Clients nicht auf die URL zugreifen und das Plug-In funktioniert nicht.

Sie können die XML-Dateien manuell bearbeiten, indem Sie den DNS-Namen durch eine IP-Adresse ersetzen. Registrieren Sie das Plug-In nach dem Bearbeiten seiner `extension.xml`-Datei neu.

Arbeiten mit aktiven Sitzungen

Sie können eine Liste der Benutzer anzeigen, die bei einem vCenter Server-System angemeldet sind, wenn Ihr vSphere-Client mit dem Server verbunden ist. Sie können Sitzungen beenden und eine Nachricht an alle Benutzer senden, die bei einer aktiven Sitzung angemeldet sind.

Diese Funktionen sind nicht verfügbar, wenn der vSphere-Client mit einem ESXi-Host verbunden ist.

Anzeigen von aktiven Sitzungen

Sie können auf der Startseite eines vSphere-Clients aktive Sitzungen anzeigen.

Vorgehensweise

- ◆ Klicken Sie auf der Startseite eines vSphere-Clients, der mit einem vCenter Server-System verbunden ist, auf die Schaltfläche **Sitzungen**.

Beenden von aktiven Sitzungen

Durch das Beenden einer aktiven Sitzung werden die vSphere Client-Sitzung sowie die während der Sitzung vom Benutzer gestarteten Remote-Konsolenverbindungen beendet.

Vorgehensweise

- 1 Klicken Sie auf der Startseite eines vSphere Clients, der mit einem vCenter Server-System verbunden ist, auf die Schaltfläche **Sitzungen**.
- 2 Klicken Sie mit der rechten Maustaste auf eine Sitzung und wählen Sie **Sitzung beenden** aus.
- 3 Klicken Sie auf **OK**, um das Beenden der Sitzung zu bestätigen.

Senden einer Meldung an alle aktiven Benutzer

Sie können eine „Meldung des Tages“ an alle aktiven Sitzungs- und neuen Benutzer senden, wenn diese sich beim vSphere-Client anmelden.

Der Text der **Meldung des Tages** wird als Benachrichtigung an alle aktiven Sitzungs- und neuen Benutzer gesendet, wenn diese sich anmelden.

Vorgehensweise

- 1 Klicken Sie auf der Startseite eines vSphere-Clients, der mit einem vCenter Server-System verbunden ist, auf die Schaltfläche **Sitzungen**.
- 2 Geben Sie im Feld **Meldung des Tages** den Meldungstext ein.
- 3 Klicken Sie auf **Ändern**.

Die Nachricht wird an alle am vSphere-Client angemeldeten Benutzer gesendet.

Konfigurieren von ESXi-Hosts und vCenter Server im vSphere Client

2

Im vSphere Client konfigurieren Sie die Einstellungen für ESXi und vCenter Server.

Dieses Kapitel behandelt die folgenden Themen:

- [„Konfigurieren von ESXi-Hosts“](#), auf Seite 25
- [„Konfigurieren von vCenter Server im vSphere Client“](#), auf Seite 28
- [„Konfigurieren der Kommunikation zwischen ESXi, vCenter Server und vSphere-Client“](#), auf Seite 35
- [„Neustarten oder Herunterfahren eines ESXi-Hosts“](#), auf Seite 35

Konfigurieren von ESXi-Hosts

Wenn Sie einen ESXi-Host oder ein vCenter Server-System mit dem vSphere Client direkt verbinden, können Sie eine Reihe von Konfigurationsaufgaben durchführen, beispielsweise Festlegen der Scratch-Partition, Umleiten der direkten Konsole und Konfigurieren von Syslog.

Hosteinschränkungen im vSphere Client

Die Hostkonfigurationsaufgaben, die Sie bei einer direkten Verbindung mit einem ESXi-Host oder einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden Hostfunktionen sind im vSphere Client nicht verfügbar bzw. schreibgeschützt:

- Rückforderung gelöschter Dateien
- Gastautorisierung
- Unabhängigkeit der Hostprofile vom Referenzhost
- Sperrmodus

Über den vSphere Web Client stehen Ihnen hingegen alle Hostfunktionen Ihrer vSphere-6.0-Umgebung zur Verfügung.

Umleiten der direkten Konsole auf einen seriellen Port mithilfe des vSphere Clients

Sie können die direkte Konsole auf den seriellen Port COM1 oder COM2 umleiten. Wenn Sie den vSphere Client verwenden, um die direkte Konsole auf einen seriellen Port umzuleiten, wird die eingestellte Startoption bei nachfolgenden Startvorgängen beibehalten.

Voraussetzungen

- Stellen Sie sicher, dass Sie vom vSphere Client aus auf den Host zugreifen können.

- Stellen Sie sicher, dass der serielle Port nicht bereits für die serielle Protokollierung und das serielle Debuggen oder die ESX Shell (tty1Port) verwendet wird.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie unter „Software“ auf **Erweiterte Einstellungen**.
- 4 Erweitern Sie im linken Bereich die **VMkernel**-Liste und wählen Sie **Starten**.
- 5 Stellen Sie sicher, dass die Felder **VMkernel.Boot.logPort** und **VMkernel.Boot.gdbPort** nicht für die Verwendung des COM-Ports eingestellt sind, an die Sie die direkte Konsole umleiten möchten.
- 6 Legen Sie **VMkernel.Boot.tty2Port** auf den seriellen Port fest, an die Sie die direkte Konsole umleiten möchten: **com1** oder **com2**.
- 7 Klicken Sie auf **OK**.
- 8 Starten Sie den Host neu.

Sie können nun den ESXi-Host remote von einer Konsole aus verwalten, die an den seriellen Port angeschlossen ist.

Festlegen der Scratch-Partition im vSphere Client

Wenn keine Scratch-Partition festgelegt ist, sollten Sie eine konfigurieren, besonders wenn nicht genügend freier Arbeitsspeicher ein Problem werden könnte. Wenn keine Scratch-Partition vorhanden ist, wird die Ausgabe von „vm-support“ auf einer Ramdisk gespeichert.

Voraussetzungen

Das Verzeichnis, das für die Scratch-Partition verwendet wird, muss auf dem Host vorhanden sein.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie unter „Software“ auf **Erweiterte Einstellungen**.
- 4 Wählen Sie **ScratchConfig**.
Im Feld **ScratchConfig.CurrentScratchLocation** wird der aktuelle Speicherort der Scratch-Partition angegeben.
- 5 Geben Sie im Feld **ScratchConfig.ConfiguredScratchLocation** einen für diesen Host eindeutigen Verzeichnispfad ein.
- 6 Starten Sie den Host neu, damit die Änderungen wirksam werden.

Konfiguration von Syslog auf ESXi -Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Diensts verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Client aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Bereich „Software“ auf **Erweiterte Einstellungen**.
- 4 Wählen Sie in der Strukturansicht **Syslog**.
- 5 Klicken Sie zum Einrichten der globalen Protokollierung auf **Global** und nehmen Sie die entsprechenden Änderungen in den rechten Feldern vor.

Option	Beschreibung
Syslog.global.defaultRotate	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis <code>/scratch</code> auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format <code>[Datenspeichername] Pfad_zur_Datei</code> aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <code>[storage1] /systemlogs</code> dem Pfad <code>/vmfs/volumes/storage1/systemlogs</code> zuzuordnen.
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von Syslog.global.LogDir angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. <code>ssl://Hostname1:514</code> . UDP (Standard), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

- 6 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll.
 - a Klicken Sie auf **loggers**.
 - b Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten, und geben Sie die gewünschte Anzahl der Rotationen und die gewünschte Protokollgröße ein.
- 7 Klicken Sie auf **OK**.

Änderungen an der syslog-Option werden sofort wirksam.

Festlegen der Akzeptanzebene des Host-Image-Profiles

Die Akzeptanzebene des Host-Image-Profiles legt fest, welche vSphere-Installationspakete (VIBs) für die Installation akzeptiert werden.

VIB-Signaturen werden auf Basis einer Kombination aus VIB-Akzeptanzebene und Akzeptanzebene des Host-Image-Profiles für die Installation geprüft und akzeptiert. VIBs werden mit einer Akzeptanzebene versehen, die ihrem Signaturstatus abhängt.

Voraussetzungen

Erforderliche Berechtigungen: **Host.Konfiguration.Sicherheitsprofil** und **Host.Konfiguration.Firewall**

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie unter „Software“ auf **Sicherheitsprofil**.
- 3 Klicken Sie unter „Akzeptanzebene des Host-Image-Profiles“ auf **Bearbeiten**.
- 4 Wählen Sie die Akzeptanzebene aus und klicken Sie auf **OK**.

Tabelle 2-1. Akzeptanzebenen des Host-Image-Profiles

Akzeptanzebene des Host-Image-Profiles	Akzeptierte Ebenen der VIBs
Von VMware zertifiziert	Von VMware zertifiziert
VMware Accepted	VMware Certified, VMware Accepted
Unterstützte Partner	VMware Certified, VMware Accepted, Unterstützte Partner
Unterstützte Community	VMware Certified, VMware Accepted, Unterstützte Partner, Unterstützte Community

Konfigurieren von vCenter Server im vSphere Client

Verwenden Sie das Einstellungsdialogfeld von vCenter Server, um Einstellungen wie Lizenzierung, Statistikerfassung, Protokollierung usw. zu konfigurieren.

vCenter Server-Einschränkungen im vSphere Client

Die Aufgaben im Zusammenhang mit vCenter Server, die Sie bei einer direkten Verbindung mit einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden vCenter Server-Funktionen sind im vSphere Client nicht verfügbar bzw. schreibgeschützt:

- Laufzeiteinstellungen
- Lizenzberichte
- Zertifikatsverwaltung
- Erstellen und Verwalten von Kategorien und Tags

Über den vSphere Web Client stehen Ihnen hingegen alle Funktionen im Zusammenhang mit vCenter Server in Ihrer vSphere-6.0-Umgebung zur Verfügung.

Konfigurieren von Lizenzeinstellungen für vCenter Server

Für die Verwendung von vCenter Server müssen Sie eine Lizenz konfigurieren. Für mehrere vSphere-Komponenten und -Funktionen sind Lizenzschlüssel erforderlich.

Voraussetzungen

Zum Konfigurieren von Lizenzen muss der vSphere-Client mit einem vCenter Server-System verbunden sein.

Erforderliche Berechtigung: **Global.Einstellungen**

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld „vCenter Server-Einstellungen“ anzuzeigen.
- 2 Wenn das vCenter Server-System zu einer verbundenen Gruppe gehört, wählen Sie den Server, den Sie konfigurieren möchten, im Dropdown-Menü **Aktueller vCenter Server** aus.
- 3 Wählen Sie im Abschnitt **vCenter-Lizenz** den Typ des Lizenzschlüssels aus, der diesem vCenter Server zugewiesen werden soll.
 - Wählen Sie **Diesem vCenter Server einen vorhandenen Lizenzschlüssel zuweisen** und wählen Sie in der Produktliste einen Lizenzschlüssel aus.
 - Wählen Sie **Diesem vCenter Server einen neuen Lizenzschlüssel zuweisen**, klicken Sie auf **Schlüssel eingeben** und geben Sie einen Lizenzschlüssel für vCenter Server und optional eine Bezeichnung für den Schlüssel ein.

HINWEIS Zur Eingabe von ESXi-Hostlizenzen wählen Sie **Ansicht > Verwaltung > Lizenzierung**.

Konfigurieren von Statistikintervallen

Über Statistikintervalle wird die Häufigkeit, mit der statistische Abfragen durchgeführt werden, sowie der Zeitraum, für den statistische Daten in der Datenbank gespeichert werden, und der erfasste Typ der statistischen Daten festgelegt.

Erforderliche Berechtigung: **Global.Einstellungen**

HINWEIS Es sind nicht alle Intervallattribute konfigurierbar.

Voraussetzungen

Zum Konfigurieren von Statistikeinstellungen muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > Einstellungen**, um das Dialogfeld **vCenter Server-Einstellungen** vCenter Server zu öffnen.
- 2 Wählen Sie im Navigationsfenster die Option **Statistik**.
- 3 Aktivieren bzw. deaktivieren Sie im Abschnitt „Statistikintervalle“ das entsprechende Kontrollkästchen für ein Erfassungsintervall, um dieses zu aktivieren bzw. zu deaktivieren.

Durch die Aktivierung eines längeren Intervalls werden automatisch alle kürzeren Intervalle aktiviert.

- 4 Wenn Sie ein Attribut eines Erfassungsintervalls ändern möchten, wählen Sie die entsprechende Zeile im Abschnitt „Statistikintervall“ aus und klicken Sie auf **Bearbeiten**, um das Dialogfeld „Erfassungsintervall bearbeiten“ zu öffnen.
 - a Wählen Sie unter **Daten beibehalten für** eine Archivierungslänge aus.
Diese Option ist nur für die Intervalle „Tag“ und „Jahr“ konfigurierbar.
 - b Wählen Sie unter **Statistikintervall** eine Intervalldauer aus.
Diese Option ist nur für das Intervall „Tag“ konfigurierbar.
 - c Wählen Sie unter **Statistikebene** eine neue Intervallebene aus.
Auf Ebene 4 wird die höchste Anzahl an statistischen Leistungsmetriken verwendet. Es ist empfehlenswert, diese Ebene nur für das Debuggen auszuwählen.

Die Statistikebene muss dem für das vorangegangene Statistikintervall festgelegten Wert für die Statistikebene entsprechen oder darunter liegen. Dabei handelt es sich um eine vCenter Server-Abhängigkeit.
- 5 (Optional) Schätzen Sie im Abschnitt „Datenbankgröße“ die Auswirkungen der Statistikeinstellungen auf die Datenbank ein.
 - a Geben Sie die Anzahl für **Physische Hosts** ein.
 - b Geben Sie die Anzahl für **Virtuelle Maschinen** ein.

Der geschätzte erforderliche Speicherplatz und die Anzahl an erforderlichen Datenbankzeilen wird berechnet und angezeigt.
 - c Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Statistikerfassung vor.
- 6 Klicken Sie auf **OK**.

Konfigurieren von Laufzeiteinstellungen

Sie können die vCenter Server-ID sowie die verwaltete IP-Adresse von vCenter Server ändern. In der Regel müssen an diesen Einstellungen keine Änderungen vorgenommen werden. Wenn Sie jedoch mehrere vCenter Server-Systeme in der gleichen Umgebung betreiben, kann es ggf. erforderlich sein, Änderungen vorzunehmen.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von Laufzeiteinstellungen muss der vSphere Client mit dem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wenn das vCenter Server-System zu einer verbundenen Gruppe gehört, wählen Sie im Dropdown-Menü **Aktueller vCenter Server** den Server, den Sie konfigurieren möchten, aus.
- 3 Wählen Sie im Navigationsfenster die Option **Laufzeiteinstellungen**.
- 4 Geben Sie unter **Eindeutige vCenter Server-ID** eine eindeutige ID ein.

Sie können diesen Wert im Zahlenbereich von 0 bis 63 festlegen, um jedes vCenter Server-System in einer gemeinsamen Umgebung eindeutig zu kennzeichnen. Standardmäßig wird ein willkürlicher ID-Wert generiert.
- 5 Geben Sie unter **Verwaltete vCenter Server-IP** die IP-Adresse des vCenter Server-Systems ein.

- 6 Geben Sie unter **Name von vCenter Server** den Namen des vCenter Server-Systems ein.
Wenn Sie den DNS-Namen von vCenter Server ändern, verwenden Sie diese Option, um den vCenter Server-Namen entsprechend zu ändern.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Weiter

Wenn Sie Änderungen an der eindeutigen ID des vCenter Server-Systems vorgenommen haben, ist ein Neustart des vCenter Server-Systems erforderlich, damit diese Änderungen wirksam werden.

Konfigurieren von Active Directory-Einstellungen

Einige der Interaktionsmethoden zwischen vCenter Server und dem Active Directory-Server können konfiguriert werden.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von Active Directory-Einstellungen muss der vSphere Client mit dem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie im Navigationsfenster **Active Directory**.
- 3 Geben Sie unter **Active Directory-Zeitüberschreitung** das Zeitüberschreitungsintervall in Sekunden für das Verbinden mit dem Active Directory-Server an.
- 4 Wählen Sie **Abfragegrenze aktivieren**, um die im Dialogfeld „Berechtigungen hinzufügen“ angezeigte Anzahl an Benutzern und Gruppen einzuschränken.
- 5 Geben Sie unter **Benutzer & Gruppen** die maximal anzuzeigende Anzahl an Benutzern und Gruppen ein.
Bei Eingabe des Werts 0 (Null) werden alle Benutzer und Gruppen angezeigt.
- 6 Wählen Sie **Validierung aktivieren**, wenn vCenter Server regelmäßig einen Abgleich der eigenen Benutzer und Gruppen mit dem Active Directory-Server vornehmen soll.
- 7 Geben Sie unter **Validierungszeitraum** den Zeitraum zwischen Synchronisierungsinstanzen in Minuten ein.
- 8 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Konfigurieren von Einstellungen für E-Mail-Absender

Sie müssen die E-Mail-Adresse des Absenderkontos konfigurieren, um vCenter Server-Vorgänge zu ermöglichen, wie z. B. das Senden von E-Mail-Benachrichtigungen als Alarmaktionen.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von SMTP-Benachrichtigungen muss der vSphere Client mit dem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie im Navigationsfenster **E-Mail**.
- 3 Geben Sie die SMTP-Serverinformationen ein.
Der SMTP-Server ist der DNS-Name oder die IP-Adresse des SMTP-Gateways, der für das Versenden von E-Mail-Nachrichten verwendet werden soll.
- 4 Geben Sie die Absenderkontoinformationen ein.
Das Absenderkonto ist die E-Mail-Adresse des Absenders.

HINWEIS Die vollständige E-Mail-Adresse muss eingegeben werden, einschließlich des Domännennamens (die Angaben nach dem @-Zeichen).

Beispiel: mail_server@datencenter.com.

- 5 Klicken Sie auf **OK**.

Weiter

Erstellen Sie zum Testen der E-Mail-Einstellungen einen Alarm, der durch eine Benutzeraktion ausgelöst werden kann, z. B. einen Alarm, der durch das Ausschalten einer virtuellen Maschine ausgelöst wird, und überprüfen Sie, ob Sie eine E-Mail erhalten, wenn der Alarm ausgelöst wird.

Konfigurieren von SNMP-Einstellungen

Sie können bis zu vier Empfänger für das Empfangen von SNMP-Traps vom vCenter Server konfigurieren. Geben Sie für jeden Empfänger einen Hostnamen, einen Port und eine Community an.

Voraussetzungen

Zum Konfigurieren von SNMP-Einstellungen muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Erforderliche Berechtigung: **Global.Einstellungen**

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie in der Liste „Einstellungen“ den Eintrag **SNMP** aus.
- 3 Geben Sie unter **Empfänger-URL** den Hostnamen oder die IP-Adresse des SNMP-Empfängers ein.
- 4 Geben Sie in das Feld neben dem Feld Empfänger-URL die Portnummer des Empfängers ein.
Bei der Portnummer muss es sich um einen Wert zwischen 1 und 65535 handeln.
- 5 Geben Sie in **Community-String** den Community-Bezeichner ein.
- 6 Klicken Sie auf **OK**.

Konfigurieren von Zeitüberschreitungseinstellungen

Sie können die Zeitüberschreitungsintervalle für vCenter Server-Vorgänge konfigurieren. Diese Intervalle geben den Zeitraum an, nach dessen Ablauf beim vSphere Client eine Zeitüberschreitung eintritt.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von Zeitüberschreitungseinstellungen muss der vSphere Client mit dem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie **Zeitüberschreitungseinstellungen** im Navigationsfenster aus.
- 3 Geben Sie unter **Normale Vorgänge** das Zeitüberschreitungsintervall für normale Vorgänge in Sekunden ein.
Legen Sie für diesen Wert nicht Null (0) fest.
- 4 Geben Sie unter **Lange Vorgänge** das Zeitüberschreitungsintervall für lange Vorgänge in Minuten ein.
Legen Sie für diesen Wert nicht Null (0) fest.
- 5 Klicken Sie auf **OK**.
- 6 Starten Sie das vCenter Server-System neu, damit die Änderungen wirksam werden.

Konfigurieren von Protokollierungsoptionen

Sie können den Umfang der Angaben konfigurieren, die vCenter Server in den Protokolldateien erfasst.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von Statistikeinstellungen muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie **Protokollierungsoptionen** im Navigationsfenster aus.
- 3 Wählen Sie in der Liste vCenter Server die Protokollierungsoptionen aus.

Option	Beschreibung
Keine (Keine Protokollierung)	Schaltet die Protokollierung aus
Fehler (Nur Fehler)	Zeigt nur Protokolleinträge für Fehler an
Warnung (Fehler und Warnungen)	Zeigt nur Protokolleinträge für Fehler und Warnungen an
Info (Normale Protokollierung)	Zeigt Protokolleinträge für Informationen, Fehler und Warnungen an
Ausführlich (Ausführliche Protokollierung)	Zeigt ausführliche Protokolleinträge für Informationen, Fehler und Warnungen an
Ausführlich (Ausführlich (erweitert))	Zeigt erweiterte ausführliche Protokolleinträge für Informationen, Fehler, Warnungen und ausführliche Protokolleinträge an

- 4 Klicken Sie auf **OK**.

Änderungen an den Protokolleinstellungen werden sofort wirksam. Es ist kein Neustart des vCenter Server-Systems erforderlich.

Konfigurieren der maximalen Anzahl von Datenbankverbindungen

Sie können die maximale Anzahl von Datenbankverbindungen konfigurieren, die gleichzeitig bestehen können.

Voraussetzungen

Zum Konfigurieren von Datenbankeinstellungen muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie im Navigationsfenster **Datenbank** aus.
- 3 Geben Sie unter **Maximale Anzahl** die Anzahl ein.

In der Regel müssen Sie diesen Wert nicht ändern. Eine Erhöhung dieser Anzahl bietet sich dann an, wenn Ihr vCenter Server-System häufig zahlreiche Vorgänge ausführt und die Leistung entscheidend ist. Eine Verringerung der Anzahl ist dann angebracht, wenn es sich um eine freigegebene Datenbank handelt und die Verbindungen zur Datenbank kostenintensiv sind. Sofern nicht eine dieser beiden Situationen auf Ihr System zutrifft, ist eine Änderung dieses Wertes jedoch nicht empfehlenswert.

- 4 Klicken Sie auf **OK**.

Konfigurieren einer Datenbankaufbewahrungsrichtlinie

Damit das Wachstum der vCenter Server-Datenbank begrenzt und nicht unnötig viel Speicherplatz in Anspruch genommen wird, können Sie die Datenbank so konfigurieren, dass Informationen zu Aufgaben oder Ereignissen nach einem angegebenen Zeitraum verworfen werden.

Verwenden Sie diese Optionen nicht, wenn Sie den vollständigen Verlauf der Aufgaben und Ereignisse für Ihren vCenter Server aufbewahren möchten.

Voraussetzungen

Zum Konfigurieren der Datenbankaufbewahrungsrichtlinie muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld „vCenter Server-Einstellungen“ anzuzeigen.
- 2 Wählen Sie die Option **Datenbankaufbewahrungsrichtlinie**.
- 3 (Optional) Wählen Sie die Option **Aufgaben beibehalten für** aus und geben Sie die gewünschte Anzahl an Tagen in das Textfeld ein.

Die Informationen zu den auf diesem vCenter Server-System ausgeführten Aufgaben werden nach der angegebenen Anzahl an Tagen verworfen.
- 4 (Optional) Wählen Sie die Option **Ereignisse beibehalten für** aus und geben Sie die gewünschte Anzahl an Tagen in das Textfeld ein.

Die Informationen zu den Ereignissen für dieses vCenter Server-System werden nach der angegebenen Anzahl an Tagen verworfen.
- 5 Klicken Sie auf **OK**.

Konfigurieren von erweiterten Einstellungen

Auf der Seite „Erweiterte Einstellungen“ können Sie die vCenter Server-Konfigurationsdatei `vpxd.cfg` ändern.

Auf dieser Seite können Sie Einträge zur Datei `vpxd.cfg` hinzufügen, Sie können Einträge jedoch nicht bearbeiten oder löschen. VMware empfiehlt Ihnen, dass Sie nur dann Änderungen an diesen Einstellungen vornehmen, wenn Sie vom technischen Support von VMware dazu aufgefordert werden oder wenn Sie die entsprechenden Anweisungen in der VMware-Dokumentation befolgen.

Erforderliche Berechtigung: **Global.Einstellungen**

Voraussetzungen

Zum Konfigurieren von Statistikeinstellungen muss der vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie bei Bedarf **Verwaltung > vCenter Server-Einstellungen** aus, um das Dialogfeld vCenter Server anzuzeigen.
- 2 Wählen Sie im Navigationsbereich die Option **Erweiterte Einstellungen**.
- 3 Geben Sie im Feld **Schlüssel** einen Schlüssel ein.
- 4 Geben Sie im Feld **Wert** den Wert für den angegebenen Schlüssel ein.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Klicken Sie auf **OK**.

Weiter

Bei vielen erweiterten Optionen ist es erforderlich, dass das vCenter Server-System neu gestartet wird, bevor die Änderungen wirksam werden. Nehmen Sie Kontakt zum technischen Support von VMware auf, um zu ermitteln, ob nach Ihren Änderungen ein Neustart erforderlich ist.

Konfigurieren der Kommunikation zwischen ESXi , vCenter Server und vSphere-Client

Der vSphere-Client kommuniziert standardmäßig über die Ports 80 und 443 mit vCenter Server und ESXi-Hosts.

Konfigurieren Sie die Firewall so, dass die Kommunikation zwischen dem vSphere-Client und vCenter Server zugelassen wird, indem Sie die Ports 80 und 443 öffnen.

vCenter Server dient als Webservice. Wenn in Ihrer Umgebung ein Web-Proxy verwendet werden muss, kann vCenter Server wie jeder andere Webservice mit einem Proxy verbunden werden.

Neustarten oder Herunterfahren eines ESXi -Hosts

Sie können jeden ESXi-Host unter Verwendung des vSphere-Clients ausschalten bzw. neu starten. Beim Ausschalten eines verwalteten Hosts wird dessen Verbindung mit vCenter Server getrennt, er wird jedoch nicht aus der Bestandsliste entfernt.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Schalten Sie alle virtuellen Maschinen aus, die auf dem ESXi-Host ausgeführt werden.

- 3 Klicken Sie mit der rechten Maustaste auf den ESXi-Host und wählen Sie **Neu starten** oder **Herunterfahren**.
 - Wenn Sie **Neu starten** auswählen, wird der ESXi-Host heruntergefahren und neu gestartet.
 - Wenn Sie **Herunterfahren** auswählen, wird der ESXi-Host heruntergefahren. Sie müssen das System manuell wieder einschalten.
- 4 Geben Sie einen Grund für das Herunterfahren an.

Diese Angabe wird dem Protokoll hinzugefügt.

Organisieren Ihrer Bestandsliste

Planen Sie die Einrichtung Ihrer virtuellen Umgebung. Eine umfangreiche vSphere-Implementierung enthält möglicherweise mehrere virtuelle Datacenter mit einer komplexen Anordnung von Hosts, Clustern, Ressourcenpools und Netzwerken. Kleinere Implementierungen erfordern möglicherweise ein einzelnes virtuelles Datacenter mit einer weniger komplexen Topologie. Überlegen Sie sich unabhängig vom Umfang Ihrer virtuellen Umgebung, wie die virtuellen Maschinen, die unterstützt werden sollen, verwendet und verwaltet werden.

Nachfolgend finden Sie Fragen, die Sie beim Erstellen und Organisieren einer Bestandsliste von virtuellen Objekten beantworten sollten:

- Benötigen einige virtuellen Maschinen dedizierte Ressourcen?
- Ist bei einigen virtuellen Maschinen mit Arbeitslastspitzen zu rechnen?
- Müssen einige virtuellen Maschinen als Gruppe verwaltet werden?
- Möchten Sie mehrere vSphere Standard-Switches oder aber einen einzelnen vSphere Distributed Switch pro Datacenter verwenden?
- Möchten Sie vMotion und DRM (Distributed Resource Management) bei einigen, aber nicht bei anderen virtuellen Maschinen verwenden?
- Benötigen einige virtuelle Objekte einen Satz von Systemberechtigungen und andere Objekte einen anderen Satz?

Ihre vSphere-Bestandsliste wird im linken Fensterbereich des vSphere Clients angezeigt. Abgesehen von den folgenden Einschränkungen können Sie Objekte beliebig hinzufügen und zusammenstellen:

- Der Name eines Bestandslistenobjekts muss mit seinem übergeordneten Objekt eindeutig sein.
- vApp-Namen müssen innerhalb der Ansicht „Virtuelle Maschinen und Vorlagen“ eindeutig sein.
- Systemberechtigungen werden übernommen und sind kaskadierend.

Aufgaben für das Organisieren Ihrer Bestandsliste

Das Auffüllen und Organisieren der Bestandsliste umfasst die folgenden Aktivitäten:

- Erstellen Sie Datacenter.
- Fügen Sie Hosts zu den Datacentern hinzu.
- Ordnen Sie Bestandslistenobjekte in Ordnern an.
- Richten Sie das Netzwerk mithilfe von vSphere Standard-Switches oder vSphere Distributed Switches ein. Für die Verwendung von Diensten wie vMotion, TCP/IP-Speicher, Virtual SAN und Fault Tolerance richten Sie das VMkernel-Netzwerk für diese Dienste ein. Weitere Informationen finden Sie unter *vSphere-Netzwerk*.

- Konfigurieren Sie Speichersysteme und erstellen Sie Bestandslistenobjekte für den Datenspeicher, um logische Container für Speichergeräte in Ihrer Bestandsliste bereitzustellen. Weitere Informationen hierzu finden Sie unter *vSphere-Speicher*.
- Erstellen Sie Cluster, um die Ressourcen von mehreren Hosts und virtuellen Maschinen zusammenzufassen. Sie können vSphere HA und vSphere DRS aktivieren, um die Verfügbarkeit zu erhöhen und die Ressourcenverwaltung flexibler zu gestalten. Weitere Informationen zum Konfigurieren von vSphere HA finden Sie unter *Handbuch zur Verfügbarkeit in vSphere*. Weitere Informationen zum Konfigurieren von vSphere DRS finden Sie unter *Handbuch zur vSphere-Ressourcenverwaltung*.
- Erstellen Sie Ressourcenpools, um die logische Abstraktion und eine flexible Verwaltung der Ressourcen in vSphere zu ermöglichen. Ressourcenpools können in Hierarchien angeordnet und zur hierarchischen Partitionierung verfügbarer CPU- und Arbeitsspeicherressourcen verwendet werden. Weitere Informationen dazu finden Sie unter *Handbuch zur vSphere-Ressourcenverwaltung*.

Dieses Kapitel behandelt die folgenden Themen:

- „[Datencenter erstellen](#)“, auf Seite 38
- „[Hosts hinzufügen](#)“, auf Seite 39
- „[Cluster erstellen](#)“, auf Seite 40
- „[Erstellen von Ressourcenpools](#)“, auf Seite 41
- „[Datenspeicher erstellen](#)“, auf Seite 41
- „[Hostweite Netzwerke erstellen](#)“, auf Seite 42
- „[Datencenterweite Netzwerke erstellen](#)“, auf Seite 43

Datencenter erstellen

Ein virtuelles Datencenter ist ein Container für alle Bestandslistenobjekte, die zum Ausbau einer voll funktionsfähigen Umgebung für die Ausführung von virtuellen Maschinen erforderlich sind. Sie können mehrere Datencenter zum Organisieren von Umgebungsgruppen erstellen. Sie können beispielsweise ein Datacenter für jede organisatorische Einheit in Ihrem Unternehmen erstellen oder manche Datencenter für Hochleistungsumgebungen und andere für weniger anspruchsvolle virtuelle Maschinen erstellen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Datencenterobjekts verfügen.

HINWEIS Bestandslistenobjekte können innerhalb eines Datencenters interagieren, aber die Möglichkeiten, über Datencenter hinweg zu interagieren, sind beschränkt. Sie können beispielsweise eine Hot-Migration von virtuellen Maschinen von einem auf einen anderen Host in demselben Datencenter durchführen, von einem Host in einem Datencenter auf einen Host in einem anderen Datencenter jedoch nicht.

Vorgehensweise

- 1 Wechseln Sie zu **Home > Bestandsliste > Hosts und Cluster**.
- 2 Wählen Sie **Datei > Neu > Datencenter**.
- 3 Benennen Sie das Datencenter um.

Weiter

Fügen Sie Hosts, Cluster, Ressourcenpools, vApps, Netzwerke, Datenspeicher und virtuelle Maschinen zum Datencenter hinzu.

Hosts hinzufügen

Sie können Hosts unter einem Datencenter-, Ordner- oder Clusterobjekt hinzufügen. Wenn ein Host virtuelle Maschinen enthält, werden diese virtuellen Maschinen zusammen mit dem Host zur Bestandsliste hinzugefügt. Informationen zum Konfigurieren von Hosts finden Sie in der Dokumentation *vSphere-Netzwerk*, *vSphere-Speicher*, *vSphere-Sicherheit* und *vSphere-Hostprofile*.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Hostobjekts verfügen.
- Stellen Sie sicher, dass ein Datencenter, ein Ordner oder ein Cluster in der Bestandsliste vorhanden ist.
- Besorgen Sie sich den Benutzernamen und das Kennwort für ein Benutzerkonto mit administrativen Berechtigungen auf dem Host.
- Stellen Sie sicher, dass Hosts hinter einer Firewall mit dem vCenter Server-System und allen anderen Hosts über Port 902 bzw. einen anderen vom Benutzer konfigurierten Port kommunizieren können.
- Stellen Sie sicher, dass alle NFS-Mounts auf dem Host aktiv sind.

Vorgehensweise

- 1 Wählen Sie **Home > Bestandsliste > Hosts und Cluster**.
- 2 Wählen Sie ein Datencenter, einen Cluster oder einen Ordner innerhalb eines Datencenters aus.
- 3 Wählen Sie **Datei > Neu > Host hinzufügen**.
- 4 Geben Sie den Hostnamen oder die IP-Adresse und die Administrator-Anmeldedaten ein und klicken Sie auf **Weiter**.
- 5 (Optional) Wählen Sie **Sperrmodus aktivieren**, um den Remotezugriff für das Administratorkonto zu deaktivieren, nachdem vCenter Server die Steuerung des Hosts übernommen hat.

Aktivieren Sie dieses Kontrollkästchen, um sicherzustellen, dass der Host ausschließlich über vCenter Server verwaltet wird. Im Sperrmodus können Sie nur einige Verwaltungsaufgaben ausführen. Hierzu ist eine Anmeldung an der lokalen Konsole des Hosts erforderlich.

- 6 Überprüfen Sie die Hostinformationen und klicken Sie auf **Weiter**.
- 7 (Optional) Weisen Sie ggf. dem Host einen Lizenzschlüssel zu und klicken Sie auf **Weiter**.
- 8 Führen Sie einen der folgenden Schritte aus:

Option	Beschreibung
Wenn Sie den Host zu einem Cluster hinzufügen	Wählen Sie eine Ressourcenpool-Option aus und klicken Sie auf Weiter .
Wenn Sie den Host nicht zu einem Cluster hinzufügen	Wählen Sie einen Speicherort, in dem Sie die virtuellen Maschinen platzieren möchten, die bereits auf dem Host vorhanden sind, und klicken Sie auf Weiter .

- 9 Überprüfen Sie die Zusammenfassung, und klicken Sie auf **Beenden**.

Der Host und dessen virtuelle Maschinen werden zur Bestandsliste hinzugefügt.

Cluster erstellen

Ein Cluster ist eine Gruppe von Hosts. Wenn Sie einem Cluster einen Host hinzufügen, werden die Ressourcen des Hosts zu den Ressourcen des Clusters hinzugefügt. Der Cluster verwaltet die Ressourcen aller zugehörigen Hosts. Cluster ermöglichen die Verwendung der Lösungen vSphere HA (vSphere High Availability) und vSphere DRS (vSphere Distributed Resource Scheduler).

Voraussetzungen

- Öffnen Sie auf dem vSphere Client eine Sitzung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Clusterobjekts verfügen.
- Stellen Sie sicher, dass in der Bestandsliste ein Datacenter bzw. ein Ordner innerhalb eines Datacenters vorhanden ist.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf ein Datacenter oder einen Ordner im vSphere Client und wählen Sie **Neuer Cluster**.
- 2 Geben Sie einen Namen für den Cluster ein.
- 3 Wählen Sie Clusterfunktionen aus.

Option	Beschreibung
Wenn Sie die Verwendung von DRS mit diesem Cluster gewählt haben	a Klicken Sie auf das Feld vSphere DRS .
	b Wählen Sie eine Automatisierungs- und eine Migrationsebene aus und klicken Sie auf Weiter .
	c Wählen Sie eine Standard-Energieverwaltungseinstellung und einen DPM-Schwellenwert aus und klicken Sie auf Weiter .
Wenn Sie die Verwendung von HA mit diesem Cluster gewählt haben	a Klicken Sie auf vSphere HA .
	b Wählen Sie, ob Sie Hostüberwachung und Zugangssteuerung aktivieren möchten.
	c Geben Sie bei Aktivierung der Zugangssteuerung eine Richtlinie an.
	d Klicken Sie auf Weiter .
	e Legen Sie das Standard-Clusterverhalten fest und klicken Sie auf Weiter .
	f Legen Sie die Einstellungen für die Überwachung der virtuellen Maschinen fest und klicken Sie auf Weiter .

- 4 Wählen Sie eine EVC-Einstellung (Enhanced vMotion Compatibility) und klicken Sie auf **Weiter**.
EVC stellt sicher, dass alle Hosts in einem Cluster denselben CPU-Funktionssatz gegenüber der virtuellen Maschine offenlegen – selbst dann, wenn die tatsächlichen CPUs auf den Hosts abweichen. Auf diese Weise wird verhindert, dass mit vMotion durchgeführte Migrationen aufgrund nicht kompatibler CPUs fehlschlagen.
- 5 Wählen Sie eine Auslagerungsdatei-Richtlinie aus und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Optionen, die Sie für den Cluster angegeben haben, und klicken Sie auf **Beenden**.

Der Cluster wird zur Bestandsliste hinzugefügt.

Weiter

Fügen Sie Hosts und Ressourcenpools zum Cluster hinzu.

Erstellen von Ressourcenpools

Sie können Ressourcenpools zum (hierarchischen) Partitionieren der verfügbaren CPU- und Arbeitsspeicherressourcen eines eigenständigen Hosts oder Clusters verwenden. Verwenden Sie Ressourcenpools, um Ressourcen zusammenzufassen und Zuweisungsrichtlinien für mehrere virtuelle Maschinen festzulegen, ohne für jede virtuelle Maschine die Ressourcen einzeln festzulegen zu müssen.

Voraussetzungen

- Stellen Sie sicher, dass der vSphere Client mit einem vCenter Server verbunden ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Erstellen eines Ressourcenpoolobjekts verfügen.
- Stellen Sie sicher, dass ein Cluster, eine vApp oder ein anderes Ressourcenpoolobjekt dem Ressourcenpool übergeordnet ist.

Vorgehensweise

- 1 Wählen Sie **Home > Bestandsliste > Hosts und Cluster**.
- 2 Wählen Sie einen Cluster, eine vApp oder einen Ressourcenpool aus.
- 3 Wählen Sie **Datei > Neu > Ressourcenpool**.
- 4 Geben Sie einen Namen ein und legen Sie die Ressourceneinstellungen fest.
- 5 Klicken Sie auf **OK**.

Der Ressourcenpool wird zur Bestandsliste hinzugefügt.

Weiter

Fügen Sie virtuelle Maschinen und vApps zu Ihrem Ressourcenpool hinzu.

Datenspeicher erstellen

Ein Datenspeicher ist ein logischer Container, der Dateien der virtuellen Maschine enthält sowie andere Dateien, die für VM-Vorgänge benötigt werden. Datenspeicher können sich auf unterschiedlichen Typen physischer Speicher befinden, einschließlich lokaler Speicher, iSCSI, Fibre-Channel-SAN oder NFS. Ein Datenspeicher kann auf VMFS oder NFS basieren.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Datenspeicherobjekts verfügen.
- Stellen Sie sicher, dass mindestens ein Host in der Bestandsliste auf den physischen Speicher zugreifen kann.

Vorgehensweise

- 1 Wählen Sie **Home > Bestandsliste > Datenspeicher**.
- 2 Klicken Sie mit der rechten Maustaste auf ein Datacenter und wählen Sie **Datenspeicher hinzufügen**.
- 3 Wählen Sie einen Host aus, und klicken Sie auf **Weiter**.

- 4 Wählen Sie einen Speichertyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Festplatte oder LUN	a Wählen Sie eine Festplatte oder eine LUN aus und klicken Sie auf Weiter .
	b Überprüfen Sie die Informationen zum Festplattenlayout und klicken Sie auf Weiter .
	c Geben Sie einen Namen für den Datenspeicher ein und klicken Sie auf Weiter .
	d Legen Sie die Maximalwerte für die Datei- und die Blockgröße fest.
	e Legen Sie die Festplatten- bzw. die LUN-Kapazität fest und klicken Sie auf Weiter .
Netzwerkdateisystem (NFS)	a Geben Sie die Server- und Ordnerinformationen ein.
	b Wählen Sie, ob die Clients das NFS als „Nur Lesen“ mounten sollen.
	c Geben Sie einen Namen ein und klicken Sie auf Weiter .

- 5 Überprüfen Sie die Zusammenfassung und klicken Sie auf **Beenden**.

Ein Datenspeicher wird zur Bestandsliste hinzugefügt.

Hostweite Netzwerke erstellen

Sie können in vSphere Standardnetzwerke und verteilte Netzwerke erstellen. Standardnetzwerke stellen eine Methode der Kommunikation zwischen den virtuellen Maschinen auf einem eigenständigen Host dar und bestehen aus Standard-Switches und Portgruppen. Verteilte Netzwerke fassen die Netzwerkfunktionen mehrerer Hosts zusammen und ermöglichen es virtuellen Maschinen, eine konsistente Netzwerkkonfiguration beizubehalten, wenn sie über Hosts hinweg migriert werden. Verteilte Netzwerke bestehen aus vSphere Distributed Switches, Uplink-Portgruppen und Portgruppen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Standard-Switches verfügen.
- Stellen Sie sicher, dass in der Bestandsliste ein Host vorhanden ist.

Vorgehensweise

- 1 Wählen Sie einen Host aus der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Abschnitt „Hardware“ auf **Netzwerk**.
- 4 Klicken Sie auf **vSphere Standard Switch**.
- 5 Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.
- 6 Wählen Sie einen Verbindungstyp aus und klicken Sie auf **Weiter**.
- 7 Wählen Sie einen vorhandenen virtuellen Switch oder erstellen Sie einen, und klicken Sie auf **Weiter**.
- 8 Geben Sie eine Bezeichnung für die Portgruppe auf dem Switch ein.
- 9 Wählen Sie eine VLAN-ID aus und klicken Sie auf **Weiter**.
- 10 Überprüfen Sie die gewählten Einstellungen, und klicken Sie auf **Beenden**.

Wenn Sie einen vorhandenen Standard-Switch verwenden, wird ihm eine neue Portgruppe hinzugefügt. Wenn Sie einen Standard-Switch erstellen, wird er mit einer Portgruppe hinzugefügt.

Datencenterweite Netzwerke erstellen

Sie können in vSphere Standardnetzwerke und verteilte Netzwerke erstellen. Standardnetzwerke stellen eine Methode der Kommunikation zwischen den virtuellen Maschinen auf einem eigenständigen Host dar und bestehen aus Standard-Switches und Portgruppen. Verteilte Netzwerke fassen die Netzwerkfunktionen mehrerer Hosts zusammen und ermöglichen es virtuellen Maschinen, eine konsistente Netzwerkkonfiguration beizubehalten, wenn sie über Hosts hinweg migriert werden. Verteilte Netzwerke bestehen aus vSphere Distributed Switches, Uplink-Portgruppen und Portgruppen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen eines Distributed Switches verfügen.
- Stellen Sie sicher, dass in der Bestandsliste ein Host vorhanden ist.

Vorgehensweise

- 1 Wählen Sie die Ansicht **Home > Bestandsliste > Netzwerk** und wählen Sie ein Datencenter aus.
- 2 Klicken Sie mit der rechten Maustaste auf das Datencenter und wählen Sie **Neuer vSphere Distributed Switch** aus.
- 3 Wählen Sie die vSphere Distributed Switch-Version aus und klicken Sie auf **Weiter**.
- 4 Geben Sie im Abschnitt „Allgemeines“ einen Namen für den Switch ein.
- 5 Legen Sie die maximale Anzahl der Uplink-Ports (physische Adapter pro Host) fest und klicken Sie auf **Weiter**.
- 6 Wählen Sie **Jetzt hinzufügen** aus, um dem Switch Hosts und ihre physischen Adapter hinzuzufügen.
Wählen Sie **Später hinzufügen** aus, um dem Switch Hosts und ihre physischen Adapter hinzuzufügen, nachdem der vSphere Distributed Switch erstellt wurde.
- 7 Wählen Sie die hinzuzufügenden Hosts im Abschnitt **Host/Physische Adapter** aus und klicken Sie auf **Weiter**.
- 8 Wählen Sie **Standard-Portgruppe automatisch erstellen** zum automatischen Erstellen einer Portgruppe aus und klicken Sie auf **Beenden**.

Ein vSphere Distributed Switch zusammen mit dessen zugewiesenen Uplink-Ports und Portgruppen wird zur Bestandsliste hinzugefügt.

Weiter

- Fügen Sie Hosts zum Switch hinzu.
- Fügen Sie Portgruppen zum Switch hinzu.
- Bearbeiten Sie die Switch-Eigenschaften.

Bearbeiten der allgemeinen Einstellungen für den vSphere Distributed Switch

Sie können die allgemeinen Einstellungen eines vSphere Distributed Switches bearbeiten, z. B. den Namen des Distributed Switches oder die Anzahl der Uplink-Ports auf dem Distributed Switch.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Allgemein**, um die Einstellungen für den vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
Name	Geben Sie den Namen für den Distributed Switch ein.
Anzahl der Uplink-Ports	Wählen Sie die Anzahl der Uplink-Ports für den Distributed Switch aus.
Notizen	Geben Sie beliebige Anmerkungen zum Distributed Switch ein.

- 4 (Optional) Bearbeiten Sie die Namen der Uplink-Ports.
 - a Klicken Sie auf **Uplink-Namen bearbeiten**.
 - b Geben Sie die neuen Namen für einen oder mehrere Uplink-Ports ein.
 - c Klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**.

Bearbeiten der erweiterten Einstellungen des vSphere Distributed Switch

Sie können erweiterte Einstellungen für den vSphere Distributed Switch ändern, beispielsweise das Cisco Discovery-Protokoll oder den maximalen MTU-Wert.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Erweitert**, um die folgenden Einstellungen des vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
Maximalwert für MTU	Maximalwert für MTU für den vSphere Distributed Switch.
Discovery-Protokollstatus	<p>Wählen Sie den Status für das Discovery-Protokoll auf dem vSphere Distributed Switch.</p> <ul style="list-style-type: none"> ■ Aktiviert. Aktiviertes Discovery-Protokoll für den vSphere Distributed Switch. <ol style="list-style-type: none"> 1 Wählen Sie Cisco Discovery-Protokoll oder Link-Layer Discovery Protocol (LLDP) im Dropdown-Menü Typ. 2 Legen Sie für Operation Überwachen, Werben oder Beide fest. ■ Deaktiviert.
Kontaktinformationen des Administrators	Geben Sie den Namen und Weitere Details für den Administrator des vSphere Distributed Switch ein.

- 4 Klicken Sie auf **OK**.

Hosts zu einem vSphere Distributed Switch hinzufügen

Sie können einem vSphere Distributed Switch nach dessen Erstellung auf der Distributed Switch-Ebene Hosts und physische Adapter hinzufügen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Host hinzufügen** aus.
- 3 Wählen Sie die hinzuzufügenden Hosts aus.
- 4 Wählen Sie unter den ausgewählten Hosts die hinzuzufügenden physischen Adapter aus und klicken Sie auf **Weiter**.

Sie können sowohl verwendete als auch nicht verwendete physische Adapter auswählen.

HINWEIS Wenn Sie einen physischen Adapter auf einen Distributed Switch verschieben, ohne zugewiesene virtuelle Adapter zu verschieben, können diese virtuellen Adapter die Netzwerkkonnektivität verlieren.

- 5 Wählen Sie für jeden virtuellen Adapter die **Zielportgruppe** im Dropdown-Menü aus, um den virtuellen Adapter auf den Distributed Switch zu migrieren, oder wählen Sie **Nicht migrieren** aus.
- 6 (Optional) Legen Sie die maximale Anzahl der Ports auf einem Host fest.
 - a Klicken Sie auf **Details anzeigen** für den Host.
 - b Wählen Sie im Dropdown-Menü die maximale Anzahl an Ports für den Host aus.
 - c Klicken Sie auf **OK**.
- 7 Klicken Sie auf **Weiter**.
- 8 (Optional) Migrieren Sie das Netzwerk virtueller Maschinen auf den Distributed Switch.
 - a Wählen Sie **Netzwerk virtueller Maschinen migrieren**.
 - b Wählen Sie für jede virtuelle Maschine die **Zielportgruppe** im Dropdown-Menü aus oder wählen Sie **Nicht migrieren** aus.
- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Wenn Sie Änderungen vornehmen müssen, klicken Sie auf **Zurück**, um zu dem gewünschten Bildschirm zu gelangen.
- 11 Überprüfen Sie die Einstellungen für den Distributed Switch und klicken Sie auf **Beenden**.

Hinzufügen einer verteilten Portgruppe

Fügen Sie eine verteilte Portgruppe zu einem vSphere Distributed Switch hinzu, um ein Distributed Switch-Netzwerk für Ihre virtuellen Maschinen zu erstellen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Neue Portgruppe** aus.
- 3 Geben Sie einen **Namen** und die **Anzahl der Ports** für Ihre neue verteilte Portgruppe ein.
- 4 Wählen Sie einen VLAN-Typ.

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

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

Bearbeiten der allgemeinen Einstellungen von verteilten Portgruppen

Sie können die Einstellungen für verteilte Portgruppen bearbeiten, beispielsweise den Namen der verteilten Portgruppe und den Portgruppentyp.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Allgemein** aus, um die folgenden Einstellungen für verteilte Portgruppen zu bearbeiten.

Option	Aktion
Name	Geben Sie den Namen für die verteilte Portgruppe ein.
Beschreibung	Geben Sie eine kurze Beschreibung der verteilten Portgruppe ein.

Option	Aktion
Anzahl der Ports	Geben Sie die Anzahl der Ports in der verteilten Portgruppe ein.
Port-Bindung	<p>Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind.</p> <ul style="list-style-type: none"> ■ Wählen Sie Statische Bindung aus, um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird. Diese Option ist nicht verfügbar, wenn der vSphere Client direkt mit ESXi verbunden ist. ■ Wählen Sie Dynamische Bindung aus, wenn einer virtuellen Maschine beim ersten Einschalten, nachdem sie mit der verteilten Portgruppe verbunden wurde, ein Port zugewiesen werden soll. Die dynamische Bindung läuft in ESXi 5.x aus. ■ Wählen Sie Flüchtig, um keine Port-Bindung einzugehen. Diese Option ist nicht verfügbar, wenn der vSphere Client direkt mit ESXi verbunden ist.

- 4 Klicken Sie auf **OK**.

Bearbeiten der erweiterten Einstellungen von verteilten Portgruppen

Sie können die Einstellungen für erweiterte verteilte Portgruppen bearbeiten, beispielsweise die Außerkraftsetzungseinstellungen und das Zurücksetzen bei Verbindungstrennung.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Erweitert**, um die Eigenschaften der verteilten Portgruppe zu bearbeiten.

Option	Beschreibung
Außerkraftsetzung von Portrichtlinien zulassen	Wählen Sie diese Option aus, um zuzulassen, dass die Richtlinien einer verteilten Portgruppe für einzelne Ports außer Kraft gesetzt werden. Klicken Sie auf Außerkraftsetzungseinstellungen bearbeiten , um auszuwählen, welche Richtlinien auf der Portebene außer Kraft gesetzt werden können.
Außerkraftsetzungseinstellungen bearbeiten	Wählen Sie aus, welche Richtlinien auf Portebene außer Kraft gesetzt werden können.
Zurücksetzen bei Verbindungstrennung konfigurieren	Wenn ein verteilter Port von einer virtuellen Maschine getrennt wird, wird seine Konfiguration auf die Einstellung der verteilten Portgruppe zurückgesetzt. Alle portspezifischen Außerkraftsetzungen werden verworfen.

- 4 Klicken Sie auf **OK**.

Verwalten von Lizenzschlüsseln im vSphere Client

4

Mit dem vSphere Client können Sie Lizenzschlüssel direkt auf einzelnen ESXi-Hosts oder zentral in der Lizenzbestandsliste eines vCenter Server-Systems verwalten.

Dieses Kapitel behandelt die folgenden Themen:

- „Lizenzierungseinschränkungen im vSphere Client“, auf Seite 49
- „Verwalten von Lizenzschlüsseln auf ESXi-Hosts“, auf Seite 49
- „Verwalten von Lizenzschlüsseln auf vCenter Server“, auf Seite 51

Lizenzierungseinschränkungen im vSphere Client

Die Lizenzierungsaufgaben, die Sie bei einer direkten Verbindung mit einem ESXi-Host oder einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden Lizenzierungsfunktionen sind im vSphere-Client nicht verfügbar:

- Lizenzberichterstellung

Über den vSphere Web Client stehen Ihnen hingegen alle Lizenzierungsfunktionen Ihrer vSphere 6.0-Umgebung zur Verfügung.

Verwalten von Lizenzschlüsseln auf ESXi -Hosts

Wenn Sie den vSphere-Client direkt mit einem ESXi-Host verbinden, können Sie Lizenzschlüssel anzeigen und zuweisen, die auf dem Host lizenzierten Funktionen anzeigen sowie den Testmodus für den Host aktivieren.

Zugreifen auf den ESXi-Lizenzschlüssel und lizenzierte Funktionen im vSphere Client

Wenn es sich bei dem Host nicht um einen lokalen Host handelt und Sie keinen Zugriff auf die direkte Konsole haben, verwenden Sie den vSphere-Client, um auf den ESXi-Lizenzschlüssel zuzugreifen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Abschnitt „Software“ auf **Lizenzierte Funktionen**.

Der Lizenzschlüssel und eine Liste der Funktionen, die Sie auf dem Host konfigurieren können, werden angezeigt. Der Lizenzschlüssel weist das Format XXXXX-XXXXX-XXXXX-XXXXX-XXXXX auf.

Zuweisen eines Lizenzschlüssels zu einem ESXi -Host

Mit dem vSphere Client können Sie einem ESXi-Host einen vorhandenen oder neuen Lizenzschlüssel zuweisen.

Wenn der vSphere Client direkt mit dem Host verbunden ist, können Sie den Lizenzschlüssel über die Registerkarte **Konfiguration** des Hosts ändern, indem Sie auf **Lizenzierte Funktionen > Bearbeiten** klicken.

Voraussetzungen

Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den Host in der Bestandsliste aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie im Bereich „Software“ auf **Lizenzierte Funktionen** und dann auf **Bearbeiten**.
- 3 Weisen Sie einen Lizenzschlüssel zu.
 - Wählen Sie **Diesem Host einen vorhandenen Lizenzschlüssel zuweisen** aus und wählen Sie aus der **Produkt**-Liste einen Lizenzschlüssel aus.
 - Wählen Sie **Diesem Host einen neuen Lizenzschlüssel zuweisen**, klicken Sie auf **Schlüssel eingeben** und geben Sie einen Lizenzschlüssel im Format XXXXX-XXXXX-XXXXX-XXXXX-XXXXX ein.
- 4 Klicken Sie auf **OK**.

Konvertieren eines ESXi -Hosts in den Testmodus

Wenn Sie einem ESXi-Host einen Lizenzschlüssel zugewiesen haben, können Sie in den Testmodus wechseln, um alle für diesen Host verfügbaren Funktionen zu testen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Abschnitt „Software“ auf **Lizenzierte Funktionen**.
- 4 Klicken Sie auf **Bearbeiten** neben „ESX Server-Lizenztyp“.
- 5 Klicken Sie auf **Testmodus**.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Der Host befindet sich im Testmodus und Sie können sämtliche Funktionen für ESXi testen. Wenn Sie den Host bereits im Testmodus verwendet haben, wird die in der Testperiode verbleibende Zeit um die bereits verwendete Zeit verkürzt. Angenommen, Sie haben den Host im Testmodus bereits seit 20 Tagen verwendet und dann dem Host einen vSphere Standard-Lizenzschlüssel zugewiesen. Wenn Sie den Host in den Testmodus zurücksetzen, können Sie alle für den Host verfügbaren Funktionen für die verbleibenden 40 Tage im Testmodus nutzen. Auf der jeweiligen Hostseite im vSphere-Client können Sie die verbleibenden Tage der Testperiode des Hosts anzeigen.

HINWEIS Nach Ablauf der Testperiode des Hosts erhalten Sie eine Warnmeldung und der Host kann mit keinem vCenter Server-System eine Verbindung herstellen. Alle eingeschalteten virtuelle Maschinen werden weiterhin ausgeführt, es können jedoch keine neuen eingeschaltet werden. Sie können die aktuelle Konfiguration der bereits verwendeten Funktionen ändern. Funktionen, die im Testmodus nicht genutzt wurden, können zu diesem Zeitpunkt jedoch nicht verwendet werden.

Der Lizenzschlüssel eines ESXi -Hosts wird ersetzt

Der Lizenzschlüssel, den Sie über eine direkte Verbindung mit dem vSphere-Client einem ESXi-Host zugewiesen haben, ändert sich.

Problem

Sie verwenden den vSphere-Client, um eine direkte Verbindung zum ESXi-Host herzustellen. Sie verwenden die Option **Konfiguration > Lizenzierte Funktionen > Bearbeiten**, um dem Host einen Lizenzschlüssel zuzuweisen. Anschließend ersetzt ein anderer Lizenzschlüssel den Lizenzschlüssel, den Sie dem Host zugewiesen haben.

Ursache

Wenn ein vCenter Server-System einen ESXi-Host verwaltet, werden die Änderungen an der Hostlizenz, die über eine direkte Verbindung zum Host vorgenommen wurden, nicht beibehalten. Dies ist darauf zurückzuführen, dass der über vCenter Server zugewiesene Lizenzschlüssel die Änderungen überschreibt.

Bei Verwendung der Option **Konfiguration > Lizenzierte Funktionen > Bearbeiten** wird die Hostlizenzkonfiguration von allen in vCenter Server durchgeführten Lizenzzuweisungen überschrieben.

Lösung

Wenn Sie vCenter Server zum Verwalten des Hosts nutzen, verwenden Sie entweder die Oberfläche **Home > Verwaltung > Lizenzierung** oder den Vorgang „Host hinzufügen“, um die Hostlizenzierung zu konfigurieren.

Verwalten von Lizenzschlüsseln auf vCenter Server

Die vSphere-Lizenzverwaltung erfolgt zentral. Sie können den vSphere Client verwenden, um alle in der Lizenzbestandsliste eines vCenter Server-Systems verfügbaren Lizenzen zu verwalten.

Zugriff auf Lizenzschlüssel und -funktionen im vCenter Server

Die in der Lizenzbestandsliste von vCenter Server verfügbaren Lizenzschlüssel und -funktionen stehen auf der Lizenzierungsseite des vSphere Client bereit.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.
- Stellen Sie sicher, dass der vSphere-Client mit dem vCenter Server-System verbunden ist.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die Option **Ansicht > Verwaltung > Lizenzierung**.

Sie können die in der Bestandsliste von vCenter Server verfügbaren Lizenzschlüssel über die Registerkarte **Management** anzeigen und verwalten.

- 2 (Optional) Klicken Sie auf **Aktualisieren**.
- 3 Wählen Sie auf der Registerkarte **Management** eine Sortieroption für die Lizenzinformationen aus.

Option	Beschreibung
Produkt	Listet die verfügbaren Lizenzschlüssel nach Produkt sortiert auf.
Lizenzschlüssel	Listet die verfügbaren Lizenzschlüssel nach Lizenzschlüssel sortiert auf.
Asset	Listet die verfügbaren Lizenzschlüssel nach dem Asset sortiert auf, dem sie zugewiesen sind: „Host“, „vCenter Server“ oder „Lösung“.

Die Registerkarte **Management** zeigt die verfügbaren Lizenzschlüssel nach Produkt, Lizenzschlüssel oder Asset sortiert an. Sie können mit der rechten Maustaste auf eines der aufgeführten Elemente klicken, um Lizenzschlüssel hinzuzufügen, zuzuweisen oder zu entfernen und um Lizenzinformationen in die Zwischenablage zu kopieren.

Weiter

Wenn Sie über einen Lizenzschlüssel verfügen, dem keine Kapazität zugewiesen ist, können Sie:

- Den Lizenzschlüssel Assets zuweisen, für die eine Lizenzierung erforderlich ist.
- Den Lizenzschlüssel entfernen, falls er nicht mehr benötigt wird.

Sie sollten nicht zugewiesene Lizenzschlüssel nicht in der vCenter Server-Lizenzbestandsliste aufbewahren.

Hinzufügen von Lizenzschlüsseln zur Bestandsliste der vCenter Server -Lizenz

Nach Erhalt der Lizenzschlüssel können Sie diese zur vCenter Server-Lizenzbestandsliste hinzufügen. Sie können mehrere Lizenzschlüssel gleichzeitig hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.
- Stellen Sie sicher, dass der vSphere-Client mit dem vCenter Server-System verbunden ist.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **Home > Verwaltung > Lizenzierung**.
- 2 Klicken Sie auf **vSphere-Lizenzen verwalten**.
- 3 Geben Sie im Textbereich **Lizenzschlüssel hinzufügen** einen Lizenzschlüssel pro Zeile an.
Sie können eine Liste mit Schlüsseln in einem Vorgang angeben.
- 4 (Optional) Geben Sie eine kurze Bezeichnung für die Schlüssel ein.
- 5 Klicken Sie auf **Lizenzschlüssel hinzufügen**.
Wenn Sie ungültige Lizenzschlüssel angeben, erhalten Sie eine Fehlermeldung, die die ungültigen Schlüssel auflistet. Sie können die ungültigen Schlüssel entweder löschen oder nach ihrer Korrektur hinzufügen.
- 6 Wenn Sie zu diesem Zeitpunkt noch keine Zuweisungen von Lizenzschlüsseln zu Assets vornehmen möchten, klicken Sie in den übrigen Bildschirmen des Assistenten auf **Weiter** und wählen Sie **Beenden**, um Ihre Änderungen zu speichern.

Die Lizenzschlüssel werden in die vCenter Server-Lizenzbestandsliste aufgenommen.

Weiter

Weisen Sie die Lizenzschlüssel den Assets zu, für die eine Lizenzierung erforderlich ist. Sie sollten nicht zugewiesene Lizenzschlüssel nicht in der vCenter Server-Lizenzbestandsliste aufbewahren.

Zuweisen eines Lizenzschlüssels zu Assets

Sie können einzelnen oder mehreren Assets einzeln oder gruppenweise Lizenzschlüssel zuweisen.

HINWEIS Falls ein ESXi-Host die Verbindung zu einem vCenter Server sofort nach der Zuweisung eines Lizenzschlüssels trennt, wird die Lizenzzuweisung nicht abgeschlossen, der Host wird aber als lizenziert angezeigt. Der Host wird dann lizenziert, wenn eine neue Verbindung zum vCenter Server hergestellt wird.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.
- Stellen Sie sicher, dass der vSphere-Client mit dem vCenter Server-System verbunden ist.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **Home > Verwaltung > Lizenzierung**.
- 2 Klicken Sie auf **vSphere-Lizenzen verwalten**.
- 3 Klicken Sie auf **Weiter**, um zur Seite „Lizenz zuweisen“ zu wechseln.
- 4 Klicken Sie auf die Registerkarte **ESX**, **vCenter Server** oder **Lösungen**, um die verfügbaren Assets anzuzeigen.
- 5 Wählen Sie die anzuzeigenden Assets aus.
- 6 Wählen Sie im Fenster Asset ein oder mehrere zu lizenzierende Assets aus.
Um mehrere Assets auszuwählen, verwenden Sie STRG-Klicken oder UMSCHALT-Klicken.
- 7 Wählen Sie im Fenster Produkt einen geeigneten Lizenzschlüssel aus und klicken Sie auf **Weiter**.
Falls der Lizenzschlüssel, den Sie zuweisen, strengen Bedingungen unterworfen ist, muss die Lizenzkapazität größer oder gleich der erforderlichen Lizenznutzung für das Asset sein. Anderenfalls können Sie den Lizenzschlüssel nicht zuweisen. Prüfen Sie das EULA der Lizenz, um zu ermitteln, ob die Lizenz strengen Bedingungen unterworfen ist.
- 8 (Optional) Wenn Sie keine Lizenzschlüssel entfernen möchten, klicken Sie auf **Weiter**, um die Seite „Lizenzschlüssel entfernen“ zu überspringen, und klicken Sie dann auf **Beenden**, um Ihre Änderungen zu speichern.

Hinzufügen eines Lizenzschlüssels und Zuweisen des Lizenzschlüssels zu einem Asset

Nachdem Sie einen Lizenzschlüssel erhalten haben, können Sie ihn zur vCenter Server-Lizenzbestandsliste hinzufügen und ihn Assets zuweisen.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.
- Stellen Sie sicher, dass der vSphere-Client mit dem vCenter Server-System verbunden ist.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **Home > Verwaltung > Lizenzierung**.
- 2 Wählen Sie auf der Registerkarte **Management** als primäres Element zum Sortieren der Lizenzhinweise **Asset**.
- 3 Klicken Sie mit der rechten Maustaste auf ein Asset und wählen Sie **Lizenzschlüssel ändern**.
- 4 Wählen Sie **Einen neuen Lizenzschlüssel zuweisen** und klicken Sie auf **Schlüssel eingeben**.
- 5 Geben Sie den Lizenzschlüssel und eine optionale Bezeichnung für den Schlüssel ein und klicken Sie auf **OK**.
- 6 Klicken Sie auf **OK**.

Der Lizenzschlüssel wird zur vCenter Server-Lizenzbestandsliste hinzugefügt und dem entsprechenden Asset zugewiesen.

Weiter

Sofern der Lizenzschlüssel über die benötigte Kapazität verfügt, weisen Sie den Lizenzschlüssel anderen Assets desselben Typs zu.

Exportieren von Lizenzinformationen

Sie können Lizenzinformationen in eine Datei exportieren, die Sie in einer Anwendung eines Drittanbieters öffnen können.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Berechtigung **Global.Lizenzen** besitzen.
- Stellen Sie sicher, dass der vSphere-Client mit dem vCenter Server-System verbunden ist.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client **Home > Verwaltung > Lizenzierung**.
- 2 Wählen Sie auf der Registerkarte **Management** die zu exportierende Ansicht aus.
 - **Produkt**
 - **Lizenzschlüssel**
 - **Asset**
- 3 Klicken Sie auf **Exportieren**.
- 4 Wählen Sie im Dialogfeld „Speichern unter“ einen Ordner, einen Dateinamen und ein Format für die exportieren Lizenzdaten aus und klicken Sie auf **Speichern**.

Verwalten von Aufgaben

Aufgaben stellen Systemaktivitäten dar, die nicht unmittelbar abgeschlossen werden, z. B. das Migrieren einer virtuellen Maschine. Sie werden durch Aktivitäten auf hoher Ebene initiiert, die Sie mit dem vSphere Client in Echtzeit ausführen, sowie durch Aktivitäten, die Sie für die Ausführung zu einem späteren Zeitpunkt oder für die wiederholte Ausführung planen.

Beispielsweise handelt es sich beim Ausschalten einer virtuellen Maschine um eine Aufgabe. Sie können diese Aufgabe jeden Abend manuell ausführen oder eine geplante Aufgabe einrichten, die die virtuelle Maschine jeden Abend für Sie ausschaltet.

HINWEIS Welche Funktionalität im vSphere Client verfügbar ist, hängt davon ab, ob der vSphere Client mit einem vCenter Server oder einem ESXi-Host verbunden ist. Soweit nicht anders angegeben, bezieht sich der Prozess, die Aufgabe und die Beschreibung auf beide Arten von vSphere Clientverbindungen. Wenn der vSphere Client mit einem ESXi-Host verbunden ist, ist die Option **Aufgaben** nicht verfügbar. Allerdings können Sie kürzlich bearbeitete Aufgaben in der **Statusleiste** des vSphere Clients anzeigen.

Dieses Kapitel behandelt die folgenden Themen:

- „Anzeigen von Aufgaben“, auf Seite 55
- „Abbrechen einer Aufgabe“, auf Seite 57
- „Planen von Aufgaben“, auf Seite 58
- „Richtlinienregeln für Aufgaben“, auf Seite 62

Anzeigen von Aufgaben

Sie können Aufgaben anzeigen, die mit einem einzelnen Objekt oder mit allen Objekten in der vSphere Client-Bestandsliste verknüpft sind. Auf der Registerkarte **Aufgaben & Ereignisse** werden alle abgeschlossenen Aufgaben und Aufgaben angezeigt, die derzeit ausgeführt werden.

Die Aufgabenliste eines Objekts enthält standardmäßig auch die Aufgaben für die untergeordneten Objekte. Sie können die Liste filtern, indem Sie auf untergeordneten Objekten ausgeführte Aufgaben entfernen und indem Sie mithilfe von Schlüsselwörtern nach Aufgaben suchen.

Anzeigen aller Aufgaben

Sie können die abgeschlossenen und aktiven Aufgaben auf der Registerkarte vSphere Client **Aufgaben & Ereignisse** anzeigen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.

Vorgehensweise

- 1 Wählen Sie im vSphere Client das Objekt in der Bestandsliste aus.
- 2 Zeigen Sie die Aufgaben für ein einzelnes Objekt oder für das gesamte vCenter Server-System an.
 - Um die Aufgaben für ein einzelnes Objekt anzuzeigen, wählen Sie das Objekt aus.
 - Wählen Sie zum Anzeigen der Aufgaben in vCenter Server den Root-Ordner aus.
- 3 Klicken Sie auf die Registerkarte **Aufgaben & Ereignisse**.
Die Aufgabenliste enthält die auf dem Objekt und seinen untergeordneten Elementen ausgeführten Aufgaben.
- 4 (Optional) Wählen Sie eine Aufgabe in der Liste aus, um Details zu der Aufgabe anzuzeigen.
Das Fenster **Aufgabendetails** zeigt Details wie den Aufgabenstatus, evtl. Fehlermeldungen im Fehler-Stack und alle verwandten Ereignisse an.

Anzeigen kürzlich bearbeiteter Aufgaben

Kürzlich bearbeitete Aufgaben für einen ESXi-Host können im vSphere Client im Bereich **Kürzlich bearbeitete Aufgaben** angezeigt werden.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Wählen Sie bei Bedarf **Ansicht > Statusleiste**, um die Statusleiste im unteren Bereich des vSphere Client anzuzeigen.
Die Aufgabenliste wird im Bereich **Kürzlich bearbeitete Aufgaben** der **Statusleiste** angezeigt.

Anzeigen geplanter Aufgaben

Sie können geplante Aufgaben im Bereich vSphere Client **Geplante Aufgaben** anzeigen. Die Liste der geplanten Aufgaben enthält Aufgaben, die zur Ausführung geplant sind, sowie bereits ausgeführte Aufgaben.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.

Vorgehensweise

- ◆ Wählen Sie im vSphere Client **Home > Management > Geplante Aufgaben** aus.

Filtern von Aufgaben für einen Host oder ein Datencenter

Wenn Sie die Aufgabenliste filtern, werden auf untergeordneten Objekten ausgeführte Aufgaben entfernt.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den Host oder das Datencenter aus und klicken Sie auf die Registerkarte **Aufgaben & Ereignisse**.
- 2 Klicken Sie unter **Ansicht** auf **Aufgaben**, um die Aufgabenliste anzuzeigen.
- 3 Wenn die Liste **Alle Einträge anzeigen** und das Suchfeld nicht unter den Schaltflächen **Aufgaben** und **Ereignisse** angezeigt werden, wählen Sie **Ansicht > Filtern**.

- 4 Klicken Sie auf **Alle Einträge anzeigen** und wählen Sie abhängig vom ausgewählten Objekt **Hosteinträge anzeigen** oder **Datencentereinträge anzeigen**.

Verwenden von Schlüsselwörtern zum Filtern der Aufgabenliste

Sie können die Aufgabenliste basierend auf Aufgabenattributen filtern, wie z. B. dem Aufgabennamen, dem Ziel, dem Status, dem Initiator, dem Änderungsverlauf und der Uhrzeit. Beim Filtern werden Elemente eingeschlossen, nicht ausgeschlossen. Wenn das Schlüsselwort in einer der ausgewählten Spalten gefunden wird, wird die Aufgabe in die gefilterte Liste aufgenommen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.

Vorgehensweise

- 1 Wählen Sie im vSphere Client das Objekt in der Bestandsliste aus.
- 2 Wenn das Suchfeld **Name, Ziel oder Status** enthält nicht über dem Fenster „Aktuelle Aufgaben“ angezeigt wird, wählen Sie **Ansicht > Filtern** aus.
- 3 Klicken Sie auf den Suchfeldpfeil und wählen Sie die Attribute aus, die in die Suche aufgenommen werden sollen.
- 4 Geben Sie im Feld ein Schlüsselwort ein und drücken Sie die Eingabetaste.

Abbrechen einer Aufgabe

Wenn eine Aufgabe abgebrochen wird, wird ihre aktuelle Ausführung gestoppt. Das Abbrechen einer geplanten Aufgabe wirkt sich nicht auf ihre nachfolgenden Ausführungen aus. Wenn Sie eine geplante Aufgabe abbrechen möchten, die nicht ausgeführt wurde, planen Sie sie neu.

HINWEIS Sie können eine Teilmenge von Aufgaben nur mithilfe des vSphere Clients abbrechen.

Erforderliche Berechtigungen:

- Manuelle Aufgaben: **Aufgaben.Aufgabe aktualisieren**
- Geplante Aufgaben: **Geplante Aufgabe.Aufgabe entfernen**
- Entsprechende Berechtigungen auf dem Host, auf dem die Aufgabe ausgeführt wird

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server.

Vorgehensweise

- 1 Suchen Sie die Aufgabe im Fenster **Kürzlich bearbeitete Aufgaben** der **Statusleiste**.

Standardmäßig wird die **Statusleiste** im unteren Bereich des vSphere Clients angezeigt. Wenn sie nicht angezeigt wird, wählen Sie **Ansicht > Statusleiste**.

- 2 Klicken Sie mit der rechten Maustaste auf die entsprechende Aufgabe und wählen Sie **Abbrechen**.

Wenn die Option zum Abbrechen nicht verfügbar ist, kann die ausgewählte Aufgabe nicht abgebrochen werden.

Das vCenter Server-System bzw. der ESXi-Host stoppt den Aufgabenfortschritt und versetzt das Objekt wieder in seinen vorherigen Zustand. Der vSphere Client zeigt die Aufgabe mit dem Status **Abgebrochen** an.

Planen von Aufgaben

Sie können Aufgaben zur einmaligen oder regelmäßigen Ausführung planen.

In der folgenden Tabelle werden die Aufgaben aufgeführt, die geplant werden können.

Tabelle 5-1. Geplante Aufgaben

Geplante Aufgabe	Beschreibung
Hinzufügen eines Hosts	Fügt den Host zum angegebenen Datencenter oder Cluster hinzu.
Ändern des Betriebszustands einer virtuellen Maschine	Schaltet die virtuelle Maschine ein oder aus, hält sie an oder setzt ihren Status zurück.
Ändern der Cluster-Stromversorgungseinstellungen	Aktiviert oder deaktiviert DPM für Hosts in einem Cluster.
Ressourceneinstellungen des Ressourcenpools oder einer virtuellen Maschine ändern	Ändert die folgenden Ressourceneinstellungen: <ul style="list-style-type: none"> ■ CPU – Anteile, Reservierung, Grenzwert. ■ Arbeitsspeicher – Anteile, Reservierung, Grenzwert.
Übereinstimmung mit einem Profil prüfen	Prüft, dass die Konfiguration eines Hosts mit der in einem Hostprofil angegebenen Konfiguration übereinstimmt.
Klonen einer virtuellen Maschine	Erstellt einen Klon der virtuellen Maschine und platziert ihn auf dem angegebenen Host oder Cluster.
Erstellen einer virtuellen Maschine	Erstellt auf dem angegebenen Host eine neue virtuelle Maschine.
Bereitstellen einer virtuellen Maschine	Erstellt eine neue virtuelle Maschine von einer Vorlage aus auf dem angegebenen Host oder Cluster.
Migrieren einer virtuellen Maschine	Migriert mithilfe der Migration oder der Migration mit vMotion eine virtuelle Maschine auf den angegebenen Host oder Datenspeicher.
Erstellen eines Snapshots einer virtuellen Maschine	Erfasst den Gesamtstatus der virtuellen Maschine zum Zeitpunkt der Erstellung des Snapshots.
Auf Updates prüfen	Durchsucht Vorlagen, virtuelle Maschinen und Hosts nach verfügbaren Updates. Diese Aufgabe ist nur verfügbar, wenn vSphere Update Manager installiert ist.
Standardisieren	Installiert fehlende Patches von den Baselines, die für die Standardisierung ausgewählt wurden, auf den Hosts, die bei der Suche gefunden wurden, und wendet die neu konfigurierten Einstellungen an. Diese Aufgabe ist nur verfügbar, wenn vSphere Update Manager installiert ist.

Sie können geplante Aufgaben mithilfe des Assistenten für geplante Aufgaben erstellen. Für einige geplante Aufgaben öffnet dieser Assistent den speziell für diese Aufgabe vorgesehenen Assistenten. Wenn Sie z. B. eine geplante Aufgabe erstellen, die eine virtuelle Maschine migriert, öffnet der Assistent für geplante Aufgaben den Assistenten für das Migrieren einer virtuellen Maschine, mit dessen Hilfe Sie die Details für die Migration festlegen können.

Das Planen einer Aufgabe zur Ausführung auf mehreren Objekten ist nicht möglich. Beispielsweise können Sie keine geplante Aufgabe auf einem Host erstellen, die alle virtuellen Maschinen auf diesem Host einschaltet. Sie müssen für jede virtuelle Maschine eine separate geplante Aufgabe erstellen.

Nachdem eine geplante Aufgabe ausgeführt wurde, können Sie sie für eine erneute Ausführung zu einem anderen Zeitpunkt planen.

Erstellen einer geplanten Aufgabe

Verwenden Sie zum Planen einer Aufgabe den Assistenten für geplante Aufgabe.

Erforderliche Berechtigung: **Aufgabe planen.Aufgaben erstellen**

Sie können mithilfe des vSphere Clients eine begrenzte Anzahl an Aufgaben planen. Falls die zu planende Aufgabe nicht verfügbar ist, verwenden Sie die vSphere-API. Weitere Informationen hierzu finden Sie im *Programmierhandbuch* zum vSphere-SDK.



VORSICHT Planen Sie keine parallel ausgeführten Aufgaben für ein Objekt. Dies kann zu unerwarteten Ergebnissen führen.

Voraussetzungen

Der vSphere Client muss zum Planen von Aufgaben mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Klicken Sie in der Navigationsleiste auf **Home > Management > Geplante Aufgaben**.
Die aktuelle Liste der geplanten Aufgaben wird angezeigt.
- 2 Klicken Sie in der Symbolleiste auf **Neu**.
- 3 Wählen Sie im Dialogfeld „Zu planende Aufgabe auswählen“ eine Aufgabe aus und klicken Sie auf **OK**, um den Assistenten für diese Aufgabe zu öffnen.

HINWEIS Für einige geplante Aufgaben öffnet der Assistent den speziell für diese Aufgabe vorgesehenen Assistenten. Beispielsweise öffnet der Assistent für geplante Aufgabe zum Migrieren einer virtuellen Maschine den Assistenten für das Migrieren einer virtuellen Maschine, mit dessen Hilfe Sie die Details für die Migration festlegen können.

- 4 Führen Sie die Schritte des Assistenten für die Aufgabe aus.
- 5 Geben Sie im Abschnitt Aufgabe planen einen Namen und eine Beschreibung für die Aufgabe ein.
- 6 Wählen Sie eine **Häufigkeit** und geben Sie eine **Startzeit** an.

Mit einer geplanten Aufgabe können Sie nur veranlassen, dass die Aufgabe einmal innerhalb eines Tages ausgeführt wird. Wenn Sie eine Aufgabe mehrmals am Tag ausgeführt werden soll, müssen Sie zusätzliche geplante Aufgaben einrichten.

Tabelle 5-2. Optionen für die Ausführungshäufigkeit von geplanten Aufgaben

Häufigkeit	Aktion
Einmal	<ul style="list-style-type: none"> ■ Wenn Sie die geplante Aufgabe sofort ausführen möchten, wählen Sie Jetzt und klicken Sie auf Weiter. ■ Wenn Sie die geplante Aufgabe zu einem späteren Zeitpunkt ausführen möchten, wählen Sie Später und geben Sie eine Uhrzeit ein. Klicken Sie auf den Pfeil Datum, um den Kalender anzuzeigen, und klicken Sie auf ein Datum.
Nach dem Start	<ul style="list-style-type: none"> ■ Geben Sie unter Verzögerung den Zeitraum in Minuten an, um den die Aufgabe verzögert werden soll.
Stündlich	<ol style="list-style-type: none"> 1 Geben Sie unter Startzeit die Anzahl an Minuten nach der vollen Stunde für die Ausführung der Aufgabe ein. 2 Geben Sie unter Intervall die Anzahl an Stunden ein, nach der die Aufgabe ausgeführt werden soll. <p>Wenn eine Aufgabe z. B. eine halbe Stunde nach einer vollen Stunde in einem Intervall von 5 Stunden gestartet werden soll, geben Sie 30 und 5 ein.</p>

Tabelle 5-2. Optionen für die Ausführungshäufigkeit von geplanten Aufgaben (Fortsetzung)

Häufigkeit	Aktion
Täglich	<ul style="list-style-type: none"> ■ Geben Sie die Startzeit und das Intervall ein. <p>Wenn die Aufgabe z. B. alle vier Tage um 14:30 Uhr ausgeführt werden soll, geben Sie 14:30 und 4 ein.</p>
Wöchentlich	<ol style="list-style-type: none"> 1 Geben Sie das Intervall und die Startzeit ein. 2 Wählen Sie alle Tage aus, an denen die Aufgabe ausgeführt werden soll. <p>Wenn die Aufgabe z. B. jeden Dienstag und Donnerstag um 6:00 Uhr ausgeführt werden soll, geben Sie 1 und 6 ein und wählen Sie Dienstag und Donnerstag aus.</p>
Monatlich	<ol style="list-style-type: none"> 1 Geben Sie die Startzeit ein. 2 Legen Sie mithilfe einer der folgenden Methoden die Tage fest. <ul style="list-style-type: none"> ■ Geben Sie ein bestimmtes Datum des Monats ein. ■ Wählen Sie die Option Ersten, Zweiten, Dritten, Vierten oder Letzten und wählen Sie den Wochentag aus. <p>Mit der Option Letzten wird die Aufgabe in der letzten Woche des Monats ausgeführt, die den ausgewählten Wochentag enthält. Wenn Sie z. B. den letzten Montag des Monats auswählen und der letzte Tag des Monats ein Sonntag ist, wird die Aufgabe sechs Tage vor dem Monatsende ausgeführt.</p> 3 Geben Sie unter Intervall die Anzahl der zwischen den einzelnen Aufgabenausführungen liegenden Monate ein.

7 Klicken Sie auf **Weiter**.

8 Richten Sie E-Mail-Benachrichtigungen ein und klicken Sie auf **Weiter**.

9 Klicken Sie auf **Beenden**.

Das vCenter Server-System fügt die Aufgabe zu der Liste im Fenster **Geplante Aufgaben** hinzu.

Ändern oder Neuplanen einer Aufgabe

Nach dem Erstellen einer geplanten Aufgabe können Sie Zeitpunkt und Häufigkeit der Ausführung einer Aufgabe sowie bestimmte aufgabenspezifische Einstellungen ändern. Sie können Aufgaben vor oder nach ihrer Ausführung bearbeiten und neu planen.

Erforderliche Berechtigung: **Aufgabe planen**, **Aufgabe ändern**

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server-System.

Vorgehensweise

- 1 Klicken Sie im vSphere Client auf **Home > Management > Geplante Aufgaben**.
- 2 Wählen Sie die Aufgabe aus.
- 3 Klicken Sie in der Symbolleiste auf **Eigenschaften**.
- 4 Ändern Sie nach Bedarf die Aufgabenattribute.
- 5 Klicken Sie auf **Weiter**, um mit der nächsten Assistentenseite fortzufahren.
- 6 Klicken Sie auf **Beenden**.

Entfernen einer geplanten Aufgabe

Durch das Entfernen einer geplanten Aufgabe werden alle zukünftigen Ausführungen der Aufgabe entfernt. Der Verlauf für alle abgeschlossenen Ausführungen der Aufgabe verbleibt in der vCenter Server-Datenbank.

Voraussetzungen

Zum Entfernen geplanter Aufgaben muss der vSphere Client mit dem vCenter Server-System verbunden sein.

Erforderliche Berechtigung: **Geplante Aufgabe.Aufgabe entfernen**

Vorgehensweise

- 1 Klicken Sie im vSphere Client auf **Startseite > Verwaltung > Geplante Aufgaben**.
- 2 Wählen Sie die Aufgabe aus.
- 3 Wählen Sie **Bestandsliste > Geplante Aufgabe > Entfernen**.
- 4 Klicken Sie auf **OK**.

Die Aufgabe wird aus der Liste der geplanten Aufgaben entfernt.

Abbrechen geplanter Aufgaben

Beim Abbrechen einer Aufgabe wird die laufende Aufgabe beendet, unabhängig davon, ob es sich um eine Echtzeitaufgabe oder eine geplante Aufgabe handelt. Dieser Vorgang bricht nur die laufende Aufgabe ab. Wenn die abgebrochene Aufgabe eine geplante Aufgabe ist, werden nachfolgende Ausführungen nicht abgebrochen.

Aufgaben, die nicht ausgeführt werden, können gelöscht werden, wenn sie sich in der Warteschlange oder im geplanten Zustand befinden. Weil in solchen Fällen der Abbruchvorgang nicht verfügbar ist, entfernen Sie entweder die Aufgabe oder planen Sie sie zur Ausführung zu einem anderen Zeitpunkt. Das Entfernen einer geplanten Aufgabe bedeutet, dass Sie sie für eine zukünftige Ausführung neu erstellen müssen, was bei einer zeitlichen Neuplanung nicht erforderlich ist.

Sie können die folgenden Aufgaben abbrechen:

- Verbinden mit einem Host
- Klonen einer virtuellen Maschine
- Bereitstellen einer virtuellen Maschine
- Migrieren einer ausgeschalteten virtuellen Maschine. Diese Aufgabe kann nur dann abgebrochen werden, wenn die Quellfestplatten nicht gelöscht wurden.

Wenn in Ihrer vSphere-Umgebung virtuelle Dienste verwendet werden, können Sie zudem die folgenden geplanten Aufgaben abbrechen:

- Ändern des Betriebszustands einer virtuellen Maschine
- Erstellen eines Snapshots einer virtuellen Maschine

Richtlinienregeln für Aufgaben

Das vCenter Server-System und die ESXi-Hosts unterliegen bei der Verwaltung von Aufgaben bestimmten Regeln.

Das vCenter Server-System und ESXi-Hosts unterliegen beim Verarbeiten von Aufgaben folgenden Regeln:

- Der Benutzer, der die Aufgabe im vSphere Client ausführt, muss über die erforderlichen Berechtigungen für die relevanten Objekte verfügen. Nachdem eine geplante Aufgabe erstellt wird, wird sie auch dann ausgeführt, wenn der Benutzer nicht mehr über die Berechtigung zum Ausführen der Aufgabe verfügt.
- Wenn die für manuelle Aufgaben und geplante Aufgaben erforderlichen Vorgänge miteinander in Konflikt geraten, wird die zuerst fällige Aktivität zuerst gestartet.
- Wenn sich eine virtuelle Maschine oder ein Host nicht im richtigen Status zum Ausführen einer manuell initiierten oder geplanten Aktivität befindet, führt vCenter Server oder der ESXi-Host die Aufgabe nicht aus. Im Protokoll wird eine Meldung aufgezeichnet.
- Wenn ein Objekt aus vCenter Server oder vom ESXi-Host entfernt wird, werden alle zugeordneten Aufgaben ebenfalls entfernt.
- Der vSphere Client und das vCenter Server-System verwenden zum Ermitteln der Startzeit einer geplanten Aufgabe die UTC-Zeit. Dadurch wird sichergestellt, dass vSphere Clientbenutzer in unterschiedlichen Zeitzonen die geplante Aufgabe in der jeweiligen Ortszeit sehen.

Ereignisse werden zu Beginn und bei Abschluss einer Aufgabe im Ereignisprotokoll aufgezeichnet. Alle beim Ausführen einer Aufgabe auftretenden Fehler werden ebenfalls im Ereignisprotokoll aufgezeichnet.



VORSICHT Planen Sie keine parallel ausgeführten Aufgaben für ein Objekt. Dies kann zu unerwarteten Ergebnissen führen.

Absichern der Verwaltungsschnittstelle

6

Sichern Sie die Verwaltungsschnittstelle eines ESXi-Hosts und des VM-Gastbetriebssystems ab, indem Sie die Dienste und Verwaltungs-Agents einschränken, die direkt mit dem Host oder der virtuellen Maschine interagieren dürfen.

Dieses Kapitel behandelt die folgenden Themen:

- „Sichern der ESXi-Hosts“, auf Seite 63
- „Sichern von virtuellen Maschinen“, auf Seite 67

Sichern der ESXi -Hosts

Die ESXi-Hypervisorarchitektur verfügt über viele integrierte Sicherheitsfunktionen wie CPU-Isolierung, Arbeitsspeicherisolierung und Geräteisolierung. Sie können weitere Funktionen wie Sperrmodus, Zertifikatsersetzung und Chipkarten-Authentifizierung zum Erhöhen der Sicherheit konfigurieren.

Ein ESXi-Host wird außerdem durch eine Firewall geschützt. Sie können Ports für eingehenden und ausgehenden Datenverkehr nach Bedarf öffnen, sollten aber den Zugriff auf Dienste und Ports einschränken. Das Verwenden des ESXi-Sperrmodus und das Einschränken des Zugriffs auf ESXi-Shell kann außerdem zu einer sichereren Umgebung beitragen. Ab vSphere 6.0 nehmen ESXi-Hosts an der Zertifikatsinfrastruktur teil. Für Hosts werden Zertifikate bereitgestellt, die standardmäßig durch die VMware-Zertifizierungsstelle (VMCA) signiert werden.

Im VMware-Whitepaper *Security of the VMware vSphere Hypervisor* finden Sie weitere Informationen zur ESXi-Sicherheit.

Zulassen oder Verweigern des Zugriffs auf einen ESXi -Dienst oder Management-Agenten

Sie können die Eigenschaften der Firewall konfigurieren, um einem Dienst oder Verwaltungs-Agenten den Zugriff zu ermöglichen oder zu verweigern.

Sie fügen Informationen über zulässige Dienste und Management-Agenten zur Hostkonfigurationsdatei hinzu. Sie können diese Dienste und Agenten mithilfe des vSphere Clients oder der Befehlszeile aktivieren bzw. deaktivieren.

HINWEIS Wenn sich die Portregeln verschiedener Dienste überschneiden, kann das Aktivieren eines Diensts möglicherweise dazu führen, dass weitere überschneidende Dienste implizit aktiviert werden. Zum Minimieren der Auswirkungen dieses Verhaltens können Sie angeben, welche IP-Adressen auf jeden Dienst auf dem Host zugreifen dürfen.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich aus.

- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend im Abschnitt „Software“ auf **Sicherheitsprofil**.

Der vSphere Client zeigt eine Liste der aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.

- 3 Klicken Sie im Abschnitt „Firewall“ auf **Eigenschaften**.

Im Dialogfeld „Firewalleigenschaften“ werden alle Regelsätze aufgelistet, die für den Host konfiguriert werden können.

- 4 Wählen Sie die zu aktivierenden Regelsätze oder heben Sie die Auswahl der zu deaktivierenden Regelsätze auf.

Die Spalten „Eingehende Ports“ und „Ausgehende Ports“ zeigen die Ports an, die der vSphere Client für den Dienst freigibt. Die Spalte „Protokoll“ gibt das Protokoll an, das der Dienst verwendet. Die Spalte „Daemon“ zeigt den Status der Daemons an, die dem Dienst zugewiesen wurden.

- 5 Klicken Sie auf **OK**.

Hinzufügen von zulässigen IP-Adressen

Sie können angeben, welche Netzwerke eine Verbindung zu jedem Dienst herstellen dürfen, der auf dem Host ausgeführt wird.

Sie können den vSphere Client oder die Befehlszeile verwenden, um die Liste der zulässigen IP-Adressen für einen Dienst zu aktualisieren. Standardmäßig sind alle IP-Adressen zugelassen.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Sicherheitsprofil**.
- 3 Klicken Sie im Abschnitt „Firewall“ auf **Eigenschaften**.
- 4 Wählen Sie einen Dienst in der Liste aus und klicken Sie auf **Firewall**.
- 5 Wählen Sie **Nur Verbindungen von den folgenden Netzwerken zulassen** und geben Sie die IP-Adressen der Netzwerke ein, die eine Verbindung zum Host herstellen dürfen.

Sie können die IP-Adressen in den folgenden Formaten eingeben: 192.168.0.0/24, 192.168.1.2, 2001::1/64 oder fd3e:29a6:0a81:e478::/64.
- 6 Klicken Sie auf **OK**.

Festlegen der Optionen für das Starten von Diensten oder Clients

Standardmäßig werden daemon-Prozesse automatisch gestartet, sobald einer der Ports geöffnet wird, und automatisch gestoppt, sobald alle Ports geschlossen sind. Sie haben die Möglichkeit, diese Startrichtlinie für den ausgewählten Dienst oder Client zu ändern.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und dann unter **Software** auf **Sicherheitsprofil**.
- 3 Klicken Sie im Abschnitt „Firewall“ auf **Eigenschaften**.

Alle Firewall-Dienste und Verwaltungsagenten, die Sie für den Host konfigurieren können, sind aufgelistet.

- 4 Wählen Sie den zu konfigurierenden Dienst oder Management-Agenten aus und klicken Sie auf **Optionen**.

Anhand dieser Konfiguration können Sie die Startrichtlinie des Dienstes festlegen, den Dienststatus überprüfen und den Dienst manuell starten, anhalten oder neu starten.

- 5 Wählen Sie in der Liste **Startrichtlinie** eine Richtlinie aus.
- 6 Klicken Sie auf **OK**.

Verwenden der ESXi-Shell

ESXi-Shell (vormals Tech Support Mode, TSM) ist standardmäßig auf ESXi-Hosts deaktiviert. Sie können bei Bedarf lokalen Zugriff und Remotezugriff auf die Shell aktivieren.

Aktivieren Sie die ESXi-Shell nur zur Fehlerbehebung. Die ESXi-Shell kann unabhängig davon, ob der Host im Sperrmodus ausgeführt wird, aktiviert und deaktiviert werden. Weitere Informationen zum Verhalten im Sperrmodus finden Sie in der Dokumentation zur *vSphere-Sicherheit*.

ESXi-Shell	Aktivieren Sie diesen Dienst, um lokal auf die ESXi-Shell zuzugreifen.
SSH	Aktivieren Sie diesen Dienst, um die ESXi-Shell remote über SSH aufzurufen. Sie können SSH-Schlüssel auf Ihre Hosts hochladen. Weitere Informationen zu SSH-Schlüsseln finden Sie in der Dokumentation zur <i>vSphere-Sicherheit</i> .
Die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI)	Wenn Sie diesen Dienst während der Ausführung im Sperrmodus aktivieren, können Sie sich bei der Benutzerschnittstelle der direkten Konsole lokal als Root-Benutzer anmelden und den Sperrmodus deaktivieren. Sie können dann über eine direkte Verbindung zum vSphere Client oder durch die Aktivierung der ESXi-Shell auf den Host zugreifen.

Der Root-Benutzer und Benutzer mit der Rolle „Administrator“ können auf die ESXi-Shell zugreifen. Benutzern, die zur Active Directory-Gruppe „ESX Admins“ gehören, wird automatisch die Rolle „Administrator“ zugewiesen. Standardmäßig kann nur der Root-Benutzer Systembefehle (z. B. `vmware -v`) über ESXi-Shell ausführen.

HINWEIS Aktivieren Sie die ESXi-Shell erst dann, wenn dies wirklich erforderlich ist.

Verwenden des vSphere Clients zum Aktivieren des Zugriffs auf die ESXi-Shell

Verwenden des vSphere Clients zum Aktivieren des lokalen und des Remotezugriffs auf die ESXi-Shell.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Sicherheitsprofil**.
- 3 Klicken Sie im Abschnitt „Dienste“ auf **Eigenschaften**.
- 4 Wählen Sie einen Dienst aus der Liste aus.
 - ESXi Shell
 - SSH
 - Benutzerschnittstelle der direkten Konsole
- 5 Klicken Sie auf **Optionen** und wählen Sie **Manuell starten und beenden**.

Wenn Sie **Manuell starten und beenden** wählen, wird der Dienst nicht gestartet, wenn Sie den Host neu starten. Wenn Sie den Dienst beim Neustart des Hosts starten möchten, wählen Sie **Mit dem Host starten und beenden**.

- 6 Wählen Sie **Starten**, um den Dienst zu aktivieren.
- 7 Klicken Sie auf **OK**.

Erstellen einer Zeitüberschreitung für die ESXi-Shell -Verfügbarkeit

Standardmäßig ist die ESXi-Shell deaktiviert. Sie können einen Zeitüberschreitungswert für die Verfügbarkeit für die ESXi-Shell festlegen, um die Sicherheit beim Aktivieren der Shell zu erhöhen.

Der Zeitüberschreitungswert für die Verfügbarkeit gibt die Zeitspanne an, während der Sie sich nach der Aktivierung der ESXi-Shell anmelden müssen. Nach Ablauf dieser Zeitspanne wird der Dienst deaktiviert und die Benutzer können sich nicht mehr anmelden.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste den Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie unter „Software“ die Option **Erweiterte Einstellungen**.
- 3 Wählen Sie im linken Fensterbereich **UserVars**.
- 4 Geben Sie im Feld „UserVars.ESXiShellTimeOut“ den Zeitüberschreitungswert für die Verfügbarkeit ein.

Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
- 5 Klicken Sie auf **OK**.

Wenn Sie zu diesem Zeitpunkt angemeldet sind, bleibt Ihre Sitzung bestehen. Wenn Sie sich jedoch abmelden oder die Sitzung beendet wird, können Sie sich nicht mehr anmelden.

Erstellen einer Zeitüberschreitung für ESXi-Shell -Sitzungen im Leerlauf

Wenn ein Benutzer die ESXi-Shell auf einem Host aktiviert, aber vergisst, sich von der Sitzung abzumelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung kann die Möglichkeit für einen privilegierten Zugriff auf den Host erhöhen. Dies können Sie verhindern, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis Sie bei interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet werden. Änderungen an den Zeitüberschreitungswerten für die Leerlaufzeit werden erst wirksam, wenn Sie sich das nächste Mal bei der ESXi-Shell anmelden. Sie gelten nicht für aktuelle Sitzungen.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste den Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie unter „Software“ die Option **Erweiterte Einstellungen**.
- 3 Wählen Sie im linken Fensterbereich **UserVars**.
- 4 Geben Sie im Feld „UserVars.ESXiShellInteractiveTimeOut“ den Zeitüberschreitungswert für die Verfügbarkeit ein.

Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
- 5 Klicken Sie auf **OK**.

Wenn Sie zu diesem Zeitpunkt angemeldet sind, bleibt Ihre Sitzung bestehen. Wenn Sie sich jedoch abmelden oder die Sitzung beendet wird, können Sie sich nicht mehr anmelden.

Aktivieren des Sperrmodus im vSphere Client

Aktivieren Sie den Sperrmodus, damit alle Konfigurationsänderungen vCenter Server durchlaufen müssen. Sie können den Sperrmodus auch über die Benutzerschnittstelle der direkten Konsole aktivieren bzw. deaktivieren.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem vCenter Server-System.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Sicherheitsprofil**.
- 3 Klicken Sie neben Sperrmodus auf den Link **Bearbeiten**.
Das Dialogfeld Sperrmodus wird angezeigt.
- 4 Wählen Sie **Aktivieren von Sperrmodus**.
- 5 Klicken Sie auf **OK**.

Sichern von virtuellen Maschinen

Das Gastbetriebssystem, das in der virtuellen Maschine läuft, ist denselben Sicherheitsrisiken ausgesetzt wie ein physisches System. Sichern Sie virtuelle Maschinen so, wie Sie physische Maschinen sichern würden.

- 1 [Verhindern des Verkleinerns von virtuellen Festplatten](#) auf Seite 68
Benutzer ohne Administratorberechtigung im Gastbetriebssystem können virtuelle Festplatten verkleinern. Durch das Verkleinern einer virtuellen Festplatte wird nicht verwendeter Speicherplatz wieder verfügbar gemacht. Wenn Sie eine Festplatte allerdings wiederholt verkleinern, wird sie möglicherweise nicht mehr verfügbar und kann eine Dienstverweigerung (Denial of Service, DoS) verursachen. Um dies zu verhindern, sperren Sie die Möglichkeit, Festplatten zu verkleinern.
- 2 [Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole](#) auf Seite 68
Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole sind standardmäßig deaktiviert. Behalten Sie aus Gründen der Umgebungssicherheit die Standardeinstellung bei. Falls Sie Kopier- und Einfügevorgänge benötigen, müssen Sie diese mit dem vSphere Web Client aktivieren.
- 3 [Ändern des variablen Speicherlimits des Gastbetriebssystems](#) auf Seite 69
Sie können das variable Speicherlimit des Gastbetriebssystems erhöhen, wenn große Mengen von benutzerdefinierten Informationen in der Konfigurationsdatei gespeichert werden.
- 4 [Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden](#) auf Seite 69
Sie können Gäste daran hindern, Name/Wert-Paare in die Konfigurationsdatei zu schreiben, die an den Host gesendet werden. Dies bietet sich an, wenn Gastbetriebssysteme am Ändern von Konfigurationseinstellungen gehindert werden müssen.

- 5 [Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt](#) auf Seite 70

Benutzer und Prozesse ohne Root- oder Administratorberechtigungen in virtuellen Maschinen haben die Möglichkeit, Geräte zu verbinden oder zu trennen, beispielsweise Netzwerkadapter und CD-ROM-Laufwerke. Sie können auch Geräteeinstellungen verändern. Entfernen Sie diese Geräte, um die Sicherheit der virtuellen Maschinen zu verstärken. Wenn Sie ein Gerät nicht dauerhaft entfernen möchten, können Sie verhindern, dass ein Benutzer oder Prozess einer virtuellen Maschine das Gerät aus dem Gastbetriebssystem heraus einbindet oder trennt.

- 6 [Konfiguration von Syslog auf ESXi-Hosts](#) auf Seite 71

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Verhindern des Verkleinerns von virtuellen Festplatten

Benutzer ohne Administratorberechtigung im Gastbetriebssystem können virtuelle Festplatten verkleinern. Durch das Verkleinern einer virtuellen Festplatte wird nicht verwendeter Speicherplatz wieder verfügbar gemacht. Wenn Sie eine Festplatte allerdings wiederholt verkleinern, wird sie möglicherweise nicht mehr verfügbar und kann eine Dienstverweigerung (Denial of Service, DoS) verursachen. Um dies zu verhindern, sperren Sie die Möglichkeit, Festplatten zu verkleinern.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere-Client beim vCenter Server-System an.
- 2 Wählen Sie in der Bestandsliste die gewünschte virtuelle Maschine aus.
- 3 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 4 Wählen Sie **Optionen > Erweitert > Allgemein** aus und klicken Sie auf **Konfigurationsparameter**.
- 5 Fügen Sie die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Name	Wert
isolation.tools.diskWiper.disable	Wahr
isolation.tools.diskShrink.disable	Wahr

- 6 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **OK**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Wenn Sie diese Funktion deaktivieren, können Sie Festplatten einer virtuellen Maschine nicht verkleinern, wenn ein Datenspeicher keinen Speicherplatz mehr hat.

Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole

Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole sind standardmäßig deaktiviert. Behalten Sie aus Gründen der Umgebungssicherheit die Standardeinstellung bei. Falls Sie Kopier- und Einfügevorgänge benötigen, müssen Sie diese mit dem vSphere Web Client aktivieren.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die virtuelle Maschine aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 3 Wählen Sie **Optionen > Erweitert > Allgemein** aus und klicken Sie auf **Konfigurationsparameter**.
- 4 Stellen Sie sicher, dass in den Spalten „Name“ und „Wert“ die folgenden Werte enthalten sind, oder klicken Sie auf **Zeile hinzufügen**, um Werte hinzuzufügen.

Name	Wert
isolation.tools.copy.disable	Wahr
isolation.tools.paste.disable	Wahr

Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

- 5 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **OK**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.
- 6 (Optional) Starten Sie die virtuelle Maschine neu, wenn Sie Änderungen an den Konfigurationsparametern vornehmen.

Ändern des variablen Speicherlimits des Gastbetriebssystems

Sie können das variable Speicherlimit des Gastbetriebssystems erhöhen, wenn große Mengen von benutzerdefinierten Informationen in der Konfigurationsdatei gespeichert werden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die gewünschte virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 3 Wählen Sie **Optionen > Erweitert > Allgemein** aus und klicken Sie auf **Konfigurationsparameter**.
- 4 Wenn das Attribut zur Größenbegrenzung nicht vorhanden ist, müssen Sie es hinzufügen.
 - a Klicken Sie auf **Zeile hinzufügen**.
 - b Geben Sie **tools.setInfo.sizeLimit** in der Spalte „Name“ ein.
 - c Geben Sie **Anzahl der Bytes** in der Spalte „Wert“ ein.

Wenn das Größenlimitattribut vorhanden ist, passen Sie es wie gewünscht an.

- 5 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **OK**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden

Sie können Gäste daran hindern, Name/Wert-Paare in die Konfigurationsdatei zu schreiben, die an den Host gesendet werden. Dies bietet sich an, wenn Gastbetriebssysteme am Ändern von Konfigurationseinstellungen gehindert werden müssen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die gewünschte virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 3 Klicken Sie auf **Optionen > Erweitert > Allgemein** und klicken Sie auf **Konfigurationsparameter**.
- 4 Klicken Sie auf **Zeile hinzufügen** und geben Sie die folgenden Werte in den Spalten „Name“ und „Wert“ ein:
 - In der Spalte „Name“: **isolation.tools.setinfo.disable**
 - In der Spalte „Wert“: **Wahr**
- 5 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **OK**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.

Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt

Benutzer und Prozesse ohne Root- oder Administratorberechtigungen in virtuellen Maschinen haben die Möglichkeit, Geräte zu verbinden oder zu trennen, beispielsweise Netzwerkadapter und CD-ROM-Laufwerke. Sie können auch Geräteeinstellungen verändern. Entfernen Sie diese Geräte, um die Sicherheit der virtuellen Maschinen zu verstärken. Wenn Sie ein Gerät nicht dauerhaft entfernen möchten, können Sie verhindern, dass ein Benutzer oder Prozess einer virtuellen Maschine das Gerät aus dem Gastbetriebssystem heraus einbindet oder trennt.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client bei einem vCenter Server-System an und wählen Sie die virtuelle Maschine aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 3 Wählen Sie **Optionen > Erweitert > Allgemein** aus und klicken Sie auf **Konfigurationsparameter**.
- 4 Fügen Sie die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Name	Wert
isolation.device.connectable.disable	Wahr
isolation.device.edit.disable	Wahr

Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

- 5 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und noch einmal auf **OK**, um das Dialogfeld „Eigenschaften der virtuellen Maschine“ zu schließen.
- 6 (Optional) Starten Sie die virtuelle Maschine neu, wenn Sie Änderungen an den Konfigurationsparametern vornehmen.

Konfiguration von Syslog auf ESXi -Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Diensts verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Client aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Bereich „Software“ auf **Erweiterte Einstellungen**.
- 4 Wählen Sie in der Strukturansicht **Syslog**.
- 5 Klicken Sie zum Einrichten der globalen Protokollierung auf **Global** und nehmen Sie die entsprechenden Änderungen in den rechten Feldern vor.

Option	Beschreibung
Syslog.global.defaultRotate	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis <code>/scratch</code> auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format <code>[Datenspeichername] Pfad_zur_Datei</code> aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <code>[storage1] /systemlogs</code> dem Pfad <code>/vmfs/volumes/storage1/systemlogs</code> zuzuordnen.
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von Syslog.global.LogDir angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. <code>ssl://Hostname1:514</code> . UDP (Standard), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

- 6 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll.
 - a Klicken Sie auf **loggers**.
 - b Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten, und geben Sie die gewünschte Anzahl der Rotationen und die gewünschte Protokollgröße ein.
- 7 Klicken Sie auf **OK**.

Änderungen an der syslog-Option werden sofort wirksam.

ESXi -Authentifizierung und Benutzerverwaltung

7

ESXi steuert die Benutzerauthentifizierung und unterstützt Benutzerberechtigungen.

Wenn Sie mit dem vSphere Client eine direkte Verbindung zum ESXi-Host herstellen, können Sie Benutzer und Gruppen erstellen, die lokal auf dem ESXi-Host vorhanden sind. Sie können diesen Benutzern und Gruppen auch Berechtigungen zuweisen.

vCenter Server kennt keine lokalen Benutzer von ESXi und ESXi kennt die vCenter Server-Benutzer nicht. Weitere Informationen zum Verwalten von Benutzern für ESXi-Hosts, die von vCenter Server verwaltet werden, finden Sie in der Dokumentation *vSphere-Sicherheit*.

Dieses Kapitel behandelt die folgenden Themen:

- [„Verwalten von Benutzern mit dem vSphere Client“](#), auf Seite 73
- [„Zuweisen der Berechtigungen für ESXi“](#), auf Seite 76
- [„Verwalten von ESXi-Rollen“](#), auf Seite 78
- [„Verwenden von Active Directory zum Verwalten von ESXi-Benutzern“](#), auf Seite 80
- [„Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne“](#), auf Seite 82
- [„Anpassen der Suchliste in großen Domänen“](#), auf Seite 83

Verwalten von Benutzern mit dem vSphere Client

Durch die Benutzerverwaltung können Sie steuern, wer berechtigt ist, sich bei ESXi anzumelden.

In vSphere 5.1 und höher gelten für die ESXi-Benutzerverwaltung folgende Einschränkungen.

- Die Benutzer, die Sie erstellen, wenn Sie sich direkt mit einem ESXi-Host verbinden, sind nicht mit den vCenter Server-Benutzern identisch. Wenn der Host von vCenter Server verwaltet wird, werden Benutzer, die direkt auf dem Host erstellt wurden, von vCenter Server ignoriert.
- Sie können keine ESXi-Benutzer mit dem vSphere Web Client erstellen. Sie müssen sich mit dem vSphere Client direkt beim Host anmelden, um ESXi-Benutzer zu erstellen.
- ESXi 5.1 und höher unterstützt keine lokalen Gruppen. Active Directory-Gruppen werden jedoch unterstützt.

Damit anonyme Benutzer wie „root“ nicht über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) oder die ESXi Shell auf den Host zugreifen können, entfernen Sie die Administratorrechte des Benutzers vom Root-Ordner des Hosts. Dies gilt sowohl für lokale Benutzer als auch für Active Directory-Benutzer und -Gruppen.

Hinzufügen eines ESXi-Benutzers

Wenn Sie einen Benutzer zur Tabelle „Benutzer“ hinzufügen, wird die vom Host verwaltete, interne Benutzerliste aktualisiert.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem ESXi-Host.
- Lesen Sie die Kennwortanforderungen in der Dokumentation zur *vSphere-Sicherheit*.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client bei ESXi an.

Sie können keine ESXi-Benutzer mit dem vSphere Web Client erstellen. Sie müssen sich mit dem vSphere Client direkt beim Host anmelden, um ESXi-Benutzer zu erstellen.

- 2 Klicken Sie auf **Benutzer**.
- 3 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle in der Tabelle „Benutzer“ und klicken Sie auf **Hinzufügen**.
- 4 Geben Sie für die Anmeldung einen Benutzernamen und ein Kennwort ein.

HINWEIS Erstellen Sie keinen Benutzer mit dem Namen **ALL**. Berechtigungen, die dem Namen **ALL** zugewiesen sind, stehen möglicherweise in manchen Situationen nicht allen Benutzern zur Verfügung. Wenn beispielsweise ein Benutzer mit dem Namen **ALL** Administratorberechtigungen besitzt, ist es möglich, dass sich ein Benutzer mit **ReadOnly**-Berechtigungen remote beim Host anmelden kann. Dies ist nicht das beabsichtigte Verhalten.

- Die Angabe des Benutzernamens ist optional.
- Erstellen Sie ein Kennwort, das den Anforderungen in Bezug auf die Länge und Komplexität entspricht. Der Host überprüft die Einhaltung der Kennwortrichtlinien mithilfe des Standardauthentifizierungs-Plug-Ins `pam_passwdqc`. So. Falls das Kennwort nicht den Richtlinien entspricht, wird der folgende Fehler angezeigt: Ein allgemeiner Systemfehler ist aufgetreten: Kennwort: Authentifizierungstoken-Manipulationsfehler.

- 5 Klicken Sie auf **OK**.

Ändern der Einstellungen für einen Benutzer auf dem Host

Sie können die Anmeldeinformationen, den Benutzernamen und das Kennwort eines Benutzers ändern.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem ESXi-Host.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client bei ESXi an.

Sie können keine ESXi-Benutzer mit dem vSphere Web Client erstellen. Sie müssen sich mit dem vSphere Client direkt beim Host anmelden, um ESXi-Benutzer zu erstellen.

- 2 Klicken Sie auf **Benutzer**.
- 3 Klicken Sie mit der rechten Maustaste auf den Benutzer und klicken Sie zum Öffnen des Dialogfelds „Benutzer bearbeiten“ auf **Bearbeiten**.

- 4 Geben Sie für die Anmeldung einen Benutzernamen und ein Kennwort ein.

HINWEIS Erstellen Sie keinen Benutzer mit dem Namen **ALL**. Berechtigungen, die dem Namen **ALL** zugewiesen sind, stehen möglicherweise in manchen Situationen nicht allen Benutzern zur Verfügung. Wenn beispielsweise ein Benutzer mit dem Namen **ALL** Administratorberechtigungen besitzt, ist es möglich, dass sich ein Benutzer mit **ReadOnly**-Berechtigungen remote beim Host anmelden kann. Dies ist nicht das beabsichtigte Verhalten.

- Die Angabe des Benutzernamens ist optional.
- Erstellen Sie ein Kennwort, das den Anforderungen in Bezug auf die Länge und Komplexität entspricht. Der Host überprüft die Einhaltung der Kennwortrichtlinien mithilfe des Standardauthentifizierungs-Plug-Ins `pam_passwdqc.so`. Falls das Kennwort nicht den Richtlinien entspricht, wird der folgende Fehler angezeigt: Ein allgemeiner Systemfehler ist aufgetreten: Kennwort: Authentifizierungstoken-Manipulationsfehler.

- 5 Klicken Sie auf **OK**.

Entfernen eines lokalen ESXi-Benutzers von einem Host

Sie können einen lokalen ESXi-Benutzer von dem Host entfernen.



VORSICHT Entfernen Sie den Root-Anwender nicht.

Wenn Sie einen Benutzer vom Host entfernen, verliert er seine Berechtigungen für alle Objekte auf dem Host und kann sich nicht mehr anmelden.

HINWEIS Angemeldete Benutzer, die aus der Domäne entfernt werden, behalten ihre Hostberechtigungen bis zum nächsten Neustart des Hosts.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client bei ESXi an.
 - 2 Klicken Sie auf die Registerkarte **Lokale Benutzer und Gruppen** und dann auf **Benutzer**.
 - 3 Klicken Sie mit der rechten Maustaste auf den zu entfernenden Benutzer und wählen Sie **Entfernen**.
- Entfernen Sie den Root-Benutzer in keinem Fall.

Sortieren, Exportieren und Anzeigen von lokalen ESXi -Benutzern

Sie können Listen mit den lokalen Benutzern eines Hosts anzeigen, sortieren und in eine Datei im HTML-, XML-, Microsoft Excel- oder CSV-Format exportieren.

Vorgehensweise

- 1 Melden Sie sich über den vSphere-Client bei ESXi an.
- 2 Klicken Sie auf die Registerkarte **Lokale Benutzer und Gruppen** und dann auf **Benutzer**.

- 3 Legen Sie die Sortierreihenfolge der Tabelle fest, und blenden Sie Spalten ein oder aus, je nachdem, welche Daten in der Exportdatei enthalten sein sollen.
 - Wenn Sie die Tabelle nach einer Spalte sortieren möchten, klicken Sie auf die entsprechende Spaltenüberschrift.
 - Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften, und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.
 - Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften, und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.
- 4 Klicken Sie mit der rechten Maustaste an eine beliebigen Stelle in der Tabelle und klicken Sie dann zum Öffnen des Dialogfelds „Speichern unter“ auf **Liste exportieren**.
- 5 Wählen Sie ein Verzeichnis aus, und geben Sie einen Dateinamen ein.
- 6 Wählen Sie den Dateityp aus und klicken Sie auf **OK**.

Zuweisen der Berechtigungen für ESXi

Für ESXi werden Berechtigungen als Zugriffsrollen definiert, die aus einem Benutzer und der dem Benutzer zugewiesenen Rolle für ein Objekt bestehen, wie z. B. einer virtuellen Maschine oder einem ESXi-Host. Berechtigungen geben Benutzern das Recht, die von der Rolle definierten Aktivitäten auf dem Objekt auszuführen, dem die Rolle zugeordnet wurde.

Wenn ein Benutzer beispielsweise Arbeitsspeicher für den Host konfigurieren möchte, benötigt er eine Rolle, die das Recht **Host.Konfiguration.Arbeitsspeicherkonfiguration** enthält. Indem Sie Benutzern verschiedene Rollen für verschiedene Objekte zuweisen, können Sie steuern, welche Aufgaben Benutzer in Ihrer vSphere-Umgebung ausführen können.

Beim direkten Verbinden mit einem Host unter Verwendung des vSphere-Clients besitzen die Benutzerkonten „root“ und „vpxuser“ dieselben Zugriffsrechte auf alle Objekte wie jeder Benutzer mit der Rolle „Administrator“.

Alle anderen Benutzer haben zunächst keine Berechtigungen für Objekte, d. h., sie können weder Objekte anzeigen noch Vorgänge an ihnen durchführen. Ein Benutzer mit Administratorrechten muss diesen Benutzern Rechte zuweisen, damit sie Aufgaben durchführen können.

Viele Aufgaben erfordern Berechtigungen für mehr als ein Objekt. Diese Regeln können Ihnen dabei helfen zu entscheiden, wo Sie Berechtigungen zuweisen müssen, um bestimmte Vorgänge zuzulassen:

- Jeder Vorgang, der Speicherplatz benötigt, wie z. B. das Erstellen einer virtuellen Festplatte oder eines Snapshots, erfordert das Recht **Datenspeicher.Speicher zuteilen** auf dem Zieldatenspeicher und das Recht, den Vorgang selbst durchzuführen.
- Das Verschieben eines Objekts in der Bestandslistenhierarchie erfordert entsprechende Berechtigungen auf dem Objekt selbst, dem übergeordneten Quellobjekt (z. B. einem Ordner oder Cluster) und dem übergeordneten Zielobjekt.
- Jeder Host und Cluster hat seinen eigenen impliziten Ressourcenpool, der alle Ressourcen des Hosts oder Clusters enthält. Das direkte Bereitstellen einer virtuellen Maschine auf einen Host oder Cluster erfordert das Recht **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**.

Die Liste der Rechte ist für ESXi und vCenter Server identisch.

Sie können über eine direkte Verbindung mit dem ESXi-Host Rollen erstellen und Berechtigungen festlegen.

Berechtigungsvalidierung

vCenter Server und ESXi-Hosts, die Active Directory verwenden, validieren Benutzer und Gruppen regelmäßig anhand der Windows Active Directory-Domäne. Die Validierung findet jedes Mal statt, wenn das Hostsystem startet, und in regelmäßigen Abständen, wie in den vCenter Server-Einstellungen angegeben.

Wenn beispielsweise Benutzer „Schmidt“ Berechtigungen zugewiesen sind und der Benutzername in der Domäne in „Schmidt2“ geändert wird, schließt der Host daraus, dass der Benutzer „Schmidt“ nicht mehr vorhanden ist, und entfernt die Berechtigungen für diesen Benutzer bei der nächsten Validierung.

Wenn Benutzer „Schmidt“ aus der Domäne entfernt wird, werden ebenfalls alle Berechtigungen bei der nächsten Validierung entfernt. Wenn ein neuer Benutzer „Schmidt“ der Domäne vor der nächsten Validierung hinzugefügt wird, erhält der neue Benutzer alle Berechtigungen des alten Benutzers mit diesem Namen.

Ändern von Berechtigungen

Wenn eine Kombination aus Benutzer und Rolle für ein Bestandslistenobjekt festgelegt wurde, können Sie Änderungen an der Rolle für den Benutzer vornehmen oder die Einstellung des Kontrollkästchens **Weitergeben** ändern. Sie können auch die Berechtigungseinstellung entfernen.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client ein Objekt in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Berechtigungen**.
- 3 Klicken Sie mit der rechten Maustaste auf das entsprechende Element, um die Kombination aus Rolle und Benutzer auszuwählen.
- 4 Wählen Sie **Eigenschaften**.
- 5 Wählen Sie aus dem Dropdown-Menü die entsprechende Rolle für den Benutzer oder die Gruppe aus.
- 6 Um die Rechte für die untergeordneten Elemente des zugewiesenen Bestandslistenobjekts zu übernehmen, aktivieren Sie das Kontrollkästchen **Weitergeben** und klicken Sie auf **OK**.

Entfernen von Berechtigungen

Durch das Entfernen einer Berechtigung für einen Benutzer wird der Benutzer nicht aus der Liste der verfügbaren Benutzer entfernt. Die Rolle wird ebenfalls nicht aus der Liste der verfügbaren Elemente entfernt. Die Kombination aus Benutzer und Rolle wird jedoch vom ausgewählten Bestandslistenobjekt entfernt.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Sitzung mit einem ESXi-Host.

Vorgehensweise

- 1 Klicken Sie im vSphere Client auf **Bestandsliste**.
- 2 Erweitern Sie die Bestandsliste nach Bedarf, und klicken Sie auf das betreffende Objekt.
- 3 Klicken Sie auf die Registerkarte **Berechtigungen**.
- 4 Klicken Sie auf das entsprechende Element, um die Kombination aus Benutzer und Rolle auszuwählen.
- 5 Wählen Sie **Bestandsliste > Berechtigungen > Löschen**.

Ändern der Einstellungen für die Berechtigungsvalidierung

vCenter Server validiert seine Benutzer- und Gruppenlisten regelmäßig anhand der Benutzer und Gruppen in der Windows Active Directory-Domäne. Er entfernt anschließend Benutzer oder Gruppen, die nicht mehr in der Domäne vorhanden sind. Sie können das Intervall zwischen Validierungen ändern.

Vorgehensweise

- 1 Wählen Sie auf dem mit dem vCenter Server-System verbundenen vSphere-Client **Verwaltung > vCenter Server-Einstellungen**.
- 2 Wählen Sie im Navigationsfenster **Active Directory**.
- 3 (Optional) Deaktivieren Sie das Kontrollkästchen **Validierung aktivieren**, um die Validierung zu deaktivieren.

Die Validierung ist standardmäßig aktiviert. Benutzer und Gruppen werden validiert, wenn das vCenter Server-System gestartet wird, selbst wenn die Validierung deaktiviert ist.

- 4 Wenn die Validierung aktiviert ist, geben Sie einen Wert in das Textfeld „Validierungszeitraum“ ein, um einen Zeitraum (in Minuten) zwischen Validierungen anzugeben.

Verwalten von ESXi -Rollen

ESXi gewährt nur denjenigen Benutzern Zugriff auf Objekte, denen Berechtigungen für das jeweilige Objekt zugewiesen wurden. Wenn Sie einem Benutzer Berechtigungen für das Objekt zuweisen, kombinieren Sie hierzu den Benutzer mit einer Rolle. Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten.

Für ESXi-Hosts gibt es drei Standardrollen. Es ist nicht möglich, die Berechtigungen für diese drei Rollen zu ändern. Jede nachfolgende Standardrolle enthält die Berechtigungen der vorhergehenden Rolle. So übernimmt beispielsweise die Rolle „Administrator“ die Rechte der Rolle „Nur lesen“. Rollen, die Sie selbst anlegen, übernehmen keine Berechtigungen von den Standardrollen.

Benutzerdefinierte Rollen können Sie mit den Rollenbearbeitungsdienstprogrammen auf dem vSphere-Client erstellen und an Ihre Anforderungen anpassen. Wenn Sie den mit vCenter Server verbundenen vSphere-Client zur Verwaltung der ESXi-Hosts verwenden, stehen Ihnen in vCenter Server zusätzliche Rollen zur Auswahl. Auf die Rollen, die Sie direkt auf einem ESX-Host erstellen, kann innerhalb von vCenter Server nicht zugegriffen werden. Sie können diese Rollen nur verwenden, wenn Sie sich direkt über den vSphere-Client am Host anmelden.

HINWEIS Wenn Sie eine benutzerdefinierte Rolle hinzufügen und ihr keine Rechte zuweisen, wird die Rolle als eine schreibgeschützte Rolle mit drei systemdefinierten Rechten erstellt: System.Anonymous, System.View und System.Read.

Wenn Sie ESXi-Hosts über vCenter Server verwalten, beachten Sie, dass die Verwendung benutzerdefinierter Rollen auf dem Host und in vCenter Server zu Verwirrung und Missbrauch führen kann. Verwenden Sie bei dieser Art der Konfiguration benutzerdefinierte Rollen nur in vCenter Server.

Sie können den vSphere-Client verwenden, um über eine direkte Verbindung mit dem ESXi-Host Hostrollen zu erstellen und Berechtigungen festzulegen.

Erstellen einer Rolle

VMware empfiehlt, dass Sie Rollen erstellen, die den in Ihrer Umgebung bestehenden Anforderungen hinsichtlich der Zugriffssteuerung entsprechen.

Voraussetzungen

Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind, beispielsweise als Benutzer „root“ oder „vpxuser“.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **Rollen**.
- 2 Klicken Sie im Informationsfenster mit der rechten Maustaste auf die Registerkarte **Rollen** und klicken Sie auf **Hinzufügen**.
- 3 Geben Sie einen Namen für die neue Rolle ein.
- 4 Wählen Sie Berechtigungen für die Rolle aus und klicken Sie auf **OK**.

Klonen einer Rolle

Sie können eine vorhandene Rolle kopieren, sie umbenennen und später bearbeiten. Wenn Sie eine Kopie erstellen, wird die neue Rolle nicht auf Benutzer bzw. Gruppen und Objekte angewendet. Sie müssen Benutzer, Gruppen und Objekten die Rolle zuweisen.

Voraussetzungen

Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind, beispielsweise als Benutzer „root“ oder „vpxuser“.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **Rollen**.
- 2 Klicken Sie zum Auswählen der zu duplizierenden Rolle in der Liste **Rollen (Roles)** auf das Objekt.
- 3 Klicken Sie zum Klonen der ausgewählten Rolle auf **Verwaltung > Rolle > Klonen**.

Der Rollenliste wird ein Duplikat der Rolle hinzugefügt. Der Name lautet *Klon von role_name*.

Bearbeiten einer Rolle

Beim Bearbeiten einer Rolle können Sie die für diese Rolle ausgewählten Berechtigungen ändern. Anschließend werden diese Berechtigungen auf alle Benutzer oder Gruppen angewendet, die der bearbeiteten Rolle zugeordnet sind.

Voraussetzungen

Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind, beispielsweise als Benutzer „root“ oder „vpxuser“.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **Rollen**.
- 2 Klicken Sie mit der rechten Maustaste auf die zu bearbeitende Rolle und wählen Sie **Rolle bearbeiten**.
- 3 Wählen Sie Berechtigungen für die Rolle aus und klicken Sie auf **OK**.

Umbenennen einer Rolle

Es erfolgen keine Änderungen an die Zuweisungen einer Rolle, wenn Sie sie umbenennen.

Voraussetzungen

Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind, beispielsweise als Benutzer „root“ oder „vpxuser“.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **Rollen**.
- 2 Klicken Sie auf das Objekt in der Liste der Rollen, das Sie umbenennen möchten.

- 3 Wählen Sie **Verwaltung > Rolle > Umbenennen**.
- 4 Geben Sie den neuen Namen ein.

Entfernen einer Rolle

Wenn Sie eine Rolle entfernen, die keinen Benutzern oder Gruppen zugeordnet ist, wird die Definition dieser Rolle aus der Liste der Rollen entfernt. Wenn Sie eine Rolle entfernen, die einem Benutzer oder einer Gruppe zugeordnet ist, können Sie alle Zuweisungen entfernen oder sie durch eine Zuweisung zu einer anderen Rolle ersetzen.



VORSICHT Stellen Sie sicher, dass Ihnen die Auswirkungen auf die Benutzer bekannt sind, bevor Sie alle Zuweisungen entfernen oder ersetzen. Benutzer, denen keine Berechtigungen zugewiesen wurden, können sich nicht anmelden.

Voraussetzungen

Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind, beispielsweise als Benutzer „root“ oder „vpxuser“.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **Rollen**.
- 2 Klicken Sie auf das Objekt, das Sie aus der Liste der Rollen entfernen möchten.
- 3 Wählen Sie **Verwaltung > Rolle > Entfernen**.
- 4 Klicken Sie auf **OK**.

Die Rolle wird aus der Liste entfernt.

Wenn die Rolle einem Benutzer oder einer Gruppe zugewiesen ist (If the role is assigned to a user or group), wird eine Warnmeldung angezeigt.

- 5 Wählen Sie eine Neuzuweisungsoption aus und klicken Sie auf **OK**.

Option	Beschreibung
Rollenzuweisungen entfernen	Entfernt auf dem Server konfigurierte Paare aus Rolle und Benutzer oder Gruppe. Wenn einem Benutzer oder einer Gruppe keine weiteren Berechtigungen zugewiesen wurden, gehen alle Berechtigungen verloren.
Betroffene Benutzer zuweisen zu	Weist allen konfigurierten Paaren aus Rolle und Benutzer oder Gruppe die ausgewählte neue Rolle neu zu.

Verwenden von Active Directory zum Verwalten von ESXi-Benutzern

Sie können ESXi so konfigurieren, dass es einen Verzeichnisdienst, wie z. B. Active Directory, zur Benutzerverwaltung verwendet.

Das Erstellen von lokalen Benutzerkonten auf jedem Host stellt Herausforderungen beim Synchronisieren von Kontonamen und Kennwörtern über mehrere Hosts hinweg dar. Weisen Sie ESXi-Hosts eine Active Directory-Domäne zu, damit Sie lokale Benutzerkonten weder erstellen noch pflegen müssen. Durch die Verwendung von Active Directory für die Authentifizierung von Benutzern wird die Konfiguration des ESXi-Hosts vereinfacht und das Risiko von Konfigurationsproblemen, die einen unbefugten Zugriff ermöglichen, reduziert.

Wenn Sie Active Directory verwenden, geben Benutzer beim Hinzufügen eines Hosts zu einer Domäne die Active Directory-Anmeldedaten und den Domänennamen des Active Directory-Servers an.

Konfigurieren eines Hosts für die Verwendung von Active Directory

Sie können den Host so konfigurieren, dass er Benutzer und Gruppen mithilfe eines Verzeichnisdienstes, wie z. B. Active Directory, verwaltet.

Voraussetzungen

- Stellen Sie sicher, dass Sie eine Active Directory-Domäne eingerichtet haben. Weitere Informationen finden Sie in der Dokumentation Ihres Verzeichnisservers.
- Stellen Sie sicher, dass der Name des ESXi-Hosts mit dem Domänennamen der Active Directory-Gesamtstruktur vollständig qualifiziert angegeben ist.

Vollständig qualifizierter Domänenname = Hostname.Domänenname

Vorgehensweise

- 1 Synchronisieren Sie mithilfe von NTP die Uhrzeit von ESXi mit der des Verzeichnisdienst-Systems.
 ESXi unterstützt das Synchronisieren der Uhrzeit mit einem externen NTPv3- oder NTPv4-Server, der mit RFC 5905 und RFC 1305 kompatibel ist. Der Microsoft Windows-W32Time-Dienst erfüllt diese Anforderungen beim Ausführen mit den Standardeinstellungen nicht. Unter der *vSphere-Sicherheit*-Dokumentation oder in der VMware-Knowledgebase finden Sie Informationen über das Synchronisieren der ESXi-Uhrzeit mit einem Microsoft-Domänencontroller.
- 2 Stellen Sie sicher, dass die DNS-Server, die Sie für den Host konfiguriert haben, die Hostnamen für die Active Directory-Controller auflösen können.
 - a Wählen Sie im vSphere-Client den gewünschten Host in der Bestandsliste aus.
 - b Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **DNS und Routing**.
 - c Klicken Sie oben rechts im Fenster auf den Link **Eigenschaften**.
 - d Vergewissern Sie sich im Dialogfeld „DNS- und Routing-Konfiguration“, dass die Informationen zu Hostnamen und DNS-Server des Hosts korrekt sind.

Weiter

Verwenden Sie den vSphere-Client, um einer Verzeichnisdienst-Domäne beizutreten.

Hinzufügen eines Hosts zu einer Verzeichnisdienst-Domäne

Für die Verwendung eines Verzeichnisdienstes müssen Sie den Host mit der Verzeichnisdienst-Domäne verbinden.

Sie können den Domänennamen auf zwei Arten eingeben:

- **name.tld** (Beispiel: **domain.com**): Das Konto wird unter dem Standardcontainer erstellt.
- **name.tld/container/path** (Beispiel: **domain.com/OU1/OU2**): Das Konto wird unter der angegebenen Organisationseinheit (Organizational Unit, OU) erstellt.

Informationen zur Verwendung des vSphere Authentication Proxy-Diensts (CAM-Dienst) finden Sie in der Dokumentation *vSphere-Sicherheit*.

Voraussetzungen

Vergewissern Sie sich, dass eine Verbindung zwischen dem vSphere Client und dem Host besteht.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients einen Host aus und klicken Sie auf die Registerkarte **Konfiguration**.

- 2 Klicken Sie unter „Software“ auf **Authentifizierungsdienste**.
- 3 Klicken Sie auf **Eigenschaften**.
- 4 Wählen Sie im Dialogfeld für die Benutzerverzeichnisdienste das gewünschte Benutzerverzeichnis aus dem Dropdown-Menü.
- 5 Geben Sie eine Domäne ein.
Verwenden Sie das Formular **name.tld** oder **name.tld/container/path**.
- 6 Klicken Sie auf **Domäne beitreten**.
- 7 Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisdienstbenutzers ein, der über die Berechtigung verfügt, den Host mit der Domäne zu verbinden, und klicken Sie auf **OK**.
- 8 Klicken Sie auf **OK** um das Dialogfeld für die Verzeichnisdienstkonfiguration zu schließen.

Anzeigen der Verzeichnisdiensteinstellungen

Sie können (soweit vorhanden) den Typ des Verzeichnisservers, den der Host zum Authentifizieren von Benutzern verwendet, sowie die Verzeichnissereinstellungen anzeigen.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients einen Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie unter „Software“ die Option **Authentifizierungsdienste**.
Auf der Seite „Authentifizierungsdiensteinstellungen“ werden der Verzeichnisdienst und die Domäneinstellungen angezeigt.

Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne

Wenn Sie einen Host zu einer Verzeichnisdienst-Domäne hinzufügen, können Sie für die Authentifizierung das vSphere Authentication Proxy anstelle von benutzerdefinierten Active Directory-Anmeldeinformationen verwenden.

Sie können den Domänennamen auf zwei Arten eingeben:

- **name.tld** (Beispiel: **domain.com**): Das Konto wird unter dem Standardcontainer erstellt.
- **name.tld/container/path** (Beispiel: **domain.com/OU1/OU2**): Das Konto wird unter der angegebenen Organisationseinheit (Organizational Unit, OU) erstellt.

Voraussetzungen

- Vergewissern Sie sich, dass eine Verbindung zwischen dem vSphere Client und dem Host besteht.
- Wenn ESXi mit einer DHCP-Adresse konfiguriert ist, richten Sie den DHCP-Bereich wie in der Dokumentation *vSphere-Sicherheit* beschrieben ein.
- Wenn ESXi mit einer statischen IP-Adresse konfiguriert ist, stellen Sie sicher, dass sein zugehöriges Profil so konfiguriert ist, dass zum Beitreten einer Domäne der vSphere Authentication Proxy-Dienst verwendet wird, damit der Authentifizierungs-Proxy-Server der IP-Adresse von ESXi vertrauen kann.
- Wenn ESXi ein selbstsigniertes Zertifikat verwendet, stellen Sie sicher, dass der Host zu vCenter Server hinzugefügt wurde. Dies ermöglicht dem Authentifizierungs-Proxy-Server ESXi zu vertrauen.

- Wenn ESXi ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwendet und nicht durch Auto Deploy bereitgestellt wird, stellen Sie sicher, dass das CA-Zertifikat wie in der Dokumentation *vSphere-Sicherheit* beschrieben zum lokalen Zertifikatspeicher des Authentifizierungs-Proxy-Servers hinzugefügt wurde.
- Führen Sie eine Authentifizierung des vSphere Authentication Proxy-Servers mit dem Host wie in der Dokumentation *vSphere-Sicherheit* beschrieben durch.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Client aus.
- 2 Wählen Sie die Registerkarte **Konfiguration** und klicken Sie auf **Authentifizierungsdienste**.
- 3 Klicken Sie auf **Eigenschaften**.
- 4 Wählen Sie im Dialogfeld „Verzeichnisdienstkonfiguration“ den Verzeichnisserver im Dropdown-Menü aus.
- 5 Geben Sie eine Domäne ein.
Verwenden Sie das Formular **name.tld** oder **name.tld/container/path**.
- 6 Aktivieren Sie das Kontrollkästchen **vSphere Authentication Proxy verwenden**.
- 7 Geben Sie die IP-Adresse des Authentication Proxy-Servers ein.
- 8 Klicken Sie auf **Domäne beitreten**.
- 9 Klicken Sie auf **OK**.

Anpassen der Suchliste in großen Domänen

Wenn Sie über Domänen mit Tausenden von Benutzern oder Gruppen verfügen oder wenn Suchvorgänge viel Zeit in Anspruch nehmen, passen Sie die Sucheinstellungen im Dialogfeld „Benutzer oder Gruppen auswählen“ an.

HINWEIS Die beschriebene Vorgehensweise bezieht sich nur auf vCenter Server-Benutzerlisten. ESXi-Host-Benutzerlisten können auf diese Weise nicht durchsucht werden.

Voraussetzungen

Zum Konfigurieren von Active Directory-Einstellungen muss der vSphere-Client mit dem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie auf dem mit dem vCenter Server-System verbundenen vSphere-Client, **Verwaltung > vCenter Server-Einstellungen**.
- 2 Wählen Sie im Navigationsfenster **Active Directory**.

- 3 Ändern Sie die Werte wie gewünscht.

Option	Beschreibung
Active Directory-Zeitüberschreitung	Zeitüberschreitungsintervall in Sekunden für das Herstellen einer Verbindung mit dem Active Directory-Server. Dieser Wert gibt an, wie lange die Suche auf der ausgewählten Domäne in vCenter Server höchstens dauern darf. Das Suchen in großen Domänen kann sehr lange dauern.
Abfragegrenze aktivieren	Aktivieren Sie das Kontrollkästchen, um die Anzahl der Benutzer und Gruppen, die vCenter Server im Dialogfeld „Berechtigungen hinzufügen“ für die ausgewählte Domäne anzeigt, einzuschränken.
Wert „Benutzer & Gruppen“	Legt die maximale Anzahl von Benutzern und Gruppen fest, die vCenter Server von der ausgewählten Domäne im Dialogfeld Benutzer und Gruppen auswählen anzeigt. Bei Eingabe des Werts 0 (Null) werden alle Benutzer und Gruppen angezeigt.

- 4 Klicken Sie auf **OK**.

Verwalten von Hosts in vCenter Server

8

Verbinden Sie Ihre Hosts mit einem vCenter Server-System, um auf alle Funktionen Ihrer Hosts zuzugreifen und die Verwaltung von mehreren Hosts zu vereinfachen.

Informationen über die Konfigurationsverwaltung von ESXi-Hosts finden Sie in der Dokumentation *vSphere-Netzwerk*, *vSphere-Speicher* oder *vSphere-Sicherheit*.

Die Ansichten und verfügbaren Funktionen variieren in Abhängigkeit davon, ob der vSphere Client mit einem vCenter Server-System oder mit einem ESXi-Host verbunden ist. Soweit nicht anders angegeben, beziehen sich Prozesse, Aufgaben und Beschreibungen auf alle Arten von vSphere Client-Verbindungen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Trennen und Herstellen einer Hostverbindung“](#), auf Seite 85
- [„Entfernen eines Hosts aus einem Cluster“](#), auf Seite 86
- [„Entfernen eines verwalteten Hosts aus vCenter Server“](#), auf Seite 87

Trennen und Herstellen einer Hostverbindung

Sie können einen Host, der von vCenter Server verwaltet wird, trennen und erneut verbinden. Beim Trennen der Verbindung eines verwalteten Hosts wird dieser nicht aus vCenter Server entfernt, sondern es werden nur vorübergehend alle Überwachungsaktivitäten von vCenter Server ausgesetzt.

Der verwaltete Host und die verknüpften virtuellen Maschinen verbleiben in der vCenter Server-Bestandsliste. Im Gegensatz dazu werden durch das Entfernen eines verwalteten Hosts von vCenter Server sowohl der verwaltete Host als auch alle verknüpften virtuellen Maschinen aus der Bestandsliste von vCenter Server entfernt.

Trennen der Verbindung zu einem verwalteten Host

Verwenden Sie den vSphere-Client, um die Verbindung zu einem verwalteten Host von vCenter Server zu trennen.

Vorgehensweise

- 1 Zeigen Sie die Bestandsliste in dem mit einem vCenter Server-System verbundenen vSphere-Client an und klicken Sie zum Trennen auf den verwalteten Host.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie im Popup-Menü **Trennen**.
- 3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Wenn die Verbindung des verwalteten Hosts getrennt wird, wird hinter dem Objektnamen in Klammern „Nicht verbunden“ angezeigt, und das Objekt wird abgeblendet dargestellt. Alle verknüpften virtuellen Maschinen werden ebenso abgeblendet dargestellt und bezeichnet.

Erneutes Verbinden mit einem verwalteten Host

Verwenden Sie den vSphere-Client, um einen verwalteten Host erneut mit einem vCenter Server-System zu verbinden.

Vorgehensweise

- 1 Zeigen Sie die Bestandsliste im mit einem vCenter Server-System verbundenen vSphere-Client an und klicken Sie zum erneuten Verbinden auf den verwalteten Host.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie im Popup-Menü **Verbinden**.

Wenn der Verbindungsstatus des verwalteten Hosts mit vCenter Server geändert wird, werden die Status der virtuellen Maschinen auf diesem Host aktualisiert, um die Änderung zu übernehmen.

Neuverbinden von Hosts nach Änderungen am vCenter Server -SSL-Zertifikat

vCenter Server verwendet ein SSL-Zertifikat, um in der vCenter Server-Datenbank gespeicherte Hostkennwörter zu verschlüsseln und zu entschlüsseln. Wenn das Zertifikat ersetzt oder geändert wird, kann vCenter Server keine Hostkennwörter entschlüsseln und daher auch keine Verbindung mit verwalteten Hosts herstellen.

Wenn ein Hostkennwort von vCenter Server nicht entschlüsselt werden kann, wird die Verbindung zwischen Host und vCenter Server getrennt. Sie müssen die Verbindung mit dem Host erneut herstellen und die Anmeldeinformationen eingeben, die mit dem neuen Zertifikat verschlüsselt und in der Datenbank gespeichert werden.

Entfernen eines Hosts aus einem Cluster

Wenn ein Host aus einem Cluster entfernt wird, werden die von ihm bereitgestellten Ressourcen von den Gesamtressourcen des Clusters abgezogen. Die auf dem Host bereitgestellten virtuellen Maschinen werden entweder auf andere Hosts innerhalb des Clusters migriert oder verbleiben auf dem Host und werden aus dem Cluster entfernt, je nach Zustand der virtuellen Maschinen, wenn der Host aus dem Cluster entfernt wird.

Sie können Hosts aus einem Cluster entfernen, indem Sie sie in der Bestandsliste auswählen und sie an eine neue Position innerhalb der Bestandsliste ziehen. Die neue Position kann ein Ordner für einen eigenständigen Host oder ein anderer Cluster sein.

Voraussetzungen

Bevor Sie einen Host aus einem Cluster entfernen können, müssen Sie alle virtuellen Maschinen, die auf dem Host ausgeführt werden, ausschalten oder unter Verwendung von vMotion auf einen neuen Host migrieren.

Vorgehensweise

- 1 Zeigen Sie auf einem mit einem vCenter Server-System verbundenen vSphere Client die Bestandsliste an.
- 2 Klicken Sie mit der rechten Maustaste auf das Symbol für den entsprechenden verwalteten Host im Bestandslistenbereich und wählen Sie im Popup-Menü **In den Wartungsmodus wechseln**.

Wenn nicht alle virtuellen Maschinen auf dem Host ausgeschaltet sind, wird der Host nicht in den Wartungsmodus versetzt.

Wenn sich der Host in einem DRS-aktivierten Cluster befindet, versucht DRS beim Eintritt des Hosts in den Wartungsmodus automatisch, mithilfe von vMotion alle eingeschalteten virtuellen Maschinen vom Host zu entfernen.

- 3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Das Bestätigungsdialogfeld fragt außerdem, ob Sie automatisch alle virtuellen Maschinen vom Host entfernen möchten, die nicht eingeschaltet sind. Dies ist hilfreich, wenn Sie möchten, dass diese virtuellen Maschinen mit einem Host innerhalb des Clusters registriert bleiben sollen.

Das Hostsymbol ändert sich, und dem Namen wird in Klammern der Begriff „Wartungsmodus“ hinzugefügt.

- 4 Wählen Sie den Host im Bestandslistenfenster aus, und ziehen Sie ihn mit der Maus an den neuen Speicherort.

Der Host kann in einen anderen Cluster oder in ein anderes Datacenter verschoben werden. Wenn die neue Position ausgewählt wurde, wird der Name des Clusters bzw. Datacenters mit einem blauen Feld umrandet.

vCenter Server verschiebt den Host an den neuen Speicherort.

- 5 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie im Popup-Menü **Wartungsmodus beenden**.
- 6 (Optional) Starten Sie die virtuellen Maschinen ggf. neu.

Entfernen eines verwalteten Hosts aus vCenter Server

Entfernen Sie einen verwalteten Host aus vCenter Server, um die Überwachung und Verwaltung des Hosts durch vCenter Server zu beenden.

Falls möglich, sollten Sie verwaltete Hosts entfernen, während diese verbunden sind. Durch das Entfernen von verwalteten Hosts mit getrennten Verbindungen wird der vCenter Server-Agent nicht vom verwalteten Host entfernt.

Voraussetzungen

Stellen Sie sicher, dass NFS-Mounts aktiv sind. Wenn keine NFS-Mounts reagieren, schlägt der Vorgang fehl.

Vorgehensweise

- 1 Zeigen Sie auf einem mit einem vCenter Server-System verbundenen vSphere-Client die Bestandsliste an.
- 2 (Optional) Wenn der Host Teil eines Clusters ist, muss er in den Wartungsmodus versetzt werden.
 - a Klicken Sie in der Bestandsliste mit der rechten Maustaste auf den verwalteten Host und wählen Sie im Popup-Menü **In den Wartungsmodus wechseln**.
 - b Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Das Hostsymbol ändert sich, und dem Namen wird in Klammern der Begriff „Wartungsmodus“ hinzugefügt.
- 3 Klicken Sie im Bestandslistenbereich mit der rechten Maustaste auf den entsprechenden Host und wählen Sie im Popup-Menü **Entfernen**.
- 4 Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um den verwalteten Host zu entfernen.

vCenter Server entfernt den verwalteten Host und die zugeordneten virtuellen Maschinen aus der vCenter Server-Umgebung. vCenter Server weist anschließend allen zugeordneten Prozessor- und Migrationslizenzen wieder den Status „Verfügbar“ zu.

Verwenden von vCenter-Zuordnungen

9

Eine vCenter-Zuordnung ist eine visuelle Darstellung Ihrer vCenter Server-Topologie. Zuordnungen zeigen die Beziehungen zwischen den für vCenter Server verfügbaren virtuellen und physischen Ressourcen.

Zuordnungen sind nur verfügbar, wenn der vSphere-Client mit einem vCenter Server-System verbunden ist.

Die Zuordnungen können Ihnen z. B. helfen, die am dichtesten gefüllten Cluster oder Hosts, die kritischsten Netzwerke und die genutzten Speichergeräte zu bestimmen. vCenter Server bietet die folgenden Zuordnungsansichten.

VM-Ressourcen	Zeigt Beziehungen an, in deren Mittelpunkt virtuelle Maschinen stehen.
Hostressourcen	Zeigt Beziehungen an, in deren Mittelpunkt Hosts stehen.
Datenspeicher-Ressourcen	Zeigt Beziehungen an, in deren Mittelpunkt Datenspeicher stehen.
vMotion-Ressourcen	Zeigt Hosts an, die für die vMotion-Migration verfügbar sind.

Sie können eine Zuordnungsansicht verwenden, um den Umfang einer Zuordnung zu begrenzen oder zu erweitern. Sie können alle Zuordnungsansichten mit Ausnahme von vMotion-Ressourcenzuordnungen anpassen. Wenn Sie über die Navigationsleiste auf Zuordnungsansichten zugreifen, stehen alle vCenter Server-Ressourcen zur Anzeige zur Verfügung. Wenn Sie die Registerkarte **Zuordnungen** eines ausgewählten Bestandslistenelements verwenden, werden nur Elemente angezeigt, die für dieses Element relevant sind. Für Bestandslistenelemente virtueller Maschinen ist die Ansicht „Reservierte Ressource für vMotion“ die einzige auf der Registerkarte **Zuordnungen** verfügbare Zuordnungsansicht.

Sie können eine Zuordnungsansicht durch Aktivieren oder Deaktivieren von Objekten im Bestandslistenfenster oder im Bereich **Beziehungen zuordnen** anpassen.

Durch Ziehen können Sie die Zuordnung neu positionieren (klicken Sie an beliebiger Stelle auf die Zuordnung, halten Sie die Maustaste gedrückt und ziehen Sie sie an die neue Position). Ein graues Feld im Übersichtsgebiet stellt den sichtbaren Abschnitt der gesamten Zuordnung dar und bewegt sich, während Sie die Zuordnung ziehen. Sie können die Größe des grauen Feldes ändern, um einen Abschnitt der Zuordnung zu vergrößern oder zu verkleinern.

Sie können auf ein beliebiges Objekt in einer Zuordnung doppelklicken, um zur **Zuordnung**-Registerkarte des Objekts zu wechseln (sofern für diesen Objekttyp eine **Zuordnung**-Registerkarte verfügbar ist).

Klicken Sie mit der rechten Maustaste auf ein beliebiges Objekt in einer Zuordnung, um auf das entsprechende Kontextmenü zuzugreifen.

Dieses Kapitel behandelt die folgenden Themen:

- „Festlegen der maximalen Anzahl an Map-Objekten“, auf Seite 90
- „Anzeigen von vCenter-Zuordnungen“, auf Seite 90

- „Drucken von vCenter-Zuordnungen“, auf Seite 90
- „Exportieren von vCenter-Zuordnungen“, auf Seite 90

Festlegen der maximalen Anzahl an Map-Objekten

In großen Umgebungen werden Zuordnungen möglicherweise nur langsam geladen und sind nicht leicht zu überschauen. Sie können die maximale Anzahl der angezeigten Objekt-Zuordnungen festlegen, damit diese schneller geladen werden und besser lesbar sind.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Registerkarte **Bearbeiten > Clienteinstellungen > Zuordnungen**.
- 2 Geben Sie die maximale Anzahl der Objekte an, für die Zuordnungen angezeigt werden sollen.
- 3 Klicken Sie auf **OK**.

Wenn ein Benutzer versucht, eine Zuordnung anzuzeigen, die über mehr Objekte als den angegebenen Grenzwert verfügt, erhält der Benutzer eine Meldung mit der Möglichkeit, die Anzeige der Zuordnung ab-zubrechen oder damit fortzufahren.

Anzeigen von vCenter-Zuordnungen

Ressourcenzuordnung ermöglichen Ihnen das Anzeigen der Beziehungen zwischen Hosts, Clustern und virtuellen Maschinen. Sie können eine Ressourcenzuordnung für ein ganzes vCenter Server-System oder für ein bestimmtes Objekt anzeigen, z. B. ein Datacenter oder Cluster. Maps für bestimmte Objekte zeigen nur die Objektbeziehungen für das Objekt an.

Vorgehensweise

- 1 Zeigen Sie das Objekt in der Bestandsliste an.
- 2 Wählen Sie das Objekt aus und klicken Sie auf die Registerkarte **Zuordnungen**.

Wählen Sie z. B. Ihr vCenter Server-System im Bestandslistenfenster aus, um die Ressourcenzuordnung für Ihr gesamtes vCenter Server-System anzuzeigen. Wählen Sie einen Host im Bestandslistenfenster aus, um seine Ressourcenzuordnung anzuzeigen.

Drucken von vCenter-Zuordnungen

Sie können die Ressourcenzuordnungen auf einem beliebigen Standarddrucker drucken.

Führen Sie diesen Vorgang auf der Registerkarte **Zuordnung** des vSphere-Clients aus.

Vorgehensweise

- 1 Wählen Sie **Datei > Zuordnungen drucken > Drucken**.
- 2 Wählen Sie den Drucker in der Liste **Name** aus.
- 3 Klicken Sie auf **Drucken**.

Exportieren von vCenter-Zuordnungen

Beim Exportieren einer Ressourcenzuordnung wird die Zuordnung in einer Image-Datei gespeichert.

Führen Sie diesen Vorgang auf der Registerkarte **Zuordnung** des vSphere-Clients aus.

Vorgehensweise

- 1 Zeigen Sie die Ressourcenzuordnung bei Bedarf an.

- 2 Wählen Sie **Datei > Exportieren > Zuordnungen exportieren**.
- 3 Navigieren Sie zum Speicherort, um die Datei zu speichern.
- 4 Geben Sie einen Namen für die Datei ein und wählen Sie ein Dateiformat.
- 5 Klicken Sie auf **Exportieren**.

Erstellen einer virtuellen Maschine im vSphere-Client

10

Virtuelle Maschinen sind die Schlüsselkomponenten in einer virtuellen Infrastruktur. Sie können zur Host-bestandsliste hinzuzufügende virtuelle Maschinen erstellen.

Wenn Sie eine virtuelle Maschine erstellen, verknüpfen Sie sie mit einem Datenspeicher und wählen Sie ein Betriebssystem und Optionen der virtuellen Hardware aus. Nach dem Einschalten der virtuellen Maschine verbraucht diese bei steigender Arbeitslast dynamisch Ressourcen oder sie gibt bei sinkender Arbeitslast Ressourcen dynamisch zurück.

Jede virtuelle Maschine verfügt über virtuelle Geräte, die die gleichen Funktionen bereitstellen wie physische Hardware. Eine virtuelle Maschine erhält CPU- und Arbeitsspeicherressourcen, Zugriff auf den Arbeitsspeicher und Netzwerkkonnektivität über den Host, auf dem sie ausgeführt wird.

Dieses Kapitel behandelt die folgenden Themen:

- [„Starten des Erstellungsvorgangs der virtuellen Maschine im vSphere-Client“](#), auf Seite 94
- [„Auswählen einer Konfigurationsoption für die neue virtuelle Maschine im vSphere-Client“](#), auf Seite 95
- [„Eingeben eines Namens und Speicherorts für die virtuelle Maschine im vSphere Client“](#), auf Seite 96
- [„Auswählen eines Hosts oder Clusters im vSphere Client“](#), auf Seite 96
- [„Auswählen eines Ressourcenpools im vSphere-Client“](#), auf Seite 97
- [„Auswählen eines Datenspeichers im vSphere Client“](#), auf Seite 97
- [„Auswählen einer Version für die virtuelle Maschine im vSphere Client“](#), auf Seite 97
- [„Auswählen eines Betriebssystems im vSphere Client“](#), auf Seite 98
- [„Auswählen der Anzahl der virtuellen CPUs im vSphere Client“](#), auf Seite 99
- [„Konfigurieren des virtuellen Arbeitsspeichers im vSphere Client“](#), auf Seite 99
- [„Konfigurieren von Netzwerken im vSphere-Client“](#), auf Seite 100
- [„Auswählen eines SCSI-Controllers im vSphere Client“](#), auf Seite 101
- [„Auswählen des Typs der virtuellen Festplatte“](#), auf Seite 102
- [„Abschließen der Erstellung virtueller Maschinen im vSphere-Client“](#), auf Seite 106

Starten des Erstellungsvorgangs der virtuellen Maschine im vSphere-Client

Mit dem Assistenten zum Erstellen neuer virtueller Maschinen können Sie eine virtuelle Maschine erstellen, die in der vSphere-Bestandsliste abgelegt wird. Sie können den Assistenten vom vSphere-Client aus öffnen.

Die Auswahl, die Sie im Assistenten zum Erstellen neuer virtueller Maschinen vornehmen, wird erst dann gespeichert, wenn Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden** klicken. Wenn Sie den Assistenten abbrechen, ohne alle Aufgaben ausgeführt zu haben, können Sie den Assistenten nicht von der Stelle aus fortsetzen, wo Sie ihn abgebrochen haben. Sie müssen eine neue Aufgabe zum Erstellen starten.

Sie können eine neue virtuelle Maschine in einem Datacenter-, Host-, Cluster-, Ressourcenpool- oder VM-Ordner erstellen.

Voraussetzungen

Stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

- **Host.Lokale Operationen.Virtuelle Maschine erstellen**
- **Virtuelle Maschine.Bestandsliste.Neu erstellen** für den Zielordner oder das Datacenter.
- **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen** für den Zielordner oder das Datacenter, wenn Sie eine neue Festplatte hinzufügen.
- **Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen** für den Zielordner oder das Datacenter, wenn Sie eine vorhandene Festplatte hinzufügen.
- **Virtuelle Maschine.Konfiguration.Raw-Gerät** für den Zielordner oder das Datacenter, wenn Sie RDM oder ein SCSI-Passthrough-Gerät verwenden.
- **Virtuelle Maschine.Konfiguration.Netzwerk**
- **Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen** auf dem Zielhost, -cluster oder -ressourcenpool.
- **Datenspeicher.Speicher zuteilen** auf dem Zieldatenspeicher oder Datenspeicherordner.
- **Netzwerk.Netzwerk zuweisen** für das Netzwerk, dem die virtuelle Maschine zugewiesen wird.

Vorgehensweise

- 1 Die Bestandslistenobjekte im vSphere-Client können unter Verwendung der Ansicht **Hosts und Cluster** oder der Ansicht **VMs und Vorlagen** angezeigt werden.
- 2 Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Neu > Virtuelle Maschine**.

Der Assistent zum Erstellen neuer virtueller Maschinen wird angezeigt.

Weiter

Wählen Sie die Konfigurationsoption **Typisch** oder **Benutzerdefiniert** im Assistenten zum Erstellen neuer virtueller Maschinen aus.

Auswählen einer Konfigurationsoption für die neue virtuelle Maschine im vSphere-Client

Die Option **Typisch** verkürzt den Erstellungsvorgang der virtuellen Maschine durch Überspringen von Optionen, deren Standardwerte Sie selten ändern müssen. Die Option **Benutzerdefiniert** bietet mehr Flexibilität und eine größere Auswahl.

Welche Informationen während der Erstellung der virtuellen Maschine eingegeben werden müssen, hängt von mehreren Beziehungen ab. Diese umfassen das Bestandslistenobjekt, in dem die virtuelle Maschine erstellt wird, die von Ihnen ausgewählte Anpassungspfadoption, den Datenspeicher, in dem sich die virtuelle Maschine und ihre Dateien befindet, sowie den Host oder Cluster, auf dem sie ausgeführt wird.

Wenn Sie die Konfiguration **Typisch** auswählen, entspricht die Hardwareversion der virtuellen Maschine standardmäßig der des Hosts, auf dem sie ausgeführt wird. Wenn Sie die Konfiguration **Benutzerdefiniert** wählen, können Sie die Vorgabe übernehmen oder eine vorherige Hardwareversion auswählen. Diese Konfiguration ist sinnvoll, wenn die Kompatibilität mit einer vorherigen Version des ESX/ESXi-Hosts aufrechterhalten werden muss.

Voraussetzungen

Stellen Sie für eine **typische** Konfiguration sicher, dass Sie die folgenden Informationen zur Hand haben:

- Name der virtuellen Maschine und Bestandslistenspeicherort.
- Standort, an dem die virtuelle Maschine ausgeführt werden soll (Cluster, Host, Ressourcenpool).
- Datenspeicher, in dem die Dateien der virtuellen Maschine gespeichert werden sollen.
- Gastbetriebssystem und -version.
- Parameter für die Größe der virtuellen Festplatte und Bereitstellungseinstellungen.

Stellen Sie sicher, dass Sie neben den Informationen für die **typische** Konfiguration auch über die folgenden Informationen für eine **benutzerdefinierte Konfiguration** verfügen:

- Version der virtuellen Maschine.
- Anzahl der CPUs und Arbeitsspeichergröße.
- Anzahl an Netzwerkkarten, Netzwerk mit dem verbunden werden soll, und Netzwerkadaptertypen.
- SCSI-Controller-Typ.
- Festplattentyp (neue Festplatte, vorhandene Festplatte, RDM oder keine Festplatte).

Vorgehensweise

- 1 Wählen Sie auf der Seite „Konfiguration“ des Assistenten Neue virtuelle Maschine eine Option zum Erstellen der virtuellen Maschine aus.
- 2 Klicken Sie auf **Weiter**.

Die Seite „Name und Speicherort“ wird angezeigt.

Weiter

Wählen Sie einen Namen und einen Standort für die virtuelle Maschine aus.

Eingeben eines Namens und Speicherorts für die virtuelle Maschine im vSphere Client

Der Name, den Sie eingeben, wird als Basisname der virtuellen Maschine in der Bestandsliste verwendet. Dieser Name wird auch als Name für die Dateien der virtuellen Maschine verwendet.

Die Länge des Namens kann maximal 80 Zeichen betragen. Zwischen Groß- und Kleinschreibung wird nicht unterschieden, sodass die Namen `meine_vm` und `Meine_VM` identisch sind.

Voraussetzungen

Stellen Sie sicher, dass Sie die entsprechenden Namenskonventionen verwenden.

Vorgehensweise

- 1 Geben Sie auf der Seite „Name und Speicherort“ des Assistenten Neue virtuelle Maschine einen Namen ein.
- 2 Wählen Sie einen Ordner oder den Root des Datencenters aus.

HINWEIS Diese Option ist nur dann verfügbar, wenn eine Verbindung mit einem vCenter Server-System besteht.

- 3 Klicken Sie auf **Weiter**.

Die Seite „Host / Cluster“ bzw. „Ressourcenpool“ wird geöffnet.

Auswählen eines Hosts oder Clusters im vSphere Client

Sie können die virtuelle Maschine in einem Cluster oder auf einem Host, der sich nicht in einem Cluster befindet, platzieren.

Ein Cluster ist eine Sammlung von ESXi-Hosts und verknüpften virtuellen Maschinen mit gemeinsam genutzten Ressourcen und einer gemeinsamen Verwaltungsoberfläche. Das Gruppieren von Hosts zu Clustern ermöglicht Ihnen das Aktivieren einer Vielzahl von optionalen Funktionen, die die Verfügbarkeit und die Flexibilität Ihrer Infrastruktur verbessern.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Host / Cluster“ des Assistenten Neue virtuelle Maschine den Host bzw. Cluster aus, in dem die virtuelle Maschine ausgeführt werden soll.

HINWEIS Die Seite „Host/Cluster“ ist nur dann verfügbar, wenn eine Verbindung mit einem vCenter Server-System besteht.

- 2 Klicken Sie auf **Weiter**.

Wenn auf dem Host Ressourcenpools konfiguriert sind, wird die Seite „Ressourcenpool“ geöffnet. Anderenfalls wird die Seite „Datenspeicher“ angezeigt.

Weiter

Wählen Sie einen Host oder Datenspeicher aus, in dem die virtuelle Maschine ausgeführt werden soll.

Auswählen eines Ressourcenpools im vSphere-Client

Mithilfe von Ressourcenpools können Sie Rechenressourcen innerhalb eines Hosts oder Clusters verwalten, indem Sie sie in einer sinnvollen Hierarchie anordnen. Virtuelle Maschinen und untergeordnete Ressourcenpools nutzen die Ressourcen der übergeordneten virtuellen Maschine gemeinsam.

Die Seite „Ressourcenpool“ wird nur angezeigt, wenn auf dem Host Ressourcenpools konfiguriert sind.

Vorgehensweise

- 1 Navigieren Sie auf der Seite „Ressourcenpool“ des Assistenten Neue virtuelle Maschine zu dem Ressourcenpool, in dem Sie die virtuelle Maschine ausführen möchten.
- 2 Wählen Sie den Ressourcenpool aus und klicken Sie auf **Weiter**.

Die virtuelle Maschine wird in den ausgewählten Ressourcenpool gestellt.

Weiter

Wählen Sie einen Datenspeicher aus, in dem die Dateien für die virtuelle Maschine gespeichert werden sollen.

Auswählen eines Datenspeichers im vSphere Client

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. Sie können Datenspeicher zum Speichern von ISO-Images und Vorlagen für virtuelle Maschinen verwenden.

Sie können aus den Datenspeichern auswählen, die Sie bereits auf dem Zielcluster oder -host konfiguriert haben.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Speicher“ des Assistenten für neue virtuelle Maschinen einen Datenspeicher aus, in dem Sie die Dateien der virtuellen Maschine speichern.
- 2 (Optional) Um Speicher-DRS für die virtuelle Maschine auszuschalten, wählen Sie die Option **Speicher-DRS für diese virtuelle Maschine deaktivieren** aus.
- 3 Klicken Sie auf **Weiter**.

Wenn Sie den Pfad für die Standardkonfiguration auswählen, wird die Seite „Gastbetriebssystem“ geöffnet. Wenn Sie den Pfad für eine benutzerdefinierte Konfiguration auswählen, wird die Seite „Version der virtuellen Maschine“ angezeigt.

Auswählen einer Version für die virtuelle Maschine im vSphere Client

Wenn der Host oder Cluster, den Sie für die virtuelle Maschine ausgewählt haben, mehrere Versionen virtueller VMware-Maschinen unterstützt, haben Sie die Möglichkeit, eine Version für die virtuelle Maschine auszuwählen.

Weitere Informationen zu VM- und Hostkompatibilitätsoptionen finden Sie unter [„VM-Hardwareversionen“](#), auf Seite 153.

Vorgehensweise

- 1 Wählen Sie eine VM-Hardwareversion aus.

Option	Beschreibung
Version 11 der virtuellen Maschine	Kompatibel mit ESXi-6.0-Hosts. Bietet die neuesten VM-Funktionen, darunter verbessertes beschleunigtes 3D-Grafikrendering. Empfohlen für virtuelle Maschinen, die nicht auf ESX/ESXi-4.x- und -5.x-Hosts migriert werden müssen.
Version 10 der virtuellen Maschine	Kompatibel mit ESXi-Hosts der Version 5.5 und höher. Empfohlen für virtuelle Maschinen, die nicht auf ESX/ESXi-4.x- und -5.1-Hosts migriert werden müssen.
Version 9 der virtuellen Maschine	Kompatibel mit ESXi-Hosts der Version 5.1 und höher. Empfohlen für virtuelle Maschinen, die nicht auf ESX/ESXi-4.x- und -5.0-Hosts migriert werden müssen.
Version 8 der virtuellen Maschine	Kompatibel mit ESXi-Hosts der Version 5.0 und höher. Empfohlen für virtuelle Maschinen, die nicht auf ESX/ESXi 4.x-Hosts migriert werden müssen.
Version 7 der virtuellen Maschine	Kompatibel mit ESX/ESXi-Hosts der Versionen 4, 4.x und höher. Empfohlen für die gemeinsame Speichernutzung oder virtuelle Maschinen mit ESX/ESXi Versionen 3.5 bis 4.1.
Version 4 der virtuellen Maschine	Kompatibel mit ESX/ESXi-Hosts der Versionen 4 und höher. Empfohlen für virtuelle Maschinen, die auf ESX/ESXi-4-Hosts ausgeführt werden müssen.

- 2 Klicken Sie auf **Weiter**.

Die Seite „Gastbetriebssystem“ wird geöffnet.

Weiter

Wählen Sie ein Gastbetriebssystem für die neue virtuelle Maschine aus.

Auswählen eines Betriebssystems im vSphere Client

Ihre Auswahl des Gastbetriebssystems bestimmt die unterstützten Geräte und die Anzahl der virtuellen CPUs, die der virtuellen Maschine zur Verfügung stehen.

Der Assistent Neue virtuelle Maschine installiert nicht das Gastbetriebssystem. Der Assistent wählt anhand dieser Informationen die richtigen Standardwerte aus, wie z. B. den benötigten Arbeitsspeicher.

Wenn Sie ein Gastbetriebssystem auswählen, ist je nach der Firmware, die das Betriebssystem unterstützt, entweder „BIOS“ oder „Extensible Firmware Interface“ (EFI) standardmäßig ausgewählt. Mac OS X Server-Gastbetriebssysteme unterstützen nur EFI. Wenn das Betriebssystem BIOS und EFI unterstützt, können Sie die Standardeinstellung auf der Registerkarte „Optionen“ des Editors „Eigenschaften der virtuellen Maschine“ ändern, nachdem Sie die virtuelle Maschine erstellt haben und bevor Sie das Gastbetriebssystem installieren. Wenn Sie EFI auswählen, können Sie kein Betriebssystem starten, das nur BIOS unterstützt, und umgekehrt.

WICHTIG Sie sollten die Firmware nach der Installation des Gastbetriebssystems nicht ändern.

Der Mac OS X-Server muss auf Apple-Hardware ausgeführt werden. Sie können einen Mac OS X-Server nicht einschalten, wenn er auf einer anderen Hardware ausgeführt wird.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Gastbetriebssystem“ des Assistenten Neue virtuelle Maschine eine Betriebssystemfamilie aus.

- 2 Wählen Sie im Dropdown-Menü ein Betriebssystem und eine Version aus und klicken Sie auf **Weiter**.
Wenn die auf dem Host verfügbaren Gesamtkerne, die maximale Anzahl virtueller CPUs, die von der Hardwareversion der virtuellen Maschine unterstützt wird, oder die maximal unterstützten CPUs auf dem Gastbetriebssystem 1 lautet, wird die Anzahl an CPUs der virtuellen Maschine auf 1 gesetzt und die Seite „Arbeitsspeicher“ geöffnet.
- 3 Wenn Sie **Anderes (32-Bit)** oder **Anderes (64-Bit)** ausgewählt haben, geben Sie in das Textfeld einen Namen für das Betriebssystem ein.
- 4 Klicken Sie auf **Weiter**.

Weiter

Sie können der virtuellen Maschine CPUs oder Arbeitsspeicher hinzufügen.

Auswählen der Anzahl der virtuellen CPUs im vSphere Client

Eine virtuelle Maschine kann über bis zu 128 virtuelle CPUs verfügen. Die Anzahl der lizenzierten CPUs auf dem Host, die Anzahl an CPUs, die das Gastbetriebssystem unterstützt, und die Hardwareversion der virtuellen Maschine bestimmen die Anzahl an virtuellen CPUs, die Sie hinzufügen können.

Mithilfe von VMware Virtual Symmetric Multiprocessing kann eine einzelne virtuelle Maschine mehrere physische Prozessoren gleichzeitig verwenden. Sie benötigen Virtual SMP zum Einschalten von virtuellen Maschinen mit mehreren Prozessoren.

Vorgehensweise

- 1 Wählen Sie auf der Seite „CPUs“ des Assistenten Neue virtuelle Maschine einen Wert aus dem Dropdown-Menü **Anzahl der virtuellen Sockets** aus.
- 2 Wählen Sie im Dropdown-Menü **Anzahl der Kerne pro Socket** einen Wert aus.
Die Gesamtzahl der Kerne wird durch Multiplizieren der Anzahl der Kerne pro Socket mit der Anzahl der virtuellen Sockets ermittelt. Die sich daraus ergebende Gesamtzahl der Kerne ist gleich oder geringer der Anzahl der logischen CPUs auf dem Host.
Die Gesamtzahl der Kerne wird angezeigt.
- 3 Klicken Sie auf **Weiter**.
Die Seite „Arbeitsspeicher“ wird geöffnet.

Weiter

Wählen Sie den Arbeitsspeicher für die virtuelle Maschine aus.

Konfigurieren des virtuellen Arbeitsspeichers im vSphere Client

Die Menge an Arbeitsspeicher, die Sie für eine virtuelle Maschine zuteilen, ist die Menge an Arbeitsspeicher, die das Gastbetriebssystem erkennt.

Die minimale Arbeitsspeichergröße beträgt 4 MB für virtuelle Maschinen, die die BIOS-Firmware verwenden. Virtuelle Maschinen, die die EFI-Firmware verwenden, benötigen mindestens 96 MB RAM. Bei weniger RAM können sie nicht eingeschaltet werden.

Die maximale Arbeitsspeichergröße einer virtuellen Maschine hängt vom physischen Arbeitsspeicher des Hosts und der Hardwareversion der virtuellen Maschine ab.

Wenn der Arbeitsspeicher der virtuellen Maschine größer als der Hostarbeitsspeicher ist, wird eine Auslagerung durchgeführt, die sich sehr stark auf die Leistung der virtuellen Maschine auswirken kann. Die Arbeitsspeichergröße muss ein Vielfaches von 4 MB sein. Der Maximalwert für beste Leistung stellt den Schwellenwert dar, bei dessen Überschreitung der physische Arbeitsspeicher des Hosts nicht ausreicht, um die virtuelle Maschine mit voller Geschwindigkeit auszuführen. Dieser Wert schwankt mit der Änderung der Bedingungen auf dem Host, wenn virtuelle Maschinen beispielsweise ein- bzw. ausgeschaltet werden.

Tabelle 10-1. Maximaler Arbeitsspeicher der virtuellen Maschine

Seit der Hostversion	Version der virtuellen Maschine	Maximale Arbeitsspeichergröße
ESXi 6.0	11	4080 GB
ESXi 5.5	10	1011 GB
ESXi 5.1	9	1011 GB
ESXi 5.0	8	1011 GB
ESX/ESXi 4.x	7	255 GB
ESX/ESXi 3.x	4	65,532 MB

Die ESXi-Hostversion gibt den Zeitpunkt an, seit dem die höhere Arbeitsspeichergröße unterstützt wird. Beispielsweise ist die Arbeitsspeichergröße einer virtuellen Maschine der Version 7, die auf ESXi 5.0 ausgeführt wird, auf 255 GB beschränkt.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Speicher“ des Assistenten Neue virtuelle Maschine die Größe des virtuellen Arbeitsspeichers aus.

Sie können den Schieberegler oder die nach oben und nach unten weisenden Pfeile zur Auswahl der Größe verwenden. Klicken Sie zum Aktivieren des Zugriffs auf die vordefinierte Standard- oder empfohlene Einstellung auf die bunten Dreiecke rechts von der Arbeitsspeicherleiste.

- 2 Klicken Sie auf **Weiter**.

Die Seite „Netzwerk“ wird geöffnet.

Weiter

Wählen Sie Netzwerkadapter für die virtuelle Maschine aus.

Konfigurieren von Netzwerken im vSphere-Client

Sie können die virtuellen Netzwerkkarten (NICs) wählen, die auf der virtuellen Maschine erstellt werden sollen, damit die virtuelle Maschine mit anderen Hosts und virtuelle Maschinen kommunizieren kann. Geben Sie für jede Netzwerkkarte den Netzwerk- und Adaptertyp an.



VORSICHT Da virtuelle Maschinen ihre physische Netzwerkhardware gemeinsam mit dem Host nutzen, ist ein versehentliches oder vorsätzliches Bridging zweier Netzwerke durch eine virtuelle Maschine möglich. Das Spanning Tree-Protokoll bietet keinen Schutz vor diesen Vorkommnissen.

Sie können während der Erstellung virtueller Maschinen lediglich vier Netzwerkkarten auswählen. Sie können weitere virtuelle Netzwerkkarten hinzufügen, indem Sie die Option **Einstellungen der virtuellen Maschine vor Fertigstellung bearbeiten** auf der Seite „Bereit zum Abschließen“ des Assistenten auswählen oder indem Sie die virtuelle Maschine nach deren Erstellung bearbeiten.

Weitere Informationen zu Netzwerken finden Sie in der *vSphere-Netzwerk-Dokumentation*.

Vorgehensweise

- 1 Wählen Sie aus dem Dropdown-Menü auf der Seite „Netzwerk“ des Assistenten zum Erstellen neuer virtueller Maschinen die Anzahl der zu verbindenden Netzwerkkarten aus.
- 2 Wählen Sie für jede Netzwerkkarte ein Netzwerk und einen Adaptertyp aus den Dropdown-Menüs aus.
In Abhängigkeit von Hostversion und Gastbetriebssystem wird nicht unbedingt eine Auswahl an Adaptertypen für jede virtuelle Netzwerkkarte angezeigt. In vielen Fällen wird nur ein Adaptertyp unterstützt. Falls mehrere Adaptertypen unterstützt werden, wird der für das Gastbetriebssystem empfohlene Typ standardmäßig ausgewählt.
- 3 (Optional) Klicken Sie auf **Beim Einschalten verbinden**, um die Netzwerkkarte zu verbinden, wenn die virtuelle Maschine eingeschaltet wird.
- 4 Klicken Sie auf **Weiter**, um einen SCSI-Controller hinzuzufügen.

Auswählen eines SCSI-Controllers im vSphere Client

Für den Zugriff auf virtuelle Festplatten verwendet eine virtuelle Maschine virtuelle SCSI-Controller. Jede virtuelle Festplatte, auf die eine virtuelle Maschine über einen der virtuellen SCSI-Controller zugreifen kann, befindet sich im VMware VMFS-Datenspeicher, im NFS-basierten Datenspeicher oder auf einer Raw-Festplatte. Die Auswahl des SCSI-Controller hat keinen Einfluss darauf, ob Sie als virtuelle Festplatte eine IDE- oder eine SCSI-Festplatte verwenden.

Der Assistent gibt den passenden Standard-Controller gemäß des auf der Seite „Gastbetriebssystem“ ausgewählten Gastbetriebssystems vor.

Die LSI Logic SAS- und VMware Paravirtual-Controller sind nur für virtuelle Maschinen mit der Hardwareversion 7 oder höher verfügbar. Detaillierte Informationen zu VMware Paravirtual-Controllern einschließlich Verwendungsbedingungen und Einschränkungen finden Sie unter [„Grundlegendes zu paravirtuellen SCSI-Controllern von VMware“](#), auf Seite 185.

Festplatten mit Snapshots weisen möglicherweise keinen Leistungsgewinn auf, wenn Sie an LSI Logic SAS- und LSI Logic Parallel-Adaptern betrieben werden.

Vorgehensweise

- 1 Übernehmen Sie die Vorgaben auf der Seite „SCSI-Controller“ des Assistenten Neue virtuelle Maschine oder wählen Sie einen SCSI-Controller-Typ aus.
 - BusLogic Parallel
 - LSI Logic Parallel
 - LSI Logic SAS
 - VMware Paravirtuell
- 2 Klicken Sie auf **Weiter**.
Die Seite „Festplatte auswählen“ wird geöffnet.

Weiter

Wählen Sie eine Festplatte aus, auf dem die Dateien und Daten des Gastbetriebssystems gespeichert werden sollen.

Auswählen des Typs der virtuellen Festplatte

Sie können eine virtuelle Festplatte erstellen, eine vorhandene virtuelle Festplatte verwenden oder Zuordnungen für Raw-Geräte (RDMs) erstellen, die Ihrer virtuellen Festplatte den direkten Zugriff auf das SAN ermöglichen. Eine virtuelle Festplatte besteht aus einer oder mehreren Dateien im Dateisystem, die dem Gastbetriebssystem als einzelne Festplatte angezeigt werden. Diese Festplatten können zwischen den einzelnen Servern verschoben werden.

Mit dem Assistenten Virtuelle Maschine erstellen können Sie virtuelle Festplatten während des Erstellens virtueller Maschinen hinzufügen. Um später Festplatten hinzuzufügen, wählen Sie die Option **Keine Festplatte erstellen** aus und verwenden Sie den Assistenten zum Hinzufügen von Hardware im Dialogfeld „Eigenschaften der virtuellen Maschine“.

HINWEIS Sie können virtuelle Festplatten einem anderen Controller-Typ nicht neu zuweisen.

Sie können aus den folgenden Optionen auswählen:

- [Erstellen einer virtuellen Festplatte im vSphere Client](#) auf Seite 102
Wenn Sie eine virtuelle Festplatte erstellen, können Sie Festplatteneigenschaften wie z. B. Größe, Format, Clusterfunktionen usw. festlegen.
- [Verwenden einer vorhandenen virtuellen Festplatte im vSphere-Client](#) auf Seite 104
Sie können eine vorhandene Festplatte verwenden, die mit einem Betriebssystem oder anderen VM-Daten konfiguriert ist. Somit können Sie die virtuelle Festplatte uneingeschränkt von einer virtuellen Maschine zur anderen virtuellen Maschine verschieben und nutzen.
- [Hinzufügen einer RDM-Festplatte zu einer virtuellen Maschine im vSphere-Client](#) auf Seite 104
Sie können die Daten der virtuellen Maschine direkt auf einer SAN LUN anstatt in einer virtuellen Festplattendatei speichern. Diese Fähigkeit ist nützlich, wenn Sie in den virtuellen Maschinen Anwendungen ausführen, die die physischen Merkmale des Speichergeräts erkennen müssen. Das Zuordnen einer SAN-LUN ermöglicht Ihnen die Verwendung vorhandener SAN-Befehle für die Speicherverwaltung der Festplatte.

Erstellen einer virtuellen Festplatte im vSphere Client

Wenn Sie eine virtuelle Festplatte erstellen, können Sie Festplatteneigenschaften wie z. B. Größe, Format, Clusterfunktionen usw. festlegen.

Detaillierte Informationen zu Festplattentypen finden Sie in der Dokumentation zum *vSphere-Speicher*.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Festplatte erstellen“ des Assistenten Neue virtuelle Maschine die Festplattengröße aus.

Sie können später im Eigenschaftendialogfeld der virtuellen Maschine die Größe der Festplatte erhöhen oder weitere Festplatten hinzufügen.

- 2 Wählen Sie das Format für die Festplatten der virtuellen Maschine aus und klicken Sie auf **Weiter**.

Option	Aktion
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. 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.
Thick-Provision Eager-Zeroed	Erstellen Sie eine Thick-Festplatte, die Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten während des Anlegens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.
Thin Provision	Verwendet das Format „Schnell bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die schnell bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.

- 3 Wählen Sie einen Speicherort aus, an dem die Dateien der virtuellen Festplatte gespeichert werden sollen, und klicken Sie auf **Weiter**.

Option	Beschreibung
Zusammen mit virtueller Maschine speichern	Speichert die Dateien mit der Konfiguration und anderen Dateien der virtuellen Maschine. Diese Option erleichtert die Dateiverwaltung.
Datenspeicher oder Datenspeicher-Cluster angeben	Speichert die Datei getrennt von anderen Dateien der virtuellen Maschine.

Die Seite „Erweiterte Optionen“ wird geöffnet.

- 4 Akzeptieren Sie den Standardknoten oder wählen Sie einen anderen Knoten des virtuellen Geräts aus.

In der Regel können Sie den Standardgeräteknoden übernehmen. Bei einer Festplatte eignet sich ein vom Standard abweichender Geräteknoden zur Steuerung der Startreihenfolge oder bei Verwendung verschiedener SCSI-Controller-Typen. Beispiel: Sie möchten von einem LSI Logic-Controller starten und sich mit einer anderen virtuellen Maschine eine Datenplatte teilen. Diese virtuelle Maschine verwendet einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist.

- 5 (Optional) Um die Art zu ändern, wie sich Snapshots auf Festplatten auswirken, klicken Sie auf **Unabhängig** und wählen Sie eine Option aus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

- 6 Klicken Sie auf **Weiter**.

Ihre Änderungen werden aufgezeichnet und die Seite „Bereit zum Abschließen“ wird geöffnet.

Weiter

Prüfen Sie Ihre Auswahl für die virtuelle Maschine auf der Seite „Bereit zum Abschließen“.

Verwenden einer vorhandenen virtuellen Festplatte im vSphere-Client

Sie können eine vorhandene Festplatte verwenden, die mit einem Betriebssystem oder anderen VM-Daten konfiguriert ist. Somit können Sie die virtuelle Festplatte uneingeschränkt von einer virtuellen Maschine zur anderen virtuellen Maschine verschieben und nutzen.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Vorhandene Festplatte auswählen“ des Assistenten Neue virtuelle Maschine eine virtuelle Festplatte aus und klicken Sie auf **OK**. Klicken Sie anschließend auf **Weiter**.
- 2 Akzeptieren Sie den Standardknoten oder wählen Sie einen anderen Knoten des virtuellen Geräts aus.

In der Regel können Sie den Standardgeräteknoten übernehmen. Bei einer Festplatte eignet sich ein vom Standard abweichender Geräteknoten zur Steuerung der Startreihenfolge oder bei Verwendung verschiedener SCSI-Controller-Typen. Beispiel: Sie möchten von einem LSI Logic-Controller starten und sich mit einer anderen virtuellen Maschine eine Datenplatte teilen. Diese virtuelle Maschine verwendet einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist.
- 3 (Optional) Um die Art zu ändern, wie sich Snapshots auf Festplatten auswirken, klicken Sie auf **Unabhängig** und wählen Sie eine Option aus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

- 4 Klicken Sie auf **Weiter**.

Ihre Änderungen werden aufgezeichnet und die Seite „Bereit zum Abschließen“ wird geöffnet.

Weiter

Überprüfen Sie die Konfiguration der virtuellen Maschine.

Hinzufügen einer RDM-Festplatte zu einer virtuellen Maschine im vSphere-Client

Sie können die Daten der virtuellen Maschine direkt auf einer SAN LUN anstatt in einer virtuellen Festplattendatei speichern. Diese Fähigkeit ist nützlich, wenn Sie in den virtuellen Maschinen Anwendungen ausführen, die die physischen Merkmale des Speichergeräts erkennen müssen. Das Zuordnen einer SAN-LUN ermöglicht Ihnen die Verwendung vorhandener SAN-Befehle für die Speicherverwaltung der Festplatte.

Wenn Sie einem VMFS-Volume eine LUN zuordnen, erstellt vCenter Server eine Datei mit der Raw-Device-Zuordnung (RDM), die auf die Raw-LUN weist. Durch Kapseln von Festplatteninformationen in einer Datei kann vCenter Server die LUN sperren, sodass zu einem gegebenen Zeitpunkt nur eine virtuelle Maschine darauf schreiben kann. Details zu RDM finden Sie in der Dokumentation *vSphere-Speicher*.

Zwar hat die RDM-Datei die Erweiterung `.vmdk`, die Datei enthält jedoch nur beschreibende Festplatteninformationen für die LUN-Zuordnung auf dem ESXi-Host. Die eigentlichen Daten werden unter Verwendung der LUN gespeichert.

Sie können die Raw-Gerätezuordnung als Ausgangsfestplatte für eine neue virtuelle Maschine erstellen oder sie einer vorhandenen virtuellen Maschine hinzufügen. Beim Erstellen der RDM geben Sie die zuzuordnende LUN und den Datenspeicher an, in dem die RDM abgelegt werden soll.

HINWEIS Sie können eine virtuelle Maschine nicht anhand einer Vorlage bereitstellen und ihre Daten auf einer LUN speichern. Sie können nur ihre Daten in einer virtuellen Festplattendatei speichern.

Vorgehensweise

- 1 Wählen Sie auf der Seite „Festplatte auswählen“ des Assistenten zum Erstellen neuer virtueller Maschinen die Option **Raw-Gerätezuordnung** aus und klicken Sie auf **Weiter**.
- 2 Wählen Sie in der Liste der SAN-Festplatten bzw. LUNs eine LUN aus, auf die die virtuelle Maschine direkt zugreifen soll, und klicken Sie auf **Weiter**.
- 3 Wählen Sie einen Datenspeicher für die LUN-Zuordnungsdatei aus und klicken Sie auf **Weiter**.

Sie können die Raw-Gerätezuordnungsdatei im selben Datenspeicher ablegen, in dem sich die Konfigurationsdatei der virtuellen Maschine befindet, oder einen anderen Datenspeicher auswählen.

HINWEIS Um vMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die RDM-Dateien der virtuellen Maschinen im selben Datenspeicher befinden. Bei aktivierter NPIV ist Storage vMotion bzw. vMotion zwischen Datenspeichern nicht möglich.

- 4 Wählen Sie einen Kompatibilitätsmodus und klicken Sie auf **Weiter**.

Option	Beschreibung
Physisch	Ermöglicht es dem Gastbetriebssystem, auf die Hardware direkt zuzugreifen. Der physische Kompatibilitätsmodus bietet sich an, wenn Sie SAN-fähige Anwendungen in der virtuellen Maschine einsetzen. Eine virtuelle Maschine, die für einen physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung konfiguriert ist, kann jedoch weder geklont noch in eine Vorlage umgewandelt noch migriert werden, wenn für die Migration die Festplatte kopiert werden muss.
Virtuell	Ermöglicht es der RDM, sich wie eine virtuelle Festplatte zu verhalten, so dass Sie Funktionen wie 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.

- 5 Akzeptieren Sie den Standardknoten oder wählen Sie einen anderen Knoten des virtuellen Geräts aus.

In der Regel können Sie den Standardgeräteknoten übernehmen. Bei einer Festplatte eignet sich ein vom Standard abweichender Geräteknoten zur Steuerung der Startreihenfolge oder bei Verwendung verschiedener SCSI-Controller-Typen. Beispiel: Sie möchten von einem LSI Logic-Controller starten und sich mit einer anderen virtuellen Maschine eine Datenplatte teilen. Diese virtuelle Maschine verwendet einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist.

- 6 (Optional) Um die Art zu ändern, wie sich Snapshots auf Festplatten auswirken, klicken Sie auf **Unabhängig** und wählen Sie eine Option aus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

- 7 Klicken Sie auf **Weiter**.

Ihre Änderungen werden aufgezeichnet und die Seite „Bereit zum Abschließen“ wird geöffnet.

Weiter

Überprüfen Sie die Konfiguration der virtuellen Maschine.

Abschließen der Erstellung virtueller Maschinen im vSphere-Client

Auf der Seite „Bereit zum Abschließen“ können Sie die Konfiguration überprüfen, die Sie für die virtuelle Maschine vorgenommen haben. Sie können vorhandene Einstellungen ändern, Ressourcen konfigurieren, Hardware hinzufügen und vieles mehr.

Sie können vor oder nach dem Beenden des Assistenten weitere Einstellungen der virtuellen Maschine konfigurieren.

Vorgehensweise

- 1 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ des Assistenten zum Erstellen neuer virtueller Maschinen die Konfigurationseinstellungen für die virtuelle Maschine.
- 2 (Optional) Wählen Sie **Einstellungen der VM vor Fertigstellung bearbeiten** und klicken Sie auf **Fortfahren**.

Der Editor „Eigenschaften virtueller Maschinen“ wird geöffnet. Wenn Sie Ihre Änderungen vorgenommen und auf **Beenden** geklickt haben, werden sowohl der Editor „Eigenschaften virtueller Maschinen“ als auch der Assistent zum Erstellen neuer virtueller Maschinen geschlossen. Sie können erst dann zurückgehen, um die Einstellungen des Assistenten zu überprüfen, wenn Sie auf **Abbrechen** geklickt haben.

- 3 (Optional) Klicken Sie auf **Abbrechen**, um zurückzugehen und die Einstellungen des Assistenten zu überprüfen.
- 4 Klicken Sie auf **Beenden**, um die Erstellungsaufgabe abzuschließen und den Assistenten zu schließen.

Die virtuelle Maschine wird im vSphere-Client in der **Bestandslistenansicht** angezeigt.

Weiter

Bevor Sie die neue virtuelle Maschine verwenden können, müssen Sie die virtuelle Festplatte partitionieren und formatieren sowie ein Gastbetriebssystem und VMware Tools installieren. In der Regel wird die Partitionierung und Formatierung der virtuellen Festplatte von dem Installationsprogramm des Betriebssystems durchgeführt.

Arbeiten mit Vorlagen und Klonen im vSphere-Client

11

Bei einem Klon handelt es sich um eine Kopie einer virtuellen Maschine. Eine Vorlage ist eine Master-Kopie einer virtuellen Maschine, die zur Erstellung vieler Klons verwendet werden kann.

Beim Klonen einer virtuellen Maschine wird eine Kopie der gesamten virtuellen Maschine, d. h., mit den Einstellungen, den konfigurierten virtuellen Geräten, der installierten Software und anderen Inhalten der VM-Festplatten, erstellt. Optional können Sie das Gastbetriebssystem anpassen und einige Eigenschaften des Klons, z. B. den Computernamen und die Netzwerkeinstellungen, ändern.

Durch das Klonen einer virtuellen Maschine können Sie Zeit einsparen, wenn Sie mehrere ähnliche virtuelle Maschinen bereitstellen möchten. Nachdem Sie zunächst auf einer virtuellen Maschine die entsprechende Software erstellt, konfiguriert und installiert haben, können Sie diese Maschine anschließend mehrmals klonen, statt jede Maschine einzeln zu erstellen und zu konfigurieren.

Wenn eine virtuelle Maschine sehr häufig geklont werden soll, machen Sie diese virtuelle Maschine zu einer Vorlage. Eine Vorlage ist eine Master-Kopie einer virtuellen Maschine, die zur Erstellung und Bereitstellung virtueller Maschinen verwendet werden kann. Vorlagen können weder eingeschaltet noch bearbeitet werden und sind schwieriger zu verändern als gewöhnliche virtuelle Maschinen. Eine Vorlage ist eine sicherere Methode zum Beibehalten der Konfiguration einer virtuellen Maschine, die mehrere Male bereitgestellt wird.

Die durch Klonen oder anhand einer Vorlage bereitgestellten virtuellen Maschinen sind unabhängig von der ursprünglichen Maschine bzw. der Vorlage. Änderungen, die Sie an der ursprünglichen virtuellen Maschine oder Vorlage vornehmen, werden in der geklonten virtuellen Maschine nicht übernommen und umgekehrt.

Dieses Kapitel behandelt die folgenden Themen:

- [„Klonen einer virtuellen Maschine im vSphere Client“](#), auf Seite 108
- [„Erstellen einer geplanten Aufgabe zum Klonen einer virtuellen Maschine im vSphere Client“](#), auf Seite 110
- [„Erstellen einer Vorlage im vSphere-Client“](#), auf Seite 111
- [„Bereitstellen einer virtuellen Maschine anhand einer Vorlage im vSphere-Client“](#), auf Seite 114
- [„Ändern des Vorlagennamens im vSphere-Client“](#), auf Seite 117
- [„Löschen von Vorlagen“](#), auf Seite 117
- [„Konvertieren einer Vorlage in eine virtuelle Maschine im vSphere-Client“](#), auf Seite 119

Klonen einer virtuellen Maschine im vSphere Client

Beim Klonen einer virtuellen Maschine wird ein Duplikat der virtuellen Maschine mit derselben Konfiguration und installierten Software wie das Original erstellt.

Optional können Sie das Gastbetriebssystem des Klon anpassen und den Namen der virtuellen Maschine, die Netzwerkeinstellungen und andere Eigenschaften ändern. Hierdurch können Sie Konflikte vermeiden, die auftreten können, wenn eine virtuelle Maschine und ein Klon mit denselben Gastbetriebseinstellungen gleichzeitig bereitgestellt werden.

Voraussetzungen

- Zum Klonen einer virtuellen Maschine müssen Sie mit vCenter Server verbunden sein. Das Klonen von virtuellen Maschinen ist nicht möglich, wenn Sie sich mit einem ESXi-Host direkt verbinden.
- Wenn das Gastbetriebssystem der virtuellen Maschine angepasst werden soll, überprüfen Sie, dass Ihr Gastbetriebssystem die Anpassungsanforderungen erfüllt. Siehe [„Anforderungen für die Anpassung des Gastbetriebssystems“](#), auf Seite 121.
- Wenn Sie eine Anpassungsspezifikation verwenden möchten, müssen Sie zunächst eine Anpassungsspezifikation erstellen oder importieren.
- Wenn der Hostname oder die IP-Adresse für die neue virtuelle Maschine mithilfe eines benutzerdefinierten Skripts generiert werden soll, konfigurieren Sie zunächst das Skript. Siehe [„Konfigurieren eines Skripts für die Generierung von Computernamen und IP-Adressen bei der Anpassung des Gastbetriebssystems im vSphere-Client“](#), auf Seite 122.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Klonen**.
- 2 Geben Sie den Namen einer virtuellen Maschine ein, wählen Sie einen Speicherort aus, und klicken Sie auf **Weiter**.
- 3 Wählen Sie den Host oder Cluster aus, auf dem die neue virtuelle Maschine ausgeführt werden soll.

Option	Aktion
Ausführen der virtuellen Maschine auf einem eigenständigen Host.	Wählen Sie den Host aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster mit automatisierter DRS-Platzierung.	Wählen Sie den Cluster aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster ohne automatisierter DRS-Platzierung.	a Wählen Sie den Cluster aus und klicken Sie auf Weiter .
	b Wählen Sie einen Host im Cluster aus und klicken Sie auf Weiter .

- 4 Wählen Sie einen Ressourcenpool aus, in dem die virtuelle Maschine ausgeführt werden soll, und klicken Sie auf **Weiter**.

- 5 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Maschine speichern möchten.

Option	Aktion
Alle Dateien der virtuellen Maschine am selben Speicherort auf einem Datenspeicher speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Alle Dateien der virtuellen Maschine in demselben Datenspeicher-Cluster speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Speichern Sie die Konfigurationsdateien der virtuellen Maschine und die Festplatte an verschiedenen Orten.	<p>a Klicken Sie auf Erweitert.</p> <p>b Klicken Sie für die Konfigurationsdatei der virtuellen Maschine und für jede virtuelle Festplatte auf Durchsuchen und wählen Sie einen Datenspeicher oder Datenspeicher-Cluster aus.</p> <p>c Klicken Sie auf Weiter.</p>

- 6 Wählen Sie das Format für die Festplatten der virtuellen Maschine aus.

Option	Aktion
Format wie Quelle	Verwendet das Format der virtuellen Quellmaschine.
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. 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.
Thick-Provision Eager-Zeroed	Erstellen Sie eine Thick-Festplatte, die Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Format „Thick-Provision Lazy-Zeroed“ werden die auf dem physischen Gerät verbleibenden Daten während des Anlegens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen.
Thin Provision	Verwendet das Format „Schnell bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die schnell bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.

- 7 Wählen Sie eine Option für die benutzerdefinierte Anpassung des Gastbetriebssystems aus.

Option	Beschreibung
Keine Anpassung	Wählen Sie Keine Anpassung und klicken Sie auf Weiter . Es werden keine Änderungen an den Einstellungen des Gastbetriebssystems vorgenommen. Alle Einstellungen sind mit den Einstellungen der virtuellen Quellmaschine identisch.
Mit dem Assistenten für benutzerdefinierte Anpassungen anpassen	Öffnet den Assistenten für benutzerdefinierte Anpassungen, sodass Sie Anpassungsoptionen für das Gastbetriebssystem auswählen können. Wählen Sie diese Option und klicken Sie auf Weiter , um den Assistenten für benutzerdefinierte Anpassungen zu öffnen. <ul style="list-style-type: none"> ■ Informationen zum Anpassen eines Linux-Gastbetriebssystems finden Sie unter „Anpassen von Linux beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 126. ■ Informationen zum Anpassen eines Windows-Gastbetriebssystems finden Sie unter „Anpassen von Windows beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 123.
Mithilfe einer vorhandenen Anpassungsspezifikation anpassen	Verwendet für die benutzerdefinierte Anpassung des Gastbetriebssystems die Einstellungen in einer gespeicherten Anpassungsspezifikation. <ol style="list-style-type: none"> Wählen Sie Mithilfe einer vorhandenen Anpassungsspezifikation anpassen. Wählen Sie die gewünschte Anpassungsspezifikation aus. (Optional) Wählen Sie die Option Sie können den Assistenten für benutzerdefinierte Anpassungen verwenden, um die Spezifikation vor der Bereitstellung vorübergehend zu ändern, wenn die Spezifikation nur für diese Bereitstellung geändert werden soll. Klicken Sie auf Weiter.

- 8 Überprüfen Sie Ihre Auswahl und wählen Sie, ob Sie die virtuelle Maschine einschalten oder die Einstellungen der VM bearbeiten möchten.

Option	Aktion
Diese virtuelle Maschine nach dem Erstellen einschalten.	Wählen Sie diese Option und klicken Sie auf Beenden . Die virtuelle Maschine wird eingeschaltet, wenn der Bereitstellungsvorgang abgeschlossen ist.
Virtuelle Hardware bearbeiten	<ol style="list-style-type: none"> Wählen Sie diese Option und klicken Sie auf Fortfahren. Nehmen Sie die Änderungen vor und klicken Sie auf OK.

Die geklonte virtuelle Maschine wird bereitgestellt. Sie können die virtuelle Maschine erst verwenden oder bearbeiten, nachdem das Klonen abgeschlossen ist. Dies kann einige Minuten dauern, falls eine virtuelle Festplatte erstellt werden muss. Sie können das Klonen jederzeit vor der benutzerdefinierten Anpassung abbrechen.

Erstellen einer geplanten Aufgabe zum Klonen einer virtuellen Maschine im vSphere Client

Bei diesem Vorgang erstellen Sie eine geplante Aufgabe zum Klonen einer virtuellen Maschine.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Klicken Sie auf der Seite „Home“ auf **Geplante Aufgaben**.

- 2 Wählen Sie **Datei > Neu > Geplante Aufgabe** oder klicken Sie auf **Neu**.

Das Dialogfeld **Zu planende Aufgabe auswählen** wird angezeigt.

- 3 Wählen Sie aus dem Dropdown-Menü die Option **Klonen einer virtuellen Maschine** und klicken Sie auf **OK**.

Der Assistent zum Klonen einer virtuellen Maschine wird geöffnet.

- 4 Wählen Sie die zu klonende virtuelle Maschine aus und klicken Sie auf **Weiter**.

- 5 Befolgen Sie im Assistenten die gleichen Schritte wie in der vorherigen Aufgabe, bei der Sie eine virtuelle Maschine geklont haben.

- 6 Geben Sie im Textfeld einen Namen und die Aufgabenbeschreibung ein.

- 7 Wählen Sie die Häufigkeit der Aufgabe aus.

- 8 Wählen Sie **Jetzt** oder **Später**. Wenn Sie **Später** auswählen, geben Sie die Zeit und das Datum für die Bereitstellung der virtuellen Maschine ein, und klicken Sie auf **Weiter**.

Um den Kalender anzuzeigen, klicken Sie auf **Später** und anschließend auf den Dropdown-Pfeil, um aus dem angezeigten Kalender ein Datum auszuwählen. Das aktuelle Datum wird durch einen roten Kreis, das geplante Ausführungsdatum wird durch einen dunklen Kreis gekennzeichnet.

- 9 Überprüfen Sie die Informationen im Fenster „Bereit zum Abschließen“ der neuen virtuellen Maschine und klicken Sie auf **Beenden**.

Optional können Sie das Kontrollkästchen aktivieren, um die neue virtuelle Maschine nach der Erstellung einzuschalten.

vCenter Server fügt die neue Aufgabe der Liste der geplanten Aufgaben hinzu und startet diese zur angegebenen Zeit. Zum Fälligkeitszeitpunkt der Aufgabe überprüft vCenter Server zunächst, ob der Benutzer, der die Aufgabe erstellt hat, noch immer über die Berechtigung zum Ausführen der Aufgabe verfügt. Wenn die festgelegten Berechtigungen nicht ausreichen, protokolliert vCenter Server eine Meldung, und die Aufgabe wird nicht ausgeführt.

Erstellen einer Vorlage im vSphere-Client

Eine Vorlage ist ein Master-Image einer virtuellen Maschine, das zur Bereitstellung vieler virtueller Maschinen verwendet werden kann.

Sie können eine Vorlage erstellen, indem Sie eine vorhandene virtuelle Maschine in eine Vorlage konvertieren, eine virtuelle Maschine in eine Vorlage klonen oder eine andere Vorlage klonen.

Konvertieren einer virtuellen Maschine in eine Vorlage im vSphere-Client

Sie können eine virtuelle Maschine direkt in eine Vorlage konvertieren, anstatt eine Kopie durch Klonen zu erstellen.

Nachdem eine virtuelle Maschine in eine Vorlage konvertiert wurde, können Sie die Vorlage weder bearbeiten noch einschalten. Sie müssen sie erst wieder in eine virtuelle Maschine zurückkonvertieren.

Voraussetzungen

- Zum Konvertieren einer virtuellen Maschine in eine Vorlage müssen Sie mit vCenter Server verbunden sein. Das Erstellen von Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit dem ESXi-Host verbunden ist.
- Bevor Sie eine virtuelle Maschine in eine Vorlage konvertieren, müssen Sie sie in der Bestandsliste auswählen und ausschalten.

Vorgehensweise

- ◆ Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Vorlage > In Vorlage konvertieren**.

vCenter Server kennzeichnet die virtuelle Maschine als Vorlage und zeigt die Aufgabe im Fenster „Aktuelle Aufgaben“ an.

Klonen einer virtuellen Maschine in eine Vorlage im vSphere Client

Beim Klonen einer virtuellen Maschine in eine Vorlage wird eine Kopie der Vorlage der virtuellen Maschine erstellt und die ursprüngliche virtuelle Maschine wird am Speicherort belassen.

Voraussetzungen

Zum Klonen einer virtuellen Maschine in eine Vorlage müssen Sie mit vCenter Server verbunden sein. Das Erstellen von Vorlagen ist nicht möglich, wenn Sie sich mit einem ESXi-Host direkt verbinden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Vorlage > In Vorlage klonen**.
- 2 Weisen Sie der neuen Vorlage einen Namen zu, wählen Sie einen Speicherort in der Bestandsliste aus, und klicken Sie dann auf **Weiter**.
- 3 Übergehen Sie die Seite zur Angabe des Zielspeicherorts und klicken Sie auf **Weiter**.
- 4 Geben Sie an, in welchem Format die virtuellen Festplatten der Vorlage gespeichert werden sollen, und klicken Sie auf **Weiter**.

Option	Aktion
Format wie Quelle	Verwendet das Format der virtuellen Quellmaschine.
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. 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.
Thick-Provision Eager-Zeroed	Erstellen Sie eine Thick-Festplatte, die Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Format „Thick-Provision Lazy-Zeroed“ werden die auf dem physischen Gerät verbleibenden Daten während des Anlegens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen.
Thin Provision	Verwendet das Format „Schnell bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die schnell bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.

- 5 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Maschine speichern möchten.

Option	Aktion
Alle Dateien der virtuellen Maschine am selben Speicherort auf einem Datenspeicher speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Alle Dateien der virtuellen Maschine in demselben Datenspeicher-Cluster speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Speichern Sie die Konfigurationsdateien der virtuellen Maschine und die Festplatte an verschiedenen Orten.	<p>a Klicken Sie auf Erweitert.</p> <p>b Klicken Sie für die Konfigurationsdatei der virtuellen Maschine und für jede virtuelle Festplatte auf Durchsuchen und wählen Sie einen Datenspeicher oder Datenspeicher-Cluster aus.</p> <p>c Klicken Sie auf Weiter.</p>

- 6 Klicken Sie auf **Beenden**.

vCenter Server zeigt den Bestandslistenbereich **Aufgaben** mit Referenzinformation an und fügt die geklonte Vorlage der Liste im Informationsfenster hinzu.

Klonen einer Vorlage im vSphere-Client

Klonen Sie eine Vorlage, um eine Kopie der Vorlage zu erstellen.

Voraussetzungen

Zum Klonen einer Vorlage müssen Sie mit vCenter Server verbunden sein. Das Erstellen von Vorlagen ist nicht möglich, wenn Sie sich mit einem ESXi-Host direkt verbinden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Klonen**.
- 2 Weisen Sie der neuen Vorlage einen eindeutigen Namen und eine Beschreibung zu und klicken Sie dann auf **Weiter**.
- 3 Wählen Sie den Host oder Cluster aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie einen Datenspeicher für die Vorlage aus und klicken Sie auf **Weiter**.
- 5 Geben Sie an, in welchem Format die virtuellen Festplatten der Vorlage gespeichert werden sollen.

Option	Aktion
Format wie Quelle	Verwendet das Format der virtuellen Quellmaschine.
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. 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.

Option	Aktion
Thick-Provision Eager-Zeroed	Erstellen Sie eine Thick-Festplatte, die Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Format „Thick-Provision Lazy-Zeroed“ werden die auf dem physischen Gerät verbleibenden Daten während des Anlegens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen.
Thin Provision	Verwendet das Format „Schnell bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die schnell bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.

- 6 Klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Angaben für die Vorlage und klicken Sie auf **Beenden**.

Sie können die neue Vorlage erst verwenden, wenn der Klonvorgang abgeschlossen ist.

vCenter Server fügt die geklonte Vorlage zur Liste der Vorlagen auf der Registerkarte **Virtuelle Maschinen** hinzu.

Bereitstellen einer virtuellen Maschine anhand einer Vorlage im vSphere-Client

Wenn Sie eine virtuelle Maschine anhand einer Vorlage bereitstellen, ist die neue virtuelle Maschine eine Kopie der Vorlage. Die neue virtuelle Maschine verfügt über dieselbe virtuelle Hardware und installierte Software sowie dieselben Eigenschaften wie die Vorlage.

Voraussetzungen

- Stellen Sie sicher, dass eine Verbindung mit dem vCenter Server besteht. Die Arbeit mit Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit dem ESXi-Host verbunden ist.
- Zum Bereitstellen einer virtuellen Maschine anhand einer Vorlage muss eine Verbindung zu vCenter Server bestehen. Die Bereitstellung anhand einer Vorlage ist nicht möglich, wenn der vSphere-Client direkt mit einem ESXi-Host verbunden ist.
- Wenn das Gastbetriebssystem der virtuellen Maschine angepasst werden soll, überprüfen Sie, dass Ihr Gastbetriebssystem die Anpassungsanforderungen erfüllt. Weitere Informationen hierzu finden Sie unter [„Anforderungen für die Anpassung des Gastbetriebssystems“](#), auf Seite 121.
- Wenn Sie eine Anpassungsspezifikation verwenden möchten, erstellen oder importieren Sie zunächst diese Anpassungsspezifikation.
- Wenn der Hostname oder die IP-Adresse für die neue virtuelle Maschine mithilfe eines benutzerdefinierten Skripts generiert werden soll, konfigurieren Sie zunächst das Skript. Weitere Informationen hierzu finden Sie unter [„Konfigurieren eines Skripts für die Generierung von Computernamen und IP-Adressen bei der Anpassung des Gastbetriebssystems im vSphere-Client“](#), auf Seite 122.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage, und wählen Sie dann **Virtuelle Maschine über diese Vorlage bereitstellen** aus.
- 2 Geben Sie den Namen einer virtuellen Maschine ein, wählen Sie einen Speicherort aus, und klicken Sie auf **Weiter**.

- 3 Wählen Sie den Host oder Cluster aus, auf dem die neue virtuelle Maschine ausgeführt werden soll.

Option	Aktion
Ausführen der virtuellen Maschine auf einem eigenständigen Host.	Wählen Sie den Host aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster mit automatisierter DRS-Platzierung.	Wählen Sie den Cluster aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster ohne automatisierter DRS-Platzierung.	a Wählen Sie den Cluster aus und klicken Sie auf Weiter . b Wählen Sie einen Host im Cluster aus und klicken Sie auf Weiter .

- 4 Wählen Sie einen Ressourcenpool aus, in dem die virtuelle Maschine ausgeführt werden soll, und klicken Sie auf **Weiter**.

- 5 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Maschine speichern möchten.

Option	Aktion
Alle Dateien der virtuellen Maschine am selben Speicherort auf einem Datenspeicher speichern.	a (Optional) Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie . Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind. b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter .
Alle Dateien der virtuellen Maschine in demselben Datenspeicher-Cluster speichern.	a (Optional) Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie . Die Liste zeigt, welche Datenspeicher mit dem ausgewählten Speicherprofil der virtuellen Maschine kompatibel bzw. inkompatibel sind. b Wählen Sie einen Datenspeicher-Cluster aus. c (Optional) Wenn Sie Speicher-DRS nicht mit dieser virtuellen Maschine verwenden möchten, wählen Sie Speicher-DRS für diese virtuelle Maschine deaktivieren und wählen Sie einen Datenspeicher im Datenspeicher-Cluster aus. d Klicken Sie auf Weiter .
De Konfigurationsdateien der virtuellen Maschine und die Festplatten an verschiedenen Speicherorten sichern.	a Klicken Sie auf Erweitert . b Klicken Sie für die Konfigurationsdatei der virtuellen Maschine und für jede virtuelle Festplatte auf Durchsuchen und wählen Sie einen Datenspeicher oder Datenspeicher-Cluster aus. c (Optional) Übernehmen Sie eine Speicherrichtlinie für eine virtuelle Maschine aus dem Dropdown-Menü VM Storage Profile . Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind. d (Optional) Wenn Sie einen Datenspeicher-Cluster ausgewählt haben und Speicher-DRS nicht mit dieser virtuellen Maschine verwenden möchten, aktivieren Sie die Option Speicher-DRS für diese virtuelle Maschine deaktivieren und wählen Sie einen Datenspeicher im Datenspeicher-Cluster aus. e Klicken Sie auf Weiter .

- 6 Wählen Sie das Format für die Festplatten der virtuellen Maschine aus.

Option	Aktion
Format wie Quelle	Verwendet das Format der virtuellen Quellmaschine.
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. 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.
Thick-Provision Eager-Zeroed	Erstellen Sie eine Thick-Festplatte, die Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Format „Thick-Provision Lazy-Zeroed“ werden die auf dem physischen Gerät verbleibenden Daten während des Anlegens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen.
Thin Provision	Verwendet das Format „Schnell bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die schnell bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugewiesene Kapazität anwachsen.

- 7 Wählen Sie eine Option für die benutzerdefinierte Anpassung des Gastbetriebssystems aus.

Option	Beschreibung
Keine Anpassung	Wählen Sie Keine Anpassung und klicken Sie auf Weiter . Es werden keine Änderungen an den Einstellungen des Gastbetriebssystems vorgenommen. Alle Einstellungen sind mit den Einstellungen der virtuellen Quellmaschine identisch.
Mit dem Assistenten für benutzerdefinierte Anpassungen anpassen	Öffnet den Assistenten für benutzerdefinierte Anpassungen, sodass Sie Anpassungsoptionen für das Gastbetriebssystem auswählen können. Wählen Sie diese Option und klicken Sie auf Weiter , um den Assistenten für benutzerdefinierte Anpassungen zu öffnen. <ul style="list-style-type: none"> ■ Informationen zum Anpassen eines Linux-Gastbetriebssystems finden Sie unter „Anpassen von Linux beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 126. ■ Informationen zum Anpassen eines Windows-Gastbetriebssystems finden Sie unter „Anpassen von Windows beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 123.
Mithilfe einer vorhandenen Anpassungsspezifikation anpassen	Verwendet für die benutzerdefinierte Anpassung des Gastbetriebssystems die Einstellungen in einer gespeicherten Anpassungsspezifikation. <ol style="list-style-type: none"> a Wählen Sie Mithilfe einer vorhandenen Anpassungsspezifikation anpassen. b Wählen Sie die gewünschte Anpassungsspezifikation aus. c (Optional) Wählen Sie die Option Sie können den Assistenten für benutzerdefinierte Anpassungen verwenden, um die Spezifikation vor der Bereitstellung vorübergehend zu ändern, wenn die Spezifikation nur für diese Bereitstellung geändert werden soll. d Klicken Sie auf Weiter.

- 8 Überprüfen Sie Ihre Auswahl und wählen Sie, ob Sie die virtuelle Maschine einschalten oder die Einstellungen der VM bearbeiten möchten.

Option	Aktion
Diese virtuelle Maschine nach dem Erstellen einschalten	Wählen Sie diese Option und klicken Sie auf Beenden . Die virtuelle Maschine wird eingeschaltet, wenn der Bereitstellungsvorgang abgeschlossen ist.
Virtuelle Hardware bearbeiten	a Wählen Sie diese Option und klicken Sie auf Fortfahren . b Nehmen Sie die Änderungen vor und klicken Sie auf OK .
Alle Speicherempfehlungen anzeigen	Diese Option wird nur angezeigt, wenn die Festplatten der virtuellen Maschine auf einem Datenspeicher-Cluster gespeichert sind und Speicher-DRS aktiviert ist. Wählen Sie diese Option und klicken Sie auf Fortfahren . In dem Dialogfeld sind die Datenspeicher im Datenspeicher-Cluster aufgelistet, die für die Platzierung der virtuellen Maschine empfohlen werden.
Speicher-DRS-Regeln bearbeiten	Diese Option wird nur angezeigt, wenn die Festplatten der virtuellen Maschine auf einem Datenspeicher-Cluster gespeichert sind. Diese Option wird ausgewählt, wenn Sie Virtuelle Hardware bearbeiten auswählen. Sie können Speicher-DRS-Regeln auf der Registerkarte Optionen des Eigenschaftendialogfelds der virtuellen Maschine bearbeiten. Aktivieren Sie das Kontrollkästchen Speicher-DRS-Regeln bearbeiten und klicken Sie auf Fortfahren .

Die virtuelle Maschine wird bereitgestellt. Sie können die neue virtuelle Maschine erst verwenden oder bearbeiten, nachdem die Bereitstellung abgeschlossen ist. Dies kann einige Minuten dauern, falls eine virtuelle Festplatte erstellt werden muss.

Ändern des Vorlagennamens im vSphere-Client

Anders als bei anderen Änderungen an der Vorlage, müssen Sie die Vorlage nicht in eine virtuelle Maschine konvertieren, wenn Sie deren Namen ändern möchten.

Voraussetzungen

Stellen Sie sicher, dass eine Verbindung mit dem vCenter Server besteht. Die Arbeit mit Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit dem ESXi-Host verbunden ist.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Umbenennen**.
- 2 Geben Sie einen neuen Namen ein und klicken Sie außerhalb des Feldes, um Ihre Änderungen zu speichern.

Löschen von Vorlagen

Sie können eine Vorlage löschen, indem Sie sie aus der Bestandsliste entfernen oder von der Festplatte löschen. Wenn Sie die Vorlage aus der Bestandsliste entfernen, wird sie auf der Festplatte beibehalten und kann später in vCenter Server neu registriert und in der Bestandsliste wiederhergestellt werden.

- [Entfernen einer Vorlage aus der Bestandsliste im vSphere-Client](#) auf Seite 118

Wenn Sie eine Vorlage aus der Bestandsliste entfernen, wird die Registrierung der Vorlage in der vCenter Server-Bestandsliste aufgehoben. Die Vorlage wird jedoch nicht aus dem Datenspeicher gelöscht.

- [Löschen einer Vorlage von der Festplatte im vSphere-Client](#) auf Seite 118

Gelöschte Vorlagen werden dauerhaft vom System entfernt.

- [Erneutes Registrieren von Vorlagen im vSphere Client](#) auf Seite 118

Die Registrierung von Vorlagen in vCenter Server wird aufgehoben, wenn die Vorlagen aus der Bestandsliste gelöscht werden oder wenn die Hosts, denen sie zugeordnet sind, aus vCenter Server entfernt und wieder hinzugefügt werden.

Entfernen einer Vorlage aus der Bestandsliste im vSphere-Client

Wenn Sie eine Vorlage aus der Bestandsliste entfernen, wird die Registrierung der Vorlage in der vCenter Server-Bestandsliste aufgehoben. Die Vorlage wird jedoch nicht aus dem Datenspeicher gelöscht.

Voraussetzungen

Zum Entfernen einer Vorlage aus der Bestandsliste muss eine Verbindung zu vCenter Server bestehen. Das Arbeiten mit Vorlagen ist nicht möglich, wenn Sie sich mit einem ESXi-Host direkt verbinden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Aus Bestandsliste entfernen**.
- 2 Klicken Sie auf **OK**, um das Entfernen der Vorlage aus der vCenter Server-Datenbank zu bestätigen.

Die Registrierung der Vorlage in der vCenter Server-Bestandsliste wird aufgehoben.

Löschen einer Vorlage von der Festplatte im vSphere-Client

Gelöschte Vorlagen werden dauerhaft vom System entfernt.

Voraussetzungen

Zum Löschen einer Vorlage müssen Sie mit vCenter Server verbunden sein. Die Arbeit mit Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit dem ESXi-Host verbunden ist.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Von Festplatte löschen**.
- 2 Klicken Sie auf **OK**, um zu bestätigen, dass die Vorlage aus dem Datenspeicher gelöscht werden soll.

Die Vorlage wird von der Festplatte gelöscht und kann nicht wiederhergestellt werden.

Erneutes Registrieren von Vorlagen im vSphere Client

Die Registrierung von Vorlagen in vCenter Server wird aufgehoben, wenn die Vorlagen aus der Bestandsliste gelöscht werden oder wenn die Hosts, denen sie zugeordnet sind, aus vCenter Server entfernt und wieder hinzugefügt werden.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Klicken Sie auf der Startseite auf **Datenspeicher und Datenspeicher-Cluster**.
- 2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher, der die Vorlage enthält, und wählen Sie **Datenspeicher durchsuchen**.
- 3 Durchsuchen Sie die Ordner des Datenspeichers nach der .vmtx-Datei.
- 4 Klicken Sie mit der rechten Maustaste auf die .vmtx-Datei und wählen Sie **Zur Bestandsliste hinzufügen**.

Der Assistent zum Hinzufügen von Objekten zur Bestandsliste wird angezeigt.

- 5 Geben Sie einen Vorlagennamen ein, wählen Sie einen Speicherort aus, und klicken Sie auf **Weiter**.
Wenn die Vorlage den Originalnamen beibehalten soll, geben Sie im Assistenten zum Hinzufügen von Objekten zur Bestandsliste keinen Namen an. vCenter Server verwendet den Originalnamen, wenn das Feld im Assistenten leer bleibt.
- 6 Wählen Sie einen Host oder Cluster aus, auf bzw. in dem die Vorlage gespeichert werden soll, und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie Ihre Auswahl, und klicken Sie auf **Beenden**.

Die Vorlage wird auf dem Host registriert. Sie können die Vorlage auf der Registerkarte **Virtuelle Maschine** des Hosts anzeigen.

Konvertieren einer Vorlage in eine virtuelle Maschine im vSphere-Client

Durch das Konvertieren einer Vorlage in eine virtuelle Maschine wird die Vorlage verändert, es wird keine Kopie erstellt. Wenn Sie eine Vorlage bearbeiten möchten, müssen Sie sie in eine virtuelle Maschine konvertieren. Sie können eine Vorlage auch in eine virtuelle Maschine konvertieren, wenn Sie sie nicht mehr als Master-Image für die Bereitstellung virtueller Maschinen benötigen.

Voraussetzungen

Zum Konvertieren einer Vorlage in eine virtuelle Maschine müssen Sie mit vCenter Server verbunden sein. Das Arbeiten mit Vorlagen ist nicht möglich, wenn Sie sich mit einem ESXi-Host direkt verbinden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **In virtuelle Maschine konvertieren**.
- 2 Wählen Sie den Host oder Cluster aus, auf dem die virtuelle Maschine ausgeführt werden soll.

Option	Aktion
Ausführen der virtuellen Maschine auf einem eigenständigen Host.	Wählen Sie den Host aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster mit automatisierter DRS-Platzierung.	Wählen Sie den Cluster aus und klicken Sie auf Weiter .
Ausführen der virtuellen Maschine in einem Cluster ohne automatisierter DRS-Platzierung.	a Wählen Sie den Cluster aus und klicken Sie auf Weiter . b Wählen Sie einen Host im Cluster aus und klicken Sie auf Weiter .

Wenn sich die Vorlage in einem älteren VMFS2-Datenspeicher befindet, müssen Sie als Ziel für die virtuelle Maschine den Host auswählen, auf dem die Vorlage erstellt wurde.

- 3 Wählen Sie einen Ressourcenpool aus, in dem die virtuelle Maschine ausgeführt werden soll, und klicken Sie auf **Weiter**.
- 4 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.

Anpassen von Gastbetriebssystemen

Wenn Sie eine virtuelle Maschine klonen oder anhand einer Vorlage bereitstellen, können Sie das Gastbetriebssystem der virtuellen Maschine anpassen und Eigenschaften wie den Computernamen, Netzwerkeinstellungen und Lizenzeinstellungen ändern.

Durch die Anpassung von Gastbetriebssystemen können Sie verhindern, dass Konflikte, z. B. aufgrund von doppelten Computernamen, auftreten, wenn virtuelle Maschinen mit identischen Einstellungen bereitgestellt werden.

Um die Anpassungseinstellungen festzulegen, starten Sie während des Klon- oder Bereitstellungsvorgangs den Assistenten Gastanpassung. Alternativ können Sie Anpassungsspezifikationen anlegen. Dabei handelt es sich um Anpassungseinstellungen, die in der vCenter Server-Datenbank gespeichert werden. Während des Klon- oder Bereitstellungsvorgangs können Sie eine Anpassungsspezifikation auswählen und auf die neue virtuelle Maschine anwenden.

Verwenden Sie den Anpassungsspezifikations-Manager zum Verwalten von Anpassungsspezifikationen, die Sie mit dem Assistenten Gastanpassung erstellt haben.

Dieses Kapitel behandelt die folgenden Themen:

- [„Anforderungen für die Anpassung des Gastbetriebssystems“, auf Seite 121](#)
- [„Konfigurieren eines Skripts für die Generierung von Computernamen und IP-Adressen bei der Anpassung des Gastbetriebssystems im vSphere-Client“, auf Seite 122](#)
- [„Anpassen von Windows beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 123](#)
- [„Anpassen von Linux beim Klonen oder Bereitstellen im vSphere Client“, auf Seite 126](#)
- [„Verwalten der Anpassungsspezifikationen im vSphere-Client“, auf Seite 127](#)

Anforderungen für die Anpassung des Gastbetriebssystems

Zum Anpassen des Gastbetriebssystems müssen Sie die virtuelle Maschine und den Gast konfigurieren, um die Anforderungen für VMware Tools und für die virtuelle Festplatte zu erfüllen. Zudem gelten je nach Gastbetriebssystemtyp weitere Anforderungen.

VMware Tools-Anforderungen

Auf der virtuellen Maschine bzw. Vorlage muss die neueste Version von VMware Tools installiert sein, damit das Gastbetriebssystem beim Klonen oder bei der Bereitstellung angepasst werden kann.

Anforderungen der virtuellen Festplatte

Das anzupassende Gastbetriebssystem muss sich auf einer Festplatte befinden, die als SCSI 0:0-Knoten in die Konfiguration der virtuellen Maschine eingebunden ist.

Voraussetzungen für Windows

Für die Anpassung von Windows-Gastbetriebssystemen gelten die folgenden Voraussetzungen:

- Auf dem vCenter Server-System müssen die Microsoft-Tools zur Systemvorbereitung (Sysprep) installiert sein.
- Der ESXi-Host, auf dem die virtuelle Maschine ausgeführt wird, muss mindestens Version 3.5 ausführen.

Die Anpassung des Gastbetriebssystems wird auf mehreren Windows-Betriebssystemen unterstützt.

Voraussetzungen für Linux

Das Anpassen von Linux-Gastbetriebssystemen setzt voraus, dass Perl auf dem Linux-Gastbetriebssystem installiert ist.

Die Anpassung des Gastbetriebssystems wird auf mehreren Linux-Distributionen unterstützt.

Überprüfen, ob die Anpassung von Gastbetriebssystemen unterstützt wird

Um zu überprüfen, ob die Anpassung von Windows-Betriebssystemen und Linux-Distributionen sowie kompatibler ESXi-Hosts unterstützt wird, lesen Sie das *VMware-Kompatibilitätshandbuch* unter <http://www.vmware.com/resources/compatibility>. Sie können dieses Online-Tool zur Suche nach dem Gastbetriebssystem und der ESXi-Version verwenden. Nachdem das Tool Ihre Liste generiert hat, klicken Sie auf das Gastbetriebssystem, um zu überprüfen, ob die Gastanpassung unterstützt wird.

Konfigurieren eines Skripts für die Generierung von Computernamen und IP-Adressen bei der Anpassung des Gastbetriebssystems im vSphere-Client

Als Alternative zum Eingeben des Computernamens oder der IP-Adressen für virtuelle Netzwerkkarten während der Anpassung von Gastbetriebssystemen können Sie eine benutzerdefinierte Anwendung erstellen und sie so konfigurieren, dass vCenter Server sie zum Erzeugen des Computernamens und der IP-Adressen verwenden kann.

Bei der Anwendung kann es sich um eine beliebige ausführbare Binärdatei oder Skriptdatei handeln, die für das entsprechende Betriebssystem geeignet ist, auf dem vCenter Server ausgeführt wird. Nachdem Sie in vCenter Server eine Anwendung zur Namens- und IP-Generierung konfiguriert haben, wird jedes Mal, wenn Sie eine Anpassung des Gastbetriebssystems für eine virtuelle Maschine initiieren, diese Anwendung ausgeführt und direkt eine XML-Zeichenfolge generiert und an ihre Standardeingabe übergeben. Die Anwendung zur Namens- und IP-Generierung sollte ihrerseits die resultierende XML-Zeichenfolge generieren und diese über ihre Standardausgabe zurückgeben.

Die Anwendung muss mit der Referenz-XML-Datei im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2007557> übereinstimmen.

Voraussetzungen

Stellen Sie sicher, dass Perl auf vCenter Server installiert ist.

Vorgehensweise

- 1 Schreiben Sie das Skript und speichern Sie es auf der lokalen Festplatte des vCenter Server-Systems.
- 2 Wählen Sie im vSphere-Client, der mit vCenter Server verbunden ist, die Option **Verwaltung > vCenter Server-Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Einstellungen**.

- 4 Geben Sie die Konfigurationsparameter für das Skript ein.
 - a Geben Sie im Textfeld **Schlüssel** den Text `config.guestcust.name-ip-generator.arg1` ein.
 - b Geben Sie in das Textfeld **Wert** die Zeichenfolge `c:\sample-generate-name-ip.pl` ein und klicken Sie auf **Hinzufügen**.
 - c Geben Sie im Textfeld **Schlüssel** den Text `config.guestcust.name-ip-generator.arg2` ein.
 - d Geben Sie im Textfeld **Wert** den Pfad zur Skriptdatei auf dem vCenter Server-System ein und klicken Sie auf **Hinzufügen**. Beispiel: Geben Sie `c:\sample-generate-name-ip.pl` ein.
 - e Geben Sie im Textfeld **Schlüssel** den Text `config.guestcust.name-ip-generator.program` ein.
 - f Geben Sie in das Textfeld **Wert** die Zeichenfolge `c:\perl\bin\perl.exe` ein und klicken Sie auf **Hinzufügen**.
- 5 Klicken Sie auf **OK**.

Sie können die Option zur Verwendung einer Anwendung zum Generieren von Computernamen oder IP-Adressen während des Anpassungsvorgangs auswählen.

Anpassen von Windows beim Klonen oder Bereitstellen im vSphere Client

Wenn Sie eine neue virtuelle Maschine aus einer Vorlage bereitstellen oder eine vorhandene virtuelle Maschine klonen, können Sie Windows-Gastbetriebssysteme für die virtuelle Maschine anpassen.

HINWEIS Das standardmäßige Administratorkennwort wird bei Windows Server 2008 nach der Anpassung nicht beibehalten. Während der Anpassung wird das Administratorkonto unter Windows Server 2008 vom Windows-Dienstprogramm Sysprep gelöscht und neu erstellt. Sie müssen das Administratorkennwort also zurücksetzen, wenn die virtuelle Maschine zum ersten Mal nach der Anpassung gestartet wird.

Voraussetzungen

Vergewissern Sie sich, dass alle für die Anpassung erforderlichen Anforderungen erfüllt werden. Siehe [„Anforderungen für die Anpassung des Gastbetriebssystems“](#), auf Seite 121.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Management > Anpassungsverwaltungs-Manager** und klicken Sie auf **Neu**, um die Windows-Gastanpassung zu starten.
- 2 Wählen Sie das **Betriebssystem der virtuellen Zielmaschine** aus und geben Sie den Namen und die Beschreibung für die Informationen zur Anpassungsspezifikation ein. Klicken Sie dann auf **Weiter**.

HINWEIS Wenn Sie eine benutzerdefinierte Sysprep-Datei verwenden möchten, wählen Sie **Benutzerdefinierte Sysprep-Antwortdatei verwenden** aus.

- 3 Geben Sie den Besitzer der virtuellen Maschine und den Namen der Organisation ein und klicken Sie auf **Weiter**.

- 4 Geben Sie den Computernamen des Gastbetriebssystems ein und klicken Sie auf **Weiter**.

Das Betriebssystem verwendet diesen Namen, um sich selbst im Netzwerk zu identifizieren. Auf Linux-Systemen wird er als der Hostname bezeichnet.

Option	Aktion
Namen eingeben	<p>a Geben Sie einen Namen ein.</p> <p>Der Name kann alphanumerische Zeichen und Bindestriche (-) enthalten. Er darf keine Punkte (.) oder Leerzeichen umfassen und darf nicht ausschließlich aus Ziffern bestehen. Bei Namen wird die Groß- und Kleinschreibung nicht berücksichtigt.</p> <p>b (Optional) Wählen Sie Einen numerischen Wert anfügen, um Eindeutigkeit zu gewährleisten, um die Eindeutigkeit des Namens zu gewährleisten. Diese Option hängt einen Bindestrich, gefolgt von einer Zahl, an den Namen der virtuellen Maschine an. Der Name wird abgeschnitten, wenn er zusammen mit dem numerischen Wert 15 Zeichen überschreitet.</p>
Den Namen der virtuellen Maschine verwenden	Der Computernamen, den vCenter Server erstellt, ist identisch mit dem Namen der virtuellen Maschine, in der das Gastbetriebssystem ausgeführt wird. Wenn der Name aus mehr als 15 Zeichen besteht, wird er abgeschnitten.
Einen Namen im Assistenten für die Bereitstellung eingeben	Der vSphere Web Client fordert Sie auf, einen Namen einzugeben, wenn das Klonen oder die Bereitstellung abgeschlossen ist.
Namen mithilfe der mit vCenter Server konfigurierten benutzerdefinierten Anwendung generieren	Geben Sie einen Parameter ein, der an die benutzerdefinierte Anwendung weitergegeben werden kann.

- 5 Geben Sie die Lizenzierungsinformationen für das Windows-Betriebssystem ein und klicken Sie auf **Weiter**.

Option	Aktion
Für Nicht-Server-Betriebssysteme	Geben Sie den Windows-Produktschlüssel für das neue Gastbetriebssystem ein.
Für Server-Betriebssysteme	<p>a Geben Sie den Windows-Produktschlüssel für das neue Gastbetriebssystem ein.</p> <p>b Wählen Sie Serverlizenzen verwenden aus.</p> <p>c Wählen Sie entweder die Option Pro Arbeitsplatz oder Pro Server aus.</p> <p>d (Optional) Wenn Sie Pro Server auswählen, geben Sie die maximale Anzahl gleichzeitiger Verbindungen an, die der Server akzeptieren soll.</p>

- 6 Konfigurieren Sie das Administratorkennwort für die virtuelle Maschine und klicken Sie auf **Weiter**.

- a Geben Sie ein Kennwort für das Administratorkonto ein und bestätigen Sie es durch erneute Eingabe.

HINWEIS Sie können das Administratorkennwort nur ändern, wenn das Administratorkennwort auf der virtuellen Windows-Quellmaschine leer ist. Wenn die virtuelle Windows-Quellmaschine oder Vorlage bereits ein Kennwort hat, wird das Administratorkennwort nicht geändert.

- b (Optional) Klicken Sie zum Anmelden von Benutzern als Administrator auf das Kontrollkästchen und wählen Sie aus, wie oft die Anmeldung automatisch erfolgen soll.

- 7 Wählen Sie eine Zeitzone für die virtuelle Maschine aus und klicken Sie auf **Weiter**.

- 8 (Optional) Geben Sie auf der Seite „Einmaliges Ausführen“ Befehle an, die beim erstmaligen Anmelden eines Benutzers beim Gastbetriebssystem ausgeführt werden sollen, und klicken Sie auf **Weiter**.

Informationen zu den RunOnce-Befehlen finden Sie in der Microsoft-Dokumentation für Sysprep.

- 9 Wählen Sie die Netzwerkeinstellungen für das Gastbetriebssystem aus.

Option	Aktion
Typische Einstellungen	Wählen Sie Typische Einstellungen und klicken Sie auf Weiter . vCenter Server konfiguriert alle Netzwerkschnittstellen von einem DHCP-Server aus und verwendet die Standardeinstellungen.
Benutzerdefinierte Einstellungen	<ul style="list-style-type: none"> a Wählen Sie Benutzerdefinierte Einstellungen und klicken Sie auf Weiter. b Klicken Sie für jede Netzwerkschnittstelle in der virtuellen Maschine auf die Schaltfläche mit dem Auslassungszeichen (...). c Geben Sie die IP-Adresse und andere Netzwerkeinstellungen ein und klicken Sie auf OK. d Wenn die Konfiguration aller Netzwerkschnittstellen abgeschlossen ist, klicken Sie auf Weiter.

- 10 Wählen Sie aus, welche Rolle die virtuelle Maschine im Netzwerk erhalten soll, und klicken Sie auf **Weiter**.

Option	Aktion
Arbeitsgruppe	Geben Sie einen Namen für die Arbeitsgruppe ein. Beispielsweise MSHOME .
Windows-Serverdomäne	<ul style="list-style-type: none"> a Geben Sie den Domänennamen ein. b Geben Sie für ein Benutzerkonto, das über die Berechtigung zum Hinzufügen von Computern zu der angegebenen Domäne verfügt, einen Benutzernamen und ein Kennwort ein.

- 11 (Optional) Wählen Sie die Option „Neue Sicherheits-ID (SID) erzeugen“ aus und klicken Sie auf **Weiter**.

Einige Windows-Betriebssysteme verwenden eine Sicherheits-IDs (SIDs), um Systeme und Benutzer eindeutig identifizieren zu können. Wenn sie diese Option nicht auswählen, erhält die neue virtuelle Maschine dieselbe SID wie die virtuelle Maschine oder die Vorlage, auf deren Grundlage sie geklont bzw. bereitgestellt wurde.

Mehrfach vergebene SIDs verursachen keine Probleme, wenn die Computer zu einer Domäne gehören und nur Domänenbenutzerkonten verwendet werden. Sind die Computer allerdings Teil einer Arbeitsgruppe oder werden lokale Benutzerkonten verwendet, können solche SIDs die Dateizugriffssteuerung beeinträchtigen. Weitere Informationen zur Konfiguration der Authentifizierung finden Sie in der Dokumentation zu Ihrem Microsoft Windows-Betriebssystem.

- 12 Speichern Sie die benutzerdefinierten Optionen als .xml-Datei.

- a Wählen Sie **Diese Spezifikationen der benutzerspezifischen Anpassung zur späteren Verwendung speichern (Save this customization specification for later use)** aus.
- b Geben Sie den Dateinamen für die Spezifikation an, und klicken Sie auf **Weiter**.

- 13 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern.

Sie kehren zum Assistenten „Vorlage bereitstellen“ oder zum Assistenten Virtuelle Maschine klonen zurück. Die Anpassung wird beendet, nachdem Sie den Assistenten zum Bereitstellen von Vorlagen oder den Assistenten Virtuelle Maschine klonen abgeschlossen haben.

Wenn die neue virtuelle Maschine zum ersten Mal gestartet wird, führt das Gastbetriebssystem Finalisierungsskripts aus, um den Anpassungsvorgang abzuschließen. Die virtuelle Maschine kann während dieses Vorgangs mehrmals starten.

Wird das Gastbetriebssystem beim Starten der neuen virtuellen Maschine angehalten, müssen Sie möglicherweise Fehler korrigieren, z. B. einen falschen Produktschlüssel oder einen ungültigen Benutzernamen. Öffnen Sie die Konsole der virtuellen Maschine, um festzustellen, ob das System auf eine Eingabe von Informationen wartet.

Weiter

Nach dem Bereitstellen und Anpassen von Windows XP- oder Windows 2003-Versionen, für die keine Volumenlizenzen erworben wurden, müssen Sie das Betriebssystem auf der neuen virtuellen Maschine möglicherweise erneut aktivieren.

Wenn auf der neuen virtuellen Maschine beim Starten Anpassungsfehler festgestellt werden, werden diese in der Datei %WINDIR%\temp\vmware-vmc protokolliert. Klicken Sie zum Anzeigen des Fehlerprotokolls auf die Windows-Schaltfläche **Start** und wählen Sie **Programme > Verwaltung > Ereignisanzeige**.

Anpassen von Linux beim Klonen oder Bereitstellen im vSphere Client

Sie können Linux-Gastbetriebssysteme für die virtuelle Maschine anpassen, wenn Sie eine neue virtuelle Maschine von einer Vorlage bereitstellen oder eine vorhandene virtuelle Maschine klonen.

Voraussetzungen

Vergewissern Sie sich, dass alle für die Anpassung erforderlichen Anforderungen erfüllt werden. Siehe [„Anforderungen für die Anpassung des Gastbetriebssystems“](#), auf Seite 121.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Management > Anpassungsverwaltungs-Manager** und klicken Sie auf **Neu**, um die Windows-Gastanpassung zu starten.
- 2 Wählen Sie das **Betriebssystem der virtuellen Zielmaschine** aus und geben Sie den Namen und die Beschreibung für die Informationen zur Anpassungsspezifikation ein. Klicken Sie dann auf **Weiter**.

HINWEIS Wenn Sie eine benutzerdefinierte Sysprep-Datei verwenden möchten, wählen Sie **Benutzerdefinierte Sysprep-Antwortdatei verwenden** aus.

- 3 Wählen Sie **Mit dem Assistenten für benutzerdefinierte Anpassungen bearbeiten** und klicken Sie **Weiter**.
- 4 Geben Sie an, wie der Host-Name ermittelt werden soll, durch den das Gastbetriebssystem im Netzwerk identifiziert wird.

Option	Aktion
Namen eingeben	<p>a Geben Sie einen Namen ein.</p> <p>Der Name kann alphanumerische Zeichen und Bindestriche (-) enthalten. Er darf keine Punkte (.) oder Leerzeichen umfassen und darf nicht ausschließlich aus Ziffern bestehen. Bei Namen wird die Groß- und Kleinschreibung nicht berücksichtigt.</p> <p>b (Optional) Wählen Sie Einen numerischen Wert anfügen, um Eindeutigkeit zu gewährleisten, um die Eindeutigkeit des Namens zu gewährleisten. Diese Option hängt einen Bindestrich, gefolgt von einer Zahl, an den Namen der virtuellen Maschine an. Der Name wird abgeschnitten, wenn er zusammen mit dem numerischen Wert 15 Zeichen überschreitet.</p>
Den Namen der virtuellen Maschine verwenden	Der Computernamen, den vCenter Server erstellt, ist identisch mit dem Namen der virtuellen Maschine, in der das Gastbetriebssystem ausgeführt wird. Wenn der Name aus mehr als 15 Zeichen besteht, wird er abgeschnitten.
Einen Namen im Assistenten für die Bereitstellung eingeben	Der vSphere Web Client fordert Sie auf, einen Namen einzugeben, wenn das Klonen oder die Bereitstellung abgeschlossen ist.
Namen mithilfe der mit vCenter Server konfigurierten benutzerdefinierten Anwendung generieren	Geben Sie einen Parameter ein, der an die benutzerdefinierte Anwendung weitergegeben werden kann.

- 5 Geben Sie den **Domännennamen** für den Computer ein und klicken Sie auf **Weiter**.
- 6 Wählen Sie eine Zeitzone für die virtuelle Maschine aus und klicken Sie auf **Weiter**.
- 7 Wählen Sie die Netzwerkeinstellungen für das Gastbetriebssystem aus.

Option	Aktion
Typische Einstellungen	Wählen Sie Typische Einstellungen und klicken Sie auf Weiter . vCenter Server konfiguriert alle Netzwerkschnittstellen von einem DHCP-Server aus und verwendet die Standardeinstellungen.
Benutzerdefinierte Einstellungen	<ol style="list-style-type: none"> a Wählen Sie Benutzerdefinierte Einstellungen und klicken Sie auf Weiter. b Klicken Sie für jede Netzwerkschnittstelle in der virtuellen Maschine auf die Schaltfläche mit dem Auslassungszeichen (...). c Geben Sie die IP-Adresse und andere Netzwerkeinstellungen ein und klicken Sie auf OK. d Wenn die Konfiguration aller Netzwerkschnittstellen abgeschlossen ist, klicken Sie auf Weiter.

- 8 Geben Sie DNS- und Domäneneinstellungen ein.
- 9 Speichern Sie die benutzerdefinierten Optionen als .xml-Datei.
 - a Wählen Sie **Diese Spezifikationen der benutzerspezifischen Anpassung zur späteren Verwendung speichern (Save this customization specification for later use)** aus.
 - b Geben Sie den Dateinamen für die Spezifikation an, und klicken Sie auf **Weiter**.
- 10 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern.

Sie kehren zum Assistenten „Vorlage bereitstellen“ oder zum Assistenten Virtuelle Maschine klonen zurück. Die Anpassung wird beendet, nachdem Sie den Assistenten zum Bereitstellen von Vorlagen oder den Assistenten Virtuelle Maschine klonen abgeschlossen haben.

Wenn die neue virtuelle Maschine zum ersten Mal gestartet wird, führt das Gastbetriebssystem Finalisierungsskripts aus, um den Anpassungsvorgang abzuschließen. Die virtuelle Maschine kann während dieses Vorgangs mehrmals starten.

Wird das Gastbetriebssystem beim Starten der neuen virtuellen Maschine angehalten, müssen Sie möglicherweise Fehler korrigieren, z. B. einen falschen Produktschlüssel oder einen ungültigen Benutzernamen. Öffnen Sie die Konsole der virtuellen Maschine, um festzustellen, ob das System auf eine Eingabe von Informationen wartet.

Weiter

Wenn auf der neuen virtuellen Maschine beim Starten Anpassungsfehler festgestellt werden, werden diese durch den Protokollierungsmechanismus des Gastbetriebssystems gemeldet. Um die Fehler anzuzeigen, öffnen Sie die Protokolldatei `/var/log/vmware-imc/toolsDeployPkg.log`.

Verwalten der Anpassungsspezifikationen im vSphere-Client

Anpassungsspezifikationen sind XML-Dateien, die Gastbetriebssystemeinstellungen für virtuelle Maschinen enthalten. Anpassungsspezifikationen erstellen Sie unter Verwendung des Assistenten Gastanpassung und verwalten sie mithilfe des Anpassungsspezifikations-Managers.

vCenter Server speichert die angepassten Konfigurationsparameter in der vCenter Server-Datenbank. Beim Speichern der angepassten Einstellungen werden die Kennwörter für Administrator und Domänenadministrator in verschlüsselter Form in der Datenbank gespeichert. Da das Zertifikat für die Verschlüsselung von Kennwörtern für jedes vCenter Server-System eindeutig ist, führt eine Neuinstallation von vCenter Server oder die Verbindung mit einer neuen Instanz des Servers dazu, dass die verschlüsselten Kennwörter ungültig werden. Die Kennwörter müssen erneut eingegeben werden, bevor eine Verwendung möglich ist.

Erstellen einer Anpassungsspezifikation für Linux im vSphere Client

Verwenden Sie den Assistenten Gastanpassung, um Gastbetriebssystemeinstellungen in einer Spezifikation zu speichern, die Sie beim Klonen von virtuellen Maschinen oder beim Bereitstellen anhand von Vorlagen anwenden können.

Voraussetzungen

Vergewissern Sie sich, dass alle für die Anpassung erforderlichen Anforderungen erfüllt werden. Siehe [„Anforderungen für die Anpassung des Gastbetriebssystems“](#), auf Seite 121.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie auf das Symbol **Neue Spezifikation erstellen**
- 3 Wählen Sie „Linux“ im Menü **Betriebssystem der virtuellen Zielmaschine** aus.
- 4 Geben Sie unter „Informationen zur Anpassungsspezifikation“ einen Namen für die Spezifikation und optional eine Beschreibung ein und klicken Sie auf **Weiter**.
- 5 Geben Sie an, wie der Host-Name ermittelt werden soll, durch den das Gastbetriebssystem im Netzwerk identifiziert wird.

Option	Aktion
Namen eingeben	<p>a Geben Sie einen Namen ein.</p> <p>Der Name kann alphanumerische Zeichen und Bindestriche (-) enthalten. Er darf keine Punkte (.) oder Leerzeichen umfassen und darf nicht ausschließlich aus Ziffern bestehen. Bei Namen wird die Groß- und Kleinschreibung nicht berücksichtigt.</p> <p>b (Optional) Wählen Sie Einen numerischen Wert anfügen, um Eindeutigkeit zu gewährleisten, um die Eindeutigkeit des Namens zu gewährleisten. Diese Option hängt einen Bindestrich, gefolgt von einer Zahl, an den Namen der virtuellen Maschine an. Der Name wird abgeschnitten, wenn er zusammen mit dem numerischen Wert 15 Zeichen überschreitet.</p>
Den Namen der virtuellen Maschine verwenden	Der Computernamen, den vCenter Server erstellt, ist identisch mit dem Namen der virtuellen Maschine, in der das Gastbetriebssystem ausgeführt wird. Wenn der Name aus mehr als 15 Zeichen besteht, wird er abgeschnitten.
Einen Namen im Assistenten für die Bereitstellung eingeben	Der vSphere Web Client fordert Sie auf, einen Namen einzugeben, wenn das Klonen oder die Bereitstellung abgeschlossen ist.
Namen mithilfe der mit vCenter Server konfigurierten benutzerdefinierten Anwendung generieren	Geben Sie einen Parameter ein, der an die benutzerdefinierte Anwendung weitergegeben werden kann.

- 6 Geben Sie den **Domänennamen** für den Computer ein und klicken Sie auf **Weiter**.
- 7 Wählen Sie eine Zeitzone für die virtuelle Maschine aus und klicken Sie auf **Weiter**.

- 8 Wählen Sie die Netzwerkeinstellungen für das Gastbetriebssystem aus.

Option	Aktion
Typische Einstellungen	Wählen Sie Typische Einstellungen und klicken Sie auf Weiter . vCenter Server konfiguriert alle Netzwerkschnittstellen von einem DHCP-Server aus und verwendet die Standardeinstellungen.
Benutzerdefinierte Einstellungen	<ul style="list-style-type: none"> a Wählen Sie Benutzerdefinierte Einstellungen und klicken Sie auf Weiter. b Klicken Sie für jede Netzwerkschnittstelle in der virtuellen Maschine auf die Schaltfläche mit dem Auslassungszeichen (...). c Geben Sie die IP-Adresse und andere Netzwerkeinstellungen ein und klicken Sie auf OK. d Wenn die Konfiguration aller Netzwerkschnittstellen abgeschlossen ist, klicken Sie auf Weiter.

- 9 Geben Sie DNS- und Domäneneinstellungen ein.

- 10 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern.

Die von Ihnen erstellte Anpassungsspezifikation wird im Anpassungsspezifikations-Manager angezeigt. Sie können die Spezifikation zum Anpassen der Gastbetriebssysteme von virtuellen Maschinen verwenden.

Erstellen einer Anpassungsspezifikation für Windows im vSphere Client

Verwenden Sie den Assistenten Gastanpassung, um Gastbetriebssystemeinstellungen in einer Spezifikation zu speichern, die Sie beim Klonen von virtuellen Maschinen oder beim Bereitstellen anhand von Vorlagen anwenden können.

HINWEIS Das standardmäßige Administratorkennwort wird bei Windows Server 2008 nach der Anpassung nicht beibehalten. Während der Anpassung wird das Administratorkonto unter Windows Server 2008 vom Windows-Dienstprogramm Sysprep gelöscht und neu erstellt. Sie müssen das Administratorkennwort also zurücksetzen, wenn die virtuelle Maschine zum ersten Mal nach der Anpassung gestartet wird.

Voraussetzungen

Vergewissern Sie sich, dass alle für die Anpassung erforderlichen Anforderungen erfüllt werden. Siehe „[Anforderungen für die Anpassung des Gastbetriebssystems](#)“, auf Seite 121.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie auf das Symbol **Neue Spezifikation erstellen**.
- 3 Wählen Sie im Assistenten Gastanpassung im Menü **Betriebssystem der virtuellen Zielmaschine** die Option „Windows“ aus.
- 4 Geben Sie unter „Informationen zur Anpassungsspezifikation“ einen Namen für die Spezifikation und optional eine Beschreibung ein und klicken Sie auf **Weiter**.
- 5 Geben Sie den Besitzer der virtuellen Maschine und den Namen der Organisation ein und klicken Sie auf **Weiter**.

- 6 Geben Sie den Computernamen des Gastbetriebssystems ein und klicken Sie auf **Weiter**.

Das Betriebssystem verwendet diesen Namen, um sich selbst im Netzwerk zu identifizieren. Auf Linux-Systemen wird er als der Hostname bezeichnet.

Option	Aktion
Namen eingeben	<p>a Geben Sie einen Namen ein.</p> <p>Der Name kann alphanumerische Zeichen und Bindestriche (-) enthalten. Er darf keine Punkte (.) oder Leerzeichen umfassen und darf nicht ausschließlich aus Ziffern bestehen. Bei Namen wird die Groß- und Kleinschreibung nicht berücksichtigt.</p> <p>b (Optional) Wählen Sie Einen numerischen Wert anfügen, um Eindeutigkeit zu gewährleisten, um die Eindeutigkeit des Namens zu gewährleisten. Diese Option hängt einen Bindestrich, gefolgt von einer Zahl, an den Namen der virtuellen Maschine an. Der Name wird abgeschnitten, wenn er zusammen mit dem numerischen Wert 15 Zeichen überschreitet.</p>
Den Namen der virtuellen Maschine verwenden	Der Computernamen, den vCenter Server erstellt, ist identisch mit dem Namen der virtuellen Maschine, in der das Gastbetriebssystem ausgeführt wird. Wenn der Name aus mehr als 15 Zeichen besteht, wird er abgeschnitten.
Einen Namen im Assistenten für die Bereitstellung eingeben	Der vSphere Web Client fordert Sie auf, einen Namen einzugeben, wenn das Klonen oder die Bereitstellung abgeschlossen ist.
Namen mithilfe der mit vCenter Server konfigurierten benutzerdefinierten Anwendung generieren	Geben Sie einen Parameter ein, der an die benutzerdefinierte Anwendung weitergegeben werden kann.

- 7 Geben Sie die Lizenzierungsinformationen für das Windows-Betriebssystem ein und klicken Sie auf **Weiter**.

Option	Aktion
Für Nicht-Server-Betriebssysteme	Geben Sie den Windows-Produktschlüssel für das neue Gastbetriebssystem ein.
Für Server-Betriebssysteme	<p>a Geben Sie den Windows-Produktschlüssel für das neue Gastbetriebssystem ein.</p> <p>b Wählen Sie Serverlizenzen verwenden aus.</p> <p>c Wählen Sie entweder die Option Pro Arbeitsplatz oder Pro Server aus.</p> <p>d (Optional) Wenn Sie Pro Server auswählen, geben Sie die maximale Anzahl gleichzeitiger Verbindungen an, die der Server akzeptieren soll.</p>

- 8 Konfigurieren Sie das Administratorkennwort für die virtuelle Maschine und klicken Sie auf **Weiter**.

- a Geben Sie ein Kennwort für das Administratorkonto ein und bestätigen Sie es durch erneute Eingabe.

HINWEIS Sie können das Administratorkennwort nur ändern, wenn das Administratorkennwort auf der virtuellen Windows-Quellmaschine leer ist. Wenn die virtuelle Windows-Quellmaschine oder Vorlage bereits ein Kennwort hat, wird das Administratorkennwort nicht geändert.

- b (Optional) Klicken Sie zum Anmelden von Benutzern als Administrator auf das Kontrollkästchen und wählen Sie aus, wie oft die Anmeldung automatisch erfolgen soll.

- 9 Wählen Sie eine Zeitzone für die virtuelle Maschine aus und klicken Sie auf **Weiter**.

- 10 (Optional) Geben Sie auf der Seite „Einmaliges Ausführen“ Befehle an, die beim erstmaligen Anmelden eines Benutzers beim Gastbetriebssystem ausgeführt werden sollen, und klicken Sie auf **Weiter**.

Informationen zu den RunOnce-Befehlen finden Sie in der Microsoft-Dokumentation für Sysprep.

- 11 Wählen Sie die Netzwerkeinstellungen für das Gastbetriebssystem aus.

Option	Aktion
Typische Einstellungen	Wählen Sie Typische Einstellungen und klicken Sie auf Weiter . vCenter Server konfiguriert alle Netzwerkschnittstellen von einem DHCP-Server aus und verwendet die Standardeinstellungen.
Benutzerdefinierte Einstellungen	<ul style="list-style-type: none"> a Wählen Sie Benutzerdefinierte Einstellungen und klicken Sie auf Weiter. b Klicken Sie für jede Netzwerkschnittstelle in der virtuellen Maschine auf die Schaltfläche mit dem Auslassungszeichen (...). c Geben Sie die IP-Adresse und andere Netzwerkeinstellungen ein und klicken Sie auf OK. d Wenn die Konfiguration aller Netzwerkschnittstellen abgeschlossen ist, klicken Sie auf Weiter.

- 12 Wählen Sie aus, welche Rolle die virtuelle Maschine im Netzwerk erhalten soll, und klicken Sie auf **Weiter**.

Option	Aktion
Arbeitsgruppe	Geben Sie einen Namen für die Arbeitsgruppe ein. Beispielsweise MSHOME .
Windows-Serverdomäne	<ul style="list-style-type: none"> a Geben Sie den Domännennamen ein. b Geben Sie für ein Benutzerkonto, das über die Berechtigung zum Hinzufügen von Computern zu der angegebenen Domäne verfügt, einen Benutzernamen und ein Kennwort ein.

- 13 (Optional) Wählen Sie die Option „Neue Sicherheits-ID (SID) erzeugen“ aus und klicken Sie auf **Weiter**.

Einige Windows-Betriebssysteme verwenden eine Sicherheits-IDs (SIDs), um Systeme und Benutzer eindeutig identifizieren zu können. Wenn sie diese Option nicht auswählen, erhält die neue virtuelle Maschine dieselbe SID wie die virtuelle Maschine oder die Vorlage, auf deren Grundlage sie geklont bzw. bereitgestellt wurde.

Mehrfach vergebene SIDs verursachen keine Probleme, wenn die Computer zu einer Domäne gehören und nur Domänenbenutzerkonten verwendet werden. Sind die Computer allerdings Teil einer Arbeitsgruppe oder werden lokale Benutzerkonten verwendet, können solche SIDs die Dateizugriffssteuerung beeinträchtigen. Weitere Informationen zur Konfiguration der Authentifizierung finden Sie in der Dokumentation zu Ihrem Microsoft Windows-Betriebssystem.

- 14 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern.

Die von Ihnen erstellte Anpassungsspezifikation wird im Anpassungsspezifikations-Manager angezeigt. Sie können die Spezifikation zum Anpassen der Gastbetriebssysteme von virtuellen Maschinen verwenden.

Erstellen einer Windows-Anpassungsspezifikation mithilfe einer benutzerdefinierten Sysprep-Antwortdatei im vSphere Client

In einer benutzerdefinierten Sysprep-Antwortdatei werden mehrere Anpassungseinstellungen, z. B. der Computernamen und Lizenzierungsinformationen sowie die Einstellungen für die Arbeitsgruppe oder Domäne, gespeichert. Sie können eine benutzerdefinierte Sysprep-Antwortdatei als Alternative zur Eingabe vieler der Einstellungen im Assistenten „Gastanpassung“ bereitstellen.

Unter Windows 2000, Windows Server 2003 und Windows XP wird die Textdatei `sysprep.inf` verwendet. Unter Windows Server 2008, Windows Vista und Windows 7 wird die XML-Datei `sysprep.xml` verwendet. Erstellen Sie diese Dateien mit einem Texteditor oder mithilfe des Installations-Managers von Microsoft. Weitere Informationen zum Erstellen benutzerdefinierter Sysprep-Antwortdateien finden Sie in der Dokumentation zum entsprechenden Betriebssystem.

Voraussetzungen

Vergewissern Sie sich, dass alle für die Anpassung erforderlichen Anforderungen erfüllt werden. Siehe „[Anforderungen für die Anpassung des Gastbetriebssystems](#)“, auf Seite 121.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie auf das Symbol **Neue Spezifikation erstellen**
- 3 Wählen Sie im Assistenten Gastanpassung im Menü **Betriebssystem der virtuellen Zielmaschine** die Option „Windows“ aus.
- 4 (Optional) Wählen Sie **Benutzerdefinierte Sysprep-Antwortdatei verwenden**.
- 5 Geben Sie unter „Informationen zur Anpassungsspezifikation“ einen Namen für die Spezifikation und optional eine Beschreibung ein und klicken Sie auf **Weiter**.
- 6 Wählen Sie die Option zum Importieren aus oder erstellen Sie eine Sysprep-Antwortdatei und klicken Sie auf **Weiter**.

Option	Beschreibung
Sysprep-Antwortdatei importieren	Klicken Sie auf Durchsuchen und navigieren Sie zu der Datei.
Sysprep-Antwortdatei erstellen	Geben Sie den Inhalt der Datei in das Textfeld ein.

- 7 Wählen Sie die Netzwerkeinstellungen für das Gastbetriebssystem aus.

Option	Aktion
Typische Einstellungen	Wählen Sie Typische Einstellungen und klicken Sie auf Weiter . vCenter Server konfiguriert alle Netzwerkschnittstellen von einem DHCP-Server aus und verwendet die Standardeinstellungen.
Benutzerdefinierte Einstellungen	<ol style="list-style-type: none"> a Wählen Sie Benutzerdefinierte Einstellungen und klicken Sie auf Weiter. b Klicken Sie für jede Netzwerkschnittstelle in der virtuellen Maschine auf die Schaltfläche mit dem Auslassungszeichen (...). c Geben Sie die IP-Adresse und andere Netzwerkeinstellungen ein und klicken Sie auf OK. d Wenn die Konfiguration aller Netzwerkschnittstellen abgeschlossen ist, klicken Sie auf Weiter.

- 8 (Optional) Wählen Sie die Option „Neue Sicherheits-ID (SID) erzeugen“ aus und klicken Sie auf **Weiter**.

Einige Windows-Betriebssysteme verwenden eine Sicherheits-IDs (SIDs), um Systeme und Benutzer eindeutig identifizieren zu können. Wenn sie diese Option nicht auswählen, erhält die neue virtuelle Maschine dieselbe SID wie die virtuelle Maschine oder die Vorlage, auf deren Grundlage sie geklont bzw. bereitgestellt wurde.

Mehrfach vergebene SIDs verursachen keine Probleme, wenn die Computer zu einer Domäne gehören und nur Domänenbenutzerkonten verwendet werden. Sind die Computer allerdings Teil einer Arbeitsgruppe oder werden lokale Benutzerkonten verwendet, können solche SIDs die Dateizugriffssteuerung beeinträchtigen. Weitere Informationen zur Konfiguration der Authentifizierung finden Sie in der Dokumentation zu Ihrem Microsoft Windows-Betriebssystem.

- 9 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern.

Die von Ihnen erstellte Anpassungsspezifikation wird im Anpassungsspezifikations-Manager angezeigt. Sie können die Spezifikation zum Anpassen der Gastbetriebssysteme von virtuellen Maschinen verwenden.

Bearbeiten einer Anpassungsspezifikation im vSphere-Client

Sie können vorhandene Spezifikationen unter Verwendung des Anpassungsspezifikations-Managers bearbeiten.

Voraussetzungen

Sie müssen über mindestens eine Anpassungsspezifikation verfügen.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie mit der rechten Maustaste auf eine Spezifikation und wählen Sie **Bearbeiten**.
- 3 Fahren Sie im Assistenten Gastanpassung fort, um Spezifikationseinstellungen zu ändern.

Entfernen einer Anpassungsspezifikation im vSphere-Client

Sie können Spezifikationen aus dem Anpassungsspezifikations-Manager entfernen.

Voraussetzungen

Sie müssen über mindestens eine Anpassungsspezifikation verfügen.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie mit der rechten Maustaste auf eine Spezifikation und wählen Sie **Entfernen**.
- 3 Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Die Spezifikation wird von der Festplatte gelöscht.

Kopieren einer Anpassungsspezifikation im vSphere-Client

Sie können eine vorhandene Anpassungsspezifikation unter Verwendung des Anpassungsspezifikations-Managers kopieren.

Voraussetzungen

Sie müssen über mindestens eine Anpassungsspezifikation verfügen.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie mit der rechten Maustaste auf eine Spezifikation und wählen Sie **Kopieren**.

Eine neue Spezifikation „Kopie von *Name_der_Spezifikation*“ wird erstellt.

Exportieren einer Anpassungsspezifikation im vSphere Client

Sie können Anpassungsspezifikationen exportieren und sie als .xml-Dateien speichern. Importieren Sie die .xml-Datei unter Verwendung des Anpassungsspezifikations-Managers, um eine exportierte Spezifikation auf eine virtuelle Maschine anzuwenden.

Voraussetzungen

Sie müssen über mindestens eine Anpassungsspezifikation verfügen.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie mit der rechten Maustaste auf eine Spezifikation und wählen Sie **Exportieren**.
- 3 Geben Sie einen Dateinamen und einen Speicherort in das Dialogfeld **Speichern unter** ein.
- 4 Klicken Sie auf **Speichern**.

Die Spezifikation wird als .xml-Datei am von Ihnen angegebenen Speicherort gespeichert.

Importieren einer Anpassungsspezifikation im vSphere-Client

Sie können eine vorhandene Spezifikation unter Verwendung des Anpassungsspezifikations-Managers importieren und die Spezifikation verwenden, um das Gastbetriebssystem einer virtuellen Maschine anzupassen.

Voraussetzungen

Bevor Sie beginnen, müssen Sie mindestens eine Anpassungsspezifikation als XML-Datei auf einem Dateisystem speichern, auf das Sie über Ihren vSphere-Client zugreifen können.

Vorgehensweise

- 1 Wählen Sie auf der Home-Seite des vSphere-Clients die Option **Anpassungsspezifikations-Manager**.
- 2 Klicken Sie auf **Import**.
- 3 Wählen Sie im Dialogfeld „Öffnen“ die zu importierende .xml-Datei aus und klicken Sie auf **Öffnen**.

Die importierte Spezifikation wird zur Liste der Anpassungsspezifikationen hinzugefügt.

Migrieren von virtuellen Maschinen im vSphere Client

13

Sie können virtuelle Maschinen mit der Cold-Migration oder im laufenden Betrieb von einem Host oder Speicherort an einen anderen Speicherort verschieben. Beispiel: Mit vMotion können Sie eingeschaltete virtuelle Maschinen von einem Host verschieben, und zwar für Wartungsarbeiten sowie zur Lastenverteilung, Zusammenführung von virtuellen Maschinen, die miteinander kommunizieren, Trennung von virtuellen Maschinen zur Fehlerminimierung, Migration auf eine neue Server-Hardware usw.

Sie können eine Cold- oder Hot-Migration durchführen, um virtuelle Maschinen auf verschiedene Hosts oder Datenspeicher zu verschieben.

Cold-Migration

Sie können eine ausgeschaltete oder angehaltene virtuelle Maschine auf einen neuen Host verschieben. Sie können auch Konfigurations- und Festplattendateien für ausgeschaltete oder angehaltene virtuelle Maschinen an neue Speicherorte verschieben. Sie können die Cold-Migration auch zum Verschieben virtueller Maschinen von einem Datacenter auf ein anderes verwenden. Für eine Cold-Migration können Sie virtuelle Maschinen manuell verschieben oder eine geplante Aufgabe vorbereiten.

Migration im laufenden Betrieb

Je nach angewendeter Migrationsart (vMotion oder Storage vMotion) können Sie eine eingeschaltete virtuelle Maschine ohne Unterbrechung der Verfügbarkeit auf einen anderen Host oder ihre Festplatten oder Ordner in einen anderen Datenspeicher verschieben. vMotion wird auch als „Live Migration“ oder „Migration im laufenden Betrieb“ bezeichnet.

Es ist nicht möglich, eine eingeschaltete virtuelle Maschine von einem Datacenter in ein anderes zu verschieben.

HINWEIS Wenn Sie eine virtuelle Maschine kopieren, wird tatsächlich eine neue virtuelle Maschine erstellt. Es handelt sich dabei nicht um eine Migration. Durch das Klonen einer virtuellen Maschine oder das Kopieren ihrer Festplatten und ihrer Konfigurationsdatei wird eine neue virtuelle Maschine erstellt. Beim Klonen handelt es sich nicht um eine Migration.

Sie haben die folgenden Migrationsoptionen in vCenter Server:

Host ändern	Eine virtuelle Maschine auf einen anderen Host verschieben, jedoch nicht ihre Datenspeicher. Sie können eine virtuelle Maschine mit der Cold-Migration oder der Migration im laufenden Betrieb verschieben. Sie können vMotion verwenden, um eine eingeschaltete virtuelle Maschine auf einen anderen Host zu verschieben.
Datenspeicher ändern	Verschieben einer virtuellen Maschine und ihrer Speicher, einschließlich virtueller Festplatten und Konfigurationsdateien oder einer Kombination davon, in einen neuen Datenspeicher auf demselben Host. Sie können den Datenspeicher mit der Cold-Migration oder der Migration im laufenden Betrieb verschieben. Sie können die Speichermigration verwenden, um eine laufende virtuelle Maschine und ihren Speicher in einen neuen Datenspeicher zu verschieben.
Host und Datenspeicher ändern	Eine virtuelle Maschine auf einen anderen Host und ihre Festplatten oder den Ordner der virtuellen Maschine in einen anderen Datenspeicher verschieben. Sie können den Host und den Datenspeicher mit der Cold-Migration oder der Migration im laufenden Betrieb verschieben. Die Migration im laufenden Betrieb ist eine Kombination von Storage vMotion und vMotion.

Um virtuelle Maschinen mit Festplatten größer als 2 TB zu migrieren, müssen die Quell- und Zielhosts ESXi 5.5 oder höher ausführen.

Dieses Kapitel behandelt die folgenden Themen:

- „[Migrieren einer eingeschalteten virtuellen Maschine mit vMotion im vSphere Client](#)“, auf Seite 136
- „[Migrieren einer virtuellen Maschine mit Storage vMotion im vSphere Client](#)“, auf Seite 137
- „[Migrieren einer ausgeschalteten oder angehaltenen virtuellen Maschine im vSphere Client](#)“, auf Seite 138
- „[CPU-Kompatibilität und EVC](#)“, auf Seite 140

Migrieren einer eingeschalteten virtuellen Maschine mit vMotion im vSphere Client

Sie können den Assistenten für die Migration verwenden, um eine eingeschaltete virtuelle Maschine von einem Host zu einem anderen unter Verwendung der vMotion-Technologie zu migrieren. Migrieren Sie die virtuelle Maschine unter Verwendung von Storage vMotion, um die Festplatten einer eingeschalteten virtuellen Maschine zu verlagern.

Voraussetzungen

Stellen Sie vor dem Migrieren einer virtuellen Maschine mit vMotion sicher, dass die Hosts und virtuellen Maschinen die Anforderungen für die Migration mit vMotion erfüllen. Weitere Informationen zur Hostkonfiguration und den Bedingungen und Einschränkungen bei virtuellen Maschinen für vMotion finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine, die Sie migrieren möchten, aus der Bestandsliste aus.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie im Popup-Menü **Migrieren** aus.
- 3 Wählen Sie **Host ändern** und klicken Sie auf **Weiter**.

- 4 Wählen Sie einen Zielhost oder -Cluster für die virtuelle Maschine aus.

Etwaige Kompatibilitätsprobleme werden im Fenster „Kompatibilität“ angezeigt. Beheben Sie dieses Problem, oder wählen Sie einen anderen Host oder Cluster aus.

Zu den Zielen gehören Hosts und vollautomatisierte DRS-Cluster. Sie können als Ziel ebenfalls einen nicht automatisierten Cluster wählen. Sie werden aufgefordert, einen Host innerhalb des nicht automatisierten Clusters auszuwählen.

- 5 Wählen Sie einen Ressourcenpool aus und klicken Sie auf **Weiter**.
- 6 Wählen Sie die Prioritätsstufe für die Migration aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Hohe Priorität	<p>Auf Hosts, auf denen ESX/ESXi Version 4.1 oder höher ausgeführt wird, versucht vCenter Server, Ressourcen sowohl auf dem Quell- als auch auf dem Zielhost zu reservieren, die bei allen gleichzeitig durchgeführten Migrationen mit vMotion gemeinsam genutzt werden sollen. vCenter Server vergibt Migrationen mit hoher Priorität einen größeren Anteil an Host-CPU-Ressourcen als Migrationen mit Standardpriorität. Migrationen laufen stets ab ungeachtet der Ressourcen, die reserviert wurden.</p> <p>Auf Hosts, auf denen ESX/ESXi Version 4.0 oder früher ausgeführt wird, versucht vCenter Server, für jede Migration eine feste Menge von Ressourcen sowohl auf dem Quell- als auch auf dem Zielhost zu reservieren. Vorgänge mit hoher Priorität werden nicht fortgesetzt, wenn die erforderlichen Ressourcen nicht verfügbar sind.</p>
Standardpriorität	<p>Auf Hosts, auf denen ESX/ESXi Version 4.1 oder höher ausgeführt wird, reserviert vCenter Server Ressourcen sowohl auf dem Quell- als auch auf dem Zielhost, die bei allen gleichzeitig durchgeführten Migrationen mit vMotion gemeinsam genutzt werden sollen. vCenter Server vergibt Migrationen mit Standardpriorität einen kleineren Anteil an Host-CPU-Ressourcen als Migrationen mit hoher Priorität. Migrationen laufen stets ab ungeachtet der Ressourcen, die reserviert wurden.</p> <p>Auf Hosts, auf denen ESX/ESXi Version 4.0 oder früher ausgeführt wird, versucht vCenter Server, für jede Migration eine feste Menge von Ressourcen auf dem Quell- und dem Zielhost zu reservieren. Migrationen mit Standardpriorität werden immer ausgeführt. Die Migration läuft möglicherweise langsamer ab oder schlägt fehl, falls nicht genügend Ressourcen verfügbar sind.</p>

- 7 Überprüfen Sie die Seite, und klicken Sie auf **Beenden**.

Es wird eine Aufgabe erstellt, die den Prozess zur Migration der virtuellen Maschine startet.

Migrieren einer virtuellen Maschine mit Storage vMotion im vSphere Client

Verwenden Sie die Migration mit Storage vMotion, um die Konfigurationsdatei und die virtuellen Festplatten einer eingeschalteten virtuellen Maschine zu verlagern.

Während einer Migration mit Storage VMotion können Sie den Ausführungshost der virtuellen Maschine nicht ändern.

Vorgehensweise

- 1 Wählen Sie die virtuelle Maschine, die Sie migrieren möchten, aus der Bestandsliste aus.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie im Popup-Menü **Migrieren** aus.
- 3 Wählen Sie **Datenspeicher ändern** und klicken Sie auf **Weiter**.

4 Auswählen eines Festplattenformats.

Option	Beschreibung
Wie Quelle	Verwenden Sie das Format der ursprünglichen virtuellen Festplatte.
Mit Thin Provisioning bereitgestellt	Verwenden Sie das Thin-Provisioning-Format, um Speicherplatz zu sparen. Die schnelle virtuelle Festplatte verwendet genau die Menge an Speicherplatz, die sie für ihre anfänglichen Vorgänge benötigt. Wenn die virtuelle Festplatte mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.
Thick	Weisen Sie der virtuellen Festplatte eine feste Menge an Festplattenspeicherplatz zu. Die virtuelle Festplatte im Thick-Format ändert ihre Größe nicht und belegt von Anfang an den gesamten für sie bereitgestellten Datenspeicherplatz.

5 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Maschine speichern möchten.

Option	Aktion
Alle Dateien der virtuellen Maschine am selben Speicherort auf einem Datenspeicher speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Alle Dateien der virtuellen Maschine in demselben Datenspeicher-Cluster speichern.	<p>a Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie.</p> <p>Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.</p> <p>b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter.</p>
Speichern Sie die Konfigurationsdateien der virtuellen Maschine und die Festplatte an verschiedenen Orten.	<p>a Klicken Sie auf Erweitert.</p> <p>b Klicken Sie für die Konfigurationsdatei der virtuellen Maschine und für jede virtuelle Festplatte auf Durchsuchen und wählen Sie einen Datenspeicher oder Datenspeicher-Cluster aus.</p> <p>c Klicken Sie auf Weiter.</p>

6 Überprüfen Sie die Seite, und klicken Sie auf **Beenden**.

Migrieren einer ausgeschalteten oder angehaltenen virtuellen Maschine im vSphere Client

Sie können den Assistenten für die Migration verwenden, um eine ausgeschaltete oder angehaltene virtuelle Maschine zu migrieren.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Migrieren**.
 - a Wählen Sie zum Suchen einer virtuellen Maschine ein Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool, einen Host oder eine vApp aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** und klicken Sie dann auf **Virtuelle Maschinen**.

- 2 Wählen Sie den Migrationstyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Nur Computing-Ressource ändern	Virtuelle Maschine auf einen anderen Host verschieben.
Nur Speicher ändern	Die Konfigurationsdatei und die virtuellen Festplatten der virtuellen Maschine verschieben.
Sowohl Computing- als auch Speicherressourcen ändern	Die virtuelle Maschine, die Konfigurationsdatei und die virtuellen Festplatten auf einen anderen Host verschieben.
Virtuelle Maschine(n) zu einem bestimmten Datacenter migrieren	Verschieben Sie die virtuelle Maschine in ein virtuelles Datacenter, wo Sie virtuellen Maschinen Richtlinien zuweisen können.

- 3 Wenn Sie die virtuelle Maschine auf einen anderen Host verschieben möchten, wählen Sie den Zielhost oder Cluster für diese VM-Migration und klicken Sie auf **Weiter**.

Etwaige Kompatibilitätsprobleme werden im Fenster „Kompatibilität“ angezeigt. Beheben Sie dieses Problem, oder wählen Sie einen anderen Host oder Cluster aus.

Mögliche Ziele sind Hosts und DRS-Cluster mit einer beliebigen Automatisierungsebene. Wenn bei einem Cluster DRS nicht aktiviert ist, wählen Sie anstatt des Clusters selbst einen bestimmten Host im Cluster aus.

- 4 Wählen Sie die Zielressource für die Migration der virtuellen Maschine aus.
- 5 Wenn Sie ausgewählt haben, die Konfigurationsdatei und die virtuellen Festplatten der virtuellen Maschine zu verschieben, wählen Sie ein Festplattenformat aus.

Option	Beschreibung
Wie Quelle	Verwenden Sie das Format der ursprünglichen virtuellen Festplatte.
Mit Thin Provisioning bereitgestellt	Verwenden Sie das Thin-Provisioning-Format, um Speicherplatz zu sparen. Die schnelle virtuelle Festplatte verwendet genau die Menge an Speicherplatz, die sie für ihre anfänglichen Vorgänge benötigt. Wenn die virtuelle Festplatte mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.
Thick	Weisen Sie der virtuellen Festplatte eine feste Menge an Festplattenspeicherplatz zu. Die virtuelle Festplatte im Thick-Format ändert ihre Größe nicht und belegt von Anfang an den gesamten für sie bereitgestellten Datenspeicherplatz.

Festplatten werden nur beim Kopieren von einem Datenspeicher auf einen anderen vom Thin- ins Thick-Format oder vom Thick- ins Thin-Format konvertiert. Wenn Sie eine Festplatte an ihrem ursprünglichen Speicherort lassen, wird das Festplattenformat nicht konvertiert, auch wenn hier eine Änderung ausgewählt wurde.

- 6 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Maschine speichern möchten.

Option	Aktion
Alle Dateien der virtuellen Maschine am selben Speicherort auf einem Datenspeicher speichern.	a (Optional) Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie . Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.
	b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter .
Alle Dateien der virtuellen Maschine in demselben Datenspeicher-Cluster speichern.	a (Optional) Übernehmen Sie eine Speicherrichtlinie für die Home-Dateien und virtuellen Festplatten der virtuellen Maschine aus dem Dropdown-Menü VM-Speicherrichtlinie . Die Liste zeigt, welche Datenspeicher mit dem ausgewählten Speicherprofil der virtuellen Maschine kompatibel bzw. inkompatibel sind.
	b Wählen Sie einen Datenspeicher-Cluster aus.
	c (Optional) Wenn Sie Speicher-DRS nicht mit dieser virtuellen Maschine verwenden möchten, wählen Sie Speicher-DRS für diese virtuelle Maschine deaktivieren und wählen Sie einen Datenspeicher im Datenspeicher-Cluster aus.
	d Klicken Sie auf Weiter .
Die Konfigurationsdateien der virtuellen Maschine und die Festplatten an verschiedenen Speicherorten speichern.	a Klicken Sie auf Erweitert .
	b Klicken Sie für die Konfigurationsdatei der virtuellen Maschine und für jede virtuelle Festplatte auf Durchsuchen und wählen Sie einen Datenspeicher oder Datenspeicher-Cluster aus.
	c (Optional) Übernehmen Sie eine Speicherrichtlinie für eine virtuelle Maschine aus dem Dropdown-Menü VM Storage Profile . Die Liste zeigt, welche Datenspeicher mit der ausgewählten Speicherrichtlinie der virtuellen Maschine kompatibel bzw. inkompatibel sind.
	d (Optional) Wenn Sie einen Datenspeicher-Cluster ausgewählt haben und Speicher-DRS nicht mit dieser virtuellen Maschine verwenden möchten, aktivieren Sie die Option Speicher-DRS für diese virtuelle Maschine deaktivieren und wählen Sie einen Datenspeicher im Datenspeicher-Cluster aus.
	e Klicken Sie auf Weiter .

- 7 Überprüfen Sie die Seite, und klicken Sie auf **Beenden**.

vCenter Server verschiebt die virtuelle Maschine auf den neuen Host. Auf der Registerkarte **Ereignisse** werden Ereignismeldungen angezeigt. Die auf der Registerkarte **Übersicht** angezeigten Daten geben den Status und den Betriebszustand während der gesamten Migration an. Wenn während der Migration Fehler auftreten, werden die virtuellen Maschinen auf ihre ursprünglichen Status und Speicherorte zurückgesetzt.

CPU-Kompatibilität und EVC

vCenter Server führt vor der Migration von ausgeführten oder angehaltenen virtuellen Maschinen Kompatibilitätsprüfungen durch, um sicherzustellen, dass die virtuelle Maschine mit dem Zielhost kompatibel ist.

vMotion überträgt den aktuellen Status einer virtuellen Maschine innerhalb der zugrunde liegenden ESXi-Systeme. Eine Live-Migration setzt voraus, dass die Prozessoren des Zielhosts die virtuelle Maschine nach der Migration mit den gleichen Instruktionen versorgen, die die Prozessoren des Quellhosts vor der Migration bereitgestellt hatten. Die Taktfrequenz, die Cachegröße und die Anzahl der Kerne können sich zwischen den Quell- und Zielprozessoren unterscheiden. Die Prozessoren müssen jedoch aus derselben Anbieterklasse stammen (AMD oder Intel), um mit vMotion kompatibel zu sein.

HINWEIS Fügen Sie keine ESXi-Hosts zu einem EVC-Cluster hinzu. Virtuelle ESXi-Maschinen werden in EVC-Clustern nicht unterstützt.

Migrationen angehaltener virtueller Maschinen erfordern zudem, dass die virtuelle Maschine die Ausführung mit gleichwertigen Anweisungen auf dem Zielhost fortsetzen kann.

Beim Initiieren einer Migration mit vMotion oder einer angehaltenen virtuellen Maschine überprüft der Assistent für das Migrieren einer virtuellen Maschine den Zielhost auf Kompatibilität und generiert eine Fehlermeldung, wenn Kompatibilitätsprobleme vorliegen, die eine Migration unmöglich machen.

Der dem Betriebssystem und den in der virtuellen Maschine ausgeführten Anwendungen zur Verfügung stehende CPU-Befehlssatz wird festgelegt, wenn die virtuelle Maschine eingeschaltet wird. Dieser Funktionssatz der CPU wird anhand der folgenden Elemente festgelegt:

- Host-CPU-Familie und -Modell
- Einstellungen im BIOS, die möglicherweise CPU-Funktionen deaktivieren
- Die ESX/ESXi-Version, die auf dem Host ausgeführt wird
- Die Kompatibilitätseinstellung der virtuellen Maschine
- Das Gastbetriebssystem der virtuellen Maschine

Zur Verbesserung der CPU-Kompatibilität zwischen Hosts mit unterschiedlichen CPU-Funktionssätzen können einige CPU-Funktionen vor der virtuellen Maschine verborgen werden, indem der Host in einem EVC-Cluster (Enhanced vMotion Compatibility) platziert wird.

HINWEIS Die Funktionen der Host-CPU können auch vor einer virtuellen Maschine verborgen werden, indem Sie auf der virtuellen Maschine eine benutzerdefinierte CPU-Kompatibilitätsmaske anwenden. Dies wird allerdings nicht empfohlen. VMware arbeitet mit CPU- und Hardwareanbietern zusammen, um eine vMotion-Kompatibilität für eine möglichst breite Palette an Prozessoren zu gewährleisten. Weitere Informationen finden Sie, indem Sie in der VMware-Knowledgebase nach *suchen (FAQ zu vMotion und CPU-Kompatibilität)*..

Erstellen eines EVC-Clusters

Erstellen Sie einen EVC-Cluster, um die vMotion-Kompatibilität zwischen den Hosts in einem Cluster sicherzustellen.

Verwenden Sie beim Erstellen eines EVC-Clusters eine der folgenden Methoden:

- Erstellen Sie einen leeren Cluster, aktivieren Sie EVC, und verschieben Sie Hosts in den Cluster.
- Aktivieren Sie EVC für einen vorhandenen Cluster.

Es wird empfohlen, einen leeren EVC-Cluster zu erstellen, da dies die einfachste Methode ist, einen EVC-Cluster mit minimalem Ausfall für die vorhandene Infrastruktur zu erstellen.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.
- Stellen Sie vor dem Aktivieren eines EVC-Clusters sicher, dass die Hosts, die Sie dem Cluster hinzufügen möchten, die in der Dokumentation zu *vCenter Server und Hostverwaltung* aufgeführten Anforderungen erfüllen.

Vorgehensweise

- 1 Klicken Sie im vSphere Client mit der rechten Maustaste auf ein Datacenter und wählen Sie **Neuer Cluster**.
- 2 Geben Sie einen Namen für den Cluster ein und wählen Sie die Clusterfunktionen aus. Klicken Sie anschließend auf **Weiter**.

Clusterfunktionen wie vSphere DRS und vSphere HA sind mit EVC vollständig kompatibel. Sie können diese Funktionen beim Erstellen des Clusters aktivieren. Weitere Informationen zu spezifischen Clusteroptionen finden Sie in der Online-Hilfe vom vSphere Client.

- 3 Wählen Sie den CPU-Anbieter und den entsprechenden EVC-Modus für die Hosts aus, die Sie dem Cluster hinzufügen möchten, und klicken Sie auf **Weiter**.
- 4 Wählen Sie die Auslagerungsdatei-Richtlinie aus und klicken Sie auf **Weiter**.
- 5 Prüfen Sie die ausgewählten Optionen für diesen Cluster und klicken Sie auf **Beenden**, um den Cluster zu erstellen.
- 6 Wählen Sie in der Bestandsliste einen Host zum Verschieben in den Cluster aus.
- 7 Wenn der Funktionssatz des Hosts größer als der EVC-Modus ist, den Sie für den EVC-Cluster aktiviert haben, stellen Sie sicher, dass auf dem Cluster keine virtuellen Maschinen eingeschaltet sind.
 - Schalten Sie alle virtuellen Maschinen auf dem Host aus.
 - Migrieren Sie die virtuellen Maschinen des Hosts mit vMotion auf einen anderen Host.
- 8 Verschieben Sie den Host in den Cluster.

Sie können die virtuellen Maschinen auf dem Host einschalten oder mit vMotion virtuelle Maschinen auf den Cluster migrieren, vorausgesetzt, sie erfüllen die CPU-Kompatibilitätsanforderungen für den EVC-Modus des Clusters. Virtuelle Maschinen, die auf Hosts mit mehr Funktionen ausgeführt werden als der EVC-Modus, müssen vor der Migration in den Cluster ausgeschaltet werden.
- 9 Wiederholen Sie [Schritt 7](#) und [Schritt 8](#) für jeden weiteren Host, den Sie in den Cluster verschieben möchten.

Aktivieren von EVC für einen vorhandenen Cluster

Aktivieren Sie EVC auf einem vorhandenen Cluster, um die VMotion-Kompatibilität zwischen den Hosts im Cluster sicherzustellen.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.
- Stellen Sie vor dem Aktivieren von EVC auf einem vorhandenen Cluster sicher, dass die Hosts im Cluster die in der Dokumentation zu *vCenter Server und Hostverwaltung* aufgeführten Anforderungen erfüllen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den Cluster aus, für den Sie EVC aktivieren möchten.
- 2 Wenn virtuelle Maschinen auf Hosts ausgeführt werden, die größere Funktionssätze als der EVC-Modus haben, den Sie aktivieren möchten, stellen Sie sicher, dass im Cluster keine virtuellen Maschinen eingeschaltet sind.
 - Schalten Sie alle virtuellen Maschinen auf den Hosts aus, die größere Funktionssätze als der EVC-Modus haben.
 - Migrieren Sie die virtuellen Maschinen des Clusters mit vMotion auf einen anderen Host.

Weil diese virtuellen Maschinen mit mehr Funktionen als der EVC-Modus ausgeführt werden, den Sie einstellen möchten, müssen Sie die virtuellen Maschinen ausschalten, um sie zurück in den Cluster zu migrieren, nachdem EVC aktiviert wurde.
- 3 Stellen Sie sicher, dass der Cluster Hosts mit CPUs von nur einem Hersteller enthält (entweder Intel oder AMD).
- 4 Bearbeiten Sie die Clustereinstellungen, und aktivieren Sie EVC.

Wählen Sie den CPU-Hersteller und Funktionssatz für die Hosts im Cluster aus.

- 5 Wenn Sie virtuelle Maschinen ausgeschaltet oder aus dem Cluster migriert haben, schalten Sie die betreffenden virtuellen Maschinen im Cluster ein oder migrieren Sie sie auf den Cluster.

Virtuelle Maschinen, die mit einem größeren Funktionssatz als der für den Cluster aktivierte EVC-Modus ausgeführt werden, müssen ausgeschaltet werden, bevor sie wieder in den Cluster verschoben werden können.

Ändern des EVC-Modus für einen Cluster

Wenn alle Hosts in einem Cluster mit dem neuen Modus kompatibel sind, können Sie den EVC-Modus eines vorhandenen EVC-Clusters ändern. Sie können den EVC-Modus erhöhen, um mehr CPU-Funktionen freizulegen, oder herabsetzen, um CPU-Funktionen zu verbergen und die Kompatibilität zu erhöhen.

Zum Erhöhen des EVC-Modus von einer CPU-Baseline mit weniger Funktionen zu einer mit mehr Funktionen müssen Sie keine der im Cluster ausgeführten virtuellen Maschinen ausschalten. Gestartete virtuelle Maschinen haben keinen Zugriff auf die neu verfügbaren Funktionen des neuen EVC-Modus, bis sie ausgeschaltet und wieder eingeschaltet wurden. Die virtuelle Maschine muss dazu vollständig ausgeschaltet und wieder eingeschaltet werden. Das Neustarten des Gastbetriebssystems oder das Anhalten und Fortsetzen der virtuellen Maschine genügt nicht.

Zum Herabsetzen des EVC-Modus von einer CPU-Baseline mit mehr Funktionen zu einer mit weniger Funktionen müssen Sie zuerst die virtuellen Maschinen im Cluster ausschalten, die einen höheren EVC-Modus aufweisen als denjenigen, die Sie aktivieren möchten, und nach dem Aktivieren des neuen Modus wieder einschalten.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.
- Wenn Sie vorhaben, den EVC-Modus herabzusetzen, schalten Sie alle ausgeführten virtuellen Maschinen aus, die einen höheren EVC-Modus aufweisen als denjenigen, die Sie aktivieren möchten. Siehe [„Ermitteln der EVC-Modi virtueller Maschinen“](#), auf Seite 144.

Vorgehensweise

- 1 Zeigen Sie den Cluster in der Bestandsliste an.
- 2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie im linken Fensterbereich **VMware EVC**.
Das Dialogfeld zeigt die aktuellen EVC-Einstellungen an.
- 4 Zum Ändern der EVC-Einstellungen klicken Sie auf **EVC-Modus ändern**.
- 5 Wählen Sie im Dropdown-Menü **VMware EVC-Modus** den Baseline-CPU-Funktionssatz, den Sie für den Cluster aktivieren möchten.
Wenn der ausgewählte EVC-Modus nicht aktiviert werden kann, zeigt das Kompatibilitätsfenster den Grund bzw. die Gründe und die dafür relevanten Hosts an.
- 6 Klicken Sie auf **OK**, um das Dialogfeld EVC-Modus zu schließen, und klicken Sie anschließend erneut auf **OK**, um das Dialogfeld für Clustereinstellungen zu schließen.

Ermitteln der EVC-Modi virtueller Maschinen

Der EVC-Modus einer virtuellen Maschine definiert die CPU-Funktionen, auf die die virtuelle Maschine zugreifen kann. Der EVC-Modus der virtuellen Maschine wird ermittelt, wenn sie in einem EVC-fähigen Cluster eingeschaltet wird.

Eine virtuelle Maschine ruft den EVC-Modus des Clusters ab, in dem sie läuft, wenn sie eingeschaltet wird. Wird der EVC-Modus des Clusters im Nachhinein erhöht, ändert die virtuelle Maschine ihren EVC-Modus nicht, bis sie aus- und wieder eingeschaltet wird. Das hat zur Folge, dass die virtuelle Maschine die zusätzlichen CPU-Funktionen im neuen EVC-Modus des Clusters erst nach dem Neustart verwenden kann.

Angenommen, in Ihrem Cluster wurden Hosts mit Prozessoren des Typs Intel Xeon 45nm Core™ 2 in den EVC-Modus „Intel® "Merom" Generation (Xeon® Core™ 2)“ versetzt. Eine der eingeschalteten virtuellen Maschinen in diesem Cluster wird im EVC-Modus „Intel "Merom" Generation (Xeon Core 2)“ ausgeführt. Wird der EVC-Modus des Clusters auf „Intel "Penryn" Generation (Xeon 45nm Core 2)“ angehoben, verbleibt die virtuelle Maschine im niedrigeren EVC-Modus „Intel "Merom" Generation (Xeon Core 2)“. Um eine der durch den höheren EVC-Modus des Clusters offengelegten Funktionen (z. B. SSE4.1) verwenden zu können, müssen Sie die virtuelle Maschine aus- und wieder einschalten.

Sie können auf der Registerkarte „Virtuelle Maschinen“ eines Clusters oder eines Hosts den EVC-Modus der ausgeführten virtuellen Maschinen ermitteln.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Wählen Sie den Cluster oder Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Virtuelle Maschinen (Virtual Machines)**.
- 3 Wird die Spalte „EVC-Modus“ nicht angezeigt, klicken Sie mit der rechten Maustaste auf die Spaltentitel und wählen Sie **EVC-Modus** aus.

Die EVC-Modi aller ausgeführten oder angehaltenen virtuellen Maschinen werden in der Spalte **EVC-Modus** angezeigt. Ausgeschaltete virtuelle Maschinen sowie virtuelle Maschinen, die sich nicht in einem EVC-Cluster befinden, zeigen als EVC-Modus „Nicht verfügbar“ an.

Vorbereiten von Clustern für AMD-Prozessoren ohne 3DNow!

Generationen von AMD-Prozessoren enthalten keine 3DNow!-Prozessoranweisungen. Wenn Hosts in einem Cluster verschiedene Generationen von AMD-Prozessoren verwenden, von denen einige 3DNow!-Anweisungssätze haben und andere nicht, können Sie virtuelle Maschinen nicht erfolgreich zwischen den Hosts migrieren. Sie müssen einen EVC-Modus oder eine CPU-Kompatibilitätsmaske verwenden, um die Anweisungen zu verbergen.

Der vCenter Server **AMD Opteron Gen. 3 (kein 3DNow!)** maskiert die 3DNow!-Anweisungen von virtuellen Maschinen. Sie können diesen EVC-Modus auf EVC-Clustern anwenden, die nur aus AMD Opteron Generation 3-Hosts bestehen, um die vMotion-Kompatibilität dieser Cluster mit AMD Opteron-Hosts zu gewährleisten, die nicht über 3DNow!-Anweisungen verfügen. Es besteht keine Möglichkeit, die vMotion-Kompatibilität von Clustern, die AMD Opteron Generation 1- oder AMD Opteron Generation 2-Hosts enthalten, mit Hosts herzustellen, die nicht über 3DNow!-Anweisungen verfügen.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.
- Stellen Sie sicher, dass der Cluster nur Hosts mit AMD Opteron Generation 3- oder neueren Prozessoren enthält.

Vorgehensweise

- ◆ Aktivieren Sie den EVC-Modus **AMD Opteron Gen. 3 (kein 3DNow!)** für Ihren EVC-Cluster.

Die Vorgehensweise für das Aktivieren des EVC-Modus hängt davon ab, ob Sie ein Cluster erstellen oder den Modus auf einem vorhandenen Cluster anwenden möchten und ob das vorhandene Cluster eingeschaltete virtuelle Maschinen enthält.

Option	Beschreibung
Erstellen eines neuen Clusters	Aktivieren Sie im Assistenten für neue Cluster EVC für AMD-Hosts und wählen Sie den EVC-Modus AMD Opteron Gen. 3 (kein 3DNow!) aus.
Bearbeiten eines Clusters ohne eingeschaltete virtuelle Maschinen	Bearbeiten Sie im Einstellungsdialogfeld des Clusters die Einstellungen VMware EVC-Einstellungen und wählen Sie den EVC-Modus AMD Opteron Gen. 3 (kein 3DNow!) aus.
Bearbeiten eines Clusters mit eingeschalteten virtuellen Maschinen	<p>AMD Opteron Gen. 3 (kein 3DNow!) Der EVC-Modus kann nicht aktiviert werden, solange im Cluster virtuelle Maschinen ausgeführt werden.</p> <ol style="list-style-type: none"> Schalten Sie alle virtuellen Maschinen in dem Cluster aus oder migrieren Sie sie mithilfe von VMotion aus dem Cluster. <p>Mit dem Migrieren der virtuellen Maschinen aus dem Cluster mithilfe von vMotion können Sie das Ausschalten der virtuellen Maschinen auf einen geeigneten Zeitpunkt verschieben.</p> <ol style="list-style-type: none"> Bearbeiten Sie im Einstellungsdialogfeld des Clusters die Einstellungen VMware EVC-Einstellungen und wählen Sie den EVC-Modus AMD Opteron Gen. 3 (kein 3DNow!) aus. Wenn Sie die virtuellen Maschinen aus dem Cluster migriert haben, können Sie sie später ausschalten und sie mittels Cold-Migration wieder in das Cluster integrieren. Schalten Sie die virtuellen Maschinen ein.

Sie können jetzt Hosts mit AMD-Prozessoren ohne 3DNow!-Anweisungen unter Beibehaltung der vMotion-Kompatibilität zwischen neuen und vorhandenen Hosts in das Cluster aufnehmen.

Anzeigen von CPUID-Details für einen EVC-Cluster

Der von einem EVC-Cluster offengelegte Funktionsumfang entspricht dem Funktionsumfang eines bestimmten Prozessortyps. Der Funktionsumfang von Prozessoren kann durch Funktions-Flags beschrieben werden, die Sie mithilfe der CPUID-Anweisung untersuchen können.

Sie können die derzeit von den Hosts in einem EVC-Cluster offengelegten CPUID-Funktions-Flags im Dialogfeld **Aktuelle CPUID-Details** anzeigen.

Voraussetzungen

- Sie müssen über den vSphere Client mit einem vCenter Server-System verbunden sein.

Vorgehensweise

- 1 Zeigen Sie den Cluster in der Bestandsliste an.
- 2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie im linken Fensterbereich **VMware EVC**.
- 4 Um die derzeit durch EVC erzwungenen CPUID-Funktions-Flags anzuzeigen, klicken Sie auf **Aktuelle CPUID-Details**.

Im Dialogfeld **Aktuelle CPUID-Details** werden die CPUID-Funktions-Flags angezeigt, die EVC für die Hosts in diesem Cluster erzwingt. Weitere Informationen zu CPUID-Funktions-Flags finden Sie im Dokument *Intel Processor Identification and the CPUID Instruction* (zu beziehen über Intel), oder im Dokument *CPUID Specification* (zu beziehen über AMD).

Bereitstellen von OVF-Vorlagen

Sie können virtuelle Maschinen, virtuelle Appliances und vApps im OVF-Format (Open Virtual Machine Format) exportieren. Die OVF-Vorlage können Sie dann in derselben oder einer anderen Umgebung bereitstellen.

Dieses Kapitel behandelt die folgenden Themen:

- „Bereitstellen einer OVF-Vorlage im vSphere Client“, auf Seite 147
- „Export einer OVF-Vorlage“, auf Seite 149

Bereitstellen einer OVF-Vorlage im vSphere Client

Wenn Sie mithilfe des vSphere Clients eine direkte Verbindung mit einem Host herstellen, können Sie eine OVF-Vorlage aus einem lokalen Dateisystem, auf das die vSphere Client-Maschine zugreifen kann, oder über eine Web-URL bereitstellen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die Option **Datei > OVF-Vorlage bereitstellen**.

Der Assistent zum Bereitstellen von OVF-Vorlagen wird angezeigt.

- 2 Legen Sie den Quellspeicherort fest und klicken Sie auf **Weiter**.

Option	Aktion
Aus Datei bereitstellen	Durchsuchen Sie Ihr Dateisystem nach einer OVF- oder OVA-Vorlage.
Aus URL bereitstellen	Geben Sie eine URL zu einer OVF-Vorlage im Internet an. Beispiel: <code>http://vmware.com/VTN/appliance.ovf</code>

- 3 Zeigen Sie die Seite Einzelheiten zur OVF-Vorlage an und klicken Sie auf **Weiter**.
- 4 Wenn Lizenzvereinbarungen für die OVF-Vorlage gelten, erscheint die Seite mit der Endbenutzer-Lizenzvereinbarung. Stimmen Sie den Lizenzbedingungen zu, und klicken Sie auf **Weiter**.
- 5 Wählen Sie die Bereitstellungskonfiguration aus dem Dropdown-Menü aus und klicken Sie auf **Weiter**.

Die ausgewählte Option steuert in der Regel die Arbeitsspeichereinstellungen, die Anzahl der CPUs und Reservierungen sowie die Konfigurationsparameter auf Anwendungsebene.

HINWEIS Diese Seite wird nur angezeigt, wenn die OVF-Vorlage Bereitstellungsoptionen enthält.

- 6 Wählen Sie einen Datenspeicher aus, in dem die bereitgestellte OVF-Vorlagendatei gespeichert werden soll, und klicken Sie auf **Weiter**.

Datenspeicher sind eine vereinheitlichende Abstraktion für Speicherorte wie z. B. Fibre-Channel, iSCSI-LUNs oder NAS-Volumes. Auf dieser Seite wählen Sie aus den Datenspeichern aus, die Sie bereits auf dem Zielcluster oder -host konfiguriert haben. Die Konfigurationsdatei der virtuellen Maschine und die virtuellen Festplattendateien werden im Datenspeicher abgelegt. Wählen Sie einen Datenspeicher aus, der für die virtuelle Maschine und alle zugehörigen Dateien der virtuellen Festplatte groß genug ist.

- 7 Wählen Sie das Festplattenformat für die virtuellen Festplatten der virtuellen Maschine aus und klicken Sie auf **Weiter**.

Format	Beschreibung
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte benötigte Speicherplatz wird zugeteilt, wenn die virtuelle Festplatte erstellt wird. Die auf dem physischen Gerät verbleibenden Daten werden während der Erstellung nicht gelöscht, sondern beim ersten Schreibvorgang der virtuellen Maschine bei Bedarf durch Nullbyte ersetzt.
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 flachen Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt, wenn die virtuelle Festplatte erstellt wird. Möglicherweise dauert es viel länger, Festplatten in diesem Format als andere Arten von Festplatten zu erstellen.
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 Datenträgergröße eingeben. Die Festplatte besitzt jedoch zunächst nur eine geringe Größe und verwendet nur so viel Datenspeicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. Der Speicherplatz wird erhöht, wenn die virtuelle Maschine mehr Speicher benötigt.

- 8 Falls die Appliance, die Sie bereitstellen, eine oder mehrere vService-Abhängigkeiten hat, wählen Sie einen Bindungsdienstanbieter aus.
- 9 Wählen Sie für jedes in der OVF-Vorlage festgelegte Netzwerk ein Netzwerk aus, indem Sie in Ihrer Infrastruktur mit der rechten Maustaste auf die Spalte **Zielnetzwerk** klicken, um die Netzwerkzuordnung einzurichten und klicken Sie auf **Weiter**.
- 10 Konfigurieren Sie auf der Seite **IP-Zuteilung**, wie IP-Adressen für die virtuelle Appliance zugeteilt werden, und klicken Sie auf **Weiter**.

Option	Beschreibung
Fest	Sie werden aufgefordert, die IP-Adressen auf der Seite Appliance-Eigenschaften einzugeben.
Vorübergehend	IP-Adressen werden beim Einschalten der Appliance aus einem angegebenen Bereich zugeteilt. Die IP-Adressen werden freigegeben, wenn die Appliance ausgeschaltet wird.
DHCP	Zum Zuteilen der IP-Adressen wird ein DHCP-Server verwendet.

Diese Seite wird nicht angezeigt, wenn die bereitgestellte OVF-Vorlage keine Informationen über das IP-Schema enthält, das sie unterstützt.

- 11 Konfigurieren Sie die vom Benutzer konfigurierbaren Eigenschaften und klicken Sie auf **Weiter**.

Die Eigenschaften, die Sie aufgefordert werden einzugeben, hängen vom ausgewählten IP-Zuteilungsschema ab. Sie werden beispielsweise nur im Falle eines festen IP-Zuteilungsschemas nach IP-bezogenen Informationen für die bereitgestellten virtuelle Maschinen gefragt.

- 12 Überprüfen Sie die gewählten Einstellungen, und klicken Sie auf **Beenden**.

Der Fortschritt der Importaufgabe wird im Statusfenster des vSphere Clients angezeigt.

Export einer OVF-Vorlage

Ein OVF-Paket erfasst den Status einer virtuellen Maschine oder vApp und legt ihn in einem unabhängigen Paket ab. Die Festplattendateien werden in einem komprimierten Format mit geringer Datendichte gespeichert.

Erforderliche Berechtigung: **vApp.Exportieren**

Vorgehensweise

- 1 Wählen Sie im vSphere Client die virtuelle Maschine oder die vApp aus und klicken Sie **Datei > Exportieren > OVF-Vorlage exportieren**.

- 2 Geben Sie im Dialogfeld OVF-Vorlage exportieren den **Namen** der Vorlage ein.

Geben Sie z. B. **MyVM** ein.

HINWEIS Wenn Sie eine OVF-Vorlage mit einem Namen exportieren, der Sternchen (*) enthält, werden diese Zeichen in Unterstriche (_) umgewandelt.

- 3 Geben Sie unter **Verzeichnis** den Speicherort ein, an dem die exportierte Vorlage für die virtuelle Maschine gespeichert ist, oder klicken Sie auf „...“, um nach dem Speicherort zu suchen.

Der Standardspeicherort für die Vorlage ist Laufwerk C:\.

Beispiel: **OvfLib**.

- 4 Legen Sie im Feld **Format** fest, wie Sie die Dateien speichern möchten.

- Wählen Sie **Dateiordner (OVF)**, um die OVF-Vorlage in Form mehrerer Dateien zu speichern (.ovf, .vmdk und .mf). Dieses Format ist optimal, wenn Sie vorhaben, die OVF-Dateien auf einem Webserver oder in einer Image-Bibliothek zu veröffentlichen. Das Paket kann importiert werden, beispielsweise in den vSphere-Client, indem Sie die URL in der .ovf-Datei veröffentlichen.
- Wählen Sie **Einzelne Datei (OVA)**, um die OVF-Vorlage in einer einzelnen .ova-Datei zu verpacken. Es ist von Vorteil, das OVF-Paket als einzelne Datei zu verteilen, wenn es explizit von einer Website heruntergeladen oder unter Verwendung eines USB-Schlüssels verschoben werden muss.

- 5 Geben Sie unter **Beschreibung** eine Beschreibung für die virtuelle Maschine ein.

Standardmäßig wird der Text aus dem Fenster **Anmerkungen** der Registerkarte **Übersicht** der virtuellen Maschine in diesem Textfeld angezeigt.

- 6 Aktivieren Sie das Kontrollkästchen, wenn Sie Images, die den Disketten- und CD-/DVD-Laufwerken zugeordnet sind, in das OVF-Paket aufnehmen möchten.

HINWEIS Dieses Kontrollkästchen zeigt nur an, ob die virtuelle Maschine mit einer ISO-Datei oder das Disketten-Laufwerk mit einem Disketten-Image verbunden ist.

- 7 Klicken Sie auf **OK**.

Der Download-Vorgang wird im Exportfenster angezeigt.

Beispiel: Ordnerstandorte für OVF- und OVA-Dateien

Wenn Sie **OvfLib** als neuen OVF-Ordner eingeben, könnten die folgenden Dateien erstellt werden:

- C:\OvfLib\MyVm\MyVm.ovfI
- C:\OvfLib\MyVm.mf

- C:\OvfLib\MyVm-disk1.vmdk

Wenn Sie **C:\NewFolder\OvfLib** als neuen OVF-Ordner eingeben, könnten die folgenden Dateien erstellt werden:

- C:\NewFolder\OvfLib\MyVm\MyVm.ovfI
- C:\NewFolder\OvfLib\MyVm.mf
- C:\NewFolder\OvfLib\MyVm-disk1.vmdk

Wenn Sie in das OVA-Format exportieren und **MyVm** eingeben, wird die Datei C:\MyVm.ova erstellt.

Konfigurieren virtueller Maschinen im vSphere Client

15

Sie können die meisten Eigenschaften virtueller Maschinen während der Erstellung einer virtuellen Maschine oder nach dem Erstellen der virtuellen Maschine und der Installation des Gastbetriebssystems hinzufügen oder konfigurieren.

Sie können drei Typen von Eigenschaften der virtuellen Maschine konfigurieren.

Hardware	Anzeigen der vorhandenen Hardwarekonfiguration und Hinzufügen oder Entfernen von Hardware.
Optionen	Anzeigen und Konfigurieren einer Vielzahl an Eigenschaften für virtuelle Maschinen, wie z. B. die Interaktion der Energieverwaltung zwischen dem Gastbetriebssystem und der virtuellen Maschine sowie VMware Tools-Einstellungen.
Ressourcen	Konfigurieren von CPUs, CPU-Hyper-Threading-Ressourcen, Arbeitsspeicher und Festplatten.

Dieses Kapitel behandelt die folgenden Themen:

- [„VM-Einschränkungen im vSphere Client“](#), auf Seite 152
- [„VM-Hardwareversionen“](#), auf Seite 153
- [„Ermitteln der Hardwareversion einer virtuellen Maschine im vSphere-Client“](#), auf Seite 154
- [„Ändern des Namens der virtuellen Maschine im vSphere Client“](#), auf Seite 155
- [„Anzeigen des Speicherorts der Konfigurationsdatei der virtuellen Maschine im vSphere-Client“](#), auf Seite 155
- [„Bearbeiten der Parameter der Konfigurationsdatei im vSphere-Client“](#), auf Seite 156
- [„Ändern des konfigurierten Gastbetriebssystems in vSphere-Client“](#), auf Seite 156
- [„Konfigurieren von virtuellen Maschinen zum automatischen Aktualisieren der VMware Tools“](#), auf Seite 157
- [„Konfiguration virtueller CPUs“](#), auf Seite 158
- [„Konfigurieren von virtuellem Arbeitsspeicher“](#), auf Seite 165
- [„Netzwerkkonfiguration virtueller Maschinen“](#), auf Seite 169
- [„Konfiguration der parallelen und seriellen Schnittstelle“](#), auf Seite 171
- [„Konfiguration der virtuellen Festplatte“](#), auf Seite 177
- [„SCSI- und SATA-Speicher-Controller – Bedingungen, Einschränkungen und Kompatibilität“](#), auf Seite 182

- „Weitere Gerätekonfigurationen für die virtuelle Maschine“, auf Seite 186
- „Konfigurieren von vServices“, auf Seite 192
- „USB-Konfiguration von einem ESXi-Host zu einer virtuellen Maschine“, auf Seite 194
- „USB-Konfiguration von einem Clientcomputer zu einer virtuellen Maschine im vSphere-Client“, auf Seite 198
- „Verwalten von Energieverwaltungseinstellungen für eine virtuelle Maschine“, auf Seite 201
- „Konfigurieren der Betriebszustände der virtuellen Maschine“, auf Seite 202
- „Verzögern der Startsequenz in vSphere-Client“, auf Seite 204
- „Aktivieren der Protokollierung im vSphere Client“, auf Seite 204
- „Deaktivieren der Beschleunigung im vSphere Client“, auf Seite 205
- „Konfigurieren des Debuggings und der Statistiken im vSphere Client“, auf Seite 205

VM-Einschränkungen im vSphere Client

Die VM-Konfigurationsaufgaben, die Sie bei einer direkten Verbindung mit einem ESXi-Host oder einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden VM-Funktionen sind im vSphere Client nicht verfügbar bzw. schreibgeschützt:

- Intel vGPU
- AMD vGPU
- 2-TB-HDD
- 128 vCPUs für virtuelle Maschinen mit Hardwareversionen bis 10
- 32 serielle Ports für virtuelle Maschinen mit Hardwareversionen bis 10
- 255 PVSCI-Geräte
- SVGA für virtuelle Maschinen mit Hardwareversionen 10 und 11
- VMCI-Firewall
- Smartcard-Authentifizierung
- SATA-Controller und Hardwareeinstellungen
- SR-IOV-Einstellungen
- GPU-3D-Rendering und Arbeitsspeichereinstellungen
- Tuning-Latenzeinstellungen
- vSphere Flash Read Cache-Einstellungen
- Verschachtelter Hypervisor
- Schnelles Setzen von Prüfpunkten
- vCPU-Referenzzähler
- Einfache und geplante Hardware-Upgrades
- Standardkompatibilitätsebene
- VMware Tools-Berichte und -Upgrades

Über den vSphere Web Client stehen Ihnen hingegen alle Funktionen für virtuelle Maschinen in Ihrer vSphere-6.0-Umgebung zur Verfügung.

VM-Hardwareversionen

Die Hardwareversion einer virtuellen Maschine spiegelt die unterstützten virtuellen Hardwarefunktionen der virtuellen Maschine wider. Diese Funktionen entsprechen der physischen Hardware, die auf dem ESXi-Host verfügbar ist, auf dem Sie die virtuelle Maschine erstellen. Zu den virtuellen Hardwarefunktionen gehören das BIOS und EFI, die verfügbaren virtuellen PCI-Steckplätze, die maximale Anzahl an CPUs, der Maximalwert für die Arbeitsspeicherkonfiguration und weitere hardwaretypische Eigenschaften.

Wenn Sie eine virtuelle Maschine erstellen, können Sie die standardmäßige Hardwareversion, die dem Host entspricht, auf dem die virtuelle Maschine erstellt wird, oder eine vorherige Version akzeptieren. In den folgenden Situationen können Sie eine frühere Hardwareversion verwenden:

- Zum Standardisieren von Tests und der Bereitstellung in Ihrer virtuellen Umgebung.
- Wenn Sie die Funktionen der neueren Version nicht benötigen.
- Um Kompatibilität mit älteren Hosts beizubehalten.

Virtuelle Maschinen mit früheren Hardwareversionen als Version 11 können auf ESXi-6.0-Hosts ausgeführt werden, verfügen aber nicht über alle Funktionen, die in der Hardwareversion 11 verfügbar sind. Beispielsweise können Sie in virtuellen Maschinen mit Hardwareversionen vor Version 11 weder 128 virtuelle Prozessoren noch 4080 GB Arbeitsspeicher verwenden.

Im vSphere Web Client und dem vSphere Client können virtuelle Maschinen nur auf die neueste Hardwareversion aktualisiert werden. Falls virtuelle Maschinen nicht kompatibel mit älteren ESX-/ESXi-Hosts bleiben müssen, können Sie sie auf ESXi 6.0-Hosts aktualisieren. In diesem Fall werden sie auf Version 11 aktualisiert.

- Um die Kompatibilität virtueller Maschinen mit ESX/ESXi 3.5-Hosts beizubehalten, aktualisieren Sie die virtuelle Maschine auf einem ESX/ESXi 3.5-Host, wodurch die virtuelle Maschine auf Version 4 aktualisiert wird.
- Um die Kompatibilität virtueller Maschinen mit ESX/ESXi 4-Hosts beizubehalten, aktualisieren Sie die virtuelle Maschine auf einem ESX/ESXi 4.x-Host, wodurch die virtuelle Maschine auf Version 7 aktualisiert wird.
- Um die Kompatibilität virtueller Maschinen mit ESXi-5.0-Hosts zu bewahren, aktualisieren Sie die virtuelle Maschine auf einem ESX-/ESXi-5.0-Host, wodurch die virtuelle Maschine auf Version 8 aktualisiert wird.
- Um die Kompatibilität virtueller Maschinen mit ESXi-5.1-Hosts zu bewahren, aktualisieren Sie die virtuelle Maschine auf einem ESX-/ESXi-5.1-Host, wodurch die virtuelle Maschine auf Version 9 aktualisiert wird.
- Um die Kompatibilität virtueller Maschinen mit ESXi-5.5-Hosts zu bewahren, aktualisieren Sie die virtuelle Maschine auf einem ESX-/ESXi-5.5-Host, wodurch die virtuelle Maschine auf Version 10 aktualisiert wird.

Eine virtuelle Maschine kann in den folgenden Fällen eine frühere Hardwareversion haben als der Host, auf dem sie ausgeführt wird:

- Sie können eine auf einem ESX/ESXi 4.x-Host (oder früher) erstellte virtuelle Maschine auf einen ESXi 5.0-Host migrieren.
- Sie erstellen eine virtuelle Maschine auf einem ESXi 5.0-Host, indem Sie eine vorhandene virtuelle Festplatte verwenden, die auf einem ESX/ESXi 4.x-Host (oder früher) erstellt wurde.
- Sie fügen eine auf einem ESX/ESXi 4.x-Host (oder früher) erstellte virtuelle Festplatte zu einer virtuellen Maschine hinzu, die auf einem ESXi 5.0-Host erstellt wurde.

Sie können unterschiedliche Versionen virtueller Maschinen auf einem Host erstellen, bearbeiten und ausführen, sofern der Host diese Versionen unterstützt. Manchmal sind die Aktionen virtueller Maschinen auf einem Host begrenzt oder die virtuelle Maschine hat keinen Zugriff auf den Host.

Tabelle 15-1. ESXi-Hosts und kompatible Hardwareversionen der virtuellen Maschine

	Versi- on 11	Versi- on 10	Versi- on 9	Version 8	Version 7	Version 4	Kompatibel mit vCenter Ser- ver-Version
ESXi 6.0	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstellen, Be- arbeiten, Ausführen	vCenter Server 6.0
ESXi 5.5	Nicht unter- stützt	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstellen, Be- arbeiten, Ausführen	vCenter Server 5.5 und höher
ESXi 5.1	Nicht unter- stützt	Nicht unter- stützt	Erstel- len, Be- arbei- ten, Aus- führen	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstellen, Be- arbeiten, Ausführen	vCenter Server 5.1 und höher
ESXi 5.0	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstellen, Be- arbeiten, Ausführen	vCenter Server 5.0 und höher
ESX/ESXi 4.x	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Erstel- len, Be- arbei- ten, Ausfüh- ren	Erstellen, Be- arbeiten, Ausführen	vCenter Server 4.x und höher
ESX/ESXi 3.x	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Nicht unter- stützt	Erstellen, Be- arbeiten, Ausführen	vCenter Server 3.5 und höher

Virtuelle Maschinen vor Hardwareversion 4 werden auf ESXi-6.0-Hosts nicht unterstützt. Zur vollständigen Nutzung dieser virtuellen Maschinen müssen Sie die virtuelle Hardware aktualisieren.

HINWEIS Die Funktionen in VM-Hardwareversionen 9, 10 und 11 gehen nicht über Hardwareversion 8 und früher hinaus, wenn sie über den vSphere Client mit einem ESXi-Host oder einem vCenter Server-System verbunden sind.

Ermitteln der Hardwareversion einer virtuellen Maschine im vSphere-Client

Sie finden die Hardwareversion einer virtuellen Maschine auf der Registerkarte **Übersicht** der virtuellen Maschine oder im Eigenschaftendialogfeld der virtuellen Maschine. Zudem finden Sie die Hardwareversion für mehrere virtuellen Maschinen auf der Registerkarte **Virtuelle Maschine** eines Datacenters, Hosts oder Clusters.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients die virtuelle Maschine aus.

- 2 Wählen Sie eine Methode zum Anzeigen der Versionsinformationen aus.

Option	Beschreibung
Klicken Sie auf die Registerkarte Übersicht (Summary).	Die Hardwareversion der virtuellen Maschine wird unter „Allgemein“ auf der Registerkarte Übersicht der virtuellen Maschine angezeigt.
Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie Einstellungen bearbeiten.	Die Hardwareversion der virtuellen Maschine wird oben rechts im Dialogfeld „Eigenschaften virtueller Maschinen“ angezeigt.
Wählen Sie ein Datacenter, Host oder Cluster aus und klicken Sie auf die Registerkarte Virtuelle Maschine.	Die Hardwareversion der virtuellen Maschine wird in der Spalte „VM-Version“ angezeigt. Falls die Spalte „VM-Version“ nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf einen Spaltentitel und wählen Sie „VM-Version“.

Ändern des Namens der virtuellen Maschine im vSphere Client

Sie können den Namen der virtuellen Maschine im Fenster **Name der virtuellen Maschine** des Eigenschaftendialogfelds der virtuellen Maschine ändern.

Wenn Sie den Namen ändern, werden die Namen von Dateien der virtuellen Maschine oder der Name des Verzeichnisses, in dem sich die Dateien befinden, nicht geändert.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf die virtuelle Maschine in der vSphere-Client-Bestandsliste zugreifen können.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **Allgemeine Optionen**.
- 3 Geben Sie einen neuen Namen für die virtuelle Maschine ein.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Anzeigen des Speicherorts der Konfigurationsdatei der virtuellen Maschine im vSphere-Client

Sie können den Speicherort der Konfigurations- und Arbeitsdateien der virtuellen Maschine anzeigen. Diese Informationen sind nützlich, wenn Sie Sicherungssysteme konfigurieren.

Voraussetzungen

- Stellen Sie sicher, dass es eine Verbindung mit dem vCenter Server oder dem ESXi-Host gibt, auf dem die virtuelle Maschine ausgeführt wird.
- Stellen Sie sicher, dass Sie auf die virtuelle Maschine in der vSphere-Client-Bestandsliste zugreifen können.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **Allgemeine Optionen**.
- 3 Notieren Sie den Speicherort der Konfigurations- und der Arbeitsdateien und klicken Sie auf „OK“, um das Dialogfeld zu schließen.

Bearbeiten der Parameter der Konfigurationsdatei im vSphere-Client

Sie können die Konfigurationsparameter einer virtuellen Maschine ändern oder hinzufügen, wenn Sie experimentell unterstützte Funktionen nutzen möchten oder hierzu von einem Mitarbeiter des technischen Supports von VMware aufgefordert werden.

In der VMware-Dokumentation wird beschrieben, wie Sie einen Parameter ändern oder hinzufügen können. In solchen Fällen können Sie das empfohlene Verfahren ohne Bedenken anwenden.

Es gelten die folgenden Bedingungen:

- Damit Sie einen Parameter ändern können, müssen Sie den vorhandenen Wert für das Paar aus Schlüsselwort und Wert ändern. Wenn Sie beispielsweise mit dem Paar aus Schlüsselwort und Wert „keyword/value“ beginnen und es in „keyword/value2“, lautet das Ergebnis „keyword=value2“.
- Sie können keinen Konfigurationsparametereintrag löschen.



VORSICHT Sie müssen einen Wert für Konfigurationsparameter-Schlüsselwörter zuweisen. Wenn Sie keinen Wert zuweisen, kann von einem Schlüsselwort der Wert Null (0), „false“ oder „disable“ zurückgegeben werden. Dies kann dazu führen, dass eine virtuelle Maschine nicht gestartet werden kann.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ die Option **Allgemein** aus.
- 3 Klicken Sie auf **Konfigurationsparameter**.
- 4 (Optional) Ändern Sie einen Parameter oder fügen Sie einen hinzu.
- 5 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu verlassen.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern des konfigurierten Gastbetriebssystems in vSphere-Client

Wenn Sie den Gastbetriebssystemtyp in den Einstellungen der virtuellen Maschine ändern, ändern Sie die Einstellung für das Gastbetriebssystem in der Konfigurationsdatei der virtuellen Maschine. Wenn Sie das Gastbetriebssystem selbst ändern möchten, müssen Sie das neue Betriebssystem in der virtuellen Maschine installieren.

Wenn Sie den Gastbetriebssystemtyp für eine neue virtuelle Maschine festlegen, wählt vCenter Server die Standardwerte für die Konfiguration auf Grundlage des Gasttyps aus. Das Ändern des Gastbetriebssystemtyps nach der Erstellung der virtuellen Maschine führt nicht zu einer nachträglichen Änderung dieser Einstellungen. Die nach der Änderung bereitgestellten Empfehlungen und Einstellungsbereiche sind jedoch davon betroffen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **Allgemeine Optionen**.
- 3 Wählen Sie einen Typ und eine Version für das Gastbetriebssystem aus.

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

Die Konfigurationsparameter der virtuellen Maschine für das Gastbetriebssystem werden geändert. Sie können das Gastbetriebssystem nun installieren.

Konfigurieren von virtuellen Maschinen zum automatischen Aktualisieren der VMware Tools

Sie können virtuelle Maschinen so konfigurieren, dass VMware Tools-Updates automatisch ausgeführt werden.

HINWEIS Das automatische Upgrade von VMware Tools wird nicht für virtuelle Maschinen mit dem Solaris- oder dem NetWare-Gastbetriebssystem unterstützt.

Voraussetzungen

- Virtuelle Maschinen müssen über eine Version der VMware Tools verfügen, die mit ESX/ESXi 3.5 oder höher mitgeliefert wird.
- Stellen Sie sicher, dass die virtuellen Maschinen auf ESX/ESXi 3.5 oder höher und vCenter Server 3.5 oder höher gehostet werden.
- Virtuelle Maschinen müssen auf einem Linux- oder Windows-Gastbetriebssystem ausgeführt werden, dass von ESX/ESXi 3.5 oder höher und von vCenter Server 3.5 oder höher unterstützt wird.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **VMware Tools**.
- 3 Wählen Sie im Fenster **Erweitert** die Option **Tools beim Aus- und erneutem Einschalten prüfen und aktualisieren**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Beim nächsten Einschalten der virtuellen Maschine wird eine Überprüfung auf eine neuere Version der VMware Tools für den ESX/ESXi durchgeführt. Wenn eine neuere Version vorhanden ist, wird diese installiert, und das Gastbetriebssystem wird bei Bedarf neu gestartet.

Konfiguration virtueller CPUs

Sie können CPU-Ressourcen hinzufügen, ändern oder konfigurieren, um die Leistung einer virtuellen Maschine zu verbessern. Sie können die meisten der CPU-Parameter beim Erstellen virtueller Maschinen oder nach der Installation des Gastbetriebssystems festlegen. Bei einigen Aktionen ist es erforderlich, die virtuelle Maschine auszuschalten, bevor Sie die Einstellungen ändern.

VMware verwendet die folgende Terminologie. Das Verständnis der folgenden Begriffe ist hilfreich, wenn Sie Ihre Strategie für die CPU-Ressourcenzuteilung planen.

CPU	Die CPU bzw. der Prozessor ist der Teil eines Computersystems, der alle Anweisungen eines Computerprogramms ausführt, und stellt das primäre Element dar, das die Funktionen des Computers ausführt. CPUs enthalten Kerne.
CPU-Socket	Ein physischer Connector auf der Hauptplatine eines Computers, der eine einzelne physische CPU akzeptiert. Viele Hauptplatinen können mehrere Sockets haben, die wiederum Prozessoren mit mehreren Kernen (Mehrkern-CPUs) akzeptieren können. Der vSphere Web Client berechnet die Gesamtzahl der virtuellen Sockets aus der Anzahl der Kerne und der Kerne pro Socket, die Sie auswählen.
Core	Umfasst eine Einheit, die einen L1-Cache und funktionale Einheiten enthält, die zur Ausführung von Programmen erforderlich sind. Kerne können Programme oder Threads unabhängig ausführen. Es können sich ein oder mehrere Kerne auf einer einzelnen CPU befinden.
Corelet	Ein AMD-Prozessor-Corelet ist einem logischen Prozessor architektonisch gleichwertig. Gewisse künftige AMD-Prozessoren werden eine Reihe von Berechnungseinheiten umfassen, wobei jede Berechnungseinheit über eine Anzahl von Corelets verfügt. Im Gegensatz zu einem herkömmlichen Prozessor-kern fehlt bei einem Corelet ein vollständiger Satz von privaten, dedizierten Ausführungsressourcen. Es teilt einige Ausführungsressourcen mit anderen Corelets, wie z. B. einen L1-Befehlscache oder eine Gleitkomma-Ausführungseinheit. AMD bezeichnet Corelets als Kerne (Cores), aber weil diese herkömmlichen Kernen unähnlich sind, verwendet VMware die Fachbezeichnung „Corelets“, um die gemeinsame Nutzung von Ressourcen offensichtlicher darzustellen.
Thread	Manche Kerne können gleichzeitig unabhängige Instruktionsstreams ausführen. Bei vorhandenen Implementierungen können Kerne gleichzeitig einen oder zwei Software-Threads ausführen, indem Sie, sofern erforderlich, für ein Multiplexing der funktionellen Einheiten des Kerns zwischen den Software-Threads sorgen. Solche Kerne werden als „duale“ oder „multithreaded“ Kerne bezeichnet.
Gemeinsame Nutzung von Ressourcen	Anteile geben die relative Priorität oder Wichtigkeit einer virtuellen Maschine oder eines Ressourcenpools an. Wenn eine virtuelle Maschine über doppelt so viele Anteile einer Ressource wie eine andere virtuelle Maschine verfügt, dann ist sie berechtigt, auch doppelt so viele Ressourcen zu verbrauchen, wenn beide Maschinen einen Anspruch auf die Ressourcen erheben.

Ressourcenzuteilung	Sie können die CPU-Einstellungen für die Ressourcenzuteilung (z. B. Anteile, Reservierung und Grenzwert) ändern, wenn die vorhandene Ressourcenkapazität nicht ausreicht. Wenn beispielsweise die Arbeitsbelastung der Buchhaltung am Jahresende wächst, können Sie die Reserve des Ressourcenpools „Buchhaltung“ erhöhen.
vSphere Virtual Symmetric Multiprocessing (Virtual SMP)	Funktion, die es einer einzelnen virtuellen Maschine ermöglicht, mehrere Prozessoren aufzuweisen

Ändern der CPU-Hotplug-Einstellungen im vSphere Client

Mit der CPU-Hotplug-Option können Sie CPU-Ressourcen für eine virtuelle Maschine hinzufügen, während die Maschine eingeschaltet ist.

Es gelten die folgenden Bedingungen:

- Die besten Ergebnisse erzielen Sie mit virtuellen Maschinen mit Hardwareversion 8 oder höher.
- Das Hinzufügen von virtuellen Mehrkern-CPU's im laufenden Betrieb wird nur von der Hardwareversion 8 oder höher unterstützt.
- Nicht alle Gastbetriebssysteme unterstützen das Hot-Add von CPUs. Sie können diese Einstellungen deaktivieren, wenn der Gast nicht unterstützt wird.
- Wenn Sie bei virtuellen Maschinen mit der Hardwareversion 7 die Funktion für das Hinzufügen von CPUs im laufenden Betrieb verwenden möchten, legen Sie für die Einstellung **Anzahl der Kerne pro Socket** den Wert „1“ fest.
- Durch das Hinzufügen von CPU-Ressourcen zu einer laufenden virtuellen Maschine mit aktivierter CPU-Hotplug-Funktionalität wird die Verbindung aller USB-Passthrough-Geräte zu dieser virtuellen Maschine getrennt und die Geräte werden wieder neu verbunden.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine unter den folgenden Bedingungen ausgeführt wird:

- VMware Tools ist jetzt installiert. Diese Bedingung ist für die Hotplug-Funktionalität mit Linux-Gastbetriebssystemen erforderlich.
- Die virtuelle Maschine verfügt über ein Gastbetriebssystem, das CPU-Hotplug unterstützt.
- Die virtuelle Maschine verwendet Hardwareversion 7 oder höher.
- Die virtuelle Maschine ist nun ausgeschaltet.
- Erforderliche Berechtigungen: **Virtuelle Maschine.Konfiguration.Einstellungen** auf der virtuellen Maschine

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter **Erweitert** die Option **Speicher/CPU-Hotplug**.
- 3 Ändern Sie die CPU-Hotplug-Einstellung.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Weiter

Sie können nun CPUs zur eingeschalteten virtuellen Maschine hinzufügen.

Ändern der Anzahl virtueller CPUs

Sie können eine virtuelle Maschine, die auf einem ESXi-Host ausgeführt wird, mit bis zu 128 virtuellen CPUs konfigurieren. Sie können die Anzahl virtueller CPUs im laufenden Betrieb ändern, oder wenn die virtuelle Maschine ausgeschaltet ist.

Das Hinzufügen virtueller CPUs im laufenden Betrieb ist bei virtuellen Maschinen möglich, die über Mehrkern-CPU-Unterstützung verfügen und unter Hardwareversion 8 oder höher laufen. Wenn die virtuelle Maschine eingeschaltet und das Hinzufügen von CPUs im laufenden Betrieb aktiviert ist, können Sie virtuelle CPUs zur laufenden virtuellen Maschine hinzufügen. Sie können nur ein Vielfaches der Anzahl der Kerne pro Socket hinzufügen. Für Mehrkern-CPU muss der Host über eine Lizenz für vSphere Virtual Symmetric Multiprocessing (Virtual SMP) verfügen.

WICHTIG Wenn Sie Ihre virtuelle Maschine für Einstellungen für virtuelle CPUs mit mehreren Kernen konfigurieren, müssen Sie sicherstellen, dass Ihre Konfiguration den Anforderungen der Endbenutzer-Lizenzvereinbarung des Gastbetriebssystems entspricht.

Voraussetzungen

- Wenn das Hinzufügen von CPUs im laufenden Betrieb nicht aktiviert ist, schalten Sie die virtuelle Maschine aus, bevor Sie CPUs hinzufügen.
- Wenn das Entfernen von CPUs im laufenden Betrieb nicht aktiviert ist, schalten Sie die virtuelle Maschine aus, bevor Sie CPUs entfernen.
- Sollen im laufenden Betrieb CPUs mit mehreren Kernen hinzugefügt werden, vergewissern Sie sich, dass die virtuelle Maschine über Hardwareversion 8 verfügt.
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.CPU-Anzahl ändern** auf der virtuellen Maschine

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **CPUs**.
- 3 Wählen Sie im Dropdown-Menü **Anzahl der virtuellen Sockets** einen Wert aus.
- 4 Wählen Sie im Dropdown-Menü **Anzahl der Kerne pro Socket** einen Wert aus.
Die sich daraus ergebende Gesamtzahl der Kerne ist gleich oder geringer der Anzahl der logischen CPUs auf dem Host.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Beispiel: Hinzufügen von Mehrkern-CPU-Ressourcen zu einer virtuellen Maschine

Möglicherweise haben Sie die folgenden vorhandenen CPU-Ressourcen, die Sie für die virtuelle Maschine während bzw. nach deren Erstellung konfiguriert haben und die sich dabei in einem ausgeschalteten Zustand befand.

Ressourceneinstellungen für CPU	Vorhandener Wert
Anzahl der virtuellen Sockets	2
Anzahl der Kerne pro Socket	2
Gesamtzahl der Kerne	4

Wenn CPU-Hotplug aktiviert ist und die virtuelle Maschine ausgeführt wird, können Sie die hinzuzufügende Anzahl an Sockets im Dropdown-Menü **Anzahl der virtuellen Sockets** auswählen. Das Dropdown-Menü **Anzahl der Kerne pro Socket** ist nicht verfügbar und behält den Wert 2 bei. Wenn Sie 3 virtuelle Sockets auswählen, fügen Sie 1 Socket mit 2 Kernen hinzu, sodass die virtuelle Maschine 6 virtuelle CPUs hat.

Ressourceneinstellungen für CPU	Vorhandener Wert	Hotplug-Wert
Anzahl der virtuellen Sockets	2	3
Anzahl der Kerne pro Socket	2	2
Gesamtzahl der Kerne	4	6

Zuteilen von CPU-Ressourcen im vSphere Client

Sie können die Anzahl der CPU-Ressourcen, die einer virtuelle Maschine zugeteilt wurden, unter Verwendung von Anteilen, Reservierungen und Grenzwerteinstellungen ändern.

Eine virtuelle Maschine verfügt über die folgenden benutzerdefinierten Einstellungen, die die Zuteilung der CPU-Ressourcen beeinflussen.

Grenzwert	Legt einen Grenzwert für den Verbrauch an CPU-Zeit für eine virtuelle Maschine fest. Dieser Wert wird in MHz angegeben.
Reservierung	Gibt die garantierte Mindestzuteilung für eine virtuelle Maschine an. Die Reservierung wird in MHz angegeben.
Anteile	Jeder virtuellen Maschine werden CPU-Anteile zugeteilt. Je mehr Anteile eine virtuelle Maschine hat, desto öfter erhält sie CPU-Zeit zugeteilt, wenn die CPU sich nicht im Leerlauf befindet. Anteile stellen eine relative Metrik zum Zuteilen von CPU-Kapazität dar.

HINWEIS Die Funktionen in VM-Hardwareversionen 9, 10 und 11 sind schreibgeschützt, wenn sie über den vSphere Client mit einem ESXi-Host oder einem vCenter Server-System verbunden sind.

Voraussetzungen

Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Ressourcen ändern**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **CPU**.
- 3 Teilen Sie dieser virtuellen Maschine die CPU-Kapazität zu.

Option	Beschreibung
Anteile	CPU-Anteile für diese virtuelle Maschine bezogen auf die Gesamtanteile der übergeordneten virtuellen Maschine. Hierarchisch gleichwertige virtuelle Maschinen nutzen Ressourcen gemeinsam auf der Basis ihrer relativen Anteilswerte, die an die Reservierung und die Grenze geknüpft sind. Wählen Sie Niedrig , Normal oder Hoch . Dadurch werden die Anteilswerte im Verhältnis 1:2:4 festgelegt. Wählen Sie die Einstellung Benutzerdefiniert , um jeder virtuellen Maschine einen bestimmten Anteil zuzuweisen, der einer proportionalen Gewichtung entspricht.
Reservierung	Garantierte CPU-Reservierung für diese virtuelle Maschine.
Grenzwert	Obergrenze für die CPU-Reservierung für diese virtuelle Maschine. Wählen Sie Unbegrenzt , wenn Sie keine Obergrenze definieren möchten.

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

Konfigurieren der erweiterten CPU-Scheduling-Einstellungen

Sie können CPU-Optionen auswählen, die die Planung der Verarbeitung virtueller Maschinen für physische Prozessorkerne und Hyper-Threads umfassen. ESXi bietet im Allgemeinen selbst dann eine ausgewogene Prozessorplanung, wenn das Hyper-Threading aktiviert ist. Diese Einstellungen sind nur für detaillierte Optimierungen kritischer virtueller Maschinen nützlich.

Konfigurieren des gemeinsamen Kernzugriffs mit Hyper-Threading im vSphere-Client

Sie können auswählen, wie die virtuellen CPUs einer virtuellen Maschine physische Kerne auf einem System mit Hyper-Threading gemeinsam verwenden können.

Durch die Hyper-Threading-Technologie kann sich ein einzelner physischer Prozessor wie zwei logische Prozessoren verhalten. Die Option für den gemeinsamen Kernzugriff mit Hyper-Threading ermöglicht eine detaillierte Kontrolle darüber, ob eine virtuelle Maschine zur gemeinsamen Nutzung eines physischen Prozessorkerns konfiguriert werden soll. Der Prozessor kann gleichzeitig zwei unabhängige Anwendungen ausführen. Obwohl durch Hyper-Threading die Systemleistung nicht verdoppelt wird, kann diese durch eine bessere Nutzung ungenutzter Ressourcen gesteigert werden.

Voraussetzungen

- Die Option für den gemeinsamen Kernzugriff mit Hyper-Threading muss in den BIOS-Einstellungen Ihres Systems aktiviert sein. Weitere Informationen hierzu finden Sie im *Handbuch zur Ressourcenverwaltung*.
- Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **Erweiterte CPU** aus.
- 3 Wählen Sie aus dem Dropdown-Menü für den **Hyper-Threading-Sharing-Modus** einen Modus aus.

Option	Beschreibung
Alle (Standard)	Die virtuellen CPUs dieser virtuellen Maschine können die Kerne mit anderen virtuellen CPUs dieser oder anderer virtueller Maschinen gemeinsam nutzen.
Keine	Die virtuellen CPUs dieser virtuellen Maschine können einen Prozessor-Core bei entsprechender Planung alleine nutzen. Der andere Hyper-Thread des Cores wird angehalten, während diese virtuelle Maschine den Core benutzt.
Intern	Auf einer virtuellen Maschine mit genau zwei virtuellen Prozessoren können die beiden virtuellen Prozessoren einen physischen Kern gemeinsam nutzen (nach Ermessen des Host-Planers), diese virtuelle Maschine nutzt jedoch in keinem Fall den Kern gemeinsam mit einer anderen virtuellen Maschine. Wenn die virtuelle Maschine nicht über genau zwei Prozessoren verfügt, entspricht diese Einstellung der Option Keine (None) .

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

Konfigurieren der Prozessorplanungs-Affinität im vSphere-Client

Die Option **Planen von Affinität** ermöglicht eine detaillierte Kontrolle über die Verteilung der CPUs virtueller Maschinen auf die physischen Kerne des Hosts (und die Hyper-Threads, sofern das Hyper-Threading aktiviert ist). Dieses Fenster wird für virtuelle Maschinen in DRS-Clustern oder im Fall von Hosts mit nur einem Prozessor-Core und ohne Hyper-Threading nicht angezeigt.

Unter Verwendung der CPU-Affinität können Sie eine virtuelle Maschine einem bestimmten Prozessor zuweisen. Durch diese Aktion können Sie die Zuweisung von virtuellen Maschinen auf einen bestimmten verfügbaren Prozessor in Systemen mit mehreren Prozessoren beschränken.

Bei potenziellen Problemen mit der CPU-Affinität können Sie das *Handbuch zur Ressourcenverwaltung* konsultieren.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **Erweiterte CPU** aus.
- 3 Geben Sie im Bereich „Planen von Affinität“ eine kommagetrennte Liste von Prozessorbereichen ein (verwenden Sie Bindestriche zum Kennzeichnen von Bereichen).

Beispielsweise gibt „0,4-7“ eine Affinität mit den CPUs 0,4,5,6 und 7 an. Die Auswahl aller Prozessoren ist identisch mit der Auswahl keiner Affinität. Sie müssen mindestens so viele Prozessoraffinitäten konfigurieren wie virtuelle CPUs vorhanden sind.

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

Ändern der Einstellungen für die CPU-Identifikationsmaske im vSphere-Client

Die CPU-Identifikation (CPU-ID) maskiert die CPU-Funktionen, die für das Gastbetriebssystem der virtuellen Maschine sichtbar sind. Das Maskieren oder Verbergen von CPU-Funktionen kann dazu führen, dass eine virtuelle Maschine ESXi-Hosts zur Migration in großem Ausmaß zur Verfügung steht. vCenter Server vergleicht die CPU-Funktionen, die einer virtuellen Maschine zur Verfügung stehen, mit den CPU-Funktionen des Zielhosts, um zu ermitteln, ob eine Migration mit vMotion zulässig ist oder nicht.

Wenn beispielsweise das AMD-Bit „No eXecute“ (NX) und das Intel-Bit „eXecute Disable“ (XD) maskiert werden, wird die virtuelle Maschine daran gehindert, diese Funktionen zu verwenden, bietet aber Kompatibilität, die Ihnen ermöglicht, virtuelle Maschine auf ESXi-Hosts zu migrieren, die nicht über diese Funktionalität verfügen. Wenn das NX/XD-Bit für das Gastbetriebssystem sichtbar ist, kann die virtuelle Maschine diese Funktion verwenden, aber Sie können die virtuelle Maschine nur dann auf Hosts migrieren, auf denen die Funktion aktiviert ist.

HINWEIS In der Regel müssen die Konfigurationseinstellungen der CPU-Identifikationsmaske nicht geändert werden. Fast alle Änderungen werden nur am NX/XD-Bit vorgenommen.

Detaillierte Informationen zur vMotion-Kompatibilität und zu CPU-Masken finden Sie unter *vCenter Server und Hostverwaltung*.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf die virtuelle Maschine in der vSphere-Client-Bestandsliste zugreifen können.
- Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ die Option **CPU-ID-Maske**.
- 3 Wählen Sie im Bereich **CPU-Identifikationsmaske** eine Option für das NX-Flag aus.

Option	Beschreibung
NX/XD-Flag für Gast ausblenden.	Erhöht die vMotion-Kompatibilität. Das Ausblenden des NX/XD-Flags erhöht zwar die vMotion-Kompatibilität zwischen Hosts, es kann jedoch zur Deaktivierung bestimmter CPU-Sicherheitsfunktionen führen.
NX/XD-Flag für Gast einblenden.	Sorgt dafür, dass alle CPU-Sicherheitsfunktionen weiterhin aktiviert bleiben.
Aktuelle erweiterte Einstellungen für NX/XD-Flag beibehalten	Sorgt dafür, dass die im Dialogfeld „CPU-Identifikationsmaske“ festgelegten Einstellungen für das NX/XD-Flag verwendet werden. Diese Option wird nur dann aktiviert, wenn die aktuellen Einstellungen etwas anderes angeben als die Einstellungen der anderen NX/XD-Flag-Optionen, z. B. wenn sich die Einstellung des NX/XD-Flag-Bits je nach Prozessormarke verändert.

- 4 (Optional) Wenn Sie andere Maskenwerte als das NX-Bit bearbeiten oder NX-Maskenwerte auf andere Werte als "0" oder "H" setzen möchten, klicken Sie auf **Erweitert**.
 - a Klicken Sie auf die entsprechende Registerkarte.
 - b Klicken Sie auf eine Zeile, und bearbeiten Sie den entsprechenden Maskenwert.
Wenn Sie eine Erläuterung zu einem Wertesymbol möchten, klicken Sie auf **Legende**.
 - c Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Eigenschaftendialogfeld der virtuellen Maschine zurückzukehren.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der CPU/MMU-Virtualisierungseinstellungen im vSphere Client

ESXi kann festlegen, ob eine virtuelle Maschine Hardware-Unterstützung für die Virtualisierung verwenden sollte. Es nimmt diese Festlegung auf Basis des Prozessortyps und der virtuellen Maschine vor. Die Außerkräftsetzung der automatischen Auswahl kann für manche Anwendungsfälle eine bessere Leistung liefern.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ die Option **CPU/MMU-Virtualisierung**.
- 3 Wählen Sie einen Befehlssatz aus.
 - **Automatisch**
 - **Software für Befehlssatz und MMU verwenden**
 - **Intel® VT-x/AMD-V für die Virtualisierung des Befehlssatzes und Software für MMU verwenden**
 - **Intel VT-x/AMD-V für die Virtualisierung des Befehlssatzes und Intel EPT/AMD RVI für die Virtualisierung der MMU verwenden**

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

Konfigurieren von virtuellem Arbeitsspeicher

Sie können VM-Arbeitsspeicherressourcen hinzufügen, ändern oder konfigurieren, um die Leistung einer virtuellen Maschine zu verbessern. Sie können die meisten der Parameter für den Arbeitsspeicher beim Erstellen virtueller Maschinen oder nach der Installation des Gastbetriebssystems festlegen. Bei einigen Aktionen ist es erforderlich, die virtuelle Maschine auszuschalten, bevor Sie die Einstellungen ändern.

Über die Arbeitsspeicherressourceneinstellung einer virtuellen Maschine wird festgelegt, welcher Anteil des Hostarbeitsspeichers der virtuellen Maschine zugeteilt wird. Die Arbeitsspeichergröße der virtuellen Hardware legt fest, wie viel Arbeitsspeicher für Anwendungen verfügbar ist, die in der virtuellen Maschine laufen. Eine virtuelle Maschine kann Arbeitsspeicherressourcen nur in dem Umfang nutzen, der für die virtuelle Hardware konfiguriert wurde. ESXi-Hosts begrenzen die Arbeitsspeicher-Ressourcennutzung für die virtuelle Maschine auf den maximal geeigneten Wert, sodass die standardmäßige Einstellung „Unbegrenzt“ übernommen werden kann.

Ändern der Arbeitsspeicherkonfiguration im vSphere Client

Sie können den Arbeitsspeicher neu konfigurieren, der der Hardware einer virtuellen Maschine zugeteilt ist.

Für virtuelle Maschinen mit BIOS-Firmware beträgt die Mindestgröße des Arbeitsspeichers 4 MB. Virtuelle Maschinen, die die EFI-Firmware verwenden, benötigen mindestens 96 MB RAM. Bei weniger RAM können sie nicht eingeschaltet werden.

Die maximale Arbeitsspeichergröße einer virtuellen Maschine hängt vom physischen Arbeitsspeicher des Hosts und der Hardwareversion der virtuellen Maschine ab.

Wenn der Arbeitsspeicher der virtuellen Maschine größer als der Hostarbeitsspeicher ist, wird eine Auslagerung durchgeführt, die sich sehr stark auf die Leistung der virtuellen Maschine auswirken kann. Die Arbeitsspeichergröße muss ein Vielfaches von 4 MB sein. Der Maximalwert für beste Leistung stellt den Schwellenwert dar, bei dessen Überschreitung der physische Arbeitsspeicher des Hosts nicht ausreicht, um die virtuelle Maschine mit voller Geschwindigkeit auszuführen. Dieser Wert schwankt mit der Änderung der Bedingungen auf dem Host, wenn virtuelle Maschinen beispielsweise ein- bzw. ausgeschaltet werden.

Tabelle 15-2. Maximaler Arbeitsspeicher der virtuellen Maschine

Seit der Hostversion	Version der virtuellen Maschine	Maximale Arbeitsspeichergröße
ESXi 6.0	11	4080 GB
ESXi 5.5	10	1011 GB
ESXi 5.1	9	1011 GB
ESXi 5.0	8	1011 GB
ESX/ESXi 4.x	7	255 GB
ESX/ESXi 3.x	4	65532 MB

Die ESXi-Hostversion gibt den Zeitpunkt an, seit dem die höhere Arbeitsspeichergröße unterstützt wird. Beispielsweise ist die Arbeitsspeichergröße einer virtuellen Maschine der Version 7 auf ESXi 5.0 auf 255 GB beschränkt.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **Arbeitsspeicher**.
- 3 Passen Sie die Größe des Arbeitsspeichers an, der der virtuellen Maschine zugeteilt ist.

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

Zuteilen von Arbeitsspeicherressourcen im vSphere Client

Sie können die Anzahl der Arbeitsspeicherressourcen, die einer virtuellen Maschine zugeteilt wurden, unter Verwendung von Anteilen, Reservierungen und Grenzwerteinstellungen ändern.

Eine virtuelle Maschine verfügt über drei benutzerdefinierte Einstellungen, die die Zuteilung der Arbeitsspeicherressourcen beeinflussen.

Grenzwert	Legt einen Grenzwert für den Verbrauch an Arbeitsspeicher für eine virtuelle Maschine fest. Dieser Wert wird in Megabyte angegeben.
Reservierung	Gibt die garantierte Mindestzuteilung für eine virtuelle Maschine an. Die Reservierung wird in Megabyte angegeben.
Anteile	Jeder virtuellen Maschine werden Arbeitsspeicheranteile zugeteilt. Je mehr Anteile eine virtuelle Maschine hat, desto häufiger wird ihr Arbeitsspeicher zugeteilt, wenn dieser ausgelastet ist. Anteile stellen eine relative Metrik zum Zuteilen von Arbeitsspeicherkapazität dar. Weitere Informationen zu Anteilswerten finden Sie im <i>Handbuch zur vSphere-Ressourcenverwaltung</i> .

Daher ist mit der Zuweisung von Reservierungen für virtuelle Maschinen, die die für sie konfigurierte Arbeitsspeichergrenze übersteigen, keinerlei Nutzen verbunden. Der vSphere Client lässt eine solche Zuweisung über die Registerkarte **Ressourcen** nicht zu. Wenn Sie einer virtuellen Maschine eine große Reservierung zuweisen und dann auf der Registerkarte **Hardware** die konfigurierte Arbeitsspeichergröße für diese virtuelle Maschine verringern, wird die Reservierung ebenfalls verringert, um eine Entsprechung mit der neu konfigurierten Arbeitsspeichergröße zu erreichen. Bevor Sie Arbeitsspeicherressourcen konfigurieren können, müssen Sie die virtuelle Maschine ausschalten.

HINWEIS Die Funktionen in VM-Hardwareversionen 9, 10 und 11 sind schreibgeschützt, wenn sie über den vSphere Client mit einem ESXi-Host oder einem vCenter Server-System verbunden sind.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **Arbeitsspeicher**.
- 3 Teilen Sie dieser virtuellen Maschine Arbeitsspeicherkapazität zu.

Option	Beschreibung
Anteile	Die Werte Niedrig , Normal , Hoch und Benutzerdefiniert werden mit der Summe aller Anteile aller virtuellen Maschinen auf dem Server verglichen. Mit Symbolwerten für die Anteilszuteilung können Sie deren Konvertierung in numerische Werte konfigurieren.
Reservierung	Garantierte Arbeitsspeicherzuteilung für diese virtuelle Maschine.
Grenzwert	Obergrenze für die Arbeitsspeicherzuteilung für diese virtuelle Maschine.
Unbegrenzt	Es ist keine Obergrenze angegeben.

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

Ändern der Einstellungen zum Hinzufügen von Arbeitsspeicher im laufenden Betrieb im vSphere-Client

Mit dem Hinzufügen von Arbeitsspeicher im laufenden Betrieb können Sie Arbeitsspeicherressourcen für eine virtuelle Maschine hinzufügen, während die Maschine eingeschaltet ist.

Voraussetzungen

- Die virtuelle Maschine verfügt über ein Gastbetriebssystem, das das Hinzufügen von Arbeitsspeicher im laufenden Betrieb unterstützt.
- Die virtuelle Maschine verwendet Hardwareversion 7 oder höher.
- VMware Tools ist jetzt installiert.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ die Option **Speicher/CPU-Hotplug**.
- 3 Aktivieren oder deaktivieren Sie das Hinzufügen von Arbeitsspeicher im laufenden Betrieb.
 - **Hinzufügen von Arbeitsspeicher im laufenden Betrieb für diese virtuelle Maschine aktivieren.**
 - **Hinzufügen von Arbeitsspeicher im laufenden Betrieb für diese virtuelle Maschine deaktivieren.**
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Verknüpfen von Arbeitsspeicherreservierungen mit einem NUMA-Knoten im vSphere-Client

Sie können festlegen, dass bei künftigen Arbeitsspeicherzuteilungen auf einer virtuellen Maschine die mit einem einzigen NUMA-Knoten verknüpften Seiten genutzt werden (auch bekannt als manuelle Arbeitsspeicheraffinität). Wenn die virtuelle Maschine auf lokalen Arbeitsspeicher zugreift, verbessert sich dadurch ihre Leistung.

Die folgenden Bedingungen gelten für Arbeitsspeicheroptimierungen mit NUMA:

- Die NUMA-Option ist nur dann auf der Seite „Erweiterter Arbeitsspeicher“ verfügbar, wenn der Host die NUMA-Arbeitsspeicherarchitektur verwendet.
- Affinitätseinstellungen sind nur dann von Bedeutung, wenn Sie zur Leistungsanpassung einer bestimmten Gruppe von virtuellen Maschinen auf einem Host verwendet werden. Diese Option ist nicht verfügbar, wenn sich die virtuelle Maschine auf einem DRS-Cluster befindet. Alle Affinitätswerte werden gelöscht, wenn Sie die virtuelle Maschine auf einen neuen Host verschieben.
- Sie können die für künftige Arbeitsspeicherzuteilungen zu verwendenden Knoten nur dann festlegen, wenn Sie auch die CPU-Affinität festgelegt haben. Wenn Sie lediglich an den Arbeitsspeicheraffinitätseinstellungen manuelle Änderungen vornehmen, wird der automatische NUMA-Ausgleich beeinträchtigt.
- Durch das Aktivieren aller Kontrollkästchen, wird keine Affinität angewendet.

Weitere Informationen zu NUMA und zu Ressourcen des erweiterten Arbeitsspeichers, einschließlich Nutzungsbeispielen, finden Sie im *Handbuch zur Ressourcenverwaltung*.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Ressourcen** und anschließend **Arbeitsspeicher**.
- 3 Im Bereich **NUMA-Arbeitsspeicheraffinität** können Sie die NUMA-Knotenaffinität für die virtuelle Maschine festlegen.
 - **Keine Affinität**
 - **Arbeitsspeicher folgender Knoten verwenden**
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern des Speicherorts der Auslagerungsdatei im vSphere-Client

Wenn eine virtuelle Maschine eingeschaltet wird, erstellt das System eine VMkernel-Auslagerungsdatei als Backing-Speicher für den RAM-Inhalt der virtuellen Maschine. Sie können den standardmäßigen Speicherort der Auslagerungsdatei akzeptieren oder die Datei an einem anderen Speicherort ablegen. Die Auslagerungsdatei wird standardmäßig im selben Verzeichnis wie die Konfigurationsdatei der virtuellen Maschine gespeichert.

Weitere Informationen über die Einstellungen der Host-Auslagerungsdatei finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*. Weitere Informationen zu den Clustereinstellungen finden Sie im *Handbuch zur Ressourcenverwaltung*.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ die Option **Speicherort der Auslagerungsdatei** aus.
- 3 Wählen Sie eine Option aus.

Option	Beschreibung
Standard	Speichert die Auslagerungsdatei der virtuellen Maschine am Standardspeicherort, der in den Einstellungen für die Host- oder Cluster-Auslagerungsdatei definiert ist.
Immer zusammen mit virtueller Maschine speichern	Speichert die Auslagerungsdatei der virtuellen Maschine in demselben Ordner wie die Konfigurationsdatei der virtuellen Maschine.
Im Datenspeicher für Auslagerungsdateien des Hosts speichern	Speichert die Auslagerungsdatei der virtuellen Maschine im Datenspeicher der Auslagerungsdatei, der in den Einstellungen für die Host- oder Cluster-Auslagerungsdatei definiert ist.

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

Netzwerkconfiguration virtueller Maschinen

Die ESXi-Netzwerkfunktionen ermöglichen die Kommunikation zwischen virtuellen Maschinen auf demselben Host, zwischen virtuellen Maschinen auf unterschiedlichen Hosts und zwischen anderen virtuellen und physischen Maschinen. Die Netzwerkfunktionen ermöglichen zudem das Management von ESXi-Hosts und bieten Kommunikation zwischen VMkernel-Diensten (NFS, iSCSI oder vSphere vMotion) und dem physischen Netzwerk. Wenn Sie die Vernetzung für eine virtuelle Maschine konfigurieren, wählen Sie einen Adaptertyp und eine Netzwerkverbindung aus oder ändern ihn bzw. sie und geben an, ob das Netzwerk beim Einschalten der virtuellen Maschine verbunden werden soll.

Ändern der Konfiguration des virtuellen Netzwerkadapters (Netzwerkkarte) in vSphere-Client

Sie können folgende Konfigurationsoptionen des virtuellen Netzwerkadapters für eine virtuelle Maschine ändern: die Einstellung zur Verbindung beim Einschalten, die MAC-Adresse und die Netzwerkverbindung.

Voraussetzungen

Erforderliche Berechtigungen:

- **Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern** zum Bearbeiten der MAC-Adresse und des Netzwerks.
- **Virtuelle Maschine.Interaktion.Geräteverbindung** zum Ändern **Verbinden** und zur **Verbindungsherstellung beim Start**.
- **Netzwerk.Netzwerk zuweisen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie die entsprechende Netzwerkkarte aus der Hardwareliste aus.
- 3 (Optional) Wenn die virtuelle Netzwerkkarte (Network Interface Card, NIC) beim Einschalten der virtuellen Maschine verbunden werden soll, wählen Sie **Beim Einschalten verbinden** aus.
- 4 (Optional) Klicken Sie auf das blaue Informationssymbol unter „DirectPath I/O“, um Einzelheiten zum DirectPath I/O-Status und zur DirectPath I/O-Funktionalität der virtuellen Netzwerkkarte anzuzeigen.
- 5 Wählen Sie eine Option für die Konfiguration der MAC-Adresse.

Option	Beschreibung
Automatisch	vSphere weist MAC-Adressen automatisch zu.
Manuell	Geben Sie die zu verwendende MAC-Adresse ein.

- 6 Konfigurieren Sie die **Netzwerkverbindung** für die virtuelle Netzwerkkarte.

Option	Beschreibung
Standardeinstellungen	Die virtuelle Netzwerkkarte wird mit einer Standard- oder einer verteilten Portgruppe verbunden. Wählen Sie im Dropdown-Menü Netzwerkbezeichnung die Portgruppe aus, zu der die virtuelle Netzwerkkarte eine Verbindung herstellen soll.
Erweiterte Einstellungen	Die virtuelle Netzwerkkarte wird mit einem bestimmten Port auf einem vSphere Distributed Switch verbunden. Diese Option erscheint nur, wenn ein vSphere Distributed Switch zur Verfügung steht. <ol style="list-style-type: none"> Klicken Sie auf Zu den erweiterten Einstellungen wechseln. Wählen Sie im Dropdown-Menü VDS einen vSphere Distributed Switch aus, den die virtuelle Netzwerkkarte verwenden soll. Geben Sie die Port-ID des verteilten Ports ein, mit dem sich die virtuelle Netzwerkkarte verbinden soll.

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

Hinzufügen eines Netzwerkadapters zu einer virtuellen Maschine im vSphere-Client

Wenn Sie einer virtuellen Maschine einen Netzwerkadapter (NIC) hinzufügen, wählen Sie den Adaptertyp und die Netzwerkverbindung aus und geben an, ob das Gerät beim Einschalten der virtuellen Maschine verbunden werden soll.

Vorgehensweise

- Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- Wählen Sie **Ethernet-Adapter (Ethernet Adapter)**, und klicken Sie auf **Weiter**.
- Wählen Sie im Dropdown-Menü einen Adaptertyp aus.
- Wählen Sie im Fenster Netzwerkverbindung ein benanntes Netzwerk mit einer angegebenen Bezeichnung oder ein Legacy-Netzwerk aus.
- Wenn die virtuelle Netzwerkkarte (Network Interface Card, NIC) beim Einschalten der virtuellen Maschine verbunden werden soll, wählen Sie **Beim Einschalten verbinden** aus.
- Klicken Sie auf **Weiter**.
- Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.
- Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfiguration der parallelen und seriellen Schnittstelle

Über parallele und serielle Schnittstellen können Peripheriegeräte an die virtuelle Maschine angeschlossen werden. Die virtuelle serielle Schnittstelle kann eine Verbindung zu einer physischen seriellen Schnittstelle oder einer Datei auf dem Hostcomputer herstellen. Darüber hinaus können Sie eine direkte Verbindung zwischen zwei virtuellen Maschinen oder eine Verbindung zwischen einer virtuellen Maschine und einer Anwendung auf dem Hostcomputer einrichten. Sie können parallele und serielle Ports hinzufügen und die Konfiguration des seriellen Ports ändern.

Verwenden von seriellen Schnittstellen mit virtuellen vSphere-Maschinen

Es gibt mehrere Möglichkeiten, Verbindungen des virtuellen seriellen Ports für virtuelle vSphere-Maschinen einzurichten. Die Verbindungsmethode, die Sie auswählen, hängt von der auszuführenden Aufgabe ab.

Sie können virtuelle serielle Schnittstellen auf folgende Art zum Senden von Daten einrichten.

Physische serielle Schnittstelle auf dem Host	Stellt die virtuelle Maschine für die Verwendung einer physischen seriellen Schnittstelle auf dem Hostcomputer ein. Diese Methode ermöglicht die Verwendung eines externen Modems oder eines Handheld-Geräts in einer virtuellen Maschine.
In Datei ausgeben	Sendet die Ausgabe von der virtuellen seriellen Schnittstelle an eine Datei auf dem Hostcomputer. Diese Methode ermöglicht Ihnen, die Daten zu erfassen, die ein Programm, das in der virtuellen Maschine ausgeführt wird, an den virtuellen seriellen Port sendet.
Mit der Named Pipe verbinden	Richtet eine direkte Verbindung zwischen zwei virtuellen Maschinen oder eine Verbindung zwischen einer virtuellen Maschine und einer Anwendung auf dem Hostcomputer ein. Diese Methode ermöglicht es zwei virtuellen Maschinen oder einer virtuellen Maschine und einem Prozess auf dem Host, so miteinander zu kommunizieren, als ob es sich um zwei durch ein seriell Kabel miteinander verbundene physische Computer handeln würde. Beispielsweise können Sie diese Option für das Remotedebuggen einer virtuellen Maschine verwenden.
Über das Netzwerk verbinden	Ermöglicht eine serielle Verbindung zu bzw. von der seriellen Schnittstelle einer virtuellen Maschine über das Netzwerk. Der Virtual Serial Port Concentrator (vSPC) aggregiert den Datenverkehr von mehreren seriellen Schnittstellen auf einer Verwaltungskonsole. vSPC verhält sich ähnlich wie Konzentratoren für physische serielle Schnittstellen. Die Verwendung von vSPC ermöglicht darüber hinaus die nahtlose Migration von Netzwerkverbindungen zu den seriellen Schnittstellen einer virtuellen Maschine, wenn die virtuelle Maschine mit vMotion migriert wird. Anforderungen und Schritte zum Konfigurieren des Avocent ACS v6000-Konzentrators für virtuelle serielle Ports finden Sie unter http://kb.vmware.com/kb/1022303 .

Server- und Clientverbindungen für Named Pipe und serielle Netzwerk-Ports

Sie können für serielle Ports eine Client- oder eine Serververbindung auswählen. Mit Ihrer Auswahl legen Sie fest, ob das System auf eine Verbindung wartet oder eine Verbindung initiiert. Um eine virtuelle Maschine über einen seriellen Port zu steuern, wählen Sie in der Regel eine Serververbindung aus. Mit dieser Auswahl können Sie die Verbindungen steuern, was nützlich ist, wenn Sie nur gelegentlich eine Verbindung zur virtuellen Maschine herstellen. Um einen seriellen Port zur Protokollierung zu verwenden, wählen Sie eine Clientverbindung aus. Mit dieser Auswahl können Sie die virtuelle Maschine mit dem Protokollierungsserver verbinden, wenn die virtuelle Maschine gestartet wird, und die Verbindung trennen, wenn sie gestoppt wird.

Unterstützte serielle Ports

Wenn Sie einen physischen seriellen Port für das Passthrough des seriellen Ports von einem ESXi-Host auf eine virtuelle Maschine auswählen, werden in das Motherboard integrierte serielle Ports unterstützt.

Nicht unterstützte serielle Ports

Wenn Sie einen physischen seriellen Port für das Passthrough des seriellen Ports von einem ESXi-Host auf eine virtuelle Maschine auswählen, werden die folgenden seriellen Ports nicht unterstützt.

- Serielle Schnittstellen, die über USB verbunden sind, werden für den Passthrough der seriellen Schnittstelle nicht unterstützt. Sie werden möglicherweise von einem USB-Passthrough von einem ESXi-Host zu einer virtuellen Maschine unterstützt. Weitere Informationen hierzu finden Sie unter [USB-Konfiguration von einem ESXi-Host zu einer virtuellen Maschine](#).

Außerdem ist keine Migration mit VMotion möglich, wenn Sie einen physischen seriellen Port für seriellies Passthrough verwenden.

Hinzufügen eines Firewall-Regelsatzes für Netzwerkverbindungen über einen seriellen Port

Wenn Sie einen seriellen Port hinzufügen oder konfigurieren, der von einer Remote-Netzwerkverbindung gestützt wird, können die ESXi-Firewall-Einstellungen Übertragungen verhindern.

Vor dem Verbinden von netzwerkgestützten virtuellen seriellen Schnittstellen müssen Sie einen der folgenden Firewall-Regelsätze hinzufügen, um zu verhindern, dass die Firewall die Kommunikation blockiert:

- **Serieller Port der VM mit vSPC verbunden.** Verwenden Sie diesen Regelsatz, um die Ausgabe der seriellen Schnittstelle mit aktivierter Option **Konzentrator für den virtuellen seriellen Port** über ein Netzwerk zu verbinden, um nur ausgehende Kommunikation vom Host zuzulassen.
- **Serieller Port der VM über das Netzwerk verbunden.** Verwenden Sie diesen Regelsatz, um die Ausgabe der seriellen Schnittstelle ohne den Konzentrador für die virtuelle serielle Schnittstelle über ein Netzwerk zu verbinden.

WICHTIG Ändern Sie nicht die Liste der zulässigen IP-Adressen für die Regelsätze. Updates der IP-Liste können sich auf andere Netzwerkdienste auswirken, die möglicherweise von der Firewall blockiert werden.

Einzelheiten zum Zulassen den Zugriffs auf einen ESXi-Dienst über die Firewall finden Sie in der Dokumentation zur *vSphere-Sicherheit*.

Hinzufügen einer seriellen Schnittstelle zu einer virtuellen Maschine in vSphere Client

Eine virtuelle Maschine kann bis zu vier virtuelle serielle Schnittstellen verwenden. Sie können den virtuellen seriellen Port mit einem physischen seriellen Port oder einer Datei auf dem Hostcomputer verbinden. Mithilfe einer hostseitigen Named Pipe können Sie zudem eine direkte Verbindung zwischen zwei virtuelle Maschinen oder eine Verbindung zwischen einer virtuellen Maschine und einer Anwendung auf dem Host herstellen. Des Weiteren können Sie unter Verwendung eines Ports oder einer vSPC URI einen seriellen Port über das Netzwerk anschließen.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Machen Sie sich mit den geeigneten Medientypen für den Port, auf den Sie zugreifen möchten, den vSPC-Verbindungen und anderen möglichen Bedingungen vertraut. Siehe [„Verwenden von seriellen Schnittstellen mit virtuellen vSphere-Maschinen“](#), auf Seite 171.

- Fügen Sie zum Anschließen einer seriellen Schnittstelle über ein Netzwerk einen Firewall-Regelsatz hinzu. Siehe [Hinzufügen eines Firewall-Regelsatzes für Netzwerkverbindungen über einen seriellen Port](#).
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **Hinzufügen**.
- 3 Wählen Sie **Serielle Schnittstelle** aus, und klicken Sie dann auf **Weiter**.
- 4 Wählen Sie auf der Seite „Typ der seriellen Ports“ den Medientyp für die Schnittstelle aus, auf die zugegriffen werden soll.

Option	Beschreibung
Physische serielle Schnittstelle auf dem Host verwenden	Klicken Sie auf Weiter und wählen Sie den Port aus dem Dropdown-Menü.
In Datei ausgeben	Klicken Sie auf Weiter und navigieren Sie zum Speicherort der Datei auf dem Host, den Sie zum Speichern der Ausgabe des virtuellen seriellen Ports verwenden möchten.
Mit der Named Pipe verbinden	<ol style="list-style-type: none"> a Klicken Sie auf Weiter und geben Sie in das Feld Pipe-Name einen Namen für die Pipe ein. b Wählen Sie in den Dropdown-Menüs die Lokale Stelle und die Gegenstelle der Pipe aus.
Verbindung über Netzwerk	<ol style="list-style-type: none"> a Klicken Sie auf Weiter, dann auf Server oder Client und geben Sie die Port-URI ein. Die URI ist das Remoteende der seriellen Ports, zu der der serielle Port der virtuellen Maschine eine Verbindung herstellen soll. b Wenn vSPC als Zwischenschritt zum Aktivieren des Zugriffs auf alle virtuelle Maschinen über eine einzelne IP-Adresse verwendet wird, wählen Sie Konzentrator für die virtuelle serielle Schnittstelle verwenden und geben Sie die vSPC-URI ein.

- 5 (Optional) Deaktivieren Sie die Option **Beim Einschalten verbinden**, wenn das Gerät mit der parallelen Schnittstelle beim Einschalten der virtuellen Maschine nicht verbunden werden soll.
- 6 (Optional) Wählen Sie **CPU-Übergabe bei Anforderung** aus.

Wählen Sie diese Option nur für Gastbetriebssysteme, die serielle Ports im Abfragemodus verwenden. Die Option verhindert, dass das Gastbetriebssystem zu viele CPUs beansprucht.
- 7 Überprüfen Sie die Information auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.

Beispiel: Herstellen von Netzwerkverbindungen über einen seriellen Port zu einem Client oder Server ohne Authentifizierungsparameter

Wenn Sie vSPC nicht verwenden und Sie Ihre virtuelle Maschine mit einer seriellen Schnittstelle konfigurieren, die als Server mit einer URI `telnet://:12345` verbunden ist, können Sie von Ihrem Linux- oder Windows-Betriebssystem aus eine Verbindung zur seriellen Schnittstelle Ihrer virtuellen Maschine herstellen.

```
telnet yourESXiServerIPAddress 12345
```

Wenn Sie gleichermaßen den Telnet Server auf Ihrem Linux-System an Port 23 (`telnet://yourLinuxBox:23`) ausführen, konfigurieren Sie die virtuelle Maschine als eine Client-URI.

```
telnet://yourLinuxBox:23
```

Die virtuelle Maschine initiiert die Verbindung zu Ihrem Linux-System an Port 23.

Ändern der Konfiguration der seriellen Schnittstelle in vSphere Client

Eine virtuelle Maschine kann bis zu vier virtuelle serielle Schnittstellen verwenden. Sie können den virtuellen seriellen Port mit einem physischen seriellen Port oder einer Datei auf dem Hostcomputer verbinden. Sie können zudem eine direkte Verbindung zwischen zwei virtuelle Maschinen oder einer virtuellen Maschine und einer Anwendung auf dem Host herstellen. Letzteres wird mithilfe einer hostseitigen Named Pipe erreicht. Des Weiteren können Sie unter Verwendung eines Ports oder einer vSPC URI einen seriellen Port über das Netzwerk anschließen.

Virtuelle Maschinen können während der Konfiguration eingeschaltet sein.

Voraussetzungen

- Machen Sie sich mit den geeigneten Medientypen für den Port, auf den Sie zugreifen möchten, den vSPC-Verbindungen und anderen möglichen Bedingungen vertraut. Siehe [„Verwenden von seriellen Schnittstellen mit virtuellen vSphere-Maschinen“](#), auf Seite 171.
- Fügen Sie zum Anschließen einer seriellen Schnittstelle über ein Netzwerk einen Firewall-Regelsatz hinzu. Siehe [Hinzufügen eines Firewall-Regelsatzes für Netzwerkverbindungen über einen seriellen Port](#).
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Geräteverbindung**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie eine serielle Schnittstelle aus der Hardwareliste aus.
- 3 (Optional) Ändern Sie die Einstellungen für den **Gerätestatus**.

Option	Beschreibung
Verbunden	Verbindet oder trennt das Gerät, während die virtuelle Maschine ausgeführt wird.
Beim Einschalten verbinden	Das Gerät wird verbunden, wenn die virtuelle Maschine eingeschaltet wird. Sie können diese Einstellung ändern, während die virtuelle Maschine ein- oder ausgeschaltet ist.

- 4 Wählen Sie einen Verbindungstyp aus.

Option	Beschreibung
Physischen seriellen Port verwenden	Wählen Sie diese Option, wenn die virtuelle Maschine einen physischen seriellen Port auf dem Hostcomputer verwenden soll. Wählen Sie im Dropdown-Menü den seriellen Port aus.
Ausgabedatei verwenden	Aktivieren Sie diese Option, wenn die Ausgabe des virtuellen seriellen Ports an eine Datei auf dem Hostcomputer übertragen werden soll. Wählen Sie eine Ausgabedatei aus, mit der der serielle Port verbunden werden soll.

Option	Beschreibung
Named Pipe verwenden	<p>Aktivieren Sie diese Option, um eine direkte Verbindung zwischen zwei virtuellen Maschinen oder eine Verbindung zwischen einer virtuellen Maschine und einer Anwendung auf dem Hostcomputer einzurichten.</p> <ol style="list-style-type: none"> Geben Sie im Feld Pipe-Name einen Namen für die Pipe ein. Wählen Sie in den Dropdown-Menüs die Lokale Stelle und die Gegenstelle der Pipe aus.
Netzwerk verwenden	<p>Wählen Sie „Netzwerk verwenden“, um die Verbindung über ein Remote-Netzwerk herzustellen.</p> <ol style="list-style-type: none"> Wählen Sie das Netzwerk-Backing aus. <ul style="list-style-type: none"> Wählen Sie Server, damit die virtuelle Maschine eingehende Verbindungen von anderen Hosts überwacht. Wählen Sie Client, damit die virtuelle Maschine das Herstellen einer Verbindung mit einem anderen Host initiiert. Geben Sie eine Port-URI ein. <p>Die URI ist das Remoteende der seriellen Ports, zu der der serielle Port der virtuellen Maschine eine Verbindung herstellen soll.</p> Wenn vSPC als Zwischenschritt für den Zugriff auf alle virtuellen Maschinen über eine einzelne IP-Adresse verwendet wird, wählen Sie Konzentrator für den virtuellen seriellen Port verwenden und geben Sie die vSPC-URI ein.

- 5 (Optional) Wählen Sie **CPU-Übergabe bei Anforderung** aus.

Wählen Sie diese Option nur für Gastbetriebssysteme, die serielle Ports im Abfragemodus verwenden. Die Option verhindert, dass das Gastbetriebssystem zu viele CPUs beansprucht.

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

Beispiel: Herstellen von Netzwerkverbindungen über einen seriellen Port zu einem Client oder Server ohne Authentifizierungsparameter

Wenn Sie vSPC nicht verwenden und Sie Ihre virtuelle Maschine mit einer seriellen Schnittstelle konfigurieren, die als Server mit einer URI `telnet://:12345` verbunden ist, können Sie von Ihrem Linux- oder Windows-Betriebssystem aus eine Verbindung zur seriellen Schnittstelle Ihrer virtuellen Maschine herstellen.

```
telnet yourESXiServerIPAddress 12345
```

Wenn Sie gleichermaßen den Telnet Server auf Ihrem Linux-System an Port 23 (`telnet://yourLinuxBox:23`) ausführen, konfigurieren Sie die virtuelle Maschine als eine Client-URI.

```
telnet://yourLinuxBox:23
```

Die virtuelle Maschine initiiert die Verbindung zu Ihrem Linux-System an Port 23.

Hinzufügen einer parallelen Schnittstelle zu einer virtuellen Maschine im vSphere Client

Sie können den Assistenten zum Hinzufügen von Hardware zum Hinzufügen und Konfigurieren eines parallelen Ports verwenden, um die Ausgabe in eine Datei auf dem Hostcomputer zu senden.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **Parallele Schnittstelle**, und klicken Sie auf **Weiter**.
- 4 Wählen Sie **In Datei ausgeben** aus und klicken Sie auf **Weiter**.
- 5 Wechseln Sie zum Verzeichnis der Ausgabedatei und aktivieren oder deaktivieren Sie das Kontrollkästchen **Beim Einschalten verbinden**, um das Gerät zu verbinden oder die Verbindung aufzuheben.
- 6 Klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Information auf der Seite Bereit zum Abschließen, und klicken Sie auf **Beenden**.

Ändern der Konfiguration der parallelen Schnittstelle in vSphere-Client

Sie können die Ausgabedatei ändern und festlegen, dass der parallele Port verbunden oder getrennt wird, wenn die virtuelle Maschine eingeschaltet wird.

Sie können einen parallelen Port auf der virtuellen Maschine verwenden, um die Ausgabe in eine Datei zu leiten. Sie können keinen physischen parallelen Port auf ESXi-Hosts verwenden.

Virtuelle Maschinen können während der Konfiguration eingeschaltet werden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie den zu ändernden parallelen Port aus.
- 3 Wählen Sie **In Datei ausgeben** und klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren.
- 4 (Optional) Deaktivieren Sie die Option **Beim Einschalten verbinden**, wenn das Gerät mit der parallelen Schnittstelle beim Einschalten der virtuellen Maschine nicht verbunden werden soll.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren der Fibre-Channel-NPIV-Einstellungen im vSphere-Client

Mithilfe der N-Port-ID-Virtualisierung (NPIV) können Sie einen einzelnen physischen Fibre-Channel-HBA-Port für mehrere virtuelle Ports mit jeweils eindeutigen Kennungen gemeinsam verwenden. Durch diese Funktionalität können Sie den Zugriff von virtuellen Maschinen auf LUNs für jede virtuelle Maschine steuern.

Jeder virtuelle Port wird durch zwei WWNs (World Wide Names) gekennzeichnet: einen World Wide Port Name (WWPN) und einen World Wide Node Name (WWNN). Diese WWNs werden durch vCenter Server zugewiesen.

Detaillierte Informationen zum Konfigurieren von NPIV für eine virtuelle Maschine finden Sie unter *vSphere-Speicher*.

Für die NPIV-Unterstützung gelten die folgenden Einschränkungen:

- NPIV muss auf dem SAN-Switch aktiviert sein. Wenn Sie Informationen zum Aktivieren von NPIV auf den Geräten benötigen, setzen Sie sich mit dem Switch-Anbieter in Verbindung.
- NPIV wird nur für virtuelle Maschinen mit RDM-Festplatten unterstützt. Virtuelle Maschinen mit herkömmlichen virtuellen Festplatten verwenden weiterhin die WWNs der physischen HBAs des Hosts.
- Die physischen HBAs auf dem ESXi-Host müssen mithilfe seiner WWNs auf eine LUN zugreifen können, sodass alle virtuellen Maschinen auf diesem Host mithilfe ihrer NPIV WWNs auf diese LUN zugreifen können. Stellen Sie sicher, dass sowohl auf den Host als auch auf die virtuellen Maschinen zugegriffen werden kann.

- Die physischen HBAs auf dem ESXi-Host müssen NPIV unterstützen. Wenn die physischen HBAs NPIV nicht unterstützen, greift die auf diesem Host ausgeführte virtuelle Maschine für den LUN-Zugriff auf die WWNs der physischen HBAs des Hosts zurück.
- Jede virtuelle Maschine kann über bis zu 4 virtuelle Ports verfügen. NPIV-fähigen virtuellen Maschinen werden genau 4 NPIV-verbundene WWNs zugewiesen, die für die Kommunikation mit physischen HBAs über virtuelle Ports verwendet werden. Daher können virtuelle Maschinen bis zu 4 physische HBAs für NPIV-Zwecke verwenden.

Auf der Registerkarte **Optionen** können Sie die WWNs der virtuellen Maschinen anzeigen oder bearbeiten.

Voraussetzungen

- Um die WWNs einer virtuellen Maschine zu bearbeiten, schalten Sie die virtuelle Maschine aus.
- Stellen Sie sicher, dass die virtuelle Maschine über einen Datenspeicher mit einer LUN verfügt, die dem Host zur Verfügung steht.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter **Erweitert** die Option **Fibre-Channel-NPIV** aus.
- 3 (Optional) Aktivieren Sie das Kontrollkästchen **NPIV für diese virtuelle Maschine vorübergehend deaktivieren**.
- 4 Zugewiesenen WWNs werden im Bereich „WWN-Zuweisungen“ aufgeführt.
 - Wählen Sie die Option **Unverändert lassen (Leave unchanged)**, um die WWNs nicht zu ändern.
 - Um über den ESXi-Host neue WWNs zu generieren, wählen Sie die Option **Neue WWNs generieren**.
 - Um die derzeitigen WWN-Zuweisungen zu entfernen, wählen Sie die Option **WWN-Zuweisungen entfernen (Remove WWN assignment)**.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
- 6 Stellen Sie Ihrem SAN-Administrator die WWN-Zuweisungen bereit.

Der Administrator benötigt die Zuweisungen, um die virtuelle Maschine für den Zugriff auf die LUN zu konfigurieren.

Konfiguration der virtuellen Festplatte

Sie können selbst im laufenden Betrieb der virtuellen Maschine große virtuelle Festplatten zu virtuellen Maschinen und mehr Speicherplatz zu vorhandenen Festplatten hinzufügen. Sie können die meisten der Parameter für die virtuelle Festplatte beim Erstellen virtueller Maschinen oder nach der Installation des Gastbetriebssystems festlegen.

Sie können Daten der virtuellen Maschine auf einer neuen virtuellen Festplatte, einer vorhandenen virtuellen Festplatte oder einer zugeordneten SAN-LUN speichern. Eine virtuelle Festplatte wird als einzelne Festplatte des Gastbetriebssystems angezeigt und besteht aus einer oder mehreren Dateien im Hostdateisystem. Sie können virtuelle Festplatten innerhalb eines Hosts oder zwischen Hosts kopieren oder verschieben.

Statt die Daten einer virtuellen Maschine, die auf einem ESXi-Host ausgeführt wird, in einer virtuellen Festplattendatei zu speichern, können Sie die Daten auch direkt auf einer SAN-LUN speichern. Diese Fähigkeit ist nützlich, wenn Sie in den virtuellen Maschinen Anwendungen ausführen, die die physischen Merkmale des Speichergeräts erkennen müssen. Das Zuordnen einer SAN-LUN ermöglicht Ihnen zusätzlich die Verwendung vorhandener SAN-Befehle für die Speicherverwaltung der Festplatte.

Um die Leistung von virtuellen Maschinen zu verbessern, können Sie sie für die Verwendung von vSphere Flash Read Cache™ konfigurieren. Einzelheiten zum Verhalten von Flash Read Cache finden Sie in der Dokumentation zu *vSphere Storage*.

Wenn Sie einem VMFS-Volumen eine LUN zuordnen, erstellt vCenter Server oder der ESXi-Host eine Datei mit der Raw-Device-Zuordnung (RDM), die auf die Raw-LUN weist. Durch Kapseln von Festplatteninformationen in einer Datei kann vCenter Server oder der ESXi-Host die LUN sperren, sodass nur eine virtuelle Maschine auf diese schreiben kann. Zwar hat die Zuordnungsdatei die Erweiterung *.vmdk*, die Datei enthält jedoch nur beschreibende Festplatteninformationen für die LUN-Zuordnung auf dem ESXi-System. Die eigentlichen Daten werden unter Verwendung der LUN gespeichert. Sie können eine virtuelle Maschine nicht anhand einer Vorlage bereitstellen und ihre Daten auf einer LUN speichern. Sie können nur ihre Daten in einer virtuellen Festplattendatei speichern.

Die Menge an freiem Speicherplatz im Datenspeicher ändert sich ständig. Stellen Sie sicher, dass für die Erstellung der virtuellen Maschine und für andere VM-Vorgänge, z. B. das Wachstum der Dateien mit geringer Datendichte, Snapshots usw., genügend Speicherplatz übrig bleibt. Informationen dazu, wie Sie die Speicherplatznutzung für den Datenspeicher nach Dateityp überprüfen können, finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*.

Mit Thin Provisioning können Sie Dateien mit geringer Datendichte, deren Blöcke beim ersten Zugriff zugeteilt werden, erstellen, wodurch eine Überbelegung des Datenspeichers möglich ist. Die Dateien mit geringer Datendichte können weiter anwachsen und den Datenspeicher füllen. Wenn der Festplattenspeicherplatz auf dem Datenspeicher nicht mehr ausreicht, während die virtuelle Maschine ausgeführt wird, kann dies dazu führen, dass die virtuelle Maschine nicht mehr funktioniert.

Ändern der Konfiguration der virtuellen Festplatte im vSphere Client

Sie können den Knoten des virtuellen Geräts, die Größe der Festplatte und den Persistenzmodus der Konfiguration der virtuellen Festplatte für eine virtuelle Maschine ändern.

HINWEIS Die Funktion „Pfade verwalten“ für RDM-Festplatten ist nicht für virtuelle Maschinen auf Legacy-Hosts verfügbar, die ESX Server-Versionen vor 3.0 ausführen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie die zu ändernde Festplatte aus.
Der Name der Festplattendatei und der Festplattentyp („thick“ oder „thin“) wird im oberen rechten Fenster angezeigt.
- 3 Wählen Sie den Typ **Knoten des virtuellen Geräts** aus dem Dropdown-Menü aus.
Diese Option ist schreibgeschützt, wenn Sie eine eingeschaltete virtuelle Maschine bearbeiten.
- 4 Geben Sie zum Ändern der Festplattengröße einen neuen Wert in das Textfeld **Bereitgestellte Größe** ein.

- 5 (Optional) Um die Art zu ändern, wie sich Snapshots auf Festplatten auswirken, klicken Sie auf **Unabhängig** und wählen Sie eine Option aus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

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

Hinzufügen einer Festplatte zu einer virtuellen Maschine in vSphere-Client

Wenn Sie einer virtuellen Maschine eine Festplatte hinzufügen, können Sie eine neue virtuelle Festplatte erstellen oder eine vorhandene virtuelle Festplatte bzw. eine zugeordnete SAN-LUN hinzufügen.

In der Regel können Sie den Standardgeräteknotten übernehmen. Bei einer Festplatte eignet sich ein vom Standard abweichender Geräteknotten zur Steuerung der Startreihenfolge oder bei Verwendung verschiedener SCSI-Controllertypen. Beispiel: Sie möchten von einem LSI Logic-Controller starten und einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist, für die gemeinsame Verwendung einer Datenfestplatte mit einer anderen virtuellen Maschine verwenden.

HINWEIS Die Migration mit vMotion kann nicht zum Migrieren von virtuelle Maschinen mit Raw-Festplatten für das Clustering verwendet werden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **Festplatte**, und klicken Sie auf **Weiter**.

4 Wählen Sie den zu verwendenden Festplattentyp.

Option	Aktion
Neue virtuelle Festplatte erstellen	<ul style="list-style-type: none"> a Geben Sie die Festplattenkapazität ein. b Auswählen eines Festplattenformats. <ul style="list-style-type: none"> ■ Thick-Provision Lazy-Zeroed erstellt eine virtuelle Festplatte im Standard-Thick-Format. ■ Thick-Provision Eager-Zeroed erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. ■ Thin Provision erstellt eine Festplatte im Thin-Format. Verwenden Sie dieses Format, um Speicherplatz zu sparen. c Wählen Sie einen Speicherort zum Aufbewahren der Festplatte aus. Gemeinsam mit virtueller Maschine speichern oder Datenspeicher angeben. d Wenn Sie die Option Datenspeicher angeben gewählt haben, wechseln Sie zum Speicherort des Datenspeichers, und klicken Sie auf Weiter.
Vorhandene virtuelle Festplatte verwenden	Suchen Sie nach dem Festplattendateipfad und klicken Sie auf Weiter .
Zuordnungen für Raw-Geräte	<p>Gewährt ihrer virtuellen Maschine Direktzugriff auf das SAN.</p> <ul style="list-style-type: none"> a Wählen Sie die LUN aus, die für die Raw-Festplatte verwendet werden soll, und klicken Sie auf Weiter. b Wählen Sie einen Datenspeicher, und klicken Sie auf Weiter. c Wählen Sie den Kompatibilitätsmodus aus. <ul style="list-style-type: none"> ■ Bei Auswahl der Option Physisch kann das Gastbetriebssystem direkt auf die Hardware zugreifen. ■ Bei Auswahl der Option Virtuell kann die virtuelle Maschine VMware-Snapshots und andere erweiterte Funktionen nutzen. d Klicken Sie auf Weiter.

5 Akzeptieren Sie den Standardknoten oder wählen Sie einen anderen Knoten des virtuellen Geräts aus.

In der Regel können Sie den Standardgeräteknoten übernehmen. Bei einer Festplatte eignet sich ein vom Standard abweichender Geräteknoten zur Steuerung der Startreihenfolge oder bei Verwendung verschiedener SCSI-Controller-Typen. Beispiel: Sie möchten von einem LSI Logic-Controller starten und sich mit einer anderen virtuellen Maschine eine Datenplatte teilen. Diese virtuelle Maschine verwendet einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist.

6 (Optional) Um die Art zu ändern, wie sich Snapshots auf Festplatten auswirken, klicken Sie auf **Unabhängig** und wählen Sie eine Option aus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

7 Klicken Sie auf **Weiter**.8 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

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

Verwenden von Festplattenfreigaben zur Priorisierung virtueller Maschinen im vSphere-Client

Sie können die Festplattenressourcen für eine virtuelle Maschine ändern. Wenn mehrere virtuelle Maschinen auf denselben VMFS-Datenspeicher und somit auf dieselbe LUN zugreifen, lassen sich mithilfe von Festplattenfreigaben Prioritäten für virtuelle Maschinen festlegen. Bei Festplattenfreigaben wird zwischen virtuellen Maschinen mit hoher und mit niedriger Priorität unterschieden.

Sie können die E/A-Bandbreite der Festplatte des Hosts den virtuellen Festplatten auf einer virtuellen Maschine zuteilen. Die Festplatten-E/A ist eine serverabhängige Ressource. Sie kann nicht clusterübergreifend eingesetzt werden.

Der Anteilswert stellt die relative Metrik zur Steuerung der Festplattenbandbreite für alle virtuellen Maschinen dar. Die Werte werden mit der Summe aller Anteile aller virtuellen Maschinen auf dem Server verglichen.

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

Sie können einen IOP-Grenzwert auswählen, der eine Obergrenze für Speicherressourcen festlegt, die einer virtuellen Maschine zugeteilt werden können. Unter IOPs versteht man die Anzahl an E/A-Vorgängen pro Sekunde.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **Festplatte**.
- 3 Wählen Sie im Bereich „Ressourcenzuteilung“ die zu ändernde virtuelle Festplatte aus.
- 4 Klicken Sie auf die Spalte **Anteile** und ändern Sie den Wert, um der virtuellen Maschine eine bestimmte Anzahl an Anteilen der Festplattenbandbreite zuzuteilen.
 - Niedrig (500)
 - Normal (1000)
 - Hoch (2000)
 - Benutzerdefiniert

Wenn Sie einen symbolischen Anteilswert auswählen, wird der numerische Wert in der Spalte **Anteilswert** angezeigt. Sie können die Option **Benutzerdefiniert** auswählen und eigene Anteilswerte angeben.
- 5 Klicken Sie auf die Spalte **Grenzwert - IOPs** und geben Sie den oberen Grenzwert für Speicherressourcen an, die der virtuellen Maschine zugeteilt werden sollen.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

SCSI- und SATA-Speicher-Controller – Bedingungen, Einschränkungen und Kompatibilität

Für den Zugriff auf virtuelle Festplatten, CD-/DVD-ROM-Laufwerke und SCSI-Geräte verwenden virtuelle Maschinen Speicher-Controller, die bei der Erstellung der virtuellen Maschine standardmäßig hinzugefügt werden. Nach der Erstellung der virtuellen Maschine können Sie weitere Controller hinzufügen oder den Typ des Controllers ändern. Sie können diese Änderungen im Assistenten für die Erstellung vornehmen. Bevor Sie einen Controller ändern oder hinzufügen, sollten Sie sich über das Verhalten von Knoten, die Controller-Einschränkungen sowie die Kompatibilität der verschiedenen Controller-Typen informieren, um Startprobleme zu vermeiden.

Funktionsweise der Speicher-Controller-Technologie

Speicher-Controller werden auf einer virtuellen Maschine als unterschiedliche Typen von SCSI-Controllern angezeigt, wie zum Beispiel BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS und VMware Paravirtual SCSI. Auch AHCI SATA-Controller sind verfügbar.

Bei der Erstellung einer virtuellen Maschine ist der Standard-Controller für eine maximale Leistung optimiert. Der Controller-Typ richtet sich nach dem Gastbetriebssystem, dem Gerätetyp und in einigen Fällen nach der Kompatibilität der virtuellen Maschine. Wenn Sie beispielsweise virtuelle Maschinen mit dem Gastbetriebssystem Apple Mac OS X und einer Kompatibilität mit ESXi 5.5 und höher erstellen, ist SATA der standardmäßige Controller-Typ für die Festplatte und das CD/DVD-Laufwerk. Wenn Sie virtuelle Maschinen mit dem Gastbetriebssystem Windows Vista oder einer neueren Windows-Version erstellen, ist ein SCSI-Controller der standardmäßige Controller für die Festplatte und ein SATA-Controller der standardmäßige Controller für das CD/DVD-Laufwerk.

Jede virtuelle Maschine kann maximal vier SCSI-Controller und vier SATA-Controller haben. Der standardmäßige SCSI- oder SATA-Controller ist 0. Wenn Sie eine virtuelle Maschine erstellen, wird die standardmäßige Festplatte dem standardmäßigen Controller 0 am Busknoten (0:0) zugewiesen.

Wenn Sie Speicher-Controller hinzufügen, werden diese sequenziell mit 1, 2 und 3 nummeriert. Wenn Sie nach dem Erstellen einer virtuellen Maschine eine Festplatte, ein SCSI- oder ein CD/DVD-ROM-Gerät hinzufügen, wird diese Festplatte bzw. dieses Gerät dem ersten verfügbaren Knoten des virtuellen Geräts auf dem standardmäßigen Controller hinzugefügt, beispielsweise (0:1).

Wenn Sie einen SCSI-Controller hinzufügen, können Sie diesem Controller eine bestehende oder eine neue Festplatte oder ein Gerät neu zuweisen. Beispielsweise können Sie das Gerät (1:z) zuweisen. Dabei ist 1 der SCSI-Controller 1 und z ein Knoten eines virtuellen Geräts von 0 bis 15. Bei SCSI-Controllern kann z nicht 7 sein. Standardmäßig wird der virtuelle SCSI-Controller dem Knoten des virtuellen Geräts (z:7) zugewiesen, sodass dieser Geräteknoten für Festplatten oder andere Geräte nicht verfügbar ist.

Wenn Sie einen SATA-Controller hinzufügen, können Sie diesem Controller eine bestehende oder eine neue Festplatte oder ein Gerät neu zuweisen. Beispielsweise können Sie das Gerät (1:z) zuweisen. Dabei ist 1 der SATA-Controller 1 und z ein Knoten des virtuellen Geräts von 0 bis 29. Bei SATA-Controllern können die Geräteknoten 0 bis 29 einschließlich 0:7 verwendet werden.

Einschränkungen bei Speicher-Controllern

Für Speicher-Controller gelten die folgenden Anforderungen und Einschränkungen:

- LSI Logic SAS und VMware Paravirtual SCSI sind für virtuelle Maschinen verfügbar, die mit ESXi 4.x und höher kompatibel sind.
- AHCI SATA ist nur für virtuelle Maschinen verfügbar, die mit ESXi 5.5 und höher kompatibel sind.

- BusLogic Parallel-Controller unterstützen keine virtuellen Maschinen, deren Festplatten größer als 2 TB sind.



VORSICHT Wenn der Controller-Typ nach der Installation des Gastbetriebssystems geändert wird, ist der Zugriff auf die Festplatte und andere Geräte, die mit dem Adapter verbunden sind, nicht mehr möglich. Bevor Sie den Controller-Typ ändern oder einen neuen Controller hinzufügen, sollten Sie sicherstellen, dass die erforderlichen Treiber auf den Installationsmedien des Gastbetriebssystems enthalten sind. Auf Windows-Gastbetriebssystemen muss der Treiber als Starttreiber installiert und konfiguriert werden.

Kompatibilität von Speicher-Controllern

Das Hinzufügen von verschiedenen Typen von Speicher-Controllern zu virtuellen Maschinen, die BIOS-Firmware verwenden, kann zu Startproblemen des Betriebssystems führen. In den folgenden Fällen kann die virtuelle Maschine möglicherweise nicht richtig gestartet werden. Sie müssen dann das BIOS-Setup aufrufen und das richtige Startgerät auswählen:

- Die virtuelle Maschine wird über LSI Logic SAS oder VMware Paravirtual SCSI gestartet und Sie fügen eine Festplatte hinzu, die BusLogic-, LSI Logic- oder AHCI SATA-Controller verwendet.
- Die virtuelle Maschine wird über AHCI SATA gestartet und Sie fügen BusLogic Parallel- oder LSI Logic-Controller hinzu.

Wenn Sie zusätzliche Festplatten zu virtuellen Maschinen hinzufügen, die EFI-Firmware verwenden, werden dadurch keine Startprobleme verursacht.

Tabelle 15-3. VMware-Kompatibilität von Speicher-Controllern

Vorhandener Controller	Hinzugefügter Controller					
	BusLogic Parallel	LSI Logic	LSI Logic SAS	VMware Paravirtual SCSI	AHCI SATA	IDE
BusLogic Parallel	Ja	Ja	Ja	Ja	Ja	Ja
LSI Logic	Ja	Ja	Ja	Ja	Ja	Ja
LSI Logic SAS	Erfordert BIOS-Setup	Erfordert BIOS-Setup	Funktioniert normalerweise	Funktioniert normalerweise	Erfordert BIOS-Setup	Ja
VMware Paravirtual SCSI	Erfordert BIOS-Setup	Erfordert BIOS-Setup	Funktioniert normalerweise	Funktioniert normalerweise	Erfordert BIOS-Setup	Ja
AHCI SATA	Erfordert BIOS-Setup	Erfordert BIOS-Setup	Ja	Ja	Ja	Ja
IDE	Ja	Ja	Ja	Ja	Ja	Nicht verfügbar

Hinzufügen von SCSI-Controllern

Sie können SCSI-Controller zu einer vorhandenen virtuellen Maschine hinzufügen, indem Sie Festplatten auf nicht verwendeten SCSI Bus-Nummern hinzufügen.

Durch das Hinzufügen einer neuen Festplatte auf einer nicht verwendeten SCSI-Bus-Nummer wird automatisch ein neuer SCSI-Controller erstellt.

Voraussetzungen

Ausreichende Berechtigungen zum Bearbeiten der virtuellen Maschine.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte „Hardware“.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie **Festplatte**, und klicken Sie auf **Weiter**.
- 5 Fahren Sie mit der nächsten Assistentenseite fort und wählen Sie die gewünschten Optionen aus.
- 6 Wählen Sie auf der Seite „Erweiterte Optionen“ im Abschnitt „Knoten des virtuellen Geräts“ eine nicht verwendete SCSI-Bus-Nummer aus.

Beispielsweise werden die Bus- und Gerätenummern 0:0 bis 0:15 vom anfänglichen SCSI-Controller verwendet. Der zweite SCSI-Controller verwendet die Bus- und Gerätenummern 1:0 bis 1:15.
- 7 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Die neue Festplatte und der neue SCSI-Controller werden gleichzeitig erstellt.

Ändern der Konfiguration der gemeinsamen Verwendung des SCSI-Busses im vSphere-Client

Sie können den Typ der gemeinsamen Verwendung des SCSI-Busses für eine virtuelle Maschine festlegen und angeben, ob der SCSI-Bus gemeinsam genutzt wird. Je nach Art der gemeinsamen Verwendung können virtuelle Maschinen gleichzeitig auf dieselbe virtuelle Festplatte auf demselben Server oder einem anderen Server zugreifen.

Sie können die SCSI-Controller-Konfiguration für eine virtuelle Maschine nur auf einem ESXi-Host ändern.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie einen SCSI-Controller aus der Hardwareliste aus.
- 3 Wählen Sie in der Liste **Gemeinsame Verwendung des SCSI-Busses** den Verwendungstyp aus.

Option	Beschreibung
Keine	Virtuelle Festplatten können nicht durch mehrere virtuelle Maschinen gemeinsam genutzt werden.
Virtuell	Virtuelle Festplatten können von virtuellen Maschinen auf dem gleichen Server gemeinsam genutzt werden.
Physisch	Virtuelle Festplatten können durch mehrere virtuelle Maschinen auf einem beliebigen Server gemeinsam genutzt werden.

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

Ändern des SCSI-Controller-Typs im vSphere Client

Sie konfigurieren virtuelle SCSI-Controller auf Ihren virtuellen Maschinen, um virtuelle Festplatten und RDMs an diese anzuhängen.

Die Auswahl des SCSI-Controller hat keinen Einfluss darauf, ob Sie als virtuelle Festplatte eine IDE- oder eine SCSI-Festplatte verwenden. Der IDE-Adapter ist immer ATAPI. Der Standard für Ihr Gastbetriebssystem ist bereits ausgewählt. Ältere Gastbetriebssysteme verwenden standardmäßig den BusLogic-Adapter.

Wenn Sie eine virtuelle Maschine mit LSI Logic erstellen und eine virtuelle Festplatte hinzufügen, die Bus-Logic-Adapter verwendet, startet die virtuelle Maschine von der Festplatte mit den BusLogic-Adapttern. LSI Logic SAS ist nur für virtuelle Maschinen mit der Hardwareversion 7 oder höher verfügbar. Festplatten mit Snapshots weisen möglicherweise keinen Leistungsgewinn auf, wenn Sie an LSI Logic SAS-, VMware Paravirtual- und LSI Logic Parallel-Adapttern betrieben werden.



VORSICHT Wenn Sie den SCSI-Controller-Typ ändern, kann dies zu einem Startfehler in einer virtuellen Maschine führen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie einen SCSI-Controller aus.
- 3 Klicken Sie im Bereich **SCSI-Controller-Typ** Sie auf **Ändern**.
- 4 Wählen Sie einen SCSI-Controller-Typ aus und klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Grundlegendes zu paravirtuellen SCSI-Controllern von VMware

Paravirtuelle VMware SCSI-Controller sind Hochleistungs-Speicher-Controller, die einen höheren Durchsatz bei geringerer CPU-Nutzung liefern können. Diese Controller sind am besten für Hochleistungs-Speicherumgebungen geeignet.

Paravirtuelle VMware SCSI-Controller sind für virtuelle Maschinen verfügbar, die mit ESXi 4.x und höher kompatibel sind. Die Leistung von Festplatten auf diesen Controllern wird möglicherweise nicht optimal gesteigert, wenn sie über Snapshots verfügen oder der Arbeitsspeicher auf dem ESXi-Host überbelegt ist. Im Vergleich zu anderen SCSI-Controller-Optionen wirkt sich dieses Verhalten bei Verwendung von paravirtuellen VMware SCSI-Controllern nicht negativ auf die Gesamtleistung aus.

Wenn Sie über virtuelle Maschinen mit paravirtuellen VMware SCSI-Controllern verfügen, können diese virtuellen Maschinen nicht Teil eines MSCS-Clusters sein.

Hinweise dazu, auf welchen Plattformen paravirtuelle VMware SCSI-Controller unterstützt werden, finden Sie im *VMware-Kompatibilitätshandbuch* auf <http://www.vmware.com/resources/compatibility>.

Hinzufügen eines paravirtuellen SCSI-Controllers

Sie können einen paravirtuellen VMware SCSI-Hochleistungs-Speicher-Controller hinzufügen, um einen verbesserten Durchsatz und eine niedrigere CPU-Nutzung zu erzielen.

Paravirtuelle VMware SCSI-Controller eignen sich am besten für Umgebungen, insbesondere SAN-Umgebungen, in denen E/A-intensive Anwendungen ausgeführt werden.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine über ein Gastbetriebssystem mit installierten VMware Tools verfügt.
- Stellen Sie sicher, dass Sie über eine virtuelle Maschine mit Hardwareversion 7 oder höher verfügen.
- Sie sollten sich mit den paravirtuellen VMware SCSI-Einschränkungen vertraut machen. Siehe „[Grundlegendes zu paravirtuellen SCSI-Controllern von VMware](#)“, auf Seite 185.
- Bevor Sie auf die an einen paravirtuellen VMware SCSI-Controller angeschlossenen Boot-Festplatten zugreifen können, stellen Sie sicher, dass die virtuelle Maschine über ein Windows 2003- oder Windows 2008-Gastbetriebssystem verfügt.

- Bevor Sie den Controllertyp ändern können, müssen Sie auf einigen Betriebssystemen zunächst eine virtuelle Maschine mit einem LSI Logic-Controller erstellen, anschließend VMware Tools installieren und in den paravirtualen Modus wechseln.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **SCSI-Gerät** und klicken Sie auf **Weiter**.
- 4 Wählen Sie im Bereich „Verbindungen“ ein SCSI-Gerät aus.
- 5 Wählen Sie einen nicht verwendeten Knoten des virtuellen Geräts aus und klicken Sie auf **Weiter**.
Beim Geräteknoten SCSI (0:2) ist 0 die Controllernummer und 2 die Nummer des Geräts, das an den Controller angeschlossen ist. Wenn Sie einen Knoten auswählen, auf dem bereits Geräte vorhanden sind (z. B. SCSI 0:3), fügen Sie ein SCSI-Gerät zum vorhandenen Controller hinzu. Wenn Sie einen neuen Controller hinzufügen möchten, müssen Sie einen nicht verwendeten Geräteknoten auf einem nicht verwendeten SCSI-Controller auswählen (z. B. 1:0).
- 6 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.
In der Hardwareliste werden **Neuer SCSI-Controller (hinzugefügt)** und **Neues SCSI-Gerät (hinzugefügt)** angezeigt.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.
- 8 Öffnen Sie den Editor "Eigenschaften virtueller Maschinen" erneut.
- 9 Wählen Sie den neuen SCSI-Controller aus und klicken Sie auf **Typ ändern**.
- 10 Wählen Sie **VMware Paravirtual** und klicken Sie auf **OK**.
- 11 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Weitere Gerätekonfigurationen für die virtuelle Maschine

Zusätzlich zum Konfigurieren der CPU und des Arbeitsspeichers virtueller Maschinen und zum Hinzufügen einer Festplatte und virtueller Netzwerkkarten können Sie virtuelle Hardware, wie z. B. DVD-/CD-ROM-Laufwerke, Diskettenlaufwerke und SCSI-Geräte, hinzufügen und konfigurieren. Nicht alle Geräte stehen zum Hinzufügen und Konfigurieren zur Verfügung. Beispielsweise können Sie keine Grafikkarte hinzufügen, aber verfügbare Grafikkarten und PCI-Geräte konfigurieren.

Hinzufügen eines CD-/DVD-Laufwerks zu einer virtuellen Maschine im vSphere Client

Mithilfe eines physischen Laufwerks des Clients bzw. Hosts oder mithilfe eines ISO-Image können Sie einer virtuellen Maschine ein CD-/DVD-Laufwerk hinzufügen.

Wenn Sie ein CD-/DVD-Laufwerk hinzufügen, das von einem USB-CD-/DVD-Laufwerk auf dem Host gestützt wird, müssen Sie das Laufwerk als ein SCSI-Gerät hinzufügen. Das Hinzufügen oder Entfernen von SCSI-Geräten von einem ESXi-Host im laufenden Betrieb wird nicht unterstützt.

Die Migration mit vMotion kann nicht für die Migration von virtuellen Maschinen verwendet werden, die über CD-Laufwerke verfügen, die vom physischen CD-Laufwerk auf dem Host gestützt werden. Sie müssen diese Geräte vor der Migration der virtuellen Maschine trennen.

Voraussetzungen

Stellen Sie zunächst sicher, dass der Host ausgeschaltet ist, bevor Sie USB-CD-/DVD-Geräte hinzufügen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Hardware** aus und klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie die Option **CD-/DVD-Laufwerk** und klicken Sie auf **Weiter**.
- 4 Wählen Sie eine Option aus.

Option	Beschreibung
Physisches Laufwerk verwenden	<ol style="list-style-type: none"> a Wählen Sie Client oder Host als Ort aus. b Wählen Sie den Verbindungstyp Passthrough (empfohlen) oder ATA-PI-Emulation aus.
ISO-Image verwenden	Geben Sie den Pfad und den Dateinamen der Image-Datei ein oder klicken Sie auf Durchsuchen , um zur Datei zu navigieren und sie auszuwählen.

- 5 Wenn das DVD-ROM-Laufwerk beim Start der virtuellen Maschine nicht verbunden werden soll, deaktivieren Sie **Beim Einschalten verbinden (Connect at power on)**.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie den vom Laufwerk in der virtuellen Maschine verwendeten Knoten des virtuellen Geräts aus und klicken Sie auf **Weiter**.
- 8 Überprüfen Sie die Informationen im Fenster **Bereit zum Abschließen** und klicken Sie auf **Beenden** oder auf **Zurück**, wenn Sie die Einstellungen ändern möchten.
- 9 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Konfiguration des CD-/DVD-Laufwerks

Sie können DVD- oder CD-Geräte so konfigurieren, dass sie mit Clientgeräten, Hostgeräten oder Datenspeicher-ISO-Dateien verbunden werden können.

Konfigurieren eines Clientgerätetyps für das DVD-/CD-ROM-Laufwerk in vSphere-Client

Sie können auf dem System, auf dem der vSphere-Client ausgeführt wird, das DVD-/CD-ROM-Gerät mit einem physischen DVD- oder CD-ROM-Gerät verbinden.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Client die virtuelle Maschine aus.
- 2 Klicken Sie auf der Symbolleiste der virtuellen Maschine auf das Symbol **CD/DVD-Verbindungen**.
- 3 Wählen Sie ein Laufwerk oder ein ISO-Image aus dem Dropdown-Menü **CD-/DVD-Laufwerk** aus.

Der Passthrough-IDE-Modus (raw) ist standardmäßig eingestellt, damit Sie eine Remote-CD beschreiben oder brennen können.

Konfigurieren eines Hostgerätetyps für das CD-/DVD-Laufwerk im vSphere Client

Sie können das CD/DVD-Gerät mit einem physischen DVD- oder CD-ROM-Gerät verbinden, das sich auf dem Host befindet.

Die Migration mit vMotion kann nicht für die Migration von virtuellen Maschinen verwendet werden, die über CD-Laufwerke verfügen, die vom physischen CD-Laufwerk auf dem Host gestützt werden. Sie müssen diese Geräte vor der Migration der virtuellen Maschine trennen.

Wenn Sie ein CD-/DVD-ROM-Laufwerk hinzufügen, das von einem USB-CD-/DVD-Laufwerk auf dem Host gestützt wird, müssen Sie das Laufwerk als ein SCSI-Gerät hinzufügen. Das Hinzufügen oder Entfernen von SCSI-Geräten von einem ESXi-Host im laufenden Betrieb wird nicht unterstützt.

Voraussetzungen

Stellen Sie zunächst sicher, dass der Host ausgeschaltet ist, bevor Sie USB-CD-/DVD-ROM-Geräte hinzufügen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf „CD-/DVD-Laufwerk“.
- 3 Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verbunden**, um das Gerät zu verbinden oder zu trennen.
- 4 Wenn das DVD-ROM-Laufwerk beim Start der virtuellen Maschine nicht verbunden werden soll, deaktivieren Sie **Beim Einschalten verbinden (Connect at power on)**.
- 5 Wählen Sie **Hostgerät** unter **Gerätetyp** und anschließend ein Gerät aus dem Dropdown-Menü aus.
- 6 (Optional) Wählen Sie im Dropdown-Menü unter **Knoten des virtuellen Geräts** den Knoten aus, den das Laufwerk in der virtuellen Maschine verwendet.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren einer Datenspeicher-ISO-Datei für das CD-/DVD-Laufwerk im vSphere Client

Sie können das CD-/DVD-Gerät mit einer ISO-Datei verbinden, die auf einem Datenspeicher gespeichert ist, auf den der Host zugreifen kann.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf „CD-/DVD-Laufwerk“.
- 3 Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verbunden**, um das Gerät zu verbinden oder zu trennen.
- 4 Wenn das DVD-ROM-Laufwerk beim Start der virtuellen Maschine nicht verbunden werden soll, deaktivieren Sie **Beim Einschalten verbinden (Connect at power on)**.
- 5 Wählen Sie **Datenspeicher-ISO-Datei** unter **Gerätetyp** aus und klicken Sie auf **Durchsuchen**, um zur Datei zu navigieren.
- 6 Wählen Sie im Dropdown-Menü unter **Knoten des virtuellen Geräts** den Knoten aus, den das Laufwerk in der virtuellen Maschine verwendet.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Hinzufügen eines Diskettenlaufwerks zu einer virtuellen Maschine im vSphere-Client

Verwenden Sie ein physisches Diskettenlaufwerk oder ein Disketten-Image, um einer virtuellen Maschine ein Diskettenlaufwerk hinzuzufügen.

ESXi unterstützt keine Diskettenlaufwerke, die von einem physischen Diskettenlaufwerk auf dem Host gestützt werden.

HINWEIS Die Migration mit vMotion kann nicht für die Migration von virtuellen Maschinen verwendet werden, die über Diskettenlaufwerke verfügen, die von einem physischen Diskettenlaufwerk auf von vCenter Server 5.0 verwalteten ESX 3.5-, 4.0- und 4.x-Hosts gestützt werden. Sie müssen diese Geräte vor der Migration der virtuellen Maschine trennen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Hardware** aus und klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **Diskettenlaufwerk**, und klicken Sie dann auf **Weiter**.
- 4 Wählen Sie den Gerätetyp aus, der für dieses virtuelle Gerät verwendet werden soll.

Option	Beschreibung
Physisches Diskettenlaufwerk verwenden	Wählen Sie diese Option aus, um das Diskettenlaufwerk mit einem physischen Diskettenlaufwerk oder einem .flp-Disketten-Image auf dem System zu verbinden, auf dem der vSphere-Client ausgeführt wird. Klicken Sie zum Verbinden des Geräts beim Einschalten der virtuellen Maschine in der Symbolleiste auf die Schaltfläche Diskettenlaufwerk verbinden .
Disketten-Image verwenden	<ol style="list-style-type: none"> a Aktivieren Sie diese Option, um das virtuelle Gerät mit einem Disketten-Image auf einem Datenspeicher zu verbinden, auf den der Host zugreifen kann. b Klicken Sie auf Durchsuchen, und wählen Sie das Disketten-Image aus.
Leeres Disketten-Image erstellen	<ol style="list-style-type: none"> a Aktivieren Sie diese Option, um ein Disketten-Image auf einem Datenspeicher zu erstellen, auf den der Host zugreifen kann. b Klicken Sie auf Durchsuchen, und navigieren Sie zum Speicherort des Disketten-Images. c Geben Sie einen Namen für das Disketten-Image ein und klicken Sie auf OK.

- 5 Wenn das Diskettenlaufwerk beim Einschalten der virtuellen Maschine mit dieser verbunden werden soll, wählen Sie die Option **Beim Einschalten verbinden**.
- 6 Klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Information auf der Seite Bereit zum Abschließen, und klicken Sie auf **Beenden**.
- 8 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Konfiguration des Diskettenlaufwerks im vSphere-Client

Sie können ein virtuelles Diskettenlaufwerkgerät für die Verbindung mit einem Clientgerät oder einem vorhandenen oder neuen Disketten-Image konfigurieren.

ESXi unterstützt keine Diskettenlaufwerke, die von einem physischen Diskettenlaufwerk auf dem Host gestützt werden.

HINWEIS Die Migration mit vMotion kann nicht für die Migration von virtuellen Maschinen verwendet werden, die über Diskettenlaufwerke verfügen, die von einem physischen Diskettenlaufwerk auf von vCenter Server 5.0 verwalteten ESX 3.5-, 4.0- und 4.x-Hosts gestützt werden. Sie müssen diese Geräte vor der Migration der virtuellen Maschine trennen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie das Diskettenlaufwerk aus.
- 3 Wählen Sie unter „Gerätstatus“ die Option **Beim Einschalten verbinden** aus, um die virtuelle Maschine beim Einschalten mit dem Diskettenlaufwerk zu verbinden.
- 4 Wählen Sie den Gerätetyp aus, der für dieses virtuelle Gerät verwendet werden soll.

Option	Beschreibung
Clientgerät	Wählen Sie diese Option aus, um das Diskettenlaufwerk mit einem physischen Diskettenlaufwerk oder einem .flp-Disketten-Image auf dem System zu verbinden, auf dem der vSphere-Client ausgeführt wird. Klicken Sie zum Verbinden des Geräts beim Einschalten der virtuellen Maschine in der Symbolleiste auf die Schaltfläche Diskettenlaufwerk verbinden .
Im Datenspeicher vorhandenes Disketten-Image verwenden	<ol style="list-style-type: none"> a Aktivieren Sie diese Option, um das virtuelle Gerät mit einem Disketten-Image auf einem Datenspeicher zu verbinden, auf den der Host zugreifen kann. b Klicken Sie auf Durchsuchen, und wählen Sie das Disketten-Image aus.
Neues Disketten-Image im Datenspeicher erstellen	<ol style="list-style-type: none"> a Aktivieren Sie diese Option, um ein Disketten-Image auf einem Datenspeicher zu erstellen, auf den der Host zugreifen kann. b Klicken Sie auf Durchsuchen, und navigieren Sie zum Speicherort des Disketten-Images. c Geben Sie einen Namen für das Disketten-Image ein und klicken Sie auf OK.

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

Hinzufügen eines SCSI-Geräts zu einer virtuellen Maschine im vSphere-Client

Sie können Hardware über den Assistenten zum Hinzufügen von Hardware zur virtuellen Maschine hinzufügen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **Hinzufügen**.
- 3 Wählen Sie **SCSI-Gerät** und klicken Sie auf **Weiter**.

- 4 Unter **Verbindung** können Sie im Dropdown-Menü ein physisches Gerät auswählen.
- 5 Wählen Sie unter **Knoten des virtuellen Geräts** den Knoten für virtuelle Geräte aus, unter dem das Gerät in der virtuellen Maschine aufgeführt werden soll.
- 6 Überprüfen Sie die Information auf der Seite Bereit zum Abschließen, und klicken Sie auf **Beenden**.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Konfiguration des SCSI-Geräts im vSphere-Client

Sie können das physische Gerät und den virtuellen Geräteknoten des verbundenen SCSI-Geräts ändern.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie ein SCSI-Gerät aus der Hardwareliste aus.
- 3 Wählen Sie unter **Verbindung (Connection)** das gewünschte physische Gerät aus.
Wählen Sie unter „Knoten des virtuellen Geräts“ den Knoten für virtuelle Geräte aus, unter dem das Gerät in der virtuellen Maschine aufgeführt werden soll.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Hinzufügen eines PCI-Geräts im vSphere-Client

Die vSphere DirectPath I/O ermöglicht einem Gastbetriebssystem auf einer virtuellen Maschine den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind. Jede virtuelle Maschine kann mit bis zu sechs PCI-Geräten verbunden werden.

Mit einem Host verbundene PCI-Geräte können über die erweiterten Hardwareeinstellungen in der Registerkarte **Konfiguration** für den Host als für Passthrough verfügbar gekennzeichnet werden.

Snapshots mit PCI vSphere Direct Path I/O-Geräten werden nicht unterstützt.

Voraussetzungen

- Wenn Sie DirectPath I/O verwenden möchten, stellen Sie sicher, dass die „Virtualization Technology for Directed I/O“ (VT-d) von Intel® oder die „I/O Virtualization Technology“ (IOMMU) von AMD im BIOS des Hosts aktiviert ist.
- Stellen Sie sicher, dass die PCI-Geräte mit dem Host verbunden und als „für Passthrough verfügbar“ gekennzeichnet sind.
- Stellen Sie sicher, dass die virtuelle Maschine Hardwareversion 7 oder höher verwendet.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie im Assistenten zum Hinzufügen von Hardware die Option **PCI-Gerät** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie das Passthrough-Gerät, mit dem Sie die virtuelle Maschine verbinden möchten, aus der Dropdown-Liste aus und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**.

Konfigurieren von Grafikkarten im vSphere-Client

Sie können die Anzahl der Anzeigen für eine virtuelle Maschine ändern, Arbeitsspeicher für die Anzeigen zuteilen und die 3D-Unterstützung aktivieren.

Die Standardeinstellung für den gesamten Video-RAM reicht für eine Mindest-Desktopauflösung aus. Bei komplexeren Anwendungen können Sie den Standardarbeitsspeicher ändern.

Einige 3D-Anwendungen benötigen einen Videoarbeitsspeicher von mindestens 64 MB. Dies sollten Sie beim Zuweisen von Videoarbeitsspeicher wissen.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **Grafikkarte**.
- 3 Wählen Sie den Typ der Anzeigeeinstellungen aus und konfigurieren Sie die verfügbaren Einstellungen.

Option	Beschreibung
Videoeinstellungen automatisch erkennen	Übernimmt häufig verwendete Videoeinstellungen für das Gastbetriebssystem.
Benutzerdefinierte Einstellungen angeben	Ermöglicht Ihnen das Festlegen der Anzahl der Anzeigen und der Gesamtmenge an Videoarbeitsspeicher.

- 4 Wählen Sie die Anzahl der Anzeigen im Dropdown-Menü aus.
Der vSphere-Client unterstützt das Festlegen einer Reihe von Anzeigen und das Erweitern des Bildschirms über diese. Echte Multimonitor-Unterstützung steht mit dem vSphere-Client nicht zur Verfügung.
- 5 Geben Sie den für die Anzeigen erforderlichen Videoarbeitsspeicher ein.
- 6 (Optional) Klicken Sie auf **Videoarbeitsspeicher-Rechner**, um basierend auf der maximalen Anzahl der Anzeigen, der Auflösung und der Farbtiefe, die das Gastbetriebssystem unterstützen muss, den erforderlichen Videoarbeitsspeicher zu berechnen. Klicken Sie anschließend auf **OK**.
- 7 (Optional) Klicken Sie auf **3D-Unterstützung aktivieren**.
Dieses Kontrollkästchen ist nur bei Gastbetriebssystemen aktiv, bei denen VMware 3D unterstützt.
- 8 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Für die Videoanzeige der virtuellen Maschine wurde eine ausreichende Arbeitsspeicherzuteilung festgelegt.

Konfigurieren von vServices

Eine vService-Abhängigkeit ermöglicht einer vApp oder einer virtuellen Maschine anzufordern, dass ein vService auf einer angegebenen Plattform zur Verfügung gestellt wird.

Ein vService ist ein spezieller Service, von dem vApps und virtuelle Maschinen abhängig sind.

Auf der Registerkarte für die vService-Konfiguration können die vService-Abhängigkeiten überwacht und verwaltet werden. Auf dieser Registerkarte werden alle Abhängigkeiten einer virtuellen Maschine oder einer vApp angezeigt sowie alle ihre Statuszustände. Jede Abhängigkeit wird mit dem Namen, der Beschreibung, der Anforderung, dem Bindungsstatus und dem Anbieternamen der Abhängigkeit angezeigt.

Hinzufügen einer vService-Abhängigkeit

Sie können einer virtuellen Maschine oder einer vApp eine vService-Abhängigkeit hinzufügen. Diese Abhängigkeit ermöglicht einer virtuellen Maschine oder einer vApp das Anfordern eines bestimmten verfügbaren vService.

Vorgehensweise

- 1 Zeigen Sie die virtuelle Maschine oder vApp in der Bestandsliste an.
- 2 Schalten Sie die virtuelle Maschine oder vApp aus.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **vServices**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Wählen Sie im Assistent zum Hinzufügen von Abhängigkeiten den Anbieter für diese Abhängigkeit aus und klicken Sie auf **Weiter**.
- 7 Geben Sie einen Namen und eine Beschreibung für die Abhängigkeit ein.
- 8 (Optional) Falls diese Abhängigkeit erforderlich ist, wählen Sie das Kontrollkästchen aus und klicken Sie auf **Weiter**.

Erforderliche Abhängigkeiten müssen vor dem Einschalten gebunden werden.

- 9 (Optional) Falls diese Abhängigkeit sofort an den Anbieter gebunden werden soll, wählen Sie die Option **Sofort an Anbieter binden** und klicken Sie nach Abschluss der Validierung auf **Weiter**.

Wenn Sie die Abhängigkeit jetzt binden möchten, wird das Validierungsergebnis angezeigt. Falls die Validierung fehlschlägt, können Sie das Hinzufügen der Abhängigkeit nicht abschließen. Deaktivieren Sie das Kontrollkästchen, um fortzufahren.

- 10 Prüfen Sie die Optionen und klicken Sie auf **Beenden**, um die Abhängigkeit zu erstellen.

Bearbeiten einer vService-Abhängigkeit

Sie können den Namen, die Beschreibung und die Erforderlichkeit einer vService-Abhängigkeit bearbeiten.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **vServices** im Dialogfeld „Einstellungen bearbeiten“ mit der rechten Maustaste auf die Abhängigkeit und wählen Sie **Bearbeiten**.
- 3 Ändern Sie im Dialogfeld „Abhängigkeitseigenschaften“ den Namen und die Beschreibung der Abhängigkeit.
- 4 Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den Status „Erforderlich“ der Abhängigkeit zu ändern.

Das Kontrollkästchen „Erforderlich“ ist deaktiviert, wenn die virtuelle Maschine bzw. die vApp läuft.

- 5 Wählen Sie einen Anbieter für die Abhängigkeit aus.

Wenn Sie einen Anbieter auswählen, wird die Anbieterbeschreibung als Beschreibung übernommen. Das Feld „Validierung“ zeigt die Validierungsergebnisse an. Wenn die Validierung fehlschlägt, wird die Schaltfläche **OK** deaktiviert, bis ein anderer oder kein Anbieter ausgewählt wird.

- 6 Klicken Sie auf **OK**.

Entfernen einer vService-Abhängigkeit

Sie können eine vService-Abhängigkeit von einer virtuellen Maschine oder einer vApp entfernen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie auf der Registerkarte **vServices** im Dialogfeld „Einstellungen bearbeiten“ die Abhängigkeit aus und klicken Sie auf **Entfernen**.

Die Abhängigkeit wird aus der Liste entfernt.

USB-Konfiguration von einem ESXi -Host zu einer virtuellen Maschine

Sie können mehrere USB-Geräte zu einer virtuellen Maschine hinzufügen, wenn die physischen Geräte an einen ESXi-Host angeschlossen sind. Die USB-Passthrough-Technologie unterstützt das Hinzufügen von USB-Geräten, wie z. B. Sicherheits-Dongles und Massenspeichergeräten, zu virtuellen Maschinen, die sich auf dem Host befinden, mit dem die Geräte verbunden sind.

Funktionsweise von USB-Geräte-Passthroughs

Ein USB-Gerät, das Sie an einen physischen Host anschließen, steht nur den virtuellen Maschinen zur Verfügung, die sich auf diesem Host befinden. Das Gerät kann keine Verbindung zu virtuellen Maschinen herstellen, die sich auf einem anderen Host im Datacenter befinden.

Ein USB-Gerät kann nicht gleichzeitig von mehreren virtuellen Maschinen verwendet werden. Wenn ein Gerät mit einer eingeschalteten virtuellen Maschine verbunden ist, steht es nicht zum Verbinden mit anderen virtuellen Maschinen zur Verfügung, die auf dem Host ausgeführt werden. Wenn Sie die aktive Verbindung eines USB-Geräts von einer virtuellen Maschine entfernen, steht es zum Verbinden mit anderen virtuellen Maschinen zur Verfügung, die auf dem Host ausgeführt werden.

Für die Verbindung eines USB-Passthrough-Geräts mit einer virtuellen Maschine, die auf dem ESXi-Host ausgeführt wird, an den das Gerät physisch angeschlossen ist, werden ein Arbitrator und ein Controller sowie ein physisches USB-Gerät oder ein Geräte-Hub benötigt.

USB-Arbitrator

Verwaltet die Verbindungsanforderungen und leitet den Datenverkehr für das USB-Gerät. Der Arbitrator ist standardmäßig auf ESXi-Hosts installiert und aktiviert. Er durchsucht den Host nach USB-Geräten und verwaltet die Geräteverbindung zu den virtuellen Maschinen auf dem Host. Er leitet den Datenverkehr an die richtige virtuelle Maschine und das entsprechende Gastbetriebssystem weiter. Der Arbitrator überwacht das USB-Gerät und verhindert, dass andere virtuelle Maschinen darauf zugreifen, bis Sie es wieder freigeben.

USB-Controller

USB-Hardware-Chip, mit dem den USB-Ports, die er verwaltet, USB-Funktionen bereitgestellt werden. Der virtuelle USB-Controller ist die Softwarevirtualisierung des USB-Hostcontrollers in der virtuellen Maschine.

Auf dem Host müssen USB-Controller-Hardware und -Module vorhanden sein, die USB-3.0-, USB-2.0- und USB-1.1-Geräte unterstützen. Acht virtuelle USB-Controller stehen für jede virtuelle Maschine zur Verfügung. Ein Controller muss bereits vorhanden sein, bevor Sie USB-Geräte zum virtuellen Computer hinzufügen können.

Der USB-Arbitrator kann bis zu 15 USB-Controller überwachen. Geräte, die mit Controllern mit der Nummer 16 oder höher verbunden sind, stehen der virtuellen Maschine nicht zur Verfügung.

USB-Geräte

Sie können einer virtuellen Maschine bis zu 20 USB-Geräte hinzufügen. Dies ist die maximale Anzahl an Geräten, die gleichzeitig an eine virtuelle Maschine angeschlossen werden können. Auf einem einzelnen ESXi-Host können maximal 20 USB-Geräte mit einer oder mehreren virtuellen Maschinen gleichzeitig verbunden werden. Eine Liste der unterstützten USB-Geräte finden Sie in der VMware-Knowledgebase unter <http://kb.vmware.com/kb/1021345>. USB-3.0-Geräte können für VMware Fusion dem Gastbetriebssystem Mac OSX hinzugefügt werden.

Hinzufügen eines USB-Controllers zu einer virtuellen Maschine im vSphere Client

Sie können virtuellen Maschinen USB-Controller hinzufügen, um USB-Passthrough von einem ESXi-Host oder von einem Clientcomputer an die virtuelle Maschine zu unterstützen.

Pro virtueller Maschine können Sie einen virtuellen xHCI-Controller, einen virtuellen EHCI-Controller und einen virtuellen UHCI-Controller hinzufügen. Für Hardwareversion 11 werden pro xHCI-Controller acht Root-Hubports unterstützt (vier logische USB 3.0-Ports und vier logische USB 2.0-Ports).

Die Bedingungen für das Hinzufügen eines Controllers variieren abhängig von der Geräteversion, dem Passthrough-Typ (Host- oder Clientcomputer) und dem Gastbetriebssystem.

Tabelle 15-4. USB-Controller-Unterstützung

Controller-Typ	Unterstützte USB-Geräteversion	Unterstützt für Passthrough vom ESXi-Host zur VM	Unterstützt für Passthrough vom Clientcomputer zur VM
EHCI+UHCI	2.0 und 1.1	Ja	Ja
xHCI	3.0, 2.0 und 1.1	Ja (nur USB 3.0-, USB 2.0- und USB 1.1-Geräte)	Ja (Linux, Windows 8 und höher sowie Windows Server 2012 und höhere Gastbetriebssysteme)

HINWEIS Treiber sind für den xHCI-Controller auf Windows-Gastbetriebssystemen nicht verfügbar.

Bei Mac OS X-Systemen ist der EHCI+UHCI-Controller, der für die Verwendung von USB-Maus und -Tastatur benötigt wird, standardmäßig aktiviert.

Virtuellen Maschinen mit Linux-Gastbetriebssystemen können Sie einen oder beide Controller hinzufügen, bei 3.0-SuperSpeed-Geräten wird jedoch der Passthrough von einem ESXi-Host zu einer virtuellen Maschine nicht unterstützt. Sie können zwei Controller desselben Typs nicht hinzufügen.

Bei einem USB-Passthrough von einem ESXi-Host zu einer virtuellen Maschine kann der USB-Arbitrator maximal 15 USB-Controller überwachen. Wenn mehr als 15 Controller in Ihrem System vorhanden sind und Sie schließen USB-Geräte an diese Controller an, stehen sie der virtuellen Maschine nicht zur Verfügung.

Voraussetzungen

- ESXi-Hosts müssen über USB-Controller-Hardware und -Module verfügen, die USB 3.0-, USB 2.0- und USB 1.1-Geräte unterstützen.

- Client-Computer müssen über USB-Controller-Hardware und -Module verfügen, die USB 3.0-, USB 2.0- und USB 1.1-Geräte unterstützen.
- Wenn Sie den xHCI-Controller auf einem Linux-Gastbetriebssystem verwenden möchten, stellen Sie sicher, dass die Linux-Kernelversion 2.6.35 oder höher ist.
- Stellen Sie sicher, dass die virtuelle Maschine eingeschaltet ist.
- Erforderliche Berechtigung (ESXi-Host-Passthrough): **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **USB-Controller** und klicken Sie auf **Weiter**.
- 4 Wählen Sie einen Controller-Typ aus und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**.

Neuer USB-Controller (hinzugefügt) wird in der Hardwareliste als **Vorhanden** aufgeführt.

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

Wenn Sie den Eigenschafteneditor erneut öffnen, wird der xHCI-Controller auf der Registerkarte **Hardware** als USB xHCI-Controller angezeigt. Der EHCI+UHCI-Controller wird als **USB-Controller** angezeigt.

Weiter

Fügen Sie ein oder mehrere USB-Geräte zur virtuellen Maschine hinzu.

Entfernen eines USB-Controllers aus einer virtuellen Maschine im vSphere-Client

Sie können den USB-Controller aus einer virtuellen Maschine entfernen, wenn Sie keine Verbindungen zu USB-Geräten herstellen möchten.

Voraussetzungen

- Stellen Sie sicher, dass alle USB-Geräte aus der virtuellen Maschine entfernt wurden.
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **USB-Controller**.
- 3 Klicken Sie auf **Entfernen**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Der Controller ist jetzt nicht mehr mit der virtuellen Maschine verbunden, steht aber weiterhin zum Hinzufügen zu einem späteren Zeitpunkt zur Verfügung.

Hinzufügen von USB-Geräten eines ESXi -Hosts zu einer virtuellen Maschine im vSphere-Client

Sie können einer virtuellen Maschine ein oder mehrere USB-Passthrough-Geräte eines ESXi-Hosts hinzufügen, wenn das physische Gerät an den Host angeschlossen ist, auf dem die virtuelle Maschine läuft.

Falls ein USB-Gerät bereits mit einer anderen virtuellen Maschine verbunden ist, können Sie es erst hinzufügen, wenn es von dieser Maschine freigegeben wurde.

HINWEIS Wenn sich ein Apple Frontpanel Controller-Gerät in Ihrer Umgebung befindet, können Sie es sicher zu einer virtuellen Maschine hinzufügen. Allerdings hat dieses Gerät keine dokumentierte Funktion und keinen bekannten Nutzen. ESXi-Hosts verwenden es nicht und bieten keine Xserver-Funktionalität für das USB-Passthrough.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine Hardwareversion 7 oder höher verwendet.
- Stellen Sie sicher, dass ein USB-Controller vorhanden ist. Weitere Informationen hierzu finden Sie unter [„Hinzufügen eines USB-Controllers zu einer virtuellen Maschine im vSphere Client“](#), auf Seite 195.
- Wenn Sie eine virtuelle Maschine mit mehreren USB-Geräten mit vMotion migrieren möchten, müssen Sie alle angeschlossenen USB-Geräte für vMotion aktivieren. Sie können USB-Geräte nicht individuell migrieren.
- Wenn Sie ein CD-/DVD-ROM-Laufwerk hinzufügen, das von einem USB-CD-/DVD-Laufwerk auf dem Host gestützt wird, müssen Sie das Laufwerk als ein SCSI-Gerät hinzufügen. Das Hinzufügen und Entfernen von SCSI-Geräten im laufenden Betrieb wird nicht unterstützt.
- Machen Sie sich mit den Anforderungen der virtuellen Maschine für USB-Geräte vertraut. Weitere Informationen hierzu finden Sie unter [USB-Konfiguration von einem ESXi-Host zu einer virtuellen Maschine](#).
- Erforderliche Rechte: **Virtuelle Maschine.Konfiguration.HostUSBDevice**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
- 3 Wählen Sie **USB-Gerät** und klicken Sie auf **Weiter**.
- 4 (Optional) Wählen Sie **VMotion unterstützen, während ein Gerät verbunden ist**.
- 5 Falls Sie nicht vorhaben, eine virtuelle Maschine mit einem verbundenen USB-Gerät zu migrieren, deaktivieren Sie die Option **vMotion unterstützen**.
Dadurch wird die Komplexität bei der Migration reduziert und eine bessere Leistung und Beständigkeit gewährleistet.
- 6 Wählen Sie ein Gerät zum Hinzufügen aus.
Sie können mehrere USB-Geräte hinzufügen, jedoch nicht gleichzeitig.
- 7 Klicken Sie auf **Beenden**.
Neues USB-Gerät (hinzugefügt) wird in der Hardware-Liste als **Vorhanden** aufgeführt.
- 8 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Wenn Sie den Eigenschafteneditor erneut öffnen, wird das USB-Gerät auf der Registerkarte **Hardware** des Eigenschafteneditors aufgeführt. Der Gerätetyp und die -ID werden im rechten Fenster angezeigt.

Entfernen eines USB-Geräts aus einer virtuellen Maschine

Wenn Sie ein USB-Gerät von einer virtuellen Maschine entfernen, kehrt es zum Host zurück und steht anderen virtuellen Maschinen, die auf dem Host ausgeführt werden, zur Verfügung.

Um Datenverluste zu minimieren, befolgen Sie die Anweisungen für Ihr Betriebssystem, um Hardware sicher zu unmounten bzw. auszuwerfen. Durch das sichere Entfernen von Hardware können angesammelte Daten in eine Datei übertragen werden. In der Regel enthalten Windows-Betriebssysteme ein Symbol „Hardware entfernen“ in der Taskleiste. Linux-Betriebssysteme verwenden den Befehl **umount**.

HINWEIS Möglicherweise muss der Befehl **sync** anstelle von oder zusätzlich zum Befehl **umount** verwendet werden, beispielsweise nachdem Sie einen **dd**-Befehl unter Linux oder anderen UNIX-Betriebssystemen aufrufen.

Vorgehensweise

- 1 Unmounten Sie das USB-Gerät oder werfen Sie es seitens des Gastbetriebssystems aus.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie das USB-Gerät aus.
- 4 Klicken Sie auf **Entfernen** und klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

USB-Konfiguration von einem Clientcomputer zu einer virtuellen Maschine im vSphere-Client

Sie können mehrere USB-Geräte zu einer virtuellen Maschine hinzufügen, wenn die physischen Geräte mit einem Clientcomputer verbunden sind, auf dem der vSphere-Client ausgeführt wird. Der vSphere Client muss bei einer Instanz von vCenter Server, die den ESXi-Host verwaltet, oder direkt bei dem Host angemeldet sein, auf dem sich die virtuellen Maschinen befinden. Die USB-Passthrough-Technologie unterstützt das Hinzufügen mehrerer USB-Geräte, wie z. B. Sicherheits-Dongles, Massenspeichergeräte und Chipkartenleser, zu virtuellen Maschinen.

Funktionsweise von USB-Geräte-Passthroughs

Der USB-Controller ist der USB-Hardware-Chip, mit dem den USB-Ports, die er verwaltet, USB-Funktionen zur Verfügung gestellt werden. USB-Controller-Hardware und -Module, die USB 3.0-, USB 2.0- und USB 1.1-Geräte unterstützen, müssen in der virtuellen Maschine vorhanden sein. Zwei USB-Controller stehen für jede virtuelle Maschine zur Verfügung. Die Controller unterstützen mehrere USB 3.0-, USB 2.0- und USB 1.1-Geräte. Der Controller muss bereits vorhanden sein, bevor Sie USB-Geräte zur virtuellen Maschine hinzufügen können.

Sie können einer virtuellen Maschine bis zu 20 USB-Geräte hinzufügen. Dies ist die maximale Anzahl an Geräten, die gleichzeitig an eine virtuelle Maschine angeschlossen werden können.

Sie können mehrere USB-Geräte zu einer virtuellen Maschine hinzufügen, jedoch nicht gleichzeitig. Die virtuelle Maschine behält ihre Verbindung zum Gerät im S1-Standby-Modus bei. USB-Geräteverbindungen werden beibehalten, wenn Sie virtuelle Maschinen auf einen anderen Host im Datacenter migrieren.

Ein USB-Gerät kann nicht gleichzeitig von mehreren eingeschalteten virtuellen Maschinen verwendet werden. Wenn eine virtuelle Maschine eine Verbindung mit einem Gerät herstellt, steht das Gerät nicht mehr für andere virtuellen Maschinen oder den Clientcomputer zur Verfügung. Wenn Sie das Gerät von der virtuellen Maschine trennen oder die virtuelle Maschine herunterfahren, ist es für den Clientcomputer verfügbar und steht dann auch anderen virtuellen Maschinen zur Verfügung, die der Clientcomputer verwaltet.

Wenn Sie beispielsweise ein USB-Massenspeichergerät an eine virtuelle Maschine anschließen, wird es vom Clientcomputer entfernt und erscheint nicht als Laufwerk mit einem Wechselmedium. Wenn Sie das Gerät von der virtuellen Maschine trennen, wird es mit dem Betriebssystem des Clientcomputers erneut verbunden und als Wechselmedium aufgelistet.

Einschränkungen bei USB 3.0-Geräten

USB 3.0-Geräte haben die folgenden Anforderungen und Einschränkungen:

- Die virtuelle Maschine, die Sie mit dem USB 3.0-Gerät verbinden, muss mit einem xHCI-Controller konfiguriert sein und über ein Linux-Gastbetriebssystem mit einem Kernel der Version 2.6.35 oder höher verfügen.
- Sie können nur ein USB 3.0-Gerät, das mit Superspeed betrieben wird, mit einer virtuellen Maschine verbinden.
- USB 3.0-Geräte sind nur für das Passthrough von einem Clientcomputer zu einer virtuellen Maschine verfügbar. Sie sind nicht für das Passthrough von einem ESXi-Host zu einer virtuellen Maschine verfügbar.

Vermeiden von Datenverlust

Bevor Sie ein Gerät mit einer virtuellen Maschine verbinden, stellen Sie sicher, dass das Gerät nicht auf dem Clientcomputer in Gebrauch ist.

Wenn die Verbindung zwischen dem vSphere-Client und vCenter Server bzw. dem Host beendet wird oder wenn Sie den Clientcomputer neu starten bzw. herunterfahren, wird auch die Verbindung zum Gerät unterbrochen. Es wird daher empfohlen, einen dedizierten Clientcomputer für die Verwendung von USB-Geräten vorzusehen oder an einen Clientcomputer angeschlossene USB-Geräte für den kurzfristigen Gebrauch zu reservieren, z. B. für das Aktualisieren von Software oder das Hinzufügen von Patches zu virtuellen Maschinen. Um USB-Geräteverbindungen zu einer virtuellen Maschine für einen längeren Zeitraum beizubehalten, verwenden Sie das USB-Passthrough von einem ESXi-Host zur virtuellen Maschine.

Anschließen von USB-Geräten an einen Clientcomputer

Sie können mehrere USB-Geräte an einem Clientcomputer anschließen, sodass virtuelle Maschinen auf diese Geräte zugreifen können. Die Anzahl der Geräte, die Sie anschließen können, ist von verschiedenen Faktoren abhängig, beispielsweise davon, wie die Geräte und Hubs verbunden sind, sowie vom Gerätetyp.

Die Anzahl der Ports auf jedem Clientcomputer wird von der physischen Konfiguration des Hosts bestimmt. Wenn Sie die Tiefe der Hub-Verkettung berechnen, beachten Sie, dass bei einem typischen Server die vorderen Ports mit einem internen Hub verbunden sind.

Der USB-Arbitrator kann bis zu 15 USB-Controller überwachen. Wenn mehr als 15 Controller in Ihrem System vorhanden sind und Sie schließen USB-Geräte an diese Controller an, stehen sie der virtuellen Maschine nicht zur Verfügung.

Voraussetzungen

Vergewissern Sie sich, dass Sie mit den Anforderungen für das Konfigurieren von USB-Geräten von einem Remotecomputer für eine virtuelle Maschine vertraut sind.

Vorgehensweise

- ◆ Verbinden Sie zum Hinzufügen eines USB-Geräts zu einem Clientcomputer das Gerät mit einem verfügbaren Port oder Hub.

Das USB-Gerät erscheint im Symbolleistemenü der virtuellen Maschine.

Weiter

Sie können das USB-Gerät jetzt zur virtuellen Maschine hinzufügen.

Hinzufügen von USB-Geräten von einem Clientcomputer zu einer virtuellen Maschine im vSphere-Client

Sie können im vSphere-Client ein oder mehrere USB-Passthrough-Geräte von einem Clientcomputer zu einer virtuellen Maschine hinzufügen. Die physischen Geräte müssen an einen Clientcomputer angeschlossen sein, der mit dem ESXi-Host verbunden ist, auf dem sich die virtuellen Maschinen befinden.

Die Geräte behalten ihre Verbindungen zur virtuellen Maschine im S1-Standby-Modus, wenn der vSphere-Client ausgeführt wird und über eine Verbindung verfügt. Nachdem Sie das USB-Gerät zur virtuellen Maschine hinzugefügt haben, wird eine Informationsmeldung auf dem Clientcomputer angezeigt, die angibt, dass das Gerät nicht verbunden ist. Die Verbindung dieses Geräts zum Clientcomputer bleibt getrennt, bis die virtuelle Maschine es freigegeben hat.

FT wird mit USB-Passthrough von einem Clientcomputer zu einer virtuellen Maschine nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass ein USB-Controller installiert ist.
- Stellen Sie sicher, dass der vSphere-Client Zugriff auf den ESXi-Host hat, auf dem die virtuellen Maschinen ausgeführt werden.
- Erforderliche Berechtigung: **Virtuelle Maschine.Interaktion.Gerät hinzufügen oder entfernen**

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients die virtuelle Maschine aus.
- 2 Klicken Sie auf der Symbolleiste der virtuellen Maschine auf das USB-Symbol.
- 3 Wählen Sie aus dem Dropdown-Menü **Mit USB-Gerät verbinden** ein verfügbares Gerät aus.

Der Status des Geräts wird mit „Verbinden“ angezeigt.

Das Gerät erscheint im Dropdown-Menü **USB-Verbindungen** und ist einsatzbereit. Das Gerät bleibt verbunden, bis Sie die virtuelle Maschine ausschalten oder die Verbindung des vSphere-Clients zum ESXi-Host trennen.

Entfernen von USB-Geräten, die über einen Clientcomputer im vSphere-Client verbunden sind

Sie können USB-Geräte von einer virtuellen Maschine entfernen, wenn sie nicht mehr benötigt werden. Wenn Sie die Verbindung eines USB-Geräts zu einer virtuellen Maschine trennen, wird das Gerät freigegeben und die virtuelle Maschine gibt es an den Clientcomputer zurück, der es dann verwendet.

Voraussetzungen

Um Datenverluste zu minimieren, befolgen Sie die Anweisungen für Ihr Betriebssystem, um Hardware sicher zu unmounten bzw. auszuwerfen. Durch das sichere Entfernen von Hardware können angesammelte Daten in eine Datei übertragen werden. In der Regel enthalten Windows-Betriebssysteme ein Symbol „Hardware entfernen“ in der Taskleiste. Linux-Betriebssysteme verwenden den Befehl **umount**.

HINWEIS Möglicherweise muss der Befehl **sync** anstelle von oder zusätzlich zum Befehl **umount** verwendet werden, beispielsweise nachdem Sie einen **dd**-Befehl unter Linux oder einen anderen UNIX-Betriebssystemen aufrufen.

Vorgehensweise

- 1 Unmounten Sie das USB-Gerät oder werfen Sie es seitens des Gastbetriebssystems aus.
- 2 Wählen Sie in der Bestandsliste des vSphere-Clients die virtuelle Maschine aus.
- 3 Klicken Sie auf der Symbolleiste der virtuellen Maschine auf **USB-Verbindungen**.
- 4 Wählen Sie das zu entfernende Gerät aus dem Dropdown-Menü aus.

Wählen Sie beispielsweise **USB-Gerät 1 > Trennen von GeräteName**.

Im Menü wird der Gerätestatus als „Trennen“ angezeigt.

Das Gerät wird erneut mit dem Clientcomputer verbunden und steht nun zum Hinzufügen zu einer anderen virtuellen Maschine zur Verfügung. In einigen Fällen erkennt Windows Explorer das Gerät und öffnet ein Dialogfeld auf dem Clientcomputer. Sie können dieses Dialogfeld schließen.

Verwalten von Energieverwaltungseinstellungen für eine virtuelle Maschine

Sie können die Energieoptionen so einstellen, dass eine virtuelle Maschine angehalten wird oder eingeschaltet bleibt, wenn das Gastbetriebssystem in den Standby-Modus versetzt wird.

Die **Energieverwaltungsoptionen** stehen nicht auf jedem Gastbetriebssystem zur Verfügung. **Wake-on-LAN** unterstützt nur Windows-Gastbetriebssysteme und steht für Vlan- oder Flexible-Netzwerkkarten im Vlan-Modus nicht zur Verfügung (das heißt, die aktuelle VMware Tools-Version ist auf dem Gastbetriebssystem nicht installiert).

Mit **Wake-on-LAN** können nur virtuelle Maschinen fortgesetzt werden, die sich in einem S1-Schlafzustand befinden. Angehaltene, ausgeschaltete oder im Ruhemodus befindliche virtuelle Maschinen können nicht fortgesetzt werden.

Nur die folgenden Netzwerkkartentypen unterstützen **Wake-on-LAN**:

- Flexibel (VMware Tools erforderlich).
- vmxnet
- vmxnet (erweitert)
- Vmxnet 3

Voraussetzungen

Sie müssen die virtuelle Maschine ausschalten.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und erweitern Sie **Energieverwaltung**.
- 3 Wählen Sie eine Energieoption aus.
 - **Virtuelle Maschine anhalten**
 - **Gastbetriebssystem in den Standby-Modus versetzen und virtuelle Maschine eingeschaltet lassen**
- 4 (Optional) Sie können **Wake-on-LAN für Datenverkehr der virtuellen Maschine über** und anschließend die virtuellen Netzwerkkarten auswählen, um diese Aktion auszulösen.
Möglicherweise werden nicht unterstützte Netzwerkkarten aufgelistet, diese stehen aber zum Verbinden nicht zur Verfügung.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren der Betriebszustände der virtuellen Maschine

Die Änderung der Betriebszustände der virtuellen Maschinen ist sinnvoll, wenn auf dem Host Wartungsarbeiten ausgeführt werden. Sie können die standardmäßigen Systemeinstellungen für die Steuerelemente zum Ein-/Ausschalten auf der Symbolleiste verwenden oder Sie können die Steuerelemente konfigurieren, um mit dem Gastbetriebssystem zu interagieren. Legen Sie beispielsweise für die Stopp-Schaltfläche in der Symbolleiste fest, dass entweder die virtuelle Maschine ausgeschaltet oder das Gastbetriebssystem heruntergefahren wird.

Sie können zahlreiche Konfigurationen der virtuellen Maschine ändern, während diese ausgeführt wird. Für einige Konfigurationseinstellungen muss jedoch möglicherweise der Betriebszustand der virtuellen Maschine geändert werden.

[Tabelle 15-5](#) gibt die verfügbaren Schaltflächen zum Ein-/Ausschalten an und beschreibt ihr Verhalten.

Tabelle 15-5. Einstellungen für die Schaltflächen zum Ein- und Ausschalten von virtuellen Maschinen





Schaltfläche zum Ein-/Ausschalten	Beschreibung
	Führt das Gastbetriebssystem herunter oder schaltet die virtuelle Maschine aus. Bei einem Ausschaltvorgang wird ein Bestätigungsdialogfeld angezeigt, in dem darauf hingewiesen wird, dass das Gastbetriebssystem evtl. nicht ordnungsgemäß heruntergefahren wird. Verwenden Sie diese Ausschalloption nur bei Bedarf.
	Sind die VMware Tools nicht installiert, wird der Betrieb der virtuellen Maschine angehalten und es wird kein Skript ausgeführt. Wenn VMware Tools installiert und verfügbar ist, führt eine Anhalteaktion ein Skript aus und hält die virtuelle Maschine an.

Tabelle 15-5. Einstellungen für die Schaltflächen zum Ein- und Ausschalten von virtuellen Maschinen (Fortsetzung)

Schaltfläche zum Ein-/Ausschalten	Beschreibung
	Mit dieser Option wird eine virtuelle Maschine eingeschaltet, wenn diese zuvor ausgeschaltet wurde, oder der Betrieb der virtuellen Maschine wird wieder aufgenommen und ein Skript wird ausgeführt, wenn die virtuelle Maschine angehalten wurde und die VMware Tools installiert und verfügbar sind. Sind die VMware Tools nicht installiert, wird der Betrieb der virtuellen Maschine wieder aufgenommen und es wird kein Skript ausgeführt.
	Nimmt ein Reset der virtuellen Maschine vor, wenn VMware Tools nicht installiert ist. Startet das Gastbetriebssystem neu, wenn VMware Tools installiert und verfügbar ist. Beim Zurücksetzen wird ein Bestätigungsdialogfeld angezeigt, in dem darauf hingewiesen wird, dass das Gastbetriebssystem nicht ordnungsgemäß heruntergefahren wird.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf mindestens eine virtuelle Maschine in der Bestandsliste haben.
- Stellen Sie sicher, dass Sie über die Berechtigungen zum Ausführen der beabsichtigten Ein-/Ausschaltvorgänge auf der virtuellen Maschine verfügen.
- Damit Sie optionale Ein-/Ausschaltfunktionen festlegen können, müssen Sie VMWare Tools in der virtuellen Maschine installieren.
- Schalten Sie die virtuelle Maschine aus, bevor Sie die VMware Tools-Optionen bearbeiten.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **VMware Tools**.
- 3 Wählen Sie im rechten Bereich die **Ein-/Ausschaltsteuerelemente** für die virtuelle Maschine aus.
- 4 Wählen Sie eine Option für die Schaltfläche **Ausschalten** aus.

Option	Beschreibung
Gast herunterfahren	Verwendet VMware Tools, um die virtuelle Maschine ordnungsgemäß herunterzufahren. Diese Art des Ausschaltens wird auch als „weich“ (Ausschalten per Software) bezeichnet. Ein „weiches“ Ausschalten ist nur dann möglich, wenn die Tools auf dem Gastbetriebssystem installiert sind.
Ausschalten	Stoppt die virtuelle Maschine sofort. Diese Art des Ausschaltens wird auch als physisches Ausschalten bezeichnet.
Systemstandard	Befolgt die Systemeinstellungen. Der aktuelle Wert der Systemeinstellungen wird in runden Klammern angezeigt.

- 5 Wählen Sie eine Option für die Schaltfläche **Anhalten** aus.

Option	Beschreibung
Anhalten	Hält alle Aktivitäten der virtuellen Maschine an.
Systemstandard	Befolgt die Systemeinstellungen. Der aktuelle Wert der Systemeinstellung wird in Klammern angezeigt.

- 6 Wählen Sie eine Option für die Schaltfläche **Zurücksetzen** aus.

Option	Beschreibung
Gast neu starten	Verwendet VMware Tools für einen ordnungsgemäßen Neustart. (Diese Art des Ausschaltens wird auch als „weiches Ausschalten“ bezeichnet. Ein weiches Ausschalten ist nur dann möglich, wenn die Tools auf dem Gastbetriebssystem installiert sind.)
Zurücksetzen	Das Gastbetriebssystem wird heruntergefahren und neu gestartet, ohne dass die virtuelle Maschine ausgeschaltet wird. (Diese Art des Zurücksetzens wird auch als „hartes Zurücksetzen“ bezeichnet.)
Systemstandard	Verwendet die Systemeinstellungen; die aktuelle Systemeinstellung wird in runden Klammern angezeigt.

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

Weiter

Konfigurieren von VMware Tools-Skripts, die vor oder nach Ein-/Ausschaltvorgängen ausgeführt werden.

Verzögern der Startsequenz in vSphere-Client

Die Zeit zwischen dem Einschalten der virtuellen Maschine und dem Zeitpunkt, zu dem das BIOS oder EFI verlassen wird und die Software des Gastbetriebssystems gestartet wird, kann kurz sein. Sie können die Startverzögerung ändern oder die virtuelle Maschine dazu zwingen, nach dem Einschalten in den BIOS- oder EFI-Setup-Bildschirm zu wechseln.

Eine Verzögerung des Startvorgangs ist bei Änderungen an den BIOS- oder EFI-Einstellungen, z. B. der Startreihenfolge, hilfreich. Sie können z. B. die BIOS- oder EFI-Einstellungen ändern, um das Starten einer virtuellen Maschine von einer CD-ROM aus zu erzwingen.

Voraussetzungen

Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Einstellungen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Optionen** und wählen Sie unter „Erweitert“ **Startoptionen**.
- 3 Wählen Sie im Bereich **Startverzögerung beim Einschalten** die Zeit in Millisekunden aus, um die der Startvorgang verzögert werden soll.
- 4 (Optional) Wählen Sie, ob beim nächsten Starten der virtuellen Maschine die Eingabe auf dem BIOS- oder EFI-Setup-Bildschirm erzwungen werden soll.
- 5 (Optional) Wählen Sie, ob nach einem fehlgeschlagenen Start ein Neustartversuch unternommen werden soll.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Aktivieren der Protokollierung im vSphere Client

Sie können die Protokollierung aktivieren, damit Protokolldateien erzeugt werden, anhand derer die Fehlerbehebung für Ihre virtuelle Maschine einfacher gehandhabt werden kann.

Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Einstellungen**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und unter „Erweitert“ auf **Allgemein**.
- 3 Wählen Sie im Fenster **Einstellungen** die Option **Protokollierung aktivieren**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Deaktivieren der Beschleunigung im vSphere Client

Sie können die Beschleunigung vorübergehend deaktivieren, damit in einer virtuellen Maschine Software erfolgreich ausgeführt oder installiert werden kann.

In seltenen Fällen kann es vorkommen, dass die virtuelle Maschine nicht mehr zu reagieren scheint, wenn in der virtuellen Maschine Software installiert oder ausgeführt wird. Im Allgemeinen tritt dieses Problem zu Beginn der Programmausführung auf. Häufig können Sie dieses Problem umgehen, indem Sie die Beschleunigung in der virtuellen Maschine vorübergehend deaktivieren.

Durch das Deaktivieren der Beschleunigung wird die Leistung der virtuellen Maschine verlangsamt. Wenn bei dem Programm keine Probleme mehr auftreten, müssen Sie die Beschleunigung wieder deaktivieren, um das Programm mit Beschleunigung auszuführen.

Sie können die Beschleunigung aktivieren und deaktivieren, während die virtuelle Maschine aktiv ist.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und unter „Erweitert“ auf **Allgemein**.
- 3 Wählen Sie im Bereich **Einstellungen** die Option **Beschleunigung deaktivieren**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren des Debuggings und der Statistiken im vSphere Client

Sie können eine virtuelle Maschine so ausführen, dass sie Debugging-Informationen und Statistiken erfasst, die dem technischen Support von VMware für das Beheben von Problemen hilfreich sind.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen** und unter „Erweitert“ auf **Allgemein**.
- 3 Zur Aktivierung des Debugging-Modus wählen Sie eine Option im Abschnitt **Debugging und Statistik**.
 - **Normal ausführen**
 - **Informationen zum Debuggen erfassen**
 - **Statistiken erfassen**
 - **Statistiken und Debuggen erfassen**
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Verwalten von virtuelle Maschinen

Wenn Sie mit dem vSphere Client eine direkte Verbindung zu einem ESXi-Host oder vCenter Server-System aufbauen, können Sie eine Konsole für alle virtuelle Maschinen des Hosts öffnen, virtuelle Maschinen in der Bestandsliste des Hosts hinzufügen oder daraus entfernen und Snapshots einer virtuellen Maschine verwalten.

Dieses Kapitel behandelt die folgenden Themen:

- „[Bearbeiten der Einstellungen zum Starten/Herunterfahren der virtuellen Maschine](#)“, auf Seite 207
- „[Öffnen einer Konsole für eine virtuelle Maschine](#)“, auf Seite 208
- „[Hinzufügen und Entfernen von virtuellen Maschinen](#)“, auf Seite 209
- „[Verwenden von Snapshots zum Verwalten virtueller Maschinen](#)“, auf Seite 210

Bearbeiten der Einstellungen zum Starten/Herunterfahren der virtuellen Maschine

Sie können virtuelle Maschinen, die auf einem ESXi-Host ausgeführt werden, so konfigurieren, dass sie zusammen mit dem Host starten und herunterfahren. Darüber hinaus können Sie die Standardzeitplanung und die Startreihenfolge für bestimmte virtuelle Maschinen festlegen. Aufgrund dieser Einstellungen kann das Betriebssystem Daten speichern, wenn der Host in den Wartungsmodus wechselt oder aus einem anderen Grund ausgeschaltet wird.

Die Funktion „Starten und Herunterfahren von virtuellen Maschinen“ (automatischer Start) ist für alle virtuellen Maschinen deaktiviert, die sich auf den in einem vSphere HA-Cluster verfügbaren Hosts befinden (oder dorthin verschoben werden). Der automatische Start wird bei Verwendung mit vSphere HA nicht unterstützt.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Client den Host aus, auf dem sich die virtuelle Maschine befindet, und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie unter „Software“ auf **VM starten/herunterfahren** und klicken Sie auf **Eigenschaften**.
Das Dialogfeld „Starten und Herunterfahren von virtuelle Maschinen“ wird geöffnet.
- 3 Aktivieren Sie die Option **Automatisches Starten und Herunterfahren von virtuelle Maschinen zulassen**.

- 4 (Optional) Konfigurieren Sie das Verhalten beim Starten und Herunterfahren.

Option	Aktion
Standardverzögerung beim Starten	Wählen Sie die Zeitdauer, um die das Starten des Betriebssystems verzögert werden soll. Diese Verzögerung gibt den VMware Tools oder dem startenden System die Möglichkeit, Skripts auszuführen.
Beim Start von VMware Tools sofort fortfahren	Wählen Sie diese Option, wenn das Betriebssystem sofort nach dem Start von VMware Tools starten soll.
Standardverzögerung beim Herunterfahren	Wählen Sie die Zeitdauer, um die das Herunterfahren jeder virtuellen Maschine verzögert werden soll. Ein verzögertes Herunterfahren ist nur dann möglich, wenn die virtuelle Maschine nicht bereits vor Ablauf des Verzögerungszeitraums heruntergefahren wurde. Wenn die virtuelle Maschine vor Ablauf des Verzögerungszeitraums heruntergefahren wird, wird für die nächste virtuelle Maschine das Herunterfahren gestartet.
Aktion beim Herunterfahren	Wählen Sie aus dem Dropdown-Menü eine Option für das Herunterfahren aus. <ul style="list-style-type: none"> ■ Ausschalten ■ Anhalten ■ Herunterfahren des Gastes
Nach oben/Nach unten	Wählen Sie in der Kategorie „Manueller Start“ eine virtuelle Maschine aus und verschieben Sie diese mithilfe der Schaltfläche Nach oben in die Kategorie „Automatischer Start“ oder „Beliebige Reihenfolge“. Wenn sich virtuelle Maschinen in der Kategorie „Automatischer Start“ befinden, können Sie diese mithilfe der Schaltflächen Nach oben und Nach unten so anordnen, dass sie in der gewünschten Reihenfolge starten. Beim Herunterfahren werden die virtuelle Maschinen in umgekehrter Reihenfolge heruntergefahren.
Bearbeiten	Klicken Sie auf Bearbeiten , um für virtuelle Maschinen ein benutzerdefiniertes Verhalten zum automatischen Starten und Herunterfahren in den Kategorien „Automatischer Start“ und „Beliebige Reihenfolge“ zu konfigurieren.

- 5 Klicken Sie auf **OK**, um das Dialogfeld zu schließen und Ihre Einstellungen zu speichern.

Öffnen einer Konsole für eine virtuelle Maschine

Mit dem vSphere-Client können Sie auf den Desktop einer virtuellen Maschine zugreifen, indem Sie eine Konsole für die virtuelle Maschine starten. Über die Konsole können Sie Aufgaben in der virtuellen Maschine ausführen, z. B. Betriebssystemeinstellungen konfigurieren, Anwendungen ausführen, die Leistung überwachen usw.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere Clients die betreffende virtuelle Maschine aus, und klicken Sie auf die Registerkarte **Übersicht (Summary)**.
- 2 Wählen Sie im Abschnitt **Befehle** die Option **Konsole öffnen**.
- 3 Klicken Sie im Konsolenfenster auf eine beliebige Stelle, um die Maus, Tastatur und andere Eingabegeräte für die Konsole zu aktivieren.

Hinzufügen und Entfernen von virtuellen Maschinen

Sie können virtuelle Maschinen über die verwalteten Hosts zur Bestandsliste von vCenter Server hinzufügen. Sie können virtuelle Maschinen aus vCenter Server, aus dem Speicher ihres verwalteten Hosts oder aus beiden entfernen.

Entfernen virtueller Maschinen von einem Host

Durch das Entfernen einer virtuellen Maschine aus der Bestandsliste wird die Registrierung dieser virtuellen Maschine beim Host aufgehoben, die virtuelle Maschine wird jedoch nicht aus dem Datenspeicher entfernt. Die Dateien der virtuellen Maschinen verbleiben am selben Speicherort und die virtuelle Maschine kann mithilfe des Datenspeicherbrowsers erneut registriert werden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine und wählen Sie **Aus Bestandsliste entfernen**.
- 2 Klicken Sie auf **Ja**, um zu bestätigen, dass die virtuelle Maschine aus der Bestandsliste entfernt werden soll.

Der Host entfernt die Referenzen auf die virtuelle Maschine und stellt die Verfolgung ihres Zustands ein.

Entfernen von virtuellen Maschinen vom Datenspeicher

Verwenden Sie die Option **Von Festplatte löschen**, um eine virtuelle Maschine von einem Host zu entfernen und alle Dateien der virtuellen Maschine, einschließlich der Konfigurationsdatei und der virtuellen Festplattendateien, aus dem Datenspeicher zu löschen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine und wählen Sie **Von Festplatte löschen**.
- 2 Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Der Host löscht die virtuelle Maschine aus dem zugehörigen Datenspeicher. Gemeinsam mit anderen virtuellen Maschinen genutzte Festplatten werden nicht gelöscht.

Zurücksetzen einer virtuellen Maschine oder Vorlage auf einen Host

Wenn Sie eine virtuelle Maschine oder eine Vorlage von einem Host, aber nicht aus dem Datenspeicher des Hosts entfernen, können Sie sie mithilfe des Datenspeicherbrowsers erneut in der Bestandsliste des Hosts wiederherstellen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client **Home > Bestandsliste > Datenspeicher und Datenspeicher-Cluster**.
- 2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Datenspeicher durchsuchen**.

- 3 Gehen Sie zu der virtuellen Maschine oder dem Vorlagenordner, die bzw. den Sie zur Bestandsliste hinzufügen möchten.
- 4 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine oder die .vmx-Datei der Vorlage und wählen Sie **Zur Bestandsliste hinzufügen**.
- 5 Führen Sie den Assistenten Zur Bestandsliste hinzufügen aus, um die virtuelle Maschine oder Vorlage zur Bestandsliste hinzuzufügen.

Verwenden von Snapshots zum Verwalten virtueller Maschinen

Beim Erstellen eines Snapshots werden der gesamte Status und alle Daten der virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung erfasst. Snapshots sind hilfreich, wenn Sie wiederholt zu einem bestimmten Status der virtuellen Maschine zurückkehren müssen, aber nicht mehrere virtuelle Maschinen erstellen möchten.

Sie können mehrere Snapshots einer virtuellen Maschine erstellen, um Wiederherstellungspositionen in einem linearen Prozess zu erstellen. Mit mehrfachen Snapshots können Sie eine Vielzahl an Positionen speichern, um viele verschiedene Arbeitsprozesse zu sichern. Snapshots werden immer für eine einzelne virtuelle Maschine erstellt. Um Snapshots von mehreren virtuellen Maschinen zu erstellen, wie beispielsweise beim Erstellen von Snapshots für alle Mitglieder eines Teams, ist es erforderlich, von jeder virtuellen Maschine eines Teammitglieds einen eigenen Snapshot zu erstellen.

Snapshots sind als kurzfristige Lösung zum Testen der Software mit unbekannten oder potenziell gefährlichen Auswirkungen hilfreich. Sie können einen Snapshot während eines linearen oder iterativen Prozesses als Wiederherstellungspunkt nutzen, beispielsweise beim Installieren von Update-Paketen oder während eines Verzweigungsprozesses, z. B. beim Installieren verschiedener Versionen eines Programms. Durch das Verwenden von Snapshots wird gewährleistet, dass jede Installation von einer identischen Baseline aus begonnen wird.

Sie können mit Snapshots auch eine Baseline aufbewahren, bevor Sie für eine virtuelle Maschine eine Snapshot-Struktur anlegen.

Der Snapshot-Manager in vSphere Web Client und der vSphere-Client bieten mehrere Funktionen zum Erstellen und Verwalten von Snapshots einer virtuellen Maschine und von Snapshot-Strukturen. Mit diesen Vorgängen können Sie Snapshots erstellen, alle Snapshots in der Snapshot-Hierarchie wiederherstellen, Snapshots löschen usw. Darüber hinaus können Sie den Zustand der virtuellen Maschine jederzeit in umfangreichen Snapshot-Strukturen speichern und später bei Bedarf die virtuelle Maschine wiederherstellen. Jede untergeordnete Struktur in einer Snapshot-Struktur kann bis zu 32 Snapshots enthalten.

Ein Snapshot enthält folgende Informationen:

- Einstellungen der VM. Das Verzeichnis der virtuellen Maschine, das die Festplatten enthält, die nach dem Erstellen des Snapshots hinzugefügt oder geändert wurden.
- Betriebszustand. Die virtuelle Maschine kann eingeschaltet, ausgeschaltet oder angehalten werden.
- Festplattenstatus. Status aller virtuellen Festplatten der virtuellen Maschine.
- (Optional) Arbeitsspeicherstatus. Der Inhalt des Arbeitsspeichers der virtuellen Maschine.

Die Snapshot-Hierarchie

Der Snapshot-Manager zeigt die Snapshot-Hierarchie als Struktur mit einer oder mehreren untergeordneten Strukturen an. Die Beziehung zwischen Snapshots entspricht der zwischen über- und untergeordneten Elementen. In einem linearen Prozess hat jeder Snapshot einen übergeordneten Snapshot und einen untergeordneten Snapshot, mit Ausnahme des letzten Snapshots, der logischerweise keine untergeordneten Snapshots hat. Jede übergeordnete Struktur kann mehrere untergeordnete Strukturen umfassen. Sie können den

aktuellen übergeordneten Snapshot zurücksetzen oder einen beliebigen über- oder untergeordneten Snapshot in der Snapshot-Struktur wiederherstellen und weitere Snapshots aus diesem Snapshot erstellen. Jedes Mal, wenn Sie einen Snapshot wiederherstellen und einen neuen Snapshot erstellen, wird eine untergeordnete Struktur oder ein untergeordneter Snapshot erstellt.

Übergeordnete Snapshots

Der erste Snapshot der virtuellen Maschine, den Sie erstellen, ist der übergeordnete Basis-Snapshot. Der übergeordnete Snapshot ist die zuletzt gespeicherte Version des aktuellen Status der virtuellen Maschine. Beim Erstellen eines Snapshots wird eine Delta-Festplattendatei für jede mit der virtuellen Maschine verbundene Festplatte und optional eine Speicherdatei erstellt. Die Delta-Festplattendateien und die Speicherdatei werden mit der vmdk-Basisdatei gespeichert. Der übergeordnete Snapshot ist immer der Snapshot, der im Snapshot-Manager direkt über dem Symbol „Sie befinden sich hier“ angezeigt wird. Wenn Sie einen Snapshot wiederherstellen oder zu diesem wechseln, wird der betreffende Snapshot zum übergeordneten Element des aktuellen Status (Sie befinden sich hier).

HINWEIS Der übergeordnete Snapshot ist nicht immer der Snapshot, den Sie zuletzt erstellt haben.

Untergeordnete Snapshots

Ein Snapshot derselben virtuellen Maschine, der nach dem übergeordneten Snapshot erstellt wird. Jeder untergeordnete Snapshot beinhaltet Delta-Dateien für jede verbundene virtuelle Festplatte und optional eine Speicherdatei, die den aktuellen Status der virtuellen Festplatte (Sie befinden sich hier) angibt. Die Deltadateien der untergeordneten Snapshots werden so lange mit den jeweils vorherigen Snapshots zusammengeführt, bis die übergeordneten Zielfestplatten erreicht sind. Eine untergeordnete Festplatte kann zu einem späteren Zeitpunkt zu einer übergeordneten Festplatte für zukünftige untergeordnete Festplatten werden.

Das Verhältnis zwischen über- und untergeordneten Snapshots kann sich ändern, wenn die Snapshot-Struktur mehrere untergeordnete Strukturen aufweist. Ein übergeordneter Snapshot kann mehrere untergeordnete Snapshots enthalten. Viele Snapshots verfügen über keine untergeordneten Elemente.

WICHTIG Nehmen Sie keine manuellen Änderungen an einzelnen untergeordneten Festplatten oder an Snapshot-Konfigurationsdateien vor. Dies kann die Snapshot-Struktur gefährden und zu Datenverlust führen. Diese Beschränkung beinhaltet die Größenänderung von Festplatten und Änderungen an der übergeordneten Basisfestplatte unter Verwendung von `vmkfstools`.

Snapshot-Verhalten

Beim Erstellen eines Snapshots wird der zu einem bestimmten Zeitpunkt vorliegende Festplattenstatus festgehalten, indem eine Serie von Delta-Festplatten für jede verbundene virtuelle Festplatte oder virtuelle RDM erstellt wird. Optional werden auch der Speicher und der Energiestatus anhand einer Speicherdatei festgehalten. Beim Erstellen eines Snapshots wird ein Snapshot-Objekt im Snapshot-Manager mit dem Status und den Einstellungen der virtuellen Maschine erstellt.

Jeder Snapshot erstellt eine zusätzliche `.vmdk`-Delta-Festplattendatei. Wenn Sie einen Snapshot erstellen, hindert der Snapshot-Mechanismus das Gastbetriebssystem daran, in die `.vmdk`-Basisdatei zu schreiben, und leitet alle Schreibvorgänge an die Delta-Festplattendatei weiter. Auf der Delta-Festplatte wird der Unterschied zwischen dem aktuellen Status der virtuellen Festplatte und ihrem Status zum Zeitpunkt der Aufnahme des vorherigen Snapshots festgehalten. Wenn mehrere Snapshots vorhanden sind, können Delta-Festplatten die Unterschiede zwischen den einzelnen Snapshots wiedergeben. Die Größe von Delta-Festplattendateien kann schnell zunehmen und die der gesamten virtuellen Festplatte annehmen, wenn das Gastbetriebssystem in jeden Block der virtuellen Festplatte schreibt.

Erstellen von Snapshots einer virtuellen Maschine

Sie können einen oder mehrere Snapshots einer virtuellen Maschine erstellen, um den Einstellungsstatus, Festplattenstatus und Speicherstatus zu verschiedenen angegebenen Zeiten zu erfassen. Wenn Sie einen Snapshot erstellen, können Sie die Dateien der virtuellen Maschine stilllegen und die Festplatten der virtuellen Maschine von Snapshots ausschließen.

Beim Erstellen von Snapshots können andere Aktivitäten, die gerade auf der virtuellen Maschine ausgeführt werden, den Snapshot-Vorgang beeinträchtigen, wenn Sie zu diesem Snapshot zurückkehren. Der optimale Zeitpunkt zum Erstellen eines Snapshots aus der Speicherperspektive ist derjenige, wenn keine große E/A-Last vorhanden ist. Der beste Zeitpunkt zum Erstellen von Snapshots ist dann, wenn gerade kein Datenaustausch zwischen einer Anwendung der virtuellen Maschine und anderen Computern stattfindet. Wenn sich virtuelle Maschinen im Datenaustausch mit anderen Computern befinden – und vor allem in Produktionsumgebungen – besteht die höchste Wahrscheinlichkeit, dass Probleme auftreten. Wenn Sie beispielsweise einen Snapshot aufzeichnen, während die virtuelle Maschine von einem Server im Netzwerk eine Datei herunterlädt, dann setzt die virtuelle Maschine das Herunterladen der Datei fort und meldet den entsprechenden Download-Fortschritt an den Server. Wenn Sie dann den Snapshot wiederherstellen, wird der Datenaustausch zwischen der virtuellen Maschine und dem Server gestört, und die Übertragung der Datei schlägt fehl. In Abhängigkeit von der ausgeführten Aufgabe können Sie einen Arbeitsspeicher-Snapshot erstellen oder aber das Dateisystem der virtuellen Maschine stilllegen.

Arbeitsspeicher-Snapshots

Dies ist die Standardeinstellung für das Erstellen von Snapshots. Wenn Sie den Speicherstatus einer virtuellen Maschine erfassen, behält der Snapshot den Live-Status der virtuellen Maschine bei. Mit Arbeitsspeicher-Snapshots wird ein Snapshot zu einem genau bestimmten Zeitpunkt erstellt, um beispielsweise ein Upgrade einer Software durchzuführen, die noch ausgeführt wird. Wenn Sie einen Arbeitsspeicher-Snapshot erstellen und das Upgrade nicht wie erwartet abgeschlossen wird oder die Software nicht Ihren Erwartungen entspricht, können Sie die virtuelle Maschine in ihrem vorherigen Zustand wiederherstellen.

Wenn Sie den Speicherstatus erfassen, müssen die Dateien der virtuellen Maschine nicht stillgelegt werden. Falls Sie den Speicherstatus nicht erfassen, wird der Live-Status der virtuellen Maschine vom Snapshot nicht gespeichert und die Festplatten sind absturzkonsistent, wenn sie nicht stillgelegt werden.

Stillgelegte Snapshots

Beim Stilllegen einer virtuellen Maschine legt VMware Tools das Dateisystem der virtuellen Maschine still. Ein Stilllegungsvorgang stellt sicher, dass eine Snapshot-Festplatte einen konsistenten Status der Gastdateisysteme darstellt. Stillgelegte Snapshots sind für automatisierte oder regelmäßige Sicherungen geeignet. Wenn Sie beispielsweise keine Informationen zu den Vorgängen der virtuellen Maschine haben, aber über mehrere kürzlich erstellte Sicherungen verfügen möchten, die Sie wiederherstellen können, können Sie die Dateiaktivitäten stilllegen.

Wenn die virtuelle Maschine ausgeschaltet ist oder keine VMware Tools verfügbar sind, ist der Parameter `Stilllegen` nicht verfügbar. Virtuelle Maschinen, die über Festplatten mit hoher Kapazität verfügen, können nicht stillgelegt werden.

WICHTIG Verwenden Sie Snapshots nicht als einzige oder langfristige Sicherungslösung.

Ändern des Festplattenmodus, um virtuelle Festplatten von Snapshots in vSphere Client auszuschließen

Sie können eine virtuelle Festplatte in den unabhängigen Modus versetzen, um die Festplatte von Snapshots auszuschließen, die von der virtuellen Maschine erstellt werden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus und löschen Sie alle vorhandenen Snapshots, bevor Sie den Festplattenmodus ändern. Beim Löschen eines Snapshots werden die vorhandenen Daten auf der Snapshot-Festplatte auf die übergeordnete Festplatte übernommen.

Erforderliche Berechtigungen:

- Virtuelle Maschine.Snapshot-Verwaltung.Snapshot entfernen
- Virtuelle Maschine.Konfiguration.Geräteinstellungen ändern

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie die auszuschließende Festplatte aus.
- 3 Wählen Sie unter **Modus** die Option **Unabhängig** aus.

Der Zustand einer unabhängigen Festplatte wird durch Snapshots nicht beeinträchtigt.

HINWEIS Unabhängig von ihrem Typ wird keine der nach einem Snapshot erstellten Festplatten angezeigt, falls Sie diesen Snapshot wiederherstellen.

- 4 Wählen Sie eine Option für den unabhängigen Festplattenmodus.

Option	Beschreibung
Unabhängig – Dauerhaft	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.
Unabhängig – Nicht dauerhaft	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.

- 5 Klicken Sie auf **OK**.

Erstellen eines Snapshots im vSphere Client

Ein Snapshot erfasst den gesamten Status einer virtuellen Maschine zum Zeitpunkt der Erstellung eines Snapshots. Snapshots können im eingeschalteten, ausgeschalteten oder angehaltenen Zustand der virtuellen Maschine erstellt werden. Wenn Sie eine virtuelle Maschine anhalten, warten Sie, bis dieser Vorgang abgeschlossen ist, bevor Sie einen Snapshot erstellen.

Wenn Sie einen Speicher-Snapshot erstellen, erfasst der Snapshot den Speicherstatus und die Energieeinstellungen der virtuellen Maschine. Wenn Sie den Speicherstatus der virtuellen Maschine erfassen, dauert der Snapshot-Vorgang länger. Die Antwort über das Netzwerk kann ebenfalls kurzzeitig verzögert sein.

Wenn Sie eine virtuelle Maschine stilllegen, legt VMware Tools das Dateisystem in der virtuellen Maschine still. Die Stilllegung hält den Status der laufenden Prozesse in der virtuellen Maschine an oder ändert ihn. Hiervon betroffen sind hauptsächlich Prozesse, die Informationen ändern können, die während einer Wiederherstellung auf der Festplatte gespeichert wurden.

HINWEIS Da die Wiederherstellung von Snapshots auf dynamischen Festplatten nicht unterstützt wird, werden für die Wiederherstellung von dynamischen Festplatten keine Snapshots von stillgelegten Prozessen verwendet. Die Snapshot-Technologie kann auf dynamische Festplatten nicht angewendet werden. Dynamische Festplatten sind als Microsoft-spezifische Dateisysteme bekannt.

Voraussetzungen

- Wenn Sie einen Speicher-Snapshot einer virtuellen Maschine erstellen, die über mehrere Festplatten in verschiedenen Festplattenmodi verfügt, stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist. Wenn beispielsweise eine Konfiguration für einen bestimmten Zweck vorhanden ist, welche die Verwendung einer unabhängigen Festplatte erforderlich macht, müssen Sie die virtuelle Maschine vor dem Erstellen eines Snapshots ausschalten.
- Stellen Sie zum Erfassen des Speicherstatus der virtuellen Maschine sicher, dass die virtuelle Maschine eingeschaltet ist.
- Um die Dateien der virtuellen Maschine stillzulegen, stellen Sie sicher, dass die virtuelle Maschine eingeschaltet und VMware Tools installiert ist.
- Erforderliche Berechtigung: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen** auf der virtuellen Maschine.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine und wählen Sie **Snapshot > Snapshot erstellen**.
- 2 Geben Sie einen Namen für den Snapshot ein.
- 3 Geben Sie eine Beschreibung für den Snapshot ein.
Das Hinzufügen eines Datums und einer Uhrzeit oder einer Beschreibung (Beispiel: Snapshot vor dem Anwenden von Patch XYZ) kann hilfreich sein, um festzulegen, welcher Snapshot wiederhergestellt oder gelöscht werden soll.
- 4 (Optional) Aktivieren Sie bei eingeschalteter virtueller Maschine das Kontrollkästchen **Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen**, um den Arbeitsspeicher der virtuellen Maschine mit einzubeziehen.
- 5 (Optional) Aktivieren Sie bei eingeschalteter virtueller Maschine das Kontrollkästchen **Gast-Dateisystem stilllegen (VMware Tools müssen installiert sein)**, um laufende Prozesse auf dem Gastbetriebssystem anzuhalten, sodass Dateisysteminhalte einen bekannten, konsistenten Status besitzen, wenn Sie den Snapshot erstellen.
- 6 Klicken Sie auf **OK**.

Wenn Sie den Snapshot erstellen, wird der Status im Feld **Kürzlich bearbeitete Aufgabe** im unteren Bereich des vSphere-Client-Fensters aufgeführt.

Wiederherstellen von Snapshots

Um eine virtuelle Maschine in ihren Ursprungsstatus zurückzusetzen oder zu einem anderen Snapshot in der Snapshot-Hierarchie zu wechseln, können Sie einen Snapshot wiederherstellen.

Wenn Sie einen Snapshot wiederherstellen, setzen Sie den Speicher, die Einstellungen und den Status der virtuellen Laufwerke der virtuellen Maschine auf den Zustand zurück, den sie zum Zeitpunkt des Erstellens des Snapshots hatten. Wenn die virtuelle Maschine beim Start angehalten, eingeschaltet oder ausgeschaltet werden soll, stellen Sie sicher, dass sie sich beim Erstellen des Snapshots im gewünschten Zustand befindet.

Snapshots lassen sich auf folgende Arten wiederherstellen:

Zu letztem Snapshot zurücksetzen	Stellt den übergeordneten Snapshot in der Hierarchie eine Ebene über der Position Sie befinden sich hier wieder her. Zu letztem Snapshot zurücksetzen aktiviert den übergeordneten Snapshot des aktuellen Zustands der virtuellen Maschine.
Zurückkehren zu	Hiermit können Sie einen beliebigen Snapshot in der Snapshot-Struktur wiederherstellen und den Snapshot als übergeordneten Snapshot des aktuellen Status der virtuellen Maschine festlegen. Weitere Snapshots erstellen einen neuen Zweig der Snapshot-Struktur.

Das Wiederherstellen von Snapshots wirkt sich folgendermaßen aus:

- Die aktuellen Status von Festplatte und Arbeitsspeicher werden verworfen und die virtuelle Maschine wird auf die Festplatten- und Arbeitsspeicherstatus des übergeordneten Snapshots zurückgesetzt.
- Vorhandene Snapshots werden nicht entfernt. Sie können diese Snapshots jederzeit wiederherstellen.
- Wenn der Snapshot den Arbeitsspeicherstatus beinhaltet, befindet sich die virtuelle Maschine im gleichen Betriebszustand, in der sie sich zum Zeitpunkt der Snapshot-Erstellung befunden hat.

Tabelle 16-1. Betriebsstatus der virtuellen Maschine nach der Wiederherstellung eines Snapshots

Status der virtuellen Maschine nach dem Erstellen eines übergeordneten Snapshots	Zustand virtueller Maschinen nach dem Wiederherstellen
Eingeschaltet (mit Speicher)	Der übergeordnete Snapshot wird wiederhergestellt und die virtuelle Maschine ist eingeschaltet und wird ausgeführt.
Eingeschaltet (ohne Speicher)	Der übergeordnete Snapshot wird wiederhergestellt und die virtuelle Maschine wird ausgeschaltet.
Ausgeschaltet (Speicher ausgenommen)	Der übergeordnete Snapshot wird wiederhergestellt und die virtuelle Maschine wird ausgeschaltet.

Virtuelle Maschinen, auf denen bestimmte Arbeitslasten ausgeführt werden, benötigen unter Umständen mehrere Minuten, bevor sie wieder antworten, nachdem ein Snapshot wiederhergestellt wurde.

HINWEIS Die vApp-Metadaten für virtuelle Maschinen innerhalb von vApps verwenden nicht die Snapshot-Semantiken für die Konfiguration virtueller Maschinen. vApp-Eigenschaften, die nach dem Erstellen eines Snapshots gelöscht, geändert oder definiert werden, bleiben intakt (d. h., sie bleiben gelöscht, geändert oder definiert), wenn die virtuelle Maschine auf diesen oder einen vorherigen Snapshot zurückgesetzt wird.

Wiederherstellen eines übergeordneten Snapshots in vSphere-Client

Sie können den übergeordneten Snapshot des aktuellen Status der virtuellen Maschine wiederherstellen.

Bei der Wiederherstellung eines Snapshots werden Festplatten, die Sie nach dem Erstellen des Snapshots hinzugefügt oder geändert haben, auf den Snapshot-Punkt zurückgesetzt. Wenn Sie beispielsweise einen Snapshot einer virtuellen Maschine erstellen, eine Festplatte hinzufügen und den Snapshot zurücksetzen, wird die hinzugefügte Festplatte entfernt.

Voraussetzungen

Erforderliche Berechtigung: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot wiederherstellen** auf der virtuellen Maschine.

Vorgehensweise

- ◆ Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der vSphere-Client-Bestandsliste und wählen Sie die Option **Aktuellen Snapshot wiederherstellen** aus.

Der Betriebs- und Datenstatus der virtuellen Maschine wird auf den Status zurückgesetzt, der zum Zeitpunkt der Erstellung des übergeordneten Snapshot vorlag. Wenn es sich bei dem übergeordneten Snapshot um einen Speicher-Snapshot handelt, wird die virtuelle Maschine auf den Status „Eingeschaltet“ zurückgesetzt.

Wechseln zu einem Snapshot im vSphere-Client

In der Snapshot-Struktur können Sie zu einem Snapshot navigieren, um die virtuelle Maschine auf den Status dieses Snapshots zurückzusetzen.

HINWEIS Virtuelle Maschinen, auf denen bestimmte Workloads ausgeführt werden, benötigen unter Umständen mehrere Minuten, bevor sie wieder antworten, nachdem ein Snapshot wiederhergestellt wurde.

Voraussetzungen

Erforderliche Berechtigung: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot wiederherstellen** auf der virtuellen Maschine

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine in der vSphere-Client-Bestandsliste und wählen Sie **Snapshot-Manager** aus.
- 2 Klicken Sie im Snapshot-Manager auf einen Snapshot, um diesen auszuwählen.
- 3 Klicken Sie auf **Wechseln zu**, um den Status der virtuellen Maschine wiederherzustellen, der dem Snapshot entspricht.
- 4 Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Nachfolgende untergeordnete Snapshots erstellen von diesem Punkt aus einen neuen Zweig in der Snapshot-Struktur. Die Delta-Festplatten für Snapshots, die Sie nach der Wiederherstellung des aktuellen Snapshots erstellt haben, werden nicht entfernt und Sie können diese Snapshots jederzeit wiederherstellen.

Löschen von Snapshots

Durch Löschen eines Snapshots wird dieser aus dem Snapshot-Manager entfernt. Die Snapshot-Dateien werden konsolidiert, auf die übergeordnete Snapshot-Festplatte geschrieben und mit der Basisfestplatte der virtuellen Maschine zusammengeführt.

Das Löschen eines Snapshots ändert nichts am aktuellen Zustand der virtuellen Maschine und allen anderen Snapshots. Beim Löschen eines Snapshots werden die Änderungen zwischen Snapshots und früheren Festplattenzuständen konsolidiert und alle Daten aus der Delta-Festplatte, die Informationen über den gelöschten Snapshot enthält, werden auf die übergeordnete Festplatte geschrieben. Wenn Sie den übergeordneten Basis-Snapshot löschen, werden alle Änderungen mit der Basis-Festplatte der virtuellen Maschine zusammengeführt.

Das Löschen von Snapshots verursacht umfangreiche Festplattenlese- und -schreibvorgänge, die die Leistung der virtuellen Maschine beeinträchtigen können, solange die Konsolidierung noch nicht abgeschlossen ist. Das Konsolidieren von Snapshots entfernt redundante Festplatten. Dadurch wird die Leistung der virtuellen Maschine erhöht und Speicherplatz gespart. Die Zeit, die zum Löschen von Snapshots und zum Konsolidieren der Snapshot-Dateien benötigt wird, hängt von der Datenmenge ab, die das Gastbetriebssystem nach Erstellung des letzten Snapshots auf die virtuellen Festplatten geschrieben hat. Die benötigte Zeit steht im Verhältnis zu der Menge der Daten, die die virtuelle Maschine während der Konsolidierung schreibt, wenn die virtuelle Maschine eingeschaltet wird.

Falls die Festplattenkonsolidierung fehlschlägt, wenn Sie einen Snapshot oder alle Snapshots löschen, und Sie eine Verschlechterung der Leistung der virtuellen Maschine beobachten, können Sie eine Liste der virtuellen Maschinen anzeigen, um zu bestimmen, ob für irgendwelche Dateien eine Konsolidierung erforderlich ist, und, falls ja, eine separate Konsolidierung ausführen. Weitere Informationen zum Feststellen und Anzeigen des Konsolidierungsstatus von mehreren virtuellen Maschinen und zum Ausführen eines separaten Konsolidierungsvorgangs finden Sie unter „[Konsolidieren von Snapshots im vSphere-Client](#)“, auf Seite 218

Löschen

Verwenden Sie die Option **Löschen**, um einen einzelnen übergeordneten oder untergeordneten Snapshot aus der Snapshot-Struktur zu entfernen. Bei Ausführung von **Löschen** werden Festplattenänderungen zwischen dem Snapshot und dem vorherigen Zustand der Delta-Festplatte auf den übergeordneten Snapshot geschrieben.

Sie können auch die Option **Löschen** zum Entfernen eines beschädigten Snapshots und dessen Dateien aus einem verwaisten Zweig der Snapshot-Struktur verwenden, ohne sie mit dem übergeordneten Snapshot zusammenzuführen.

Alle löschen

Verwenden Sie die Option **Alle löschen**, um alle Snapshots aus dem Snapshot-Manager zu löschen. Beim Ausführen von **Alle löschen** werden die Änderungen zwischen Snapshots und den vorherigen Zuständen von Delta-Festplatten konsolidiert, auf der übergeordneten Basisfestplatte geschrieben und mit der Basis-VM-Festplatte zusammengeführt.

Verwenden Sie zuerst den Befehl **Wechseln zu**, um einen vorherigen Snapshot wiederherzustellen, damit verhindert wird, dass Snapshot-Dateien mit dem übergeordneten Snapshot zusammengeführt werden, z. B. bei fehlgeschlagenen Updates oder Installationsvorgängen. Diese Aktion macht die Snapshot-Delta-Festplatten ungültig und löscht die Arbeitsspeicherdatei. Anschließend können Sie die Option **Löschen** verwenden, um den Snapshot und alle zugeordneten Dateien zu entfernen.

Löschen eines Snapshots im vSphere-Client

Sie können den Snapshot-Manager zum Löschen eines einzigen Snapshots oder aller Snapshots in der Snapshot-Struktur verwenden.

Seien Sie vorsichtig, wenn Sie Snapshots löschen. Sie können ein gelöscht Snapshot nicht wiederherstellen. Sie möchten beispielsweise mehrere Browser, a, b und c, installieren und den Status der virtuellen Maschine nach der Installation eines jeden Browsers erfassen. Der erste, der sogenannte Basis-Snapshot, erfasst die virtuelle Maschine mit Browser a und der zweite Snapshot erfasst Browser b. Wenn Sie den Basis-Snapshot, der Browser a enthält, wiederherstellen und einen dritten Snapshot erstellen, um Browser c zu erfassen, und anschließend den Snapshot löschen, der Browser b enthält, können Sie zum Zustand der virtuellen Maschine zurückkehren, der Browser b enthält.

Voraussetzungen

- Stellen Sie sicher, dass Sie mit den Aktionen „Löschen“ und „Alles löschen“ und deren Auswirkung auf die Leistung virtueller Maschinen vertraut sind. Weitere Informationen hierzu finden Sie unter „[Löschen von Snapshots](#)“, auf Seite 217.
- Erforderliche Berechtigung: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot entfernen** auf der virtuellen Maschine.

Vorgehensweise

- 1 Wählen Sie **Bestandsliste > Virtuelle Maschine > Snapshot > Snapshot wiederherstellen**.
- 2 Klicken Sie im Snapshot-Manager auf einen Snapshot, um diesen auszuwählen.
- 3 Wählen Sie eine Löschoption aus.

Option	Beschreibung
Löschen	Konsolidiert die Snapshot-Daten in den übergeordneten Snapshot und entfernt den ausgewählten Snapshot aus dem Snapshot-Manager und der virtuellen Maschine.
Alle löschen	Konsolidiert alle Snapshots unmittelbar vor dem aktuellen Status „Sie befinden sich hier“ auf die übergeordnete Basisfestplatte und entfernt alle vorhandenen Snapshots aus dem Snapshot-Manager und der virtuellen Maschine.

- 4 Klicken Sie auf **Ja**.

Konsolidieren von Snapshots im vSphere-Client

Der Konsolidierungsbefehl für Snapshots sucht nach zu kombinierenden Hierarchien oder Delta-Festplatten, ohne gegen die Datenabhängigkeit zu verstoßen. Redundante Festplatten werden nach der Konsolidierung entfernt. Dadurch wird die Leistung der virtuellen Maschine erhöht und Speicherplatz gespart.

Die Konsolidierung von Snapshots ist nützlich, wenn Snapshot-Festplatten nach einem Vorgang des Typs **Löschen** oder **Alle löschen** nicht komprimiert werden können oder die Festplatte nicht konsolidiert werden konnte. Dies könnte beispielsweise geschehen, wenn Sie einen Snapshot löschen, sich dessen zugewiesene Festplatte aber nicht zurück zur Basisfestplatte festschreiben lässt.

In der Spalte „Konsolidierung erforderlich“ des vSphere-Clients werden die virtuellen Maschinen angezeigt, die konsolidiert werden müssen, und auf der Registerkarte **Übersicht** der virtuellen Maschine wird eine Meldung zu Konfigurationsproblemen angezeigt, falls die virtuelle Maschine konsolidiert werden muss. Falls Fehler auftreten, z. B. der Speicherplatz nicht ausreicht, beheben Sie sie und führen Sie die Konsolidierungsaufgabe durch.

Voraussetzungen

Erforderliche Berechtigung: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot entfernen**

Vorgehensweise

- 1 Zeigen Sie die Spalte „Konsolidierung erforderlich“ im vSphere-Client an.
 - a Wählen Sie vCenter Server, einen Host oder einen Cluster aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
 - b Klicken Sie mit der rechten Maustaste auf die Menüleiste für eine VM-Spalte und wählen Sie aus dem Menü **Konsolidierung erforderlich** aus.

Die Spalte „Konsolidierung erforderlich“ erscheint. Der Status „Ja“ gibt an, dass die Snapshot-Dateien für die virtuellen Maschinen konsolidiert werden sollen und auf der Registerkarte **Aufgaben und Ereignisse** der virtuellen Maschine ein Konfigurationsproblem angezeigt wird. Der Status „Nein“ gibt an, dass die Dateien in Ordnung sind.

- 2 Klicken Sie zum Konsolidieren der Dateien mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Snapshot > Konsolidieren** aus.
- 3 Überprüfen Sie die Spalte „Konsolidierung erforderlich“, um sich zu vergewissern, dass die Aufgabe erfolgreich durchgeführt wurde.

Sofern die Aufgabe ordnungsgemäß durchgeführt wurde, sollte die Meldung unter „Konfigurationsprobleme“ nicht mehr erscheinen und unter „Konsolidierung erforderlich“ der Wert „Nein“ stehen.

Verwalten von Multi-Tier-Anwendungen mit vSphere vApp im vSphere-Client

17

Sie können VMware vSphere als Plattform für die Ausführung von virtuellen Maschinen sowie Anwendungen verwenden. Die Anwendungen können für die Ausführung direkt unter VMware vSphere bereitgestellt werden. Das Format, in dem die Anwendungen bereitgestellt und verwaltet werden, heißt vSphere vApp.

Eine vApp ist ein mit einem Ressourcenpool vergleichbarer Container, der eine oder mehrere virtuelle Maschinen enthalten kann. Darüber hinaus weist eine vApp einige Merkmale auf, über die auch virtuelle Maschinen verfügen. Eine vApp kann ein- und ausgeschaltet sowie geklont werden.

Im vSphere-Client werden vApps sowohl in der Ansicht „Hosts und Cluster“ als auch in der Ansicht „VMs und Vorlagen“ angezeigt. Jede Ansicht hat eine eigene Übersichtsseite mit dem aktuellen Status des Dienstes und relevanten zusammengefassten Informationen sowie den Dienstoperationen.

Das Distributionsformat für vApp ist OVF.

HINWEIS Da die vApp-Metadaten in der vCenter Server-Datenbank gespeichert werden, kann eine vApp auf mehrere ESXi-Hosts verteilt werden. Diese Informationen können verloren gehen, wenn die Daten der vCenter Server-Datenbank gelöscht oder ein eigenständiger ESXi-Host, der eine vApp enthält, von vCenter Server entfernt wird. Sie sollten vApps in einem OVF-Paket sichern, damit keine Metadaten verloren gehen.

vApp-Metadaten für virtuelle Maschinen innerhalb von vApps verwenden nicht die Snapshot-Semantiken für die Konfiguration virtueller Maschinen. Somit bleiben vApp-Eigenschaften, die nach dem Erstellen eines Snapshots gelöscht, geändert oder definiert werden, intakt (d. h., gelöscht, geändert oder definiert), wenn die virtuelle Maschine auf diesen oder einen vorherigen Snapshot zurückgesetzt wird.

Sie können VMware Studio verwenden, um das Erstellen von zur Bereitstellung bereiten vApps durch vorab festgelegte Anwendungssoftware und Betriebssysteme zu automatisieren. VMware Studio fügt einen Netzwerk-Agenten zum Gastbetriebssystem hinzu, sodass vApps das Bootstrapping mit geringem Aufwand durchführen können. Für vApps angegebene Konfigurationsparameter erscheinen als OVF-Eigenschaften im Bereitstellungsassistenten von vCenter Server. Weitere Informationen über VMware Studio und zum Herunterladen der Software finden Sie auf der Entwicklerseite zu VMware Studio auf der VMware-Website.

Dieses Kapitel behandelt die folgenden Themen:

- „Erstellen einer vApp“, auf Seite 222
- „Einschalten einer vApp im vSphere-Client“, auf Seite 223
- „vApp klonen“, auf Seite 224
- „Ausschalten einer vApp im vSphere-Client“, auf Seite 224
- „Anhalten einer vApp im vSphere-Client“, auf Seite 225
- „Fortsetzen einer vApp im vSphere-Client“, auf Seite 225

- „Auffüllen der vApp“, auf Seite 225
- „Bearbeiten der vApp-Einstellungen im vSphere-Client“, auf Seite 226
- „Konfigurieren von IP-Pools“, auf Seite 231
- „Bearbeiten einer vApp-Anmerkung im vSphere-Client“, auf Seite 233

Erstellen einer vApp

Eine vApp ermöglicht Ihnen, Ressourcenverwaltung und andere Verwaltungsaktivitäten, z. B. Betriebsvorgänge, für mehrere virtuelle Maschinen gleichzeitig auszuführen. Stellen Sie sich eine vApp als Container für die virtuellen Maschinen vor. Die Vorgänge können Sie für den Container ausführen.


Wenn Sie eine vApp erstellen, können Sie sie zu einem Ordner, einem eigenständigen Host, einem Ressourcenpool, einem für DRS aktivierten Cluster oder einer anderen vApp hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass eines der folgenden Objekte in Ihrem Datacenter verfügbar ist:

- Ein eigenständiger Host, auf dem ESX 4.0 oder höher ausgeführt wird.
- Ein Cluster, der für DRS aktiviert ist.

Vorgehensweise

- 1 Gehen Sie zu einem Objekt, das die vApp-Erstellung unterstützt, und wählen Sie das Symbol „Neue vApp“ aus ().
- 2 Geben Sie im Textfeld **vApp-Name** einen Namen für die vApp ein.
- 3 Wählen Sie den Speicherort der vApp-Bestandsliste aus und klicken Sie auf **Weiter**.
 - Wenn Sie die Aktion aus einem Ordner oder einer vApp starten, werden Sie nach einem Host, Cluster oder Ressourcenpool gefragt.
 - Wenn Sie die Aktion aus einem Ressourcenpool, Host oder Cluster starten, werden Sie nach einem Ordner oder Datacenter gefragt.

- 4 Weisen Sie dieser vApp auf der Seite „Ressourcenzuteilung“ CPU- und Arbeitsspeicherressourcen zu.
- a Teilen Sie dieser vApp CPU-Ressourcen zu.

Option	Beschreibung
Anteile	CPU-Anteile für diese vApp bezogen auf die Gesamtanteile der übergeordneten vApp. Hierarchisch gleichwertige vApps teilen sich Ressourcen auf der Basis ihrer relativen Anteilswerte, die durch die Reservierung und Grenzwerte begrenzt sind. Wählen Sie Niedrig , Normal oder Hoch . Dadurch werden die Anteilswerte im Verhältnis 1:2:4 festgelegt. Wählen Sie die Option Benutzerdefiniert , um jeder vApp einen bestimmten Anteil zuzuweisen, der einer proportionalen Gewichtung entspricht.
Reservierung	Garantierte CPU-Zuteilung für diese vApp.
Typ der Reservierung	Wählen Sie das Kontrollkästchen Erweiterbar aus, um die Reservierung erweiterbar zu machen. Wenn eine vApp eingeschaltet wird und die gesamten Reservierungen ihrer virtuellen Maschinen größer als die Reservierung der vApp sind, kann die vApp Ressourcen von übergeordneten vApps verwenden.
Grenzwert	Die Obergrenze der CPU-Zuteilung für diese vApp. Wählen Sie Unbegrenzt , wenn Sie keine Obergrenze definieren möchten.

- b Teilen Sie dieser vApp Arbeitsspeicherressourcen zu.

Option	Beschreibung
Anteile	Arbeitsspeicheranteile für diese vApp bezogen auf die Gesamtanteile der übergeordneten vApp. Hierarchisch gleichwertige vApps teilen sich Ressourcen auf der Basis ihrer relativen Anteilswerte, die durch die Reservierung und Grenzwerte begrenzt sind. Wählen Sie Niedrig , Normal oder Hoch . Dadurch werden die Anteilswerte im Verhältnis 1:2:4 festgelegt. Wählen Sie die Option Benutzerdefiniert , um jeder vApp einen bestimmten Anteil zuzuweisen, der einer proportionalen Gewichtung entspricht.
Reservierung	Garantierte Arbeitsspeicherzuteilung für diese vApp.
Typ der Reservierung	Wählen Sie das Kontrollkästchen Erweiterbar aus, um die Reservierung erweiterbar zu machen. Wenn eine vApp eingeschaltet wird und die gesamten Reservierungen ihrer virtuellen Maschinen größer als die Reservierung der vApp sind, kann die vApp Ressourcen von übergeordneten vApps verwenden.
Grenzwert	Die Obergrenze der Arbeitsspeicherzuteilung für diese vApp. Wählen Sie Unbegrenzt , wenn Sie keine Obergrenze definieren möchten.

- 5 Klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die vApp-Einstellungen und klicken Sie auf **Fertigstellen**.

Einschalten einer vApp im vSphere-Client

Jede virtuelle Maschine in der vApp wird der konfigurierten Startreihenfolge entsprechend eingeschaltet.

Beim Einschalten einer vApp in einem DRS-Cluster im manuellen Modus werden keine DRS-Empfehlungen für die Platzierung virtueller Maschine generiert. Der Einschaltvorgang verläuft für die erste Platzierung der virtuellen Maschinen so, als ob DRS im halb- oder vollautomatischen Modus ausgeführt wird. Dies hat keine Auswirkungen auf vMotion-Empfehlungen. Empfehlungen für individuelles Einschalten und Ausschalten von virtuellen Maschinen werden ebenfalls für vApps generiert, die ausgeführt werden.

Vorgehensweise

- ◆ Klicken Sie auf der Übersichtsseite des Dienstes auf **Einschalten**.

Wenn eine Verzögerung in den Starteinstellungen festgelegt ist, hält die vApp die festgelegte Wartezeit ein, bevor sie diese virtuelle Maschine einschaltet.

In der Registerkarte **Übersicht** wird angezeigt, ob die vApp gestartet wurde und verfügbar ist. Links zu Produkt- und Anbieterwebsites finden Sie ebenfalls im Abschnitt „Allgemein“.

vApp klonen

Das Klonen einer vApp ähnelt dem Klonen einer virtuellen Maschine.

Voraussetzungen

Zum Klonen einer vApp muss der vSphere-Client mit dem vCenter Server-System verbunden sein.

In der Bestandsliste muss entweder ein Host mit ESX 4.0 oder höher oder ein mit DRS aktivierter Cluster ausgewählt sein.

Vorgehensweise

- 1 Wählen Sie die vApp in der Bestandsliste aus.
- 2 Wählen Sie **Bestandsliste > vApp > Klonen**.

Führen Sie die Anweisungen auf den Seiten des Assistenten zum Klonen von vApp aus.

- 3 Wählen Sie das vApp-Ziel aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Host an und klicken Sie auf **Weiter**.

HINWEIS Dieser Schritt ist nur verfügbar, wenn Sie einen Cluster auswählen, der sich im manuellen DRS-Modus befindet.

- 5 Geben Sie einen Namen für den vApp-Klon ein, wählen Sie **Speicherort der vApp-Bestandsliste** und klicken Sie auf **Weiter**.
- 6 Wählen Sie einen Datenspeicher, und klicken Sie auf **Weiter**.
- 7 Wählen Sie ein Festplattenformat für die virtuellen Festplatten der virtuellen Maschine aus und klicken Sie auf **Weiter**.
 - **Format wie Quelle**
 - **Format 'Schnell bereitgestellt'**
 - **Thick-Format**
- 8 Überprüfen Sie die vApp-Einstellungen und klicken Sie auf **Beenden**.

Ausschalten einer vApp im vSphere-Client

Jede virtuelle Maschine innerhalb der vApp wird in der umgekehrten Startreihenfolge ausgeschaltet.

Vorgehensweise

- ◆ Klicken Sie in der Übersichtsseite des Dienstes auf **Ausschalten**.

Wenn eine Verzögerung in den Einstellungen für das Herunterfahren festgelegt ist, hält die vApp die festgelegte Wartezeit ein, bevor sie diese virtuelle Maschine ausschaltet.

Anhalten einer vApp im vSphere-Client

Eine angehaltene vApp hält alle ihre laufenden virtuellen Maschinen so lange an, bis Sie die vApp fortsetzen.

Die virtuellen Maschinen innerhalb einer vApp werden gemäß ihrer Stoppreihenfolge angehalten. Alle virtuellen Maschinen werden ohne Berücksichtigung der Stoppaktion angehalten.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die vApp aus, die Sie in den angehaltenen Zustand versetzen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf die vApp und wählen Sie **Anhalten**.

Fortsetzen einer vApp im vSphere-Client

Sie können die Aktivität der virtuellen Maschinen innerhalb einer vApp, die sich im Zustand „Angehalten“ befindet, fortsetzen.

Die angehaltenen virtuellen Maschinen innerhalb der vApp werden in der umgekehrten Reihenfolge fortgesetzt, in der sie angehalten wurden.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die vApp aus.
- 2 Klicken Sie mit der rechten Maustaste auf die vApp und wählen Sie **Einschalten**.

Auffüllen der vApp

Virtuelle Maschinen und andere vApps können einer vApp hinzugefügt oder aus einer vApp entfernt werden.

Nach dem Erstellen einer vApp können Sie sie mit virtuellen Maschinen oder anderen vApps auffüllen.

Erstellen eines Objekts innerhalb der vApp im vSphere-Client

Innerhalb einer vApp können Sie eine neue virtuelle Maschine, einen Ressourcenpool oder eine weitere vApp erstellen.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste die vApp aus, in der Sie das Objekt erstellen möchten.
- 2 Wählen Sie die Menüoption zum Erstellen des gewünschten Objekts aus.

Menüoption	Beschreibung
Bestandsliste > vApp > Neue virtuelle Maschine	Erstellt eine neue virtuelle Maschine in der vApp. Führen Sie die Schritte des Assistenten „Neue virtuelle Maschine erstellen“ aus. Informationen zum Erstellen einer neuen virtuellen Maschine finden Sie in Kapitel 10, „Erstellen einer virtuellen Maschine im vSphere-Client“ , auf Seite 93.
Bestandsliste > vApp > Neuer Ressourcenpool	Fügt einen Ressourcenpool innerhalb der vApp hinzu. Führen Sie die Schritte im Fenster Ressourcenpool erstellen aus.
Bestandsliste > vApp > Neue vApp	Erstellt eine neue vApp innerhalb der ausgewählten vApp. Führen Sie die Schritte des Assistenten „Neue vApp“ aus. Informationen zum Erstellen einer neuen vApp finden Sie in „Erstellen einer vApp“ , auf Seite 222.

Das neue Objekt wird in der Bestandsliste als Teil der vApp angezeigt.

Hinzufügen eines Objekts zu einer vApp im vSphere-Client

Sie können einer vorhandenen vApp ein Objekt hinzufügen, z. B. eine virtuelle Maschine oder eine weitere vApp.

Eine vorhandene virtuelle Maschine oder eine andere vApp, die noch nicht in der vApp enthalten ist, kann in die ausgewählte vApp verschoben werden.

Vorgehensweise

- 1 Zeigen Sie das Objekt in der Bestandsliste an.
- 2 Klicken Sie auf das Objekt und ziehen Sie es auf das Zielobjekt.
 - Wenn der Verschiebevorgang zulässig ist, wird um das Zielobjekt herum ein Kästchen angezeigt, das angibt, dass es ausgewählt ist.
 - Wenn der Verschiebevorgang nicht zulässig ist, wird eine Null mit einem Schrägstrich angezeigt und das Objekt wird nicht verschoben.
- 3 Lassen Sie die Maustaste los.

Entweder wird das Objekt daraufhin auf den neuen Standort verschoben, oder es wird eine Fehlermeldung mit Informationen darüber angezeigt, wie Sie das Verschieben des Objekts ermöglichen können.

Bearbeiten der vApp-Einstellungen im vSphere-Client

Sie können verschiedene vApp-Einstellungen bearbeiten und konfigurieren, z. B. Startreihenfolge, Ressourcen und benutzerdefinierte Eigenschaften.

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen**, um vApp-Eigenschaften zu bearbeiten oder anzuzeigen.

HINWEIS In der Regel bearbeitet die bereitstellende Person die IP-Zuteilungsrichtlinie und -Eigenschaften. Der Autor der vApp bearbeitet gewöhnlich die anderen, erweiterten Einstellungen.

- 3 Klicken Sie auf die Registerkarte **Startreihenfolge**, um die vApp-Optionen für das Starten und das Herunterfahren zu bearbeiten.
- 4 Klicken Sie auf **OK**.

Bearbeiten der vApp-Optionen für das Starten und das Herunterfahren

Sie können die Reihenfolge ändern, in der virtuelle Maschinen und eingebettete vApps in einer vApp gestartet und heruntergefahren werden. Sie können außerdem beim Starten und Herunterfahren durchzuführende Aktionen und Verzögerungen festlegen.

Erforderliche Berechtigung: **vApp.vApp-Anwendungskonfiguration**

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Wählen Sie auf der Registerkarte **Startreihenfolge** des Fensters vApp-Einstellungen bearbeiten eine virtuelle Maschine aus und verwenden Sie die Pfeiltasten, um die Startreihenfolge zu ändern.

Virtuelle Maschinen und vApps mit der gleichen Startreihenfolge (bzw. mit der gleichen Gruppierung) werden gleichzeitig gestartet.

Für das Herunterfahren wird die umgekehrte Reihenfolge verwendet.

- 3 Wählen Sie die Aktion beim Starten und beim Herunterfahren für jede virtuelle Maschine aus.
- 4 (Optional) Verwenden Sie die Pfeiltasten, um die Zeitverzögerung für das Starten und das Herunterfahren für jede virtuelle Maschine zu ändern.
- 5 Klicken Sie auf **OK**.

Bearbeiten von vApp-Ressourcen

Sie können die CPU- und Arbeitsspeicher-Ressourcenzuteilung für die vApp bearbeiten.

Erforderliche Berechtigung: **vApp.vApp-Anwendungskonfiguration**

Reservierungen auf vApps und allen ihren untergeordneten Ressourcenpools, untergeordneten vApps und untergeordneten virtuellen Maschinen werden den übergeordneten Ressourcen nur dann angerechnet, wenn sie eingeschaltet sind.

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste Optionen auf **Ressourcen**.
- 3 Bearbeiten Sie die CPU- und Arbeitsspeicher-Ressourcenzuteilung.
- 4 Klicken Sie auf **OK**.

Bearbeiten von vApp-Eigenschaften

Sie können jede vApp-Eigenschaft bearbeiten, die in der Erweiterten Eigenschaftskonfiguration definiert ist.

Erforderliche Berechtigung: **vApp.vApp-Anwendungskonfiguration**

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste **Optionen** auf **Eigenschaften**.
- 3 Bearbeiten Sie die vApp-Eigenschaften.
- 4 Klicken Sie auf **OK**.

Bearbeiten der IP-Zuteilungsrichtlinie

Sie können für die vApp die Art der Zuteilung von IP-Adressen ändern.

Voraussetzungen

- Damit die automatische (vorübergehende) IP-Zuteilung funktioniert, müssen Sie den vSphere-Client zum Konfigurieren eines IP-Pools verwenden. Weitere Informationen hierzu finden Sie unter „[Konfigurieren von IP-Pools](#)“, auf Seite 231.

Erforderliche Berechtigung: **vApp.vApp-Instanzkonfiguration**.

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste Optionen auf **IP-Zuteilungsrichtlinie**.

- 3 Wählen Sie eine Zuteilungsoption für IP-Adressen.

Option	Beschreibung
Fest	IP-Adressen werden manuell konfiguriert. Es wird keine automatische Zuteilung vorgenommen.
Vorübergehend	IP-Adressen werden beim Einschalten der vApp automatisch mithilfe von IP-Pools aus einem angegebenen Bereich zugeteilt. Die IP-Adressen werden freigegeben, wenn die Appliance ausgeschaltet wird.
DHCP	Zum Zuteilen der IP-Adressen wird ein DHCP-Server verwendet. Die vom DHCP-Server zugewiesenen Adressen sind in den OVF-Umgebungen von virtuellen Maschinen sichtbar, die in der vApp gestartet wurden.

- 4 Klicken Sie auf **OK**.

Hinzufügen einer vService-Abhängigkeit

Sie können einer virtuellen Maschine oder einer vApp eine vService-Abhängigkeit hinzufügen. Diese Abhängigkeit ermöglicht einer virtuellen Maschine oder einer vApp das Anfordern eines bestimmten verfügbaren vService.

Vorgehensweise

- 1 Zeigen Sie die virtuelle Maschine oder vApp in der Bestandsliste an.
- 2 Schalten Sie die virtuelle Maschine oder vApp aus.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **vServices**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Wählen Sie im Assistent zum Hinzufügen von Abhängigkeiten den Anbieter für diese Abhängigkeit aus und klicken Sie auf **Weiter**.
- 7 Geben Sie einen Namen und eine Beschreibung für die Abhängigkeit ein.
- 8 (Optional) Falls diese Abhängigkeit erforderlich ist, wählen Sie das Kontrollkästchen aus und klicken Sie auf **Weiter**.

Erforderliche Abhängigkeiten müssen vor dem Einschalten gebunden werden.

- 9 (Optional) Falls diese Abhängigkeit sofort an den Anbieter gebunden werden soll, wählen Sie die Option **Sofort an Anbieter binden** und klicken Sie nach Abschluss der Validierung auf **Weiter**.

Wenn Sie die Abhängigkeit jetzt binden möchten, wird das Validierungsergebnis angezeigt. Falls die Validierung fehlschlägt, können Sie das Hinzufügen der Abhängigkeit nicht abschließen. Deaktivieren Sie das Kontrollkästchen, um fortzufahren.

- 10 Prüfen Sie die Optionen und klicken Sie auf **Beenden**, um die Abhängigkeit zu erstellen.

Bearbeiten einer vService-Abhängigkeit

Sie können den Namen, die Beschreibung und die Erforderlichkeit einer vService-Abhängigkeit bearbeiten.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Registerkarte **vServices** im Dialogfeld „Einstellungen bearbeiten“ mit der rechten Maustaste auf die Abhängigkeit und wählen Sie **Bearbeiten**.

- 3 Ändern Sie im Dialogfeld „Abhängigkeitseigenschaften“ den Namen und die Beschreibung der Abhängigkeit.
- 4 Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den Status „Erforderlich“ der Abhängigkeit zu ändern.
Das Kontrollkästchen „Erforderlich“ ist deaktiviert, wenn die virtuelle Maschine bzw. die vApp läuft.
- 5 Wählen Sie einen Anbieter für die Abhängigkeit aus.
Wenn Sie einen Anbieter auswählen, wird die Anbieterbeschreibung als Beschreibung übernommen. Das Feld „Validierung“ zeigt die Validierungsergebnisse an. Wenn die Validierung fehlschlägt, wird die Schaltfläche **OK** deaktiviert, bis ein anderer oder kein Anbieter ausgewählt wird.
- 6 Klicken Sie auf **OK**.

Entfernen einer vService-Abhängigkeit

Sie können eine vService-Abhängigkeit von einer virtuellen Maschine oder einer vApp entfernen.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere Client auf die virtuelle Maschine oder vApp und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie auf der Registerkarte **vServices** im Dialogfeld „Einstellungen bearbeiten“ die Abhängigkeit aus und klicken Sie auf **Entfernen**.

Die Abhängigkeit wird aus der Liste entfernt.

Konfigurieren erweiterter vApp-Eigenschaften

Sie können erweiterte Einstellungen bearbeiten und konfigurieren, z. B. Produkt- und Anbieterinformationen, benutzerdefinierte Eigenschaften und IP-Reservierung.

Erforderliche Berechtigung: **vApp.vApp-Anwendungskonfiguration**

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste Optionen auf **Erweitert**.
- 3 Legen Sie die Einstellungen, die auf der Übersichtsseite der virtuellen Maschine angezeigt werden, fest und konfigurieren Sie sie.

vApp-Einstellung	Beschreibung
Produktname	Produktname.
Version	vApp-Version.
Vollversion	Vollversion von vApp.
Produkt-URL	Wenn Sie eine Produkt-URL eingeben, kann ein Benutzer auf der Zusammenfassungsseite einer virtuellen Maschine auf den Produktnamen klicken, um zur Webseite des Produkts zu gelangen.

vApp-Einstellung	Beschreibung
Anbieter-URL	Wenn Sie eine Anbieter-URL eingeben, kann ein Benutzer auf der Zusammenfassungsseite einer virtuellen Maschine auf den Anbieternamen klicken, um zur Webseite des Anbieters zu gelangen.
Anwendungs-URL	Wenn Sie zum Angeben der IP-Adresse der virtuellen Maschine Eigenschaften verwenden, können Sie eine dynamische Anwendungs-URL eingeben, die auf eine Webseite verweist, die von der laufenden virtuellen Maschine offengelegt wird. Wenn Sie eine gültige Anwendungs-URL eingeben, ändert sich der Status der virtuellen Maschine in den Link Verfügbar , wenn die Ausführung der virtuellen Maschine beginnt.

Wenn Sie die virtuelle Maschine zum Verwenden der Eigenschaft *webserver_ip* konfigurieren und sie über einen Webserver verfügt, können Sie **http://\${webserver_ip}/** als **Anwendungs-URL** eingeben.

- 4 (Optional) Klicken Sie auf **Ansicht**, um die **Produkt-URL** und die **Anbieter-URL** zu testen.
- 5 Klicken Sie zum Bearbeiten der benutzerdefinierten vApp-Eigenschaften auf **Eigenschaften**.
- 6 Klicken Sie zum Bearbeiten der unterstützten IP-Zuteilungsschemen dieser vApp auf **IP-Reservierung**.
- 7 Klicken Sie auf **OK**.

Festlegen von Eigenschaften der OVF-Umgebung

Sie können die Eigenschaften der OVF-Umgebung für die vApp anzeigen oder ändern.

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste Optionen auf **Erweitert**.
- 3 Klicken Sie auf **Eigenschaften**.
- 4 Sie können im Dialogfeld „Erweiterte Eigenschaftskonfiguration“ folgende Aktionen durchführen:
 - Klicken Sie auf **Neu**, um eine neue benutzerdefinierte Eigenschaft hinzuzufügen.
 - Wählen Sie die Eigenschaft aus und klicken Sie auf **Bearbeiten**, um eine Eigenschaft zu bearbeiten.
 - Klicken Sie auf **Löschen**, um eine Eigenschaft zu löschen.
- 5 Klicken Sie auf **OK**.

Bearbeiten von erweiterten IP-Zuteilungseigenschaften

Sie können das IP-Zuteilungsschema für die vApp bearbeiten.

Vorgehensweise

- 1 Klicken Sie auf der Übersichtsseite der vApp auf **Einstellungen bearbeiten**.
- 2 Klicken Sie in der Liste **Optionen** auf **Erweitert**.
- 3 Klicken Sie auf **IP-Zuteilung**.
- 4 Im Dialogfeld „Erweiterte IP-Zuteilung“ können Sie die folgenden Aktionen ausführen.
 - Wählen Sie ein Zuteilungsschema für IP-Adressen.
 - Wählen Sie die IP-Protokolle aus, die von der vApp unterstützt werden: IPv4, IPv6 oder beide.
- 5 Klicken Sie auf **OK**.

Konfigurieren von IP-Pools

IP-Pools bieten vApps eine Netzwerkkidentität. Ein IP-Pool ist eine Netzwerkkonfiguration, die einem von einer vApp verwendeten Netzwerk zugewiesen wird. Die vApp kann daraufhin vCenter Server verwenden, um eine automatische IP-Konfiguration ihrer virtuellen Maschinen vorzunehmen.

Festlegen eines IP-Adressbereichs

Sie können einen IP-Adressbereich festlegen, indem Sie einen Host-Adressbereich innerhalb eines Netzwerks angeben.

IP-Pool-Bereiche werden mit IPv4 und IPv6 konfiguriert. Diese Bereiche werden von vCenter Server für die dynamische Zuteilung von IP-Adressen zu virtuellen Maschinen verwendet, wenn eine vApp für die Verwendung der vorübergehenden IP-Reservierung eingerichtet ist.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste das Datacenter aus, das die vApp enthält.
- 2 Klicken Sie auf der Registerkarte „IP-Pools“ mit der rechten Maustaste auf den IP-Pool, den Sie bearbeiten möchten, und wählen Sie **Eigenschaften**.

Wenn keine IP-Pools angezeigt werden, klicken Sie auf **Hinzufügen**, um einen neuen IP-Pool hinzuzufügen.
- 3 Wählen Sie im Eigenschaftendialogfeld die Registerkarte „IPv4“ oder „IPv6“ aus, je nachdem, welches IP-Protokoll Sie verwenden.
- 4 Geben Sie das **IP-Subnetz** und das **Gateway** in die entsprechenden Felder ein.
- 5 (Optional) Wählen Sie das Kontrollkästchen **IP-Pool aktivieren** aus.
Aktivieren Sie diese Einstellung, um einen IP-Adressbereich festzulegen.
- 6 (Optional) Geben Sie in das Feld **Bereiche** eine kommasetrennte Liste von Host-Adressbereichen ein.
Ein Bereich besteht aus einer IP-Adresse, einer Raute (#) und einer Zahl, die die Länge des Bereichs angibt.
Das Gateway und die Bereiche müssen im Subnetz liegen und dürfen die Gateway-Adresse nicht enthalten.

Beispielsweise zeigt 10.20.60.4#10, 10.20.61.0#2 an, dass die IPv4-Adressen im Bereich von „10.20.60.4“ bis „10.20.60.13“ und „10.20.61.0“ bis „10.20.61.1“ liegen können.
- 7 Klicken Sie auf **OK**.

Auswählen von DHCP

Sie können festlegen, dass ein IPv4- oder IPv6-DHCP-Server im Netzwerk verfügbar ist.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste das Datacenter aus, das die vApp enthält, die Sie konfigurieren.
- 2 Klicken Sie auf der Registerkarte **IP-Pools** mit der rechten Maustaste auf den IP-Pool, den Sie bearbeiten möchten, und wählen Sie **Eigenschaften**.

Wenn keine „IP-Pools“ angezeigt werden, klicken Sie auf **Hinzufügen**, um einen neuen IP-Pool hinzuzufügen.
- 3 Wählen Sie im Eigenschaftendialogfeld die Registerkarte **DHCP** aus.

- 4 Aktivieren Sie das Kontrollkästchen **IPv4 DHCP vorhanden** oder **IPv6 DHCP vorhanden**, um anzugeben, dass einer der DHCP-Server in diesem Netzwerk verfügbar ist.
- 5 Klicken Sie auf **OK**.

Festlegen von DNS-Einstellungen

Geben Sie die DNS-Einstellungen für die vApp ein.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste das Datacenter aus, das die vApp enthält, die Sie konfigurieren.
- 2 Klicken Sie auf der Registerkarte „IP-Pools“ mit der rechten Maustaste auf den IP-Pool, den Sie bearbeiten möchten, und wählen Sie **Eigenschaften**.

Wenn keine IP-Pools angezeigt werden, klicken Sie auf **Hinzufügen**, um einen neuen IP-Pool hinzuzufügen.

- 3 Wählen Sie im Eigenschaftendialogfeld die Registerkarte **DNS** aus.
- 4 Geben Sie die DNS Server-Informationen ein.

Geben Sie die Server durch IP-Adressen an, die durch ein Komma, Semikolon oder Leerzeichen getrennt sind.

Sie können die folgenden DNS-Informationstypen eingeben:

- DNS-Domäne
- Host-Präfix
- DNS-Suchpfad
- IPv4 DNS-Server
- IPv6 DNS-Server

- 5 Klicken Sie auf **OK**.

Festlegen eines Proxy-Servers

Legen Sie einen HTTP Proxy-Server für die vApp fest.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste das Datacenter aus, das die vApp enthält.
- 2 Klicken Sie auf der Registerkarte „IP-Pools“ mit der rechten Maustaste auf den IP-Pool, den Sie bearbeiten möchten, und wählen Sie **Eigenschaften**.

Wenn keine IP-Pools angezeigt werden, klicken Sie auf **Hinzufügen**, um einen neuen IP-Pool hinzuzufügen.

- 3 Wählen Sie im Eigenschaftendialogfeld die Registerkarte **Proxy** aus.
- 4 Geben Sie den Servernamen und die Portnummer für den Proxy-Server ein.

Der Servername kann einen Doppelpunkt und eine Portnummer enthalten.

Beispielsweise ist `web-proxy:3912` ein gültiger Proxy-Server.

- 5 Klicken Sie auf **OK**.

Auswählen von Netzwerkverknüpfungen

Sie können einem IP-Pool ein oder mehrere Netzwerke zuordnen.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste das Datacenter aus, das die vApp enthält.
- 2 Klicken Sie auf der Registerkarte **IP-Pools** mit der rechten Maustaste auf den IP-Pool, den Sie bearbeiten möchten, und wählen Sie **Eigenschaften**.

Wenn keine „IP-Pools“ angezeigt werden, klicken Sie auf **Hinzufügen**, um einen neuen IP-Pool hinzuzufügen.
- 3 Wählen Sie im Eigenschaftendialogfeld die Registerkarte **Verknüpfungen** aus.
- 4 Wählen Sie die Netzwerke aus, die diesen IP-Pool verwenden.

Ein Netzwerk kann nur einem IP-Pool auf einmal zugewiesen werden.
- 5 Klicken Sie auf **OK**.

Bearbeiten einer vApp-Anmerkung im vSphere-Client

Sie können Anmerkungen für eine bestimmte vApp hinzufügen oder bearbeiten.

Vorgehensweise

- 1 Wählen Sie die vApp in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Übersicht** für die vApp.
- 3 Klicken Sie im Abschnitt „Anmerkung“ auf **Bearbeiten**.
- 4 Geben Sie Ihre Kommentare im Fenster vApp-Anmerkung bearbeiten ein.
- 5 Klicken Sie auf **OK**.

Ihre Kommentare werden unter „Anmerkung“ angezeigt.

Überwachen von Lösungen mit vCenter Solutions Manager

18

Ein vSphere-Administrator verwendet vCenter Solutions Manager im vSphere Client, um die installierten Lösungen aufzulisten, detaillierte Informationen zu den Lösungen anzuzeigen und den Systemstatus der Lösung zu überwachen. Sie können diese Aufgaben auch im vSphere Web Client ausführen.

Sie können vSphere-Lösungen aus dem vSphere-Client oder dem vSphere Web Client überwachen und verwalten. Beide Clients zeigen eine Bestandsliste von vSphere-Lösungen und Details über jede Lösung an.

Eine Lösung ist eine Erweiterung von vCenter Server, die einer vCenter Server-Instanz neue Funktionen hinzufügt. Beispielsweise ist ESX Agent Manager eine Standard-vCenter-Lösung von VMware, mit der Sie ESX-Host-Agenten verwalten können, die den ESX-Hosts neue Funktionen hinzufügen. Eine weitere von vSphere angebotene Standardlösung ist vService-Manager. VMware-Produkte, die mit vCenter Server integriert werden können, werden ebenfalls als Lösungen betrachtet. Sie können eine Lösung installieren, um die Standardfunktionen von vCenter Server mit Funktionalität von Drittanbietern zu erweitern. Lösungen werden in der Regel als OVF-Pakete bereitgestellt. Sie können Lösungen mithilfe des vSphere-Client installieren und bereitstellen. Lösungen können in vCenter Solutions Manager integriert werden.

Wenn eine Lösung auf einer virtuellen Maschine oder einer vApp ausgeführt wird, erscheint in der Bestandslistenansicht des vSphere-Client ein benutzerdefiniertes Symbol neben der Lösung. Wenn Sie eine virtuelle Maschine oder eine vApp ein- bzw. ausschalten, werden Sie darüber benachrichtigt, dass Sie den Vorgang auf einem Element durchführen, die vom Lösungs-Manager verwaltet wird.

Jede Lösung registriert ein eindeutiges Symbol, um anzugeben, dass die virtuelle Maschine oder vApp von der Lösung verwaltet wird. Die Symbole zeigen Betriebszustände (eingeschaltet, angehalten, ausgeschaltet) an.

Die Lösungen zeigen möglicherweise mehrere Symboltypen an, wenn sie mehrere Typen von virtuellen Maschinen oder vApps verwalten.

Wenn Sie versuchen, einen Vorgang auf einer virtuellen Maschine oder einer vApp auszuführen, die von einer Lösung verwaltet wird, erscheint eine Meldung mit einer entsprechenden Warnung.

Weitere Informationen finden Sie in der Dokumentation *Entwickeln und Bereitstellen von vSphere-Lösungen, vServices und ESX-Agenten*.

Dieses Kapitel behandelt die folgenden Themen:

- „Anzeigen von Lösungen“, auf Seite 236
- „Überwachungsagenten“, auf Seite 236
- „Überwachen von vServices“, auf Seite 237

Anzeigen von Lösungen

Sie können Lösungen, die in einer vCenter Server-Instanz installiert wurden, mit vCenter Solutions Manager bereitstellen, überwachen und mit ihnen arbeiten. Der Solutions Manager zeigt Informationen über den Status einer Lösung an.

Sie können von der Startseite des vSphere-Client aus zum Solutions Manager navigieren. In der Solutions Manager-Ansicht werden Informationen über die Lösung angezeigt.

- Lösungsname
- Lösungsstatus
- vService-Anbieter

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Client auf das Solutions Manager-Symbol.
- 2 Navigieren Sie durch die Registerkarten des Solutions Managers.
 - Registerkarte **Übersicht**. Listet die Anzahl der installierten Lösungen und eine kurze Statusübersicht für jede Lösung auf.
 - Registerkarte **Lösungen**. Listet alle verwalteten Lösungen auf.
 - Registerkarte **Status**. Gibt den Systemzustand der vCenter-Dienste an. Zudem werden für jeden Dienst die Alarme oder Warnungen angezeigt.
- 3 Klicken Sie in der Solutions Manager-Bestandsliste auf eine der Lösungen.
 - Registerkarte **Übersicht**. Listet Informationen zur Lösung auf, einschließlich eines Links zum Produkt und den Anbieter-Websites, eines Links zum Starten der Management-UI in einem separaten Fenster sowie eines Links zur virtuellen Maschine bzw. zur vApp, die diese Lösung ausführt.

Durch die Auswahl des Anbieter-Website-Links gelangen Sie zur Seite „Übersicht“ der virtuellen Maschine oder vApp. Ein Link unter „Verwaltet von“ führt Sie zur Lösung zurück.
 - Registerkarte **Virtuelle Maschinen**. Listet alle virtuelle Maschinen auf, die zur Lösung gehören
 - Registerkarte **vService-Anbieter**.
 - Registerkarte **Management** oder eine andere Registerkarte, die die Lösung angegeben hat.

Überwachungsagenten

vCenter Solutions Manager zeigt die Agenten des vSphere ESX Agent Manager an, die Sie zum Bereitstellen und Verwalten der verwandten Agenten auf ESX/ESXi-Hosts verwenden können.

Sie können den Solutions Manager verwenden, um zu überwachen, ob die Agenten einer Lösung erwartungsgemäß funktionieren. Ausstehende Probleme werden durch den Status des ESX Agent Manager der Lösung und eine Liste von Problemen wiedergegeben.

Wenn sich der Status einer Lösung ändert, aktualisiert der Solutions Manager den Zusammenfassungsstatus und Status des ESX Agent Manager. Administratoren verwenden diesen Status, um zu überwachen, ob der Zielzustand erreicht wurde.

Der Systemstatus des Agenten wird durch eine bestimmte Farbe gekennzeichnet.

Tabelle 18-1. ESX Agent Manager-Integritätsstatus

Status	Beschreibung
Rot	Die Lösung muss intervenieren, damit ESX Agent Manager fortfahren kann. Wenn beispielsweise ein VM-Agent auf einer Computing-Ressource manuell ausgeschaltet wird und ESX Agent Manager nicht versucht, den Agenten einzuschalten. Diese Aktion wird vom ESX Agent Manager an die Lösung gemeldet, und diese sendet eine Meldung an den Administrator, den Agenten einzuschalten.
Gelb	ESX Agent Manager arbeitet aktiv daran, einen Zielzustand zu erreichen. Der Zielzustand kann aktiviert, deaktiviert oder deinstalliert werden. Wenn z. B. eine Lösung registriert wird, hat sie so lange den Status Gelb, bis ESX Agent Manager die Agenten der Lösungen für alle angegebenen Computing-Ressourcen bereitstellt. Eine Lösung muss nicht eingreifen, wenn ESX Agent Manager seinen ESX Agent Manager-Systemstatus als Gelb meldet.
Grün	Eine Lösung und alle ihre Agenten haben den Zielzustand erreicht.

Überwachen von vServices

Ein vService ist ein Dienst oder eine Funktion, der bzw. die virtuelle Maschinen und vApps eine Lösung bereitstellt. Eine Lösung kann einen oder mehrere vServices anbieten. Diese vServices werden in die Plattform integriert und können die Umgebung ändern, in der die vApp oder die virtuelle Maschine ausgeführt wird.

Ein vService ist eine Art Dienst, den eine vCenter-Erweiterung einer virtuellen Maschine und einer vApp bereitstellt. Virtuelle Maschinen und vApps können vServices-Abhängigkeiten haben. Jede Abhängigkeit ist mit einem vService-Typ verknüpft. Der vService-Typ muss an eine bestimmte vCenter-Erweiterung gebunden sein, die diesen vService-Typ implementiert. Dieser vService-Typ ähnelt einem virtuellen Hardwaregerät. Eine virtuelle Maschine kann beispielsweise ein Netzwerkgerät haben, das bei der Bereitstellung mit einem bestimmten Netzwerk verbunden sein muss.

Der vService-Manager ermöglicht, dass sich eine Lösung in Vorgänge, die OVF-Vorlagen betreffen, einklinken kann:

- Importieren von OVF-Vorlagen Ein Callback wird erhalten, wenn OVF-Vorlagen mit einer vService-Abhängigkeit eines bestimmten Typs importiert werden.
- Exportieren von OVF-Vorlagen OVF-Abschnitte werden eingefügt, wenn eine virtuelle Maschine exportiert wird.
- Generieren einer OVF-Umgebung. OVF-Abschnitte werden beim Einschalten in die OVF-Umgebung eingefügt.

Auf der Registerkarte **vServices** im Lösungs-Manager werden Details für jede vCenter-Erweiterung angezeigt. Diese Informationen ermöglichen Ihnen das Überwachen der vService-Anbieter und das Auflisten der virtuellen Maschinen oder vApps, an die sie gebunden sind.

Verwenden von Hostprofilen im vSphere-Client

19

Die Hostprofilfunktion erstellt ein Profil, das die Hostkonfiguration enthält und für deren Verwaltung hilfreich ist, insbesondere in Umgebungen, in denen ein Administrator mehrere Hosts oder Cluster in vCenter Server verwaltet.

Diese Funktion macht die hostbasierte, die manuelle oder die benutzeroberflächenbasierte Hostkonfiguration überflüssig und sorgt durch die Verwendung von Hostprofilrichtlinien für die Konsistenz und Korrektheit der Konfiguration innerhalb des gesamten Datencenters. Diese Richtlinien halten den Entwurf einer bekannten, validierten Konfiguration des Referenzhosts fest und konfigurieren davon ausgehend das Netzwerk, den Speicher, die Sicherheit und andere Einstellungen auf mehreren Hosts oder Clustern. Sie können dann einen Host oder Cluster mit der Konfiguration eines Profils vergleichen, um Abweichungen zu erkennen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Modell für die Verwendung von Hostprofilen“](#), auf Seite 239
- [„Zugreifen auf die Ansicht „Hostprofile““](#), auf Seite 240
- [„Erstellen eines Hostprofils“](#), auf Seite 241
- [„Exportieren eines Hostprofils“](#), auf Seite 242
- [„Importieren eines Hostprofils“](#), auf Seite 242
- [„Klonen eines Hostprofils“](#), auf Seite 243
- [„Bearbeiten eines Hostprofils“](#), auf Seite 243
- [„Verwalten von Profilen“](#), auf Seite 246
- [„Prüfen der Übereinstimmung“](#), auf Seite 250
- [„Hostprofile und vSphere Auto Deploy“](#), auf Seite 251

Modell für die Verwendung von Hostprofilen

Sie führen Hostprofilaufgaben in einer bestimmten Reihenfolge aus.

Es muss eine vSphere-Installation mit mindestens einem ordnungsgemäß konfigurierten Host vorhanden sein.

- 1 Richten Sie den Host, der als Referenzhost verwendet wird, ein und konfigurieren Sie ihn.
Ein Referenzhost ist der Host, aus dem das Profil erstellt wird.
- 2 Erstellen Sie mithilfe des festgelegten Referenzhosts ein Profil.
- 3 Hängen Sie einen Host oder einen Cluster an das Profil an.

- 4 Überprüfen Sie die Übereinstimmung des Hosts mit dem Profil des Referenzhosts. Wenn alle Hosts mit dem Referenzhost übereinstimmen, sind sie ordnungsgemäß konfiguriert.
- 5 Übernehmen Sie das Hostprofil des Referenzhosts für andere Hosts oder Hostcluster.

Die Verwendung von Hostprofilen wird nur für VMware vSphere 4.0-Hosts (oder höher) unterstützt. Diese Funktion wird für VMware Infrastructure-Hosts der Version 3.5 oder früher nicht unterstützt. Wenn vCenter Server 4.0 VMware Infrastructure-Hosts der Version 3.5 oder früher verwaltet, kann beim Verwenden von Hostprofilen für diese Hosts Folgendes eintreten:

- Sie können kein Hostprofil erstellen, das einen VMware Infrastructure-Host der Version 3.5 oder früher als Referenzhost verwendet.
- Sie können kein Hostprofil auf VMware Infrastructure-Hosts der Version 3.5 oder früher anwenden. Die Übereinstimmungsprüfung schlägt fehl.
- Sie können zwar ein Hostprofil an einen gemischten Cluster anhängen, der VMware Infrastructure 3.5-Hosts oder früher enthält, die Überprüfung der Richtlinien Einhaltung für diese früheren Hosts schlägt jedoch fehl.

Hostprofile sind als Lizenzfunktion von vSphere nur dann verfügbar, wenn die entsprechende Lizenzierung vorhanden ist. Wenn Fehler auftreten, stellen Sie sicher, dass die entsprechende vSphere-Lizenzierung für Ihren Host vorhanden ist.

Wenn das Hostprofil Verzeichnisdienste für die Authentifizierung verwenden soll, muss der Referenzhost darauf konfiguriert werden, einen Verzeichnisdienst zu verwenden. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Hosts, die mit vSphere® Auto Deploy bereitgestellt werden

Für Hosts, die mit vSphere Auto Deploy bereitgestellt werden, gehört vCenter Server die gesamte Hostkonfiguration, die in einem Hostprofil erfasst wird. In den meisten Fällen reichen die Hostprofilinformationen aus, um alle Informationen zur Konfiguration zu speichern. Manchmal wird der Benutzer aufgefordert, eine Eingabe vorzunehmen, wenn der mit Auto Deploy bereitgestellte Host gestartet wird. Der Antwortdateimechanismus kümmert sich um diese Fälle. Weitere Informationen hierzu finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.

Zugreifen auf die Ansicht „Hostprofile“

In der Hauptansicht für Hostprofile sind alle verfügbaren Profile aufgelistet. Administratoren können über die Hauptansicht „Hostprofile“ auch Vorgänge zu Hostprofilen ausführen und Profile konfigurieren.

Die Hauptansicht „Hostprofile“ sollte von erfahrenen Administratoren verwendet werden, die Hostprofilvorgänge durchführen sowie erweiterte Optionen und Richtlinien konfigurieren möchten. Die meisten Vorgänge, wie das Erstellen neuer Profile, das Anhängen von Elementen und das Übernehmen von Profilen, können über die Ansicht „Hosts und Cluster“ durchgeführt werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- ◆ Wählen Sie **Ansicht > Management > Hostprofile**.

Alle vorhandenen Profile werden auf der linken Seite der Profilliste aufgelistet. Wenn ein Profil in der Profilliste ausgewählt wird, werden die Informationen zu dem Profil auf der rechten Seite angezeigt.

Erstellen eines Hostprofils

Zum Erstellen eines neuen Hostprofils verwenden Sie die Konfiguration des festgelegten Referenzhosts.

Ein Hostprofil kann wie folgt erstellt werden:

- Über die Hauptansicht „Hostprofil“
- Über das Kontextmenü eines Hosts

Erstellen eines Host-Profils über die Ansicht „Host-Profile“

Sie können über die Hauptansicht „Host-Profile“ mithilfe der Konfiguration eines bestehenden Hosts ein Host-Profil erstellen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Es müssen eine vSphere-Installation und mindestens ein ordnungsgemäß konfigurierter Host in der Bestandsliste vorhanden sein.

Vorgehensweise

- 1 Klicken Sie in der Hauptansicht „Hostprofile“ auf das Symbol **Profil erstellen**.
Der Assistent zum Erstellen von Profilen wird angezeigt.
- 2 Wählen Sie die Option zum Erstellen eines neuen Profils aus und klicken Sie auf **Weiter**.
- 3 Wählen Sie den Host aus, den Sie als Referenzhost für das neue Hostprofil festlegen möchten, und klicken Sie auf **Weiter**.
Der Referenzhost muss ein gültiger Host sein.
- 4 Geben Sie den Namen und eine Beschreibung für das neue Profil ein und klicken Sie dann auf **Weiter**.
- 5 Überprüfen Sie die zusammengefassten Informationen für das neue Profil und klicken Sie auf **Beenden**, um die Erstellung des Profils abzuschließen.

Das neue Profil wird in der Profilliste angezeigt.

Erstellen eines Host-Profils über den Host

Sie können in der Bestandslistenansicht „Hosts und Cluster“ über das Kontextmenü eines Hosts ein neues Hostprofil erstellen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Es müssen eine vSphere-Installation und mindestens ein ordnungsgemäß konfigurierter Host in der Bestandsliste vorhanden sein.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, den Sie als Referenzhost für das neue Hostprofil festlegen möchten.
Der Host muss ein gültiger Host sein, damit er als Referenzhost verwendet werden kann.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Hostprofil > Profil vom Host erstellen**.
Der Assistent Profil vom Host erstellen wird geöffnet.

- 3 Geben Sie den Namen und eine Beschreibung für das neue Profil ein und klicken Sie dann auf **Weiter**.
- 4 Überprüfen Sie die zusammengefassten Informationen für das neue Profil und klicken Sie auf **Beenden**, um die Erstellung des Profils abzuschließen.

Das neue Profil wird auf der Registerkarte „Übersicht“ des Hosts angezeigt.

Exportieren eines Hostprofils

Sie können ein Profil in eine Datei exportieren, die das VMware-Profilformat (.vpf) besitzt.

HINWEIS Beim Exportieren von Hostprofilen werden Administrator- und Benutzerprofilkennwörter nicht exportiert. Mit dieser Sicherheitsmaßnahme wird verhindert, dass Kennwörter unverschlüsselt mit dem Profil exportiert werden. Nachdem das Profil importiert und das Kennwort auf einen Host angewendet wurde, werden Sie aufgefordert, Kennwortwerte erneut einzugeben.

Vorgehensweise

- 1 Wählen Sie auf der Ansichtseite „Host-Profile“ in der Profilliste das zu exportierende Profil aus.
- 2 Klicken Sie mit der rechten Maustaste auf das Profil und wählen Sie die Option **Profil exportieren**.
- 3 Wählen Sie den Speicherort aus und geben Sie den Namen der Datei ein, in die das Profil exportiert wird.
- 4 Klicken Sie auf **Speichern (Save)**.

Importieren eines Hostprofils

Sie können ein Profil aus einer Datei importieren, die das VMware-Profilformat (.vpf) besitzt.

HINWEIS Beim Exportieren von Hostprofilen werden Administrator- und Benutzerprofilkennwörter nicht exportiert. Mit dieser Sicherheitsmaßnahme wird verhindert, dass Kennwörter unverschlüsselt mit dem Profil exportiert werden. Nachdem das Profil importiert und das Kennwort auf einen Host angewendet wurde, werden Sie aufgefordert, Kennwortwerte erneut einzugeben.

Vorgehensweise

- 1 Klicken Sie in der Hauptansicht „Host-Profile“ auf das Symbol **Profil erstellen**.
Der Assistent zum Erstellen von Profilen wird angezeigt.
- 2 Wählen Sie die Option zum Importieren eines Profils aus und klicken Sie auf **Weiter**.
- 3 Geben Sie die zu importierende Datei im VMware-Profilformat an oder suchen Sie nach ihr. Klicken Sie anschließend auf **Weiter**.
- 4 Wählen Sie einen gültigen Host aus, den Sie als Referenzhost für das importierte Profil festlegen möchten, und klicken Sie auf **Weiter**.
- 5 Geben Sie den Namen und eine Beschreibung für das importierte Profil an. Klicken Sie auf **Weiter**, wenn Sie fertig sind.
- 6 Überprüfen Sie die zusammengefassten Informationen für das importierte Profil und klicken Sie auf **Beenden**, um den Import des Profils abzuschließen.

Das importierte Profil wird in der Profilliste angezeigt.

Klonen eines Hostprofils

Ein Klon eines Hostprofils ist eine Kopie eines vorhandenen Hostprofils.

Vorgehensweise

- 1 Wählen Sie in der Hauptansicht „Hostprofile“ das zu klonende Profil aus.
- 2 Klicken Sie auf **Profil klonen**.
- 3 Ein Klon des Profils wird in der Ansicht „Hostprofile“ angezeigt.

Bearbeiten eines Hostprofils

Sie können Hostprofil-Richtlinien anzeigen und bearbeiten, eine Richtlinie auswählen, die auf Übereinstimmung geprüft werden soll, sowie den Namen oder die Beschreibung der Richtlinie ändern.

Vorgehensweise

- 1 Wählen Sie auf der Hauptansicht „Hostprofile“ in der Profilliste das zu bearbeitende Profil aus.
- 2 Klicken Sie auf **Hostprofil bearbeiten**.
- 3 (Optional) Ändern Sie den Namen oder die Beschreibung des Profils in den Feldern im oberen Bereich des Profileditors.
- 4 Bearbeiten Sie die Richtlinie.
- 5 (Optional) Aktivieren oder deaktivieren Sie die Übereinstimmungsprüfung für die Richtlinie.
- 6 Klicken Sie auf **OK**, um den Profileditor zu schließen.

Bearbeiten einer Richtlinie

Eine Richtlinie beschreibt, wie eine bestimmte Konfigurationseinstellung angewendet werden soll. Mit dem Profileditor können Sie die zu einem bestimmten Hostprofil gehörenden Richtlinien bearbeiten.

Auf der linken Seite des Profileditors können Sie das Hostprofil erweitern. Jedes Hostprofil besteht aus mehreren Unterprofilen, die nach Funktionsgruppen ausgewählt werden und Konfigurationsinstanzen darstellen. Jedes Unterprofil enthält viele Richtlinien und Kompatibilitätsprüfungen, die die dem Profil entsprechende Konfiguration beschreiben. Sie können bestimmte Unterprofile, Beispielrichtlinien und Überprüfungen der Richtlinieneneinhaltung konfigurieren.

Jede Richtlinie besteht aus einer oder mehreren Optionen, die einen oder mehrere Parameter enthalten. Jeder Parameter besteht aus einem Schlüssel und einem Wert. Der Wert kann einen der grundlegenden Typen aufweisen, beispielsweise Ganzzahl, Zeichenfolge, Zeichenfolgen-Array oder Ganzzahl-Array.

Tabelle 19-1. Untermenge der Konfigurationen der Unterprofile von Hostprofilen

Unterprofilkonfiguration	Beispielrichtlinien und Übereinstimmungsprüfungen	Anmerkungen
Arbeitsspeicherreservierung	Legen Sie die Arbeitsspeicherreservierung auf einen festen Wert fest.	
Speicher	Konfigurieren Sie Speicheroptionen, wie Natives Multipathing (NMP), Pluggable Storage Architecture (PSA), FCoE- und iSCSI-Adapter und NFS-Speicher.	<ul style="list-style-type: none"> ■ Konfigurieren bzw. ändern Sie unter Verwendung von vSphere-CLI zuerst die NMP- und PSA-Richtlinien auf einem Referenzhost und extrahieren Sie anschließend das Hostprofil dieses Hosts. Wenn Sie den Profileditor für die Bearbeitung der Richtlinien verwenden, sollten Sie die Zusammenhänge zwischen den NMP- und PSA-Richtlinien kennen und mit den Konsequenzen vertraut sein, die sich aus der Änderung einzelner Richtlinien ergeben, um Übereinstimmungsfehler zu vermeiden. Informationen zu NMP und PSA finden Sie in der Dokumentation zu <i>vSphere-Speicher</i>. ■ Das Einstellen der Werte für die IPv6-Adresse des Initiators und die IPv6-Präfixoptionen des Initiators in einem Hostprofil mit unabhängigen Hardware-iSCSI-Adaptoren hat keine Auswirkungen auf den HBA, da die unabhängigen iSCSI-HBAs über keine IPv6-Unterstützung verfügen. ■ Fügen Sie die Regeln hinzu, die Geräteattribute ändern, bevor Sie das Hostprofil vom Referenzhost extrahieren. Wenn Sie einen Host an das Hostprofil angehängt haben, werden Sie nach dem Bearbeiten des Profils und Ändern der Geräteattribute (z. B. Maskieren von Gerätepfaden oder Hinzufügen von SATP-Regeln, um das Gerät als SSD zu markieren) aufgefordert, den Host neu zu starten, damit die Änderungen vorgenommen werden. Nach dem Neustart treten allerdings Übereinstimmungsfehler auf, weil die Attribute geändert wurden. Da Hostprofile Geräteattribute vor dem Neustart extrahieren, werden Übereinstimmungsfehler gemeldet, wenn nach dem Neustart vorgenommene Änderungen erkannt werden.
Netzwerk	Konfigurieren Sie den virtuellen Switch, die Portgruppen, die physische Netzwerkartengeschwindigkeit, die Sicherheits- und NIC-Gruppierungsrichtlinien, den vSphere Distributed Switch und den Uplink-Port des vSphere Distributed Switch.	Wenn DHCPv6 im Netzwerk-Unterprofil aktiviert ist, muss auch der entsprechende Regelsatz im Firewall-Unterprofil manuell aktiviert werden.

Tabelle 19-1. Untermenge der Konfigurationen der Unterprofile von Hostprofilen (Fortsetzung)

Unterprofilkonfiguration	Beispielrichtlinien und Übereinstimmungsprüfungen	Anmerkungen
Datum und Uhrzeit	Konfigurieren Sie die Zeiteinstellungen und die Serverzeitzone.	Geben Sie für die Zeitzone eine UTC-Zeichenfolge ein. Beispiel: „Amerika/Los_Angeles“ für die Zeitzone „Pacific“. Die Standard-Zeitzone wird gemäß der lokalen Zeit und des Standorts der vSphere-Client-Maschine festgelegt. NTP (Network Time Protocol) sollte ordnungsgemäß konfiguriert sein. Sie können die NTP-Einstellungen auf der Registerkarte „Konfiguration“ des Hosts konfigurieren. Klicken Sie auf Uhrzeitkonfiguration und anschließend in der oberen rechten Ecke des Bereichs auf „Eigenschaften“.
Firewall	Aktivieren oder deaktivieren Sie einen Regelsatz.	
Sicherheit	Fügen Sie einen Benutzer oder eine Benutzergruppe hinzu und definieren Sie das Root-Kennwort.	
Dienst	Konfigurieren Sie die Einstellungen für einen Dienst.	
Erweitert	Ändern Sie die erweiterten Optionen.	<ul style="list-style-type: none"> ■ Hostprofile überprüfen die erweiterten Einstellungen nicht, wenn diese mit den Standardeinstellungen identisch sind. vCenter Server kopiert nur die Einstellungen der erweiterten Konfiguration, die sich geändert haben und sich von den Standardwerten unterscheiden. Außerdem werden Übereinstimmungsprüfungen nur für die Einstellungen durchgeführt, die kopiert werden. ■ Hostprofile unterstützen nicht die Konfiguration von PCI-Geräten für das Passthrough virtueller Maschinen auf dem ESXi-Host.

Weitere Profilkonfigurationskategorien sind: Benutzergruppe, Authentifizierung, Kernelmodul, DCUI-Tastatur, Hostcache-Einstellungen, SFCB, Ressourcenpools, Anmelde-Banner, SNMP-Agent, Stromversorgungssystem und CIM-Indication-Abonnements.

Vorgehensweise

- 1 Öffnen Sie den Profileditor für das Profil, das bearbeitet werden soll.
- 2 Erweitern Sie die Unterprofile auf der linken Seite des Profileditors, bis Sie zu der Richtlinie gelangen, die Sie bearbeiten möchten.
- 3 Wählen Sie die Richtlinie aus.
Die Optionen und Parameter für die Richtlinie werden rechts im Profileditor auf der Registerkarte **Konfigurationsinformationen** angezeigt.
- 4 Wählen Sie im Dropdown-Menü eine Richtlinienoption aus und legen Sie ihren Parameter fest.
- 5 Klicken Sie auf **OK**, wenn Sie mit dem Bearbeiten des Profils fertig sind.

HINWEIS Die Änderung wird vorgenommen, wenn die Aufgabe „Hostprofil aktualisieren“ im Status „Kürzlich bearbeitete Aufgaben“ abgeschlossen ist. Wenn Sie versuchen, das Profil vor dem Abschluss der Aufgabe zu übernehmen, enthält die Profilkonfiguration die Änderung nicht.

- 6 (Optional) Wenn Sie eine Änderung an einer Richtlinie vorgenommen haben, jedoch die Standardoption wiederherstellen möchten, klicken Sie auf **Wiederherstellen**. Die Option wird zurückgesetzt.

Aktivieren der Überprüfung der Richtlinieneinhaltung

Sie können während der Prüfung auf Übereinstimmung festlegen, ob eine Hostprofil-Richtlinie berücksichtigt werden soll.

Vorgehensweise

- 1 Öffnen Sie den Profileditor für ein Profil und navigieren Sie zu der Richtlinie, die Sie für die Übereinstimmungsprüfung aktivieren möchten.
- 2 Wählen Sie auf der rechten Seite des Profileditors die Registerkarte **Übereinstimmungsinformationen**.
- 3 Aktivieren Sie das Kontrollkästchen für die Richtlinie.

HINWEIS Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie das Kontrollkästchen deaktivieren, damit diese Richtlinie nicht auf Übereinstimmung geprüft wird, werden die anderen Richtlinien, die für die Übereinstimmungsprüfung aktiviert sind, dennoch überprüft.

Verwalten von Profilen

Nachdem Sie ein Hostprofil erstellt haben, können Sie es verwalten, indem Sie es an einen bestimmten Host oder Cluster anhängen und es anschließend für den Host oder Cluster übernehmen.

Sie können ein Profil mit einem Host oder Cluster verknüpfen, indem Sie das Profil dem Host oder Cluster oder indem Sie den Host oder Cluster dem Profil zuweisen. Sie können anschließend das Profil auf den Host oder Cluster anwenden.

HINWEIS Dem Hostprofil muss ein gültiger Referenzhost zugewiesen sein, bevor Sie das Profil verwalten können.

Anhängen von Hosts oder Clustern an ein Hostprofil

Wenn Sie einen Host so einrichten möchten, dass er dieselbe Konfiguration wie ein Referenzhost verwendet, können Sie den Host an ein Profil anhängen. Sie können auch einen Cluster an ein Profil anhängen.

Profile können auch einem Cluster zugewiesen werden. Zur Übereinstimmung müssen alle Hosts innerhalb eines zugewiesenen Clusters dem Profil gemäß konfiguriert werden. Hosts werden nicht automatisch gemäß dem Hostprofil konfiguriert, das mit dem Cluster angehängt wird, wenn es dem Cluster hinzugefügt wird. Wenn ein Host zu einem Cluster hinzugefügt wird, der einem Profil angehängt ist, wird der Host automatisch an das Profil angehängt.

Sie können einen Host oder Cluster wie folgt an ein Profil anhängen:

- Hauptansicht „Hostprofile“
- Über das Kontextmenü eines Hosts
- Über das Kontextmenü eines Clusters
- Registerkarte „Profil-Übereinstimmung“ des Clusters

Anhängen von Elementen über die Ansicht „Hostprofile“

Bevor Sie das Profil für ein Element (einen Host oder Hostcluster) übernehmen können, müssen Sie das Element an das Profil oder das Profil an das Element anhängen.

Sie können über die Hauptansicht „Hostprofile“ einen Host oder Cluster an ein Profil anhängen.

Wenn ein Hostprofil an einen Cluster angehängt wird, wird den Hosts in diesem Cluster ebenfalls das Hostprofil zugewiesen. Wenn das Hostprofil allerdings vom Cluster getrennt wird, bleibt die Verbindung zwischen dem Host bzw. dem Host im Cluster mit diesem Hostprofil bestehen.

Vorgehensweise

- 1 Wählen Sie in der Hauptansicht „Hostprofile“ in der Profilliste das Profil aus, zu dem Sie den Host oder Cluster hinzufügen möchten.
- 2 Klicken Sie auf das Symbol **Host/Cluster anhängen**.
- 3 Wählen Sie den Host oder Cluster in der erweiterten Liste aus und klicken Sie auf **Anhängen**.
Der Host bzw. Cluster wird zur Liste der angehängten Einheiten hinzugefügt.
- 4 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Anhängen von Profilen über den Host

Bevor Sie das Profil auf einen Host anwenden können, müssen Sie den Host an das Profil oder das Profil an den Host anhängen.

Sie können in der Bestandslistenansicht „Hosts und Cluster“ über das Kontextmenü eines Hosts ein Profil an den Host anhängen.

Wenn ein Hostprofil an einen Cluster angehängt wird, wird den Hosts in diesem Cluster ebenfalls das Hostprofil zugewiesen. Wenn das Hostprofil allerdings vom Cluster getrennt wird, bleibt die Verbindung zwischen dem Host bzw. dem Host im Cluster mit diesem Hostprofil bestehen.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, dem Sie ein Profil anhängen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Hostprofil > Profil verwalten**.

HINWEIS Wenn Ihre Bestandsliste keine Hostprofile enthält, wird ein Dialogfeld mit der Frage angezeigt, ob Sie den Host erstellen und ihn an dieses Profil anhängen möchten.

- 3 Wählen Sie im Dialogfeld Profil anhängen das Profil aus, das Sie an den Host anhängen möchten, und klicken Sie auf **OK**.

Das Hostprofil wird auf der Registerkarte **Übersicht** des Hosts aktualisiert.

Übernehmen von Profilen

Um einen Host in den im Profil angegebenen Zustand zu versetzen, sollten Sie das Profil auf den Host anwenden.

Sie können ein Profil für einen Host wie folgt übernehmen:

- Hauptansicht „Hostprofile“
- Über das Kontextmenü eines Hosts
- Registerkarte „Profil-Übereinstimmung“ des Clusters

Wenn das Profil nicht angewendet oder nicht mit dem im Profil angegebenen Inhalt konfiguriert wird, schlägt bei der nächsten Überprüfung der Richtlinieneinhaltung der Übereinstimmungsstatus für das Profil fehl. Sie können dieses Problem beheben, indem Sie das Profil auf den Host anwenden.

Anwenden eines Profils über die Ansicht „Hostprofile“

Sie können über die Hauptansicht „Hostprofile“ ein Profil auf einen Host anwenden.

Voraussetzungen

Das Profil muss an den Host angehängt sein und der Host muss sich im Wartungsmodus befinden, bevor ein Profil auf ihn angewendet werden kann.

Vorgehensweise

- 1 Wählen Sie in der Hauptansicht „Hostprofile“ das Profil aus, das Sie auf den Host anwenden möchten.
- 2 Wählen Sie die Registerkarte **Hosts und Cluster** aus.
Die Liste der angehängten Hosts wird unter „Elementname“ angezeigt.
- 3 Klicken Sie auf **Profil übernehmen**.
Im Profileditor werden Sie möglicherweise aufgefordert, die für das Übernehmen des Profils erforderlichen Parameter einzugeben.
- 4 Geben Sie die Parameter ein und klicken Sie auf **Weiter**.
- 5 Fahren Sie fort, bis alle erforderlichen Parameter eingegeben sind.
- 6 Klicken Sie auf **Beenden**.

Der Übereinstimmungsstatus wird aktualisiert.

Anwenden eines Profils über den Host

Sie können ein Profil auf einen Host über dessen Kontextmenü anwenden.

Voraussetzungen

Der Host muss sich im Wartungsmodus befinden, bevor ein Profil auf ihn angewendet wird.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, auf den Sie ein Profil anwenden möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Hostprofil > Profil übernehmen**.
- 3 Geben Sie im Profileditor die Parameter ein und klicken Sie auf **Weiter**.
- 4 Fahren Sie fort, bis alle erforderlichen Parameter eingegeben sind.
- 5 Klicken Sie auf **Beenden**.

Der Übereinstimmungsstatus wird aktualisiert.

Referenz-Host ändern

Zum Erstellen des Hostprofils wird die Konfiguration des Referenzhosts verwendet.

Sie können diese Aufgabe über die Hauptansicht „Hostprofile“ oder über das Kontextmenü des Hosts ausführen.

Voraussetzungen

Das Hostprofil muss bereits vorhanden sein.

Vorgehensweise

- 1 Klicken Sie in der Hauptansicht „Host-Profile“ mit der rechten Maustaste auf das Profil aus, für das Sie den Referenzhost ändern möchten, und wählen Sie **Referenzhost ändern**.
- 2 Erweitern Sie die Bestandsliste und wählen Sie den Host aus, den Sie als neuen Referenzhost für das Profil verwenden möchten.
- 3 Klicken Sie auf **Aktualisieren**.
Der **Referenzhost** wird aktualisiert.
- 4 Klicken Sie auf **OK**.

Auf der Registerkarte „Übersicht“ für das Hostprofil wird der aktualisierte Referenzhost aufgelistet.

Verwalten von Profilen über einen Cluster

Sie können über das Kontextmenü des Clusters Profile erstellen, Profile anhängen oder Referenzhosts aktualisieren.

Vorgehensweise

- ◆ Klicken Sie in der Ansicht „Hosts und Cluster“ mit der rechten Maustaste auf einen Cluster und wählen Sie **Hostprofil > Profil verwalten**. Je nach Hostprofil-Setup kann eines der folgenden Ergebnisse eintreten:

Profilstatus und Aufgabe	Ergebnis
Wenn der Cluster keinem Hostprofil angehängt ist und in Ihrer Bestandsliste kein Profil aufgeführt wird, erstellen Sie ein Profil.	a Es wird ein Dialogfeld geöffnet, in dem Sie wählen können, ob Sie ein Profil erstellen und dieses dem Cluster anhängen möchten. b Wenn Sie Ja wählen, wird der Assistent zum Erstellen von Profilen geöffnet.
Wenn der Cluster keinem Hostprofil angehängt ist und in Ihrer Bestandsliste mindestens ein Profil aufgeführt wird, hängen Sie ein Profil an.	a Das Dialogfeld Profil anhängen wird geöffnet. b Wählen Sie das Profil aus, das Sie dem Cluster anhängen möchten, und klicken Sie auf OK .
Wenn der Cluster bereits einem Hostprofil angehängt ist, trennen Sie ein Profil oder hängen Sie den Cluster einem anderen Profil an.	Klicken Sie im Dialogfeld auf Trennen , um das Profil vom Cluster zu trennen, oder auf Ändern , um dem Cluster ein anderes Profil anzuhängen.

Aktualisieren von Profilen vom Referenzhost

Falls Änderungen an der Konfiguration des Hosts, von dem ein Profil erstellt wurde (d. h. der Referenzhost), vorgenommen werden, können Sie das lokale Profil so aktualisieren, dass die Konfiguration des lokalen Hosts mit der Konfiguration des Referenzhosts übereinstimmt.

Nachdem Sie ein Hostprofil erstellt haben, müssen Sie möglicherweise am Profil inkrementelle Aktualisierungen vornehmen. Hierfür gibt es zwei Methoden:

- Nehmen Sie die Konfigurationsänderungen am Referenzhost im vSphere-Client vor und aktualisieren Sie anschließend das Profil vom Referenzhost. Die Einstellungen innerhalb des vorhandenen Profils werden aktualisiert, sodass sie mit denen des Referenzhosts übereinstimmen.
- Aktualisieren Sie das Profil direkt mithilfe des Profileditors.

Das Aktualisieren des Profils mithilfe des Profileditors ist zwar umfangreicher und bietet mehr Optionen, aber das Aktualisieren des Profils vom Referenzhost ermöglicht Ihnen das Validieren der Konfiguration, bevor sie anderen Hosts bereitgestellt wird, die dem Profil angehängt sind.

Das Aktualisieren des Profils vom Referenzhost wird vom Hauptmenü „Hostprofile“ durchgeführt.

Vorgehensweise

- ◆ Klicken Sie in der Hauptansicht „Host-Profil“ mit der rechten Maustaste auf das Profil, das Sie aktualisieren möchten, und wählen Sie **Profil aus Referenzhost aktualisieren**.

Prüfen der Übereinstimmung

Beim Prüfen der Übereinstimmung wird sichergestellt, dass der Host oder Cluster weiterhin korrekt konfiguriert ist.

Nachdem ein Host oder Cluster mit dem Profil des Referenzhost konfiguriert wurde, kann beispielsweise eine manuelle Änderungen zu einer fehlerhaften Konfiguration führen. Durch regelmäßiges Prüfen der Übereinstimmung wird sichergestellt, dass der Host oder Cluster weiterhin korrekt konfiguriert ist.

Prüfen der Übereinstimmung über die Ansicht „Hostprofile“

Sie können über die Hauptansicht „Hostprofile“ die Übereinstimmung eines Hosts oder Clusters mit einem Profil prüfen.

Vorgehensweise

- 1 Wählen Sie in der Liste „Hostprofile“ das zu prüfende Profil aus.
- 2 Wählen Sie auf der Registerkarte **Hosts und Cluster** den Host oder Cluster in der Liste unter „Elementname“ aus.
- 3 Klicken Sie auf **Jetzt auf Übereinstimmung prüfen**.

Der Übereinstimmungsstatus wird als „Übereinstimmung“, „Unbekannt“ oder „Nicht übereinstimmend“ aktualisiert.

Wenn der Übereinstimmungsstatus „Nicht übereinstimmend“ lautet, können Sie das Profil dem Host zuweisen.

Prüfen der Host-Übereinstimmung

Führen Sie nach dem Zuweisen eines Profils zu einem Host über das Kontextmenü des Hosts eine Überprüfung der Richtlinieneinhaltung aus, um die Konfiguration zu überprüfen.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Host aus, für den Sie die Übereinstimmungsprüfung durchführen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Hostprofil > Übereinstimmung prüfen**.

Der Übereinstimmungsstatus des Hosts wird auf der Registerkarte **Zusammenfassung** angezeigt.

Wenn der Host nicht übereinstimmt, müssen Sie das Profil auf den Host anwenden.

Prüfen der Clusterübereinstimmung

Ein Cluster kann auf Übereinstimmung mit einem Host-Profil oder mit bestimmten Clusteranforderungen und -einstellungen geprüft werden.

Vorgehensweise

- 1 Wählen Sie in der Ansicht „Hosts und Cluster“ den Cluster aus, für den Sie die Übereinstimmungsprüfung durchführen möchten.

- 2 Klicken Sie auf der Registerkarte „Profil-Übereinstimmung“ auf **Jetzt auf Übereinstimmung prüfen**, um die Übereinstimmung des Clusters mit dem angehängten Hostprofil und ggf. den Clusteranforderungen zu prüfen.
 - Der Cluster wird auf Übereinstimmung mit bestimmten Einstellungen für Hosts im Cluster geprüft, z. B. DRS, HA und DPM. So kann beispielsweise geprüft werden, ob vMotion aktiviert ist. Der Übereinstimmungsstatus für die Clusteranforderungen wird aktualisiert. Die Prüfung wird auch durchgeführt, wenn dem Cluster kein Hostprofil angehängt ist.
 - Wenn dem Cluster ein Hostprofil angehängt ist, wird der Cluster auf Übereinstimmung mit dem Hostprofil geprüft. Der Übereinstimmungsstatus für das Hostprofil wird aktualisiert.
- 3 (Optional) Klicken Sie neben den Clusteranforderungen auf **Beschreibung**, um eine Liste der Clusteranforderungen anzuzeigen.
- 4 (Optional) Klicken Sie neben den Hostprofilen auf **Beschreibung**, um eine Liste der Übereinstimmungsprüfungen der Hostprofile anzuzeigen.
- 5 (Optional) Klicken Sie auf **Ändern**, um das Hostprofil zu ändern, das dem Cluster angehängt ist.
- 6 (Optional) Klicken Sie auf **Entfernen**, um das Hostprofil zu trennen, das dem Cluster angehängt ist.

Wenn der Cluster nicht übereinstimmt, muss das Profil auf jeden Host im Cluster separat angewendet werden.

Hostprofile und vSphere Auto Deploy

Hostprofile unterstützen die Bereitstellung der physischen ESXi-Hosts durch vSphere Auto Deploy mit Informationen zum Konfigurationszustand (virtuelle Switches, Treibereinstellungen, Startparameter usw.).

Informationen zum Konfigurationszustand können nicht direkt auf einem Host gespeichert werden, der mit Auto Deploy bereitgestellt wurde. Stattdessen können Sie einen Referenzhost erstellen und mit den gewünschten Einstellungen konfigurieren. Anschließend erstellen Sie ein Hostprofil mit diesem Referenzhost. Auto Deploy kann das Hostprofil auf diese Hosts anwenden, sodass diese mit diesen Einstellungen konfiguriert werden, oder Sie können das Hostprofil mit dem Client anwenden.

Um ein Hostprofil auf einen Host anzuwenden, muss der Host in den Wartungsmodus versetzt werden. Der Benutzer wird aufgefordert, beim Anwenden des Hostprofils Antworten für die Richtlinien einzugeben, die während der Erstellung des Hostprofils festgelegt wurden.

Ein mit Auto Deploy bereitgestellter Host kann neu gestartet werden, während das Hostprofil an den Host angehängt ist. Nach dem Neustart helfen die in der Antwortdatei gespeicherten Werte dem mit Auto Deploy bereitgestellten Host, das Profil anzuwenden. Es wird eine Antwortdatei erstellt, die eine Vielzahl von Schlüssel-Wert-Paaren für die Optionen zur Benutzereingabe enthält.

Die Antwortdatei enthält die Benutzereingaberichtlinien für ein Hostprofil. Die Datei wird erstellt, wenn das Profil auf einen bestimmten Host anfänglich angewendet wird.

HINWEIS Wenn Sie ESXi über Hostprofile bereitstellen, konfigurieren Sie syslog, um Protokolle auf einem Remoteserver zu speichern. Anweisungen finden Sie unter „Einrichten von Syslog über die Schnittstelle Hostprofile“ im *Installations- und Einrichtungshandbuch*.

Weitere Informationen hierzu finden Sie unter „Einrichten eines Auto Deploy-Referenzhosts“ in der Dokumentation zu vSphere Auto Deploy.

Prüfen des Antwortdateistatus

Der Antwortdateistatus gibt den Status der Antwortdatei an. Der Status einer Antwortdatei kann „Vollständig“, „Unvollständig“, „Fehlt“ oder „Unbekannt“ sein.

Voraussetzungen

Der Status der Antwortdatei kann nur dann überprüft werden, wenn das Hostprofil an einen Host angehängt ist.

Vorgehensweise

- ◆ Klicken Sie in der Hostprofilansicht auf **Antwortdatei prüfen**.

Der Antwortdateistatus für das Hostprofil wird aktualisiert. Der Status gibt einen der folgenden Statuszustände an:

Unvollständig	In der Antwortdatei fehlen einige der erforderlichen Benutzereingabe-Antworten.
Vollständig	In der Antwortdatei sind alle erforderlichen Benutzereingabe-Antworten enthalten.
Unbekannt	Der Host und das zugehörige Profil sind vorhanden, aber der Status der Antwortdatei ist nicht bekannt. Dies ist der Ausgangszustand einer Antwortdatei.

Antwortdatei aktualisieren

Sie können die Benutzereingabeparameter für die Hostprofil-Richtlinien in der Antwortdatei aktualisieren oder ändern.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf das Hostelement und wählen Sie **Antwortdatei aktualisieren**.
- 2 Geben Sie bei Aufforderung den Benutzereingabeparameter ein bzw. ändern Sie ihn und klicken Sie auf **Weiter**.
- 3 Klicken Sie auf **Aktualisieren**, nachdem Sie die Änderungen eingegeben haben.

Antwortdatei importieren

Sie können eine bereits exportierte Antwortdatei importieren, um sie einem Hostprofil zuzuweisen.

Voraussetzungen

Die importierte Antwortdatei muss mindestens einem Host zugewiesen werden.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf das Hostelement und wählen Sie **Antwortdatei importieren**.
- 2 Wählen Sie die zu importierende Antwortdatei aus.

Antwortdatei exportieren

Sie können eine Antwortdatei exportieren, damit sie importiert und von einem anderen Hostprofil verwendet werden kann.

Die Antwortdatei enthält möglicherweise vertrauliche Daten, wie z. B. Kennwörter und IP-Adressen. Nach dem Export sind diese Informationen unbefugten Zugriffen ausgesetzt. Während des Exportvorgangs werden alle Kennwörter aus der Antwortdatei entfernt. Die Kennwortinformationen müssen erneut eingegeben werden, wenn die Antwortdatei importiert wird.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf das Hostelement und wählen Sie **Antwortdatei exportieren**.
- 2 Wählen Sie den Speicherort zum Speichern der Antwortdatei aus.

Netzwerke beim vSphere Client

Wenn Sie mithilfe des vSphere Client eine direkte Verbindung mit einem Host oder einem vCenter Server-System herstellen, werden vSphere Standard Switches auf diesem Host angezeigt und konfiguriert.

Dieses Kapitel behandelt die folgenden Themen:

- [„Netzwerkeinschränkungen im vSphere Client“](#), auf Seite 255
- [„Anzeigen der Netzwerkinformationen im vSphere-Client“](#), auf Seite 256
- [„Anzeigen der Netzwerkkarteninformationen auf dem vSphere Client“](#), auf Seite 256
- [„Einrichten von Netzwerken mit vSphere Standard-Switches“](#), auf Seite 257
- [„Einrichten von Netzwerken mit vSphere Distributed Switches“](#), auf Seite 261

Netzwerkeinschränkungen im vSphere Client

Die Netzwerkaufgaben, die Sie bei einer direkten Verbindung mit einem ESXi-Host oder einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden Netzwerkfunktionen sind im vSphere Client nicht verfügbar bzw. schreibgeschützt:

- vSphere vMotion über mehrere vCenter Server-Systemen
- vSphere vMotion über große geografische Entfernungen
- Netzwerk-DRS
- DRS-Anti-Affinitätsregeln
- Network I/O Control
- vSwitch öffnen
- Automatische Skalierung des Proxy-Switch
- Opake Netzwerke
- SR-IOV
- LACP
- Multicast
- TCP/IP-Stack und -Upgrade bei mehreren Instanzen
- IPv6-Unterstützung für ESX-Architektur, NFS-4.1-Speichervorgänge, iSCSI, Gastbetriebssystemanpassungen, virtuelle Datacenter

Über den vSphere Web Client stehen Ihnen hingegen alle Netzwerkfunktionen Ihrer vSphere-6.0-Umgebung zur Verfügung.

Anzeigen der Netzwerkinformationen im vSphere-Client

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

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 (Optional) Wählen Sie den Typ des anzuzeigenden Netzwerks aus.

Option	Beschreibung
vSphere Standard-Switch	Zeigt das vSphere Standard-Switch-Netzwerk auf dem Host an.
vSphere Distributed Switch	Zeigt das vSphere Distributed Switch-Netzwerk auf dem Host an.

Die Option **vSphere Distributed Switch** wird nur auf Hosts angeboten, die mit einem oder mehreren vSphere Distributed Switches verbunden sind.

Für jeden virtuellen Switch auf dem Host werden Netzwerkinformationen angezeigt.

Anzeigen der Netzwerkadapterinformationen auf dem vSphere Client

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

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client beim ESXi-Host an und wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerkadapter (Network Adapters)**.

Das Netzwerkadapterfenster zeigt die folgenden Informationen an.

Tabelle 20-1. Parameter für Netzwerkadapter

Option	Beschreibung
Gerät	Name des Netzwerkadapters.
Geschwindigkeit	Tatsächliche Geschwindigkeit und Duplex des Netzwerkadapters.
Konfiguriert	Konfigurierte Geschwindigkeit und Duplex des Netzwerkadapters.
Switch	vSphere Standard-Switch oder vSphere Distributed Switch, der dem Netzwerkadapter zugeordnet ist.
MAC-Adresse	MAC-Adresse des Netzwerkadapters.
Überwachte IP-Bereiche	IP-Adressen, auf die der Netzwerkadapter wahrscheinlich zugreifen kann.
Wake-on-LAN unterstützt	Fähigkeit des Netzwerkadapters zur Unterstützung von Wake-on-LAN.

Einrichten von Netzwerken mit vSphere Standard-Switches

vSphere Standard-Switches steuern den Datenverkehr auf dem Netzwerk auf Hostebene in einer vSphere-Bereitstellung.

Hinzufügen einer Portgruppe für virtuelle Maschinen

VM-Portgruppen stellen virtuellen Maschinen das Netzwerk bereit.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client beim ESXi-Host an und wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Standard-Switch“ aus.
Standard-Switches werden in einer Übersicht angezeigt, die ein detailliertes Layout enthält.
- 4 Klicken Sie auf der rechten Bildschirmseite auf **Netzwerk hinzufügen (Add Networking)**.
- 5 Akzeptieren Sie den Standardverbindungstyp **Virtuelle Maschine** und klicken Sie auf **Weiter**.
- 6 Wählen Sie **vSphere Standard-Switch erstellen** oder einen der aufgelisteten vorhandenen Standard-Switches und die zugewiesenen physischen Adapter aus, die für diese Portgruppe verwendet werden sollen.

Sie können einen Standard-Switch mit oder ohne Ethernet-Adapter erstellen.

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

- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie unter Eigenschaften der Portgruppe (Port Group Properties) eine Netzwerkbezeichnung für die zu erstellende Portgruppe ein.
Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts kennzeichnen.
- 9 (Optional) Wenn Sie ein VLAN verwenden, geben Sie für **VLAN-ID** eine Ziffer zwischen 1 und 4094 ein.
Wenn Sie 0 eingeben oder diese Option leer lassen, kann die Portgruppe nur nicht gekennzeichneten (Nicht-VLAN-)Datenverkehr erkennen. Wenn Sie 4095 eingeben, kann die Portgruppe jeden Datenverkehr in einem VLAN erkennen, und die VLAN-Kennzeichen bleiben intakt.
- 10 Klicken Sie auf **Weiter**.
- 11 Überprüfen Sie die ordnungsgemäße Konfiguration des Switches noch einmal, und klicken Sie dann auf **Beenden**.

Einrichten von VMkernel-Netzwerken auf einem vSphere Standard-Switch

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

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client beim ESXi-Host an und wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Klicken Sie in der Ansicht „vSphere Standard-Switch“ auf **Netzwerk hinzufügen**.
- 4 Wählen Sie **VMkernel (VMkernel)** aus, und klicken Sie auf **Weiter**.
- 5 Wählen Sie den zu verwendenden vSphere Standard-Switch oder wählen Sie **vSphere Standard-Switch erstellen** aus, um einen neuen vSphere Standard-Switch zu erstellen.
- 6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSphere Standard-Switch verwenden soll.

Wählen Sie für jeden vSphere Standard-Switch Adapter aus, sodass die virtuellen Maschinen oder sonstigen Dienste, die an diesen Adapter angeschlossen sind, auf das richtige Ethernet-Segment zugreifen können. Wenn unter „Neuen vSphere Standard-Switch erstellen“ keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSphere Standard-Switches oder vSphere Distributed Switches verwendet werden. Sie können entweder einen neuen vSphere Standard-Switch ohne Netzwerkadapter erstellen oder einen Netzwerkadapter auswählen, der von einem bereits vorhandenen vSphere Standard-Switch verwendet wird.

- 7 Klicken Sie auf **Weiter**.
- 8 Wählen Sie eine Netzwerkbezeichnung und eine VLAN-ID aus oder erstellen Sie sie.

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

- 9 (Optional) Aktivieren Sie **Diese Portgruppe für vMotion verwenden**, damit diese Portgruppe einem anderen Host melden kann, dass sie als die Netzwerkverbindung dient, über die vMotion-Datenverkehr gesendet werden soll.
- 10 (Optional) Wählen Sie **Diese Portgruppe für die Fault Tolerance-Protokollierung verwenden**.
- 11 (Optional) Wählen Sie **Diese Portgruppe für den Verwaltungsdatenverkehr verwenden**.
- 12 Wenn IPv6 auf dem Host aktiviert ist, wählen Sie **IP (Standardwert)**, **IPv6** oder **IP- und IPv6-Netzwerk**.
Diese Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt. Die IPv6-Konfiguration kann nicht mit abhängigen Hardware-iSCSI-Adaptoren verwendet werden.
- 13 Klicken Sie auf **Weiter**.

- 14 Geben Sie an, wie die IP-Einstellungen bezogen werden sollen.

Option	Beschreibung
IP-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden.
Die folgenden IP-Einstellungen verwenden	<p>IP-Einstellungen manuell festlegen.</p> <ul style="list-style-type: none"> a Geben Sie die IP-Adresse und die Subnetzmaske der VMkernel-Schnittstelle ein. b Klicken Sie auf Bearbeiten, um das VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. VMotion, NAS und iSCSI, zu verwenden. <p>Auf der Registerkarte DNS-Konfiguration ist standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.</p> <ul style="list-style-type: none"> c Klicken Sie auf OK und anschließend auf Weiter.

- 15 Wenn Sie IPv6 für die VMkernel-Schnittstelle verwenden, wählen Sie eine Option zum Abrufen der IPv6-Adressen aus.

Option	Beschreibung
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.
Statische IPv6-Adressen	<ul style="list-style-type: none"> a Klicken Sie auf Hinzufügen, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf OK. c Klicken Sie auf Bearbeiten, um das Standard-Gateway des VMkernels zu ändern.

- 16 Klicken Sie auf **Weiter**.
- 17 Überprüfen Sie die Informationen, klicken Sie auf **Zurück**, wenn Sie Einträge ändern möchten, und klicken Sie auf **Beenden**.

Anzeigen von VMkernel-Routing-Informationen auf einem vSphere Standard-Switch

Sie können IP- und IPv6-Routing-Informationen wie Netzwerk, Präfix und Gateway für einen VMkernel-Netzwerkadapter auf einem vSphere Standard-Switch anzeigen.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client beim ESXi-Host an und wählen Sie den Host im Bestandslistenbereich aus.
- 2 Klicken Sie auf die **Eigenschaften** des Standard-Switches, der der anzuzeigenden VMkernel-Schnittstelle zugeordnet ist.
- 3 Wählen Sie auf der Registerkarte „Ports“ den anzuzeigenden VMkernel-Netzwerkadapter aus und klicken Sie unter „IP-Einstellungen“ oder „IPv6-Einstellungen“ auf **Routing-Tabelle anzeigen**.

Eine Routing-Tabelle mit Informationen über Netzwerk, Präfix und Gateway des ausgewählten VMkernel-Netzwerkadapters wird angezeigt.

Ändern der Anzahl an Ports für einen vSphere Standard-Switch

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

Vorgehensweise

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

Weiter

Änderungen werden erst bei Neustart des Systems wirksam.

Ändern der Geschwindigkeit eines Uplink-Adapters

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

Vorgehensweise

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

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

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

- 7 Klicken Sie auf **OK**.

Hinzufügen von Uplink-Adaptern

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

Vorgehensweise

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

Option	Beschreibung
Aktive Adapter	Adapter, die vom Standard-Switch verwendet werden.
Standby-Adapter	Adapter, die aktiv werden, wenn einer oder mehrere der aktiven Adapter ausfallen.

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

Die Liste der Netzwerkadapter mit den nun dem Standard-Switch zugewiesenen Adaptern wird erneut angezeigt.
- 10 Klicken Sie auf **Schließen**, um das Dialogfeld zu verlassen.

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

Einrichten von Netzwerken mit vSphere Distributed Switches

Mit vSphere Distributed Switches können Sie in einer vSphere-Umgebung Netzwerke einrichten und konfigurieren.

Hinzufügen eines vSphere Distributed Switch

Erstellen Sie einen vSphere Distributed Switch auf einem vCenter Server-Datencenter, um den Netzwerkverkehr aller zugeordneten Hosts im Datencenter bewältigen zu können.

Wenn Ihr System komplexe Anforderungen an die Portgruppe stellt, ist es empfehlenswert, eine verteilte Portgruppe und keine Standard-Portgruppe zu erstellen.

Vorgehensweise

- 1 Wählen Sie im vSphere Client die Bestandslistenansicht „Netzwerk“ aus und wählen Sie das Datencenter aus.
- 2 Wählen Sie **Bestandsliste > Datencenter > Neuer vSphere Distributed Switch** aus.

- 3 Wählen Sie die Version des vSphere Distributed Switch aus.

Option	Beschreibung
Version des vSphere Distributed Switch: 5.0.0	Kompatibel mit ESXi Version 5.0 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version des vSphere Distributed Switch:	Kompatibel mit ESXi Version 5.1 und höher.
Version des vSphere Distributed Switch: 5.5.0	Kompatibel mit ESXi Version 5.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version des vSphere Distributed Switch: 6.0.0	Kompatibel mit ESXi Version 6.0 und höher.

- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie im Textfeld **Name** einen Namen für den neuen vSphere Distributed Switch ein.
- 6 Verwenden Sie die Pfeilschaltflächen, um die **Anzahl der Uplink-Ports** auszuwählen, und klicken Sie auf **Weiter**.
- Uplink-Ports verbinden den verteilten Distributed Switch mit physischen Netzwerkkarten auf zugehörigen Hosts. Die Anzahl der Uplink-Ports ist die maximale Anzahl der zulässigen physischen Verbindungen zum verteilten Switch pro Host.
- 7 Wählen Sie aus, ob Hosts und ihre physischen Adapter sofort oder erst später zum vSphere Distributed Switch hinzugefügt werden sollen.
- Wenn Sie **Jetzt hinzufügen** möchten, wählen Sie die zu verwendenden Hosts und physischen Adapter aus, indem Sie auf das Kontrollkästchen neben dem jeweiligen Host bzw. Adapter klicken. Sie können nur während der Erstellung eines Distributed Switches nicht zugewiesene physische Adapter zu einem vSphere Distributed Switch hinzufügen.
- 8 (Optional) Legen sie die maximale Anzahl der Ports auf einem Host fest.
- Klicken Sie auf **Details anzeigen** für den Host.
 - Wählen Sie im Dropdown-Menü die maximale Anzahl an Ports für den Host aus.
 - Klicken Sie auf **OK**.
- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Wählen Sie, ob Sie eine **Standard-Portgruppe automatisch erstellen** möchten.
- Diese Option erstellt eine verteilte Portgruppe mit Standardeinstellungen.
- 11 Klicken Sie auf **Beenden**.

Weiter

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

Netzwerkadapter können über die Hostkonfigurationsseite des vSphere Clients mithilfe der Funktion „Hosts verwalten“ oder mithilfe von Hostprofilen hinzugefügt werden.

Hosts zu einem vSphere Distributed Switch hinzufügen

Sie können einem vSphere Distributed Switch nach dessen Erstellung auf der Distributed Switch-Ebene Hosts und physische Adapter hinzufügen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Host hinzufügen** aus.
- 3 Wählen Sie die hinzuzufügenden Hosts aus.
- 4 Wählen Sie unter den ausgewählten Hosts die hinzuzufügenden physischen Adapter aus und klicken Sie auf **Weiter**.

Sie können sowohl verwendete als auch nicht verwendete physische Adapter auswählen.

HINWEIS Wenn Sie einen physischen Adapter auf einen Distributed Switch verschieben, ohne zugewiesene virtuelle Adapter zu verschieben, können diese virtuellen Adapter die Netzwerkkonnektivität verlieren.

- 5 Wählen Sie für jeden virtuellen Adapter die **Zielpportgruppe** im Dropdown-Menü aus, um den virtuellen Adapter auf den Distributed Switch zu migrieren, oder wählen Sie **Nicht migrieren** aus.
- 6 (Optional) Legen Sie die maximale Anzahl der Ports auf einem Host fest.
 - a Klicken Sie auf **Details anzeigen** für den Host.
 - b Wählen Sie im Dropdown-Menü die maximale Anzahl an Ports für den Host aus.
 - c Klicken Sie auf **OK**.
- 7 Klicken Sie auf **Weiter**.
- 8 (Optional) Migrieren Sie das Netzwerk virtueller Maschinen auf den Distributed Switch.
 - a Wählen Sie **Netzwerk virtueller Maschinen migrieren**.
 - b Wählen Sie für jede virtuelle Maschine die **Zielpportgruppe** im Dropdown-Menü aus oder wählen Sie **Nicht migrieren** aus.
- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Wenn Sie Änderungen vornehmen müssen, klicken Sie auf **Zurück**, um zu dem gewünschten Bildschirm zu gelangen.
- 11 Überprüfen Sie die Einstellungen für den Distributed Switch und klicken Sie auf **Beenden**.

Verwalten von Hosts auf einem vSphere Distributed Switch

Sie können die Konfiguration der Hosts und der physischen Adapter auf einem vSphere Distributed Switch ändern, nachdem sie zum Distributed Switch hinzugefügt wurden.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Hosts verwalten**.
- 3 Wählen Sie die zu verwaltenden Hosts aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie die physischen Adapter aus, die hinzugefügt werden sollen, heben Sie die Auswahl der physischen Adapter auf, die entfernt werden sollen, und klicken Sie auf **Weiter**.
- 5 Wählen Sie für jeden virtuellen Adapter die **Zielportgruppe** im Dropdown-Menü aus, um den virtuellen Adapter auf den Distributed Switch zu migrieren, oder wählen Sie **Nicht migrieren**.
- 6 Klicken Sie auf **Weiter**.
- 7 Migrieren Sie das Netzwerk virtueller Maschinen auf den vSphere Distributed Switch.
 - a Wählen Sie **Netzwerk virtueller Maschinen migrieren**.
 - b Wählen Sie für jede virtuelle Maschine die **Zielportgruppe** im Dropdown-Menü aus oder wählen Sie **Nicht migrieren**.
- 8 Klicken Sie auf **Weiter**.
- 9 (Optional) Wenn Sie Änderungen vornehmen müssen, klicken Sie auf **Zurück**, um zu dem gewünschten Bildschirm zu gelangen.
- 10 Überprüfen Sie die Einstellungen für den Distributed Switch und klicken Sie auf **Beenden**.

Festlegen der Anzahl der Ports pro Host auf einem vSphere Distributed Switch

Legen Sie die maximale Anzahl an Ports auf einem Host fest, um die Anzahl der verteilten Ports zu beschränken, die auf einem oder mehreren Hosts existieren können, die mit einem vSphere Distributed Switch verknüpft sind.

Vorgehensweise

- 1 Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
- 2 Wählen Sie den zu ändernden Host im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 4 Wählen Sie die Ansicht **vSphere Distributed Switch** aus.
- 5 Klicken Sie zum Ändern neben dem vSphere Distributed Switch auf **Eigenschaften**.
- 6 Wählen Sie die maximale Anzahl an Ports aus dem Dropdown-Menü aus und klicken Sie auf **OK**.

Weiter

Wenn Sie die maximale Anzahl an Ports für einen Host ändern, nachdem der Host zum Distributed Switch hinzugefügt wurde, müssen Sie den Host neu starten, bevor der neue Maximalwert wirksam wird.

Bearbeiten der allgemeinen Einstellungen für den vSphere Distributed Switch

Sie können die allgemeinen Einstellungen eines vSphere Distributed Switches bearbeiten, z. B. den Namen des Distributed Switches oder die Anzahl der Uplink-Ports auf dem Distributed Switch.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Allgemein**, um die Einstellungen für den vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
Name	Geben Sie den Namen für den Distributed Switch ein.
Anzahl der Uplink-Ports	Wählen Sie die Anzahl der Uplink-Ports für den Distributed Switch aus.
Notizen	Geben Sie beliebige Anmerkungen zum Distributed Switch ein.

- 4 (Optional) Bearbeiten Sie die Namen der Uplink-Ports.
 - a Klicken Sie auf **Uplink-Namen bearbeiten**.
 - b Geben Sie die neuen Namen für einen oder mehrere Uplink-Ports ein.
 - c Klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**.

Bearbeiten der erweiterten Einstellungen des vSphere Distributed Switch

Sie können erweiterte Einstellungen für den vSphere Distributed Switch ändern, beispielsweise das Cisco Discovery-Protokoll oder den maximalen MTU-Wert.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Erweitert**, um die folgenden Einstellungen des vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
Maximalwert für MTU	Maximalwert für MTU für den vSphere Distributed Switch.
Discovery-Protokollstatus	<p>Wählen Sie den Status für das Discovery-Protokoll auf dem vSphere Distributed Switch.</p> <ul style="list-style-type: none"> ■ Aktiviert. Aktiviertes Discovery-Protokoll für den vSphere Distributed Switch. <ol style="list-style-type: none"> 1 Wählen Sie Cisco Discovery-Protokoll oder Link-Layer Discovery Protocol (LLDP) im Dropdown-Menü Typ. 2 Legen Sie für Operation Überwachen, Werben oder Beide fest. ■ Deaktiviert.
Kontaktinformationen des Administrators	Geben Sie den Namen und Weitere Details für den Administrator des vSphere Distributed Switch ein.

- 4 Klicken Sie auf **OK**.

Anzeigen von Netzwerkkadapterinformationen für einen vSphere Distributed Switch

Zeigen Sie physische Netzwerkkadapter und Uplink-Zuweisungen für einen vSphere Distributed Switch über die Netzwerk-Bestandslistenansicht des vSphere Clients an.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Auf der Registerkarte **Netzwerkkadapter** können Sie Netzwerkkadapter und Uplink-Zuweisungen für zugewiesene Hosts anzeigen.

Diese Registerkarte ist schreibgeschützt. Distributed Switch-Netzwerkkadapter müssen auf Hostebene konfiguriert werden.

- 4 Klicken Sie auf **OK**.

Upgrade eines vSphere Distributed Switch auf eine neuere Version

Ein vSphere Distributed Switch ab Version 4.0 kann auf eine neuere Version aktualisiert werden. Damit kann der Distributed Switch die Vorteile der nur in der neueren Version verfügbaren Funktionen nutzen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Wählen Sie in der Registerkarte **Übersicht** neben **Version** die Option **Upgrade** aus.

Der Upgrade-Assistent liefert Informationen zu den Funktionen, die dem aktualisierten Distributed Switch zur Verfügung stehen, aber nicht der vorherigen Version.

- 4 Wählen Sie die Version des vSphere Distributed Switch aus, auf die aktualisiert werden soll.

Option	Beschreibung
Version des vSphere Distributed Switch: 4.1.0	Mit ESX/ESXi Version 4.1 und höher kompatibel. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version des vSphere Distributed Switch: 5.0.0	Kompatibel mit ESXi Version 5.0 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version des vSphere Distributed Switch: 5.1.0	Kompatibel mit ESXi Version 5.1 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.

Option	Beschreibung
Version des vSphere Distributed Switch: 5.5.0	Kompatibel mit ESXi Version 5.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version des vSphere Distributed Switch: 6.0.0	Kompatibel mit ESXi Version 6.0 und höher.

- 5 Klicken Sie auf **Weiter**.

Der Upgrade-Assistent führt die diesem vSphere Distributed Switch zugewiesenen Hosts auf und informiert darüber, ob sie mit der aktualisierten Version des vSphere Distributed Switch kompatibel sind oder nicht. Sie können nur dann mit dem Upgrade fortfahren, wenn alle Hosts mit der neuen Version des vSphere Distributed Switch kompatibel sind.

Neben jedem nicht kompatiblen Host steht der Grund für die Inkompatibilität.

- 6 Klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Richtigkeit der aufgeführten Upgrade-Informationen und klicken Sie auf **Beenden**.

Verteilte Portgruppen

Eine verteilte Portgruppe gibt Port-Konfigurationsoptionen für jeden Port der Portgruppe auf einem vSphere Distributed Switch an. Verteilte Portgruppen legen fest, wie eine Verbindung zum Netzwerk hergestellt wird.

Hinzufügen einer verteilten Portgruppe

Fügen Sie eine verteilte Portgruppe zu einem vSphere Distributed Switch hinzu, um ein Distributed Switch-Netzwerk für Ihre virtuellen Maschinen zu erstellen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Neue Portgruppe** aus.
- 3 Geben Sie einen **Namen** und die **Anzahl der Ports** für Ihre neue verteilte Portgruppe ein.
- 4 Wählen Sie einen VLAN-Typ.

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

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

Bearbeiten der allgemeinen Einstellungen von verteilten Portgruppen

Sie können die Einstellungen für verteilte Portgruppen bearbeiten, beispielsweise den Namen der verteilten Portgruppe und den Portgruppentyp.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Allgemein** aus, um die folgenden Einstellungen für verteilte Portgruppen zu bearbeiten.

Option	Aktion
Name	Geben Sie den Namen für die verteilte Portgruppe ein.
Beschreibung	Geben Sie eine kurze Beschreibung der verteilten Portgruppe ein.
Anzahl der Ports	Geben Sie die Anzahl der Ports in der verteilten Portgruppe ein.
Port-Bindung	<p>Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind.</p> <ul style="list-style-type: none"> ■ Wählen Sie Statische Bindung aus, um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird. Diese Option ist nicht verfügbar, wenn der vSphere Client direkt mit ESXi verbunden ist. ■ Wählen Sie Dynamische Bindung aus, wenn einer virtuellen Maschine beim ersten Einschalten, nachdem sie mit der verteilten Portgruppe verbunden wurde, ein Port zugewiesen werden soll. Die dynamische Bindung läuft in ESXi 5.x aus. ■ Wählen Sie Flüchtig, um keine Port-Bindung einzugehen. Diese Option ist nicht verfügbar, wenn der vSphere Client direkt mit ESXi verbunden ist.

- 4 Klicken Sie auf **OK**.

Bearbeiten der erweiterten Einstellungen von verteilten Portgruppen

Sie können die Einstellungen für erweiterte verteilte Portgruppen bearbeiten, beispielsweise die Außerkraftsetzungseinstellungen und das Zurücksetzen bei Verbindungstrennung.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.

- 3 Wählen Sie **Erweitert**, um die Eigenschaften der verteilten Portgruppe zu bearbeiten.

Option	Beschreibung
Außerkräftsetzung von Portrichtlinien zulassen	Wählen Sie diese Option aus, um zuzulassen, dass die Richtlinien einer verteilten Portgruppe für einzelne Ports außer Kraft gesetzt werden. Klicken Sie auf Außerkräftsetzungseinstellungen bearbeiten , um auszuwählen, welche Richtlinien auf der Portebene außer Kraft gesetzt werden können.
Außerkräftsetzungseinstellungen bearbeiten	Wählen Sie aus, welche Richtlinien auf Portebene außer Kraft gesetzt werden können.
Zurücksetzen bei Verbindungstrennung konfigurieren	Wenn ein verteilter Port von einer virtuellen Maschine getrennt wird, wird seine Konfiguration auf die Einstellung der verteilten Portgruppe zurückgesetzt. Alle portspezifischen Außerkräftsetzungen werden verworfen.

- 4 Klicken Sie auf **OK**.

Überwachen des Zustands eines verteilten Ports

vSphere kann verteilte Ports überwachen und Informationen zum aktuellen Zustand eines jeden Ports und der Laufzeitstatistik eines Ports liefern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Ports** auf **Port-Status-Überwachung starten**.

Die Tabelle auf der Registerkarte „Ports“ für den Distributed Switch enthält jetzt Laufzeitstatistiken für jeden verteilten Port, einschließlich des Broadcast-, Multicast-, Unicast Ingress- und Egress-Datenverkehrs sowie der Pakete.

Die Spalte **Zustand** gibt den aktuellen Zustand der verteilten Ports an.

Tabelle 20-2. Verteilte Ports – Zustände

Zustand	Beschreibung
Link aktiviert	Die Verbindung für diesen verteilten Port ist aktiv.
Link deaktiviert	Die Verbindung für diesen verteilten Port ist nicht aktiv.
Blockiert	Dieser verteilte Port ist blockiert.
--	Der Zustand dieses verteilten Ports ist derzeit nicht verfügbar.

Konfigurieren der Einstellungen für verteilte Ports

Sie können allgemeine Einstellungen für verteilte Ports ändern, wie z. B. Portnamen und -beschreibung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.

- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Allgemein**.
- 5 Ändern Sie den Namen und die Beschreibung des Ports.
- 6 Klicken Sie auf **OK**.

Private VLANs

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

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

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

Erstellen eines privaten VLAN

Sie können ein privates VLAN erstellen, das auf einem vSphere Distributed Switch und seinen zugeordneten verteilten Ports verwendet wird.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie die Registerkarte **Privates VLAN** aus.
- 4 Klicken Sie unter ID des primären privaten VLANs auf **[ID eines privaten VLAN hier eingeben]** und geben Sie die Nummer des primären privaten VLANs ein.
- 5 Klicken Sie auf eine beliebige Stelle im Dialogfeld und wählen Sie dann das primäre private VLAN aus, das Sie gerade hinzugefügt haben.

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

- 6 Klicken Sie für jedes neue sekundäre private VLAN unter „ID des sekundären privaten VLANs“ auf **[ID eines privaten VLAN hier eingeben]** und geben Sie die Nummer des sekundären privaten VLANs ein.

- 7 Klicken Sie auf eine beliebige Stelle im Dialogfeld, wählen Sie das gerade hinzugefügte, sekundäre private VLAN aus und wählen Sie als Port-Typ entweder **Isoliert** oder **Community** aus.
- 8 Klicken Sie auf **OK**.

Entfernen eines primären privaten VLAN

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

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.
- Bevor Sie ein privates VLAN entfernen, stellen Sie sicher, dass keine Portgruppen für seine Verwendung konfiguriert sind.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie die Registerkarte **Privates VLAN** aus.
- 4 Wählen Sie das primäre private VLAN aus, das entfernt werden soll.
- 5 Klicken Sie unter „ID des primären privaten VLANs“ auf **Entfernen** und klicken Sie auf **OK**.

Beim Entfernen eines primären privaten VLANs werden auch alle zugeordneten sekundären privaten VLANs entfernt.

Entfernen eines sekundären privaten VLAN

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

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bearbeiten eines Distributed Switches verfügen.
- Bevor Sie ein privates VLAN entfernen, stellen Sie sicher, dass keine Portgruppen für seine Verwendung konfiguriert sind.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie die Registerkarte **Privates VLAN** aus.
- 4 Wählen Sie ein primäres privates VLAN aus, um die ihm zugewiesenen sekundären privaten VLANs anzuzeigen.
- 5 Wählen Sie das sekundäre private VLAN aus, das entfernt werden soll.
- 6 Klicken Sie unter „ID des sekundären privaten VLANs“ auf **Entfernen** und klicken Sie auf **OK**.

Verwalten physischer Adapter

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

Hinzufügen eines Uplinks zu einem vSphere Distributed Switch

Für jeden Host, der mit einem vSphere Distributed Switch verbunden ist, müssen Sie dem vSphere Distributed Switch mindestens einen physischen Netzwerkadapter oder Uplink zuweisen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie die Ansicht **vSphere Distributed Switch** aus.
- 4 Klicken Sie auf **Physische Adapter verwalten**.
- 5 Klicken Sie für den Uplink-Port, zu dem ein Uplink hinzugefügt werden soll, auf **Klicken Sie, um eine Netzwerkkarte hinzuzufügen**.
- 6 Wählen Sie den physischen Adapter aus, der hinzugefügt werden soll.
Wenn Sie einen Adapter auswählen, der mit einem anderen Switch verbunden ist, wird er von diesem Switch entfernt und diesem vSphere Distributed Switch neu zugeordnet.
- 7 Klicken Sie auf **OK**.

Entfernen eines Uplinks aus einem vSphere Distributed Switch

Sie können einen Uplink bzw. physischen Netzwerkadapter von einem vSphere Distributed Switch entfernen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie die Ansicht **vSphere Distributed Switch** aus.
- 4 Klicken Sie auf **Physische Adapter verwalten**.
- 5 Klicken Sie auf **Entfernen**, um den Uplink aus dem vSphere Distributed Switch zu entfernen.
- 6 Klicken Sie auf **OK**.

Entfernen von Netzwerkkarten aus aktiven virtuellen Maschinen

Wenn Sie Netzwerkkarten aus aktiven virtuellen Maschinen entfernen, werden die entfernten Netzwerkkarten möglicherweise weiterhin im vSphere-Client angezeigt.

Entfernen von Netzwerkkarten von einer aktiven virtuellen Maschine ohne installiertes Gastbetriebssystem

Sie können Netzwerkkarten nicht von einer aktiven virtuellen Maschine entfernen, wenn auf der virtuellen Maschine kein Betriebssystem installiert ist.

Der vSphere-Client meldet möglicherweise, dass die Netzwerkkarte entfernt wurde, aber sie wird weiterhin als der virtuellen Maschine zugehörig angezeigt.

Entfernen von Netzwerkkarten von einer aktiven virtuellen Maschine mit installiertem Gastbetriebssystem

Sie können eine Netzwerkkarte von einer aktiven virtuellen Maschine entfernen, aber dies wird dem vSphere-Client möglicherweise erst einige Zeit später gemeldet. Wenn Sie das Dialogfeld **Einstellungen bearbeiten** für die virtuelle Maschine öffnen, wird die Netzwerkkarte, die Sie entfernt haben, möglicherweise weiterhin angezeigt, selbst wenn die Aufgabe abgeschlossen ist. Das Dialogfeld **Einstellungen bearbeiten** für die virtuelle Maschine zeigt die Netzwerkkarte nicht sofort als entfernt an.

Die Netzwerkkarte wird möglicherweise weiterhin als der virtuellen Maschine zugeordnet angezeigt, wenn das Gastbetriebssystem der virtuellen Maschine das Entfernen von Netzwerkkarten im laufenden Betrieb nicht unterstützt.

Verwalten von virtuellen Netzwerkadaptern

Virtuelle Netzwerkadapter verwalten Netzwerkdienste eines Hosts über einen vSphere Distributed Switch.

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

Erstellen eines VMkernel-Netzwerkadapters auf einem vSphere Distributed Switch

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Distributed Switch“ aus.
- 4 Klicken Sie auf **Virtuelle Adapter verwalten**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Wählen Sie **Neuer virtueller Adapter** und klicken Sie auf **Weiter**.
- 7 Wählen Sie **VMkernel (VMkernel)** aus, und klicken Sie auf **Weiter**.

- 8 Wählen Sie für den virtuellen Adapter eine Verbindung über einen verteilten Port oder über eine verteilte Portgruppe.

Option	Beschreibung
Portgruppe auswählen	Wählen Sie im Dropdown-Menü die verteilte Portgruppe aus, zu der der virtuelle Adapter eine Verbindung herstellen soll.
Port auswählen	Geben Sie die Port-ID des verteilten Ports für den virtuellen Netzweradapter ein, zu dem eine Verbindung hergestellt werden soll.

- 9 Wählen Sie **Diesen virtuellen Adapter für vMotion verwenden**, damit diese Portgruppe auf einem anderen ESXi-Host für sich werben kann als die Netzwerkverbindung, an die vMotion-Datenverkehr gesendet wird.

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

- 10 Entscheiden Sie, ob Sie **Diesen virtuellen Adapter für die Fault Tolerance-Protokollierung verwenden** möchten.
- 11 Wählen Sie, ob Sie **Diesen virtuellen Adapter für den Verwaltungsdatenverkehr verwenden** möchten, und klicken Sie auf **Weiter**.
- 12 Geben Sie unter „IP-Einstellungen“ die IP-Adresse und die Subnetzmaske an.
IPv6 kann nicht mit einem abhängigen Hardware-iSCSI-Adapter verwendet werden.
- 13 Klicken Sie auf **Bearbeiten**, um das VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. vMotion, NAS und iSCSI, zu verwenden.
- 14 Auf der Registerkarte **DNS-Konfiguration** ist standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen.
- 15 Geben Sie auf der Registerkarte **Routing** die Gateway-Angaben für den VMkernel ein. Ein Gateway wird zur Verbindung mit Computern benötigt, die sich nicht im selben IP-Subnetz wie der VMkernel befinden.

Statische IP-Einstellungen sind voreingestellt. Verwenden Sie kein Routing mit Software-iSCSI-Multipathing-Konfigurationen oder mit abhängigen Hardware-iSCSI-Adaptern.
- 16 Klicken Sie auf **OK** und dann auf **Weiter**.
- 17 Klicken Sie auf **Beenden**.

Migrieren eines vorhandenen virtuellen Adapters auf einen vSphere Distributed Switch

Sie können einen vorhandenen virtuellen Adapter von einem vSphere Standard-Switch zu einem vSphere Distributed Switch migrieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Distributed Switch“ aus.
- 4 Klicken Sie auf **Virtuelle Adapter verwalten**.

- 5 Klicken Sie auf **Hinzufügen**.
- 6 Wählen Sie **Vorhandene virtuelle Netzwerkadapter migrieren** und klicken Sie auf **Weiter**.
- 7 Wählen Sie mindestens einen zu migrierenden virtuellen Netzwerkadapter aus.
- 8 Wählen Sie für jeden ausgewählten Adapter eine Portgruppe aus dem Dropdown-Menü **Portgruppe auswählen** aus.
- 9 Klicken Sie auf **Weiter**.
- 10 Klicken Sie auf **Beenden**.

Migrieren eines virtuellen Adapters auf einen vSphere Standard-Switch

Sie können einen vorhandenen virtuellen Adapter von einem vSphere Distributed Switch zu einem vSphere Standard-Switch migrieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Distributed Switch“ aus.
- 4 Klicken Sie auf **Virtuelle Adapter verwalten**.
- 5 Wählen Sie den zu migrierenden virtuellen Adapter aus und klicken Sie auf **Migrieren**.
- 6 Wählen Sie den Standard-Switch aus, auf den der Adapter migriert werden soll, und klicken Sie auf **Weiter**.
- 7 Geben Sie eine **Netzwerkbezeichnung** und optional eine **VLAN-ID** für den virtuellen Adapter ein und klicken Sie auf **Weiter**.
- 8 Klicken Sie auf **Beenden**, um den Assistenten abzuschließen und den virtuellen Adapter zu migrieren.

Bearbeiten der VMkernel-Konfiguration für einen vSphere Distributed Switch

Sie können einen virtuellen Netzwerkadapter von VMkernel auf einem vSphere Distributed Switch bearbeiten, um die IP-Einstellungen, z. B. die IP-Adresse, die Subnetzmaske, das Standard-Gateway und die DNS-Konfiguration, zu ändern. Sie können auch auswählen, ob der virtuelle Adapter für vMotion oder für die Fehlertoleranzprotokollierung verwendet werden soll.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Distributed Switch“ aus.
- 4 Klicken Sie auf **Virtuelle Adapter verwalten**.
- 5 Wählen Sie den VMkernel-Adapter aus, der geändert werden soll, und klicken Sie auf **Bearbeiten**.
- 6 Wählen Sie zum Hinzufügen dieses virtuellen Adapters unter „Netzwerkverbindung“ **vSphere Distributed Switch** und **Portgruppe** oder **Port** aus.

- 7 Wählen Sie **Diesen virtuellen Adapter für vMotion verwenden**, um dieser Portgruppe zu ermöglichen, bei einem anderen Host als die Netzwerkverbindung, über die der vMotion-Datenverkehr gesendet werden soll, zu werben.

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

- 8 (Optional) Wählen Sie **Diesen virtuellen Adapter für die Fehlertoleranzprotokollierung verwenden**.

- 9 (Optional) Wählen Sie **Diesen virtuellen Adapter für den Verwaltungsdatenverkehr verwenden**.

- 10 Geben Sie unter „IP-Einstellungen“ die **IP-Adresse** und die **Subnetzmaske** an oder wählen Sie **IP-Einstellungen automatisch abrufen**.

- 11 Klicken Sie auf **Bearbeiten**, um das VMkernel-Standard-Gateway für VMkernel-Dienste, wie z. B. vMotion, NAS und iSCSI, zu verwenden.

Der Name des Hosts erscheint standardmäßig im Namensfeld der Registerkarte **DNS-Konfiguration**. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.

Ein Gateway wird auf der Registerkarte **Routing** für die Verbindung mit Maschinen benötigt, die sich nicht in demselben IP-Subnetz wie der VMkernel befinden.

Statische IP-Einstellungen sind voreingestellt.

- 12 Verwenden Sie die Pfeile zum Setzen der MTU für den VMkernel-Adapter.

- 13 Klicken Sie auf **OK**.

Anzeigen von VMkernel-Routing-Informationen auf einem vSphere Distributed Switch

Sie können IP- und IPv6-Routing-Informationen wie Netzwerk, Präfix und Gateway für einen VMkernel-Netzwerkadapter auf einem vSphere Distributed Switch anzeigen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Klicken Sie in der Ansicht „vSphere Distributed Switch“ auf **Virtuelle Adapter verwalten**.
- 4 Wählen Sie den anzuzeigenden VMkernel-Adapter aus und klicken Sie unter „IP-Einstellungen“ oder „IPv6-Einstellungen“ auf **Routing-Tabelle anzeigen**.

Eine Routing-Tabelle mit Informationen über Netzwerk, Präfix und Gateway des ausgewählten VMkernel-Adapters wird angezeigt.

Entfernen eines virtuellen Adapters

Im Dialogfeld „Virtuelle Adapter verwalten“ können Sie einen virtuellen Netzwerkadapter aus einem vSphere Distributed Switch entfernen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Distributed Switch“ aus.
- 4 Klicken Sie auf **Virtuelle Adapter verwalten**.
- 5 Wählen Sie den zu entfernenden virtuellen Adapter aus und klicken Sie auf **Entfernen**.
Ein Dialogfeld mit der Meldung „Möchten Sie *Adaptername* wirklich löschen?“ wird angezeigt.
- 6 Klicken Sie auf **Ja**.

Konfigurieren von Netzwerken von virtuellen Maschinen auf einem vSphere Distributed Switch

Verbinden Sie virtuelle Maschinen mit einem vSphere Distributed Switch entweder durch die Konfiguration einer individuellen virtuellen Netzwerkkarte oder durch die Migration von Gruppen virtueller Maschinen vom vSphere Distributed Switch selbst.

Verbinden Sie virtuelle Maschinen mit vSphere Distributed Switches, indem Sie die ihnen zugewiesenen virtuellen Netzwerkadapter mit verteilten Portgruppen verbinden. Dies kann entweder für eine individuelle virtuelle Maschine durch Ändern der Konfiguration des Netzwerkadapters der virtuellen Maschine oder für eine Gruppe von virtuellen Maschinen durch ihre Migration von einem vorhandenen virtuellen Netzwerk auf einen vSphere Distributed Switch geschehen.

Migrieren von virtuelle Maschinen auf einen oder von einem vSphere Distributed Switch

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste auf das Datacenter und wählen Sie **Netzwerk virtueller Maschinen migrieren**.

Der Assistent zum Migrieren von Netzwerken virtueller Maschinen wird angezeigt.

- 3 Wählen Sie ein **Quellnetzwerk** aus, von dem Adapter migriert werden sollen.

Option	Beschreibung
Alle Netzwerkadapter der virtuellen Maschine berücksichtigen, die mit folgendem Netzwerk verbunden sind (Filtern nach Netzwerk):	Migriert VM-Netzwerkadapter von einem bestimmten Netzwerk. Wählen Sie das Quellnetzwerk aus dem Dropdown-Menü Netzwerk aus.
Alle Netzwerkadapter der virtuellen Maschine berücksichtigen, die mit folgendem Netzwerk verbunden sind (Filtern nach vDS):	Migriert VM-Netzwerkadapter von einem Netzwerk auf einem bestimmten vSphere Distributed Switch. Wählen Sie zum Migrieren von einem Netzwerk Switch und Netzwerk aus den Dropdown-Menüs aus.
Alle Netzwerkadapter der virtuellen Maschine berücksichtigen, die mit keinem Netzwerk verbunden sind	Migriert VM-Netzwerkadapter, die mit keinem Netzwerk verbunden sind.

- 4 Wählen Sie ein **Zielnetzwerk** aus, auf das die Adapter migriert werden sollen.

Option	Beschreibung
Filtern nach Netzwerk	Migriert VM-Netzwerkadapter auf ein bestimmtes Netzwerk. Wählen Sie das Zielnetzwerk aus dem Dropdown-Menü Netzwerk aus.
Filtern nach VDS	Migriert VM-Netzwerkadapter auf ein Netzwerk auf einem bestimmten vSphere Distributed Switch. Wählen Sie zum Migrieren auf ein Netzwerk Switch und Netzwerk aus den Dropdown-Menüs aus.

- 5 Klicken Sie auf **Weiter**.
- 6 (Optional) Markieren Sie eine virtuelle Maschine oder einen Adapter, um die entsprechenden Details anzuzeigen.
- 7 Wählen Sie die virtuellen Maschinen und Adapter aus, die auf das Zielnetzwerk migriert werden sollen, und klicken Sie auf **Weiter**.
- 8 Vergewissern Sie sich, dass das Quellnetzwerk, das Zielnetzwerk und die Anzahl der zu migrierenden virtuellen Maschinen korrekt sind, und klicken Sie auf **OK**.

Verbinden einer individuellen virtuellen Maschine mit einer verteilten Portgruppe

Verbinden Sie eine individuelle virtuelle Maschine durch Ändern ihrer Netzwerkkartenkonfiguration mit einem vSphere Distributed Switch.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Verwalten von Netzwerkressourcen

vSphere bietet mehrere unterschiedliche Methoden zur Vereinfachung der Verwaltung von Netzwerkressourcen.

Dieses Kapitel behandelt die folgenden Themen:

- [„vSphere Network I/O Control“](#), auf Seite 279
- [„TCP-Segmentierungs-Offload und Jumbo-Frames“](#), auf Seite 282
- [„DirectPath I/O“](#), auf Seite 284
- [„Single Root I/O Virtualization \(SR-IOV\)“](#), auf Seite 286

vSphere Network I/O Control

Verwenden Sie vSphere Network I/O Control, um geschäftskritischen Anwendungen Netzwerkbandbreite zuzuteilen und Situationen zu beheben, in denen verschiedene Datenverkehrstypen die gleichen Ressourcen beanspruchen.

Aktivieren von Network I/O Control auf einem vSphere Distributed Switch

Aktivieren Sie die Netzwerkressourcenverwaltung, um den Netzwerkverkehr mithilfe von Netzwerkressourcenpools nach Typ zu priorisieren.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Stellen Sie sicher, dass Ihr Datacenter wenigstens über einen vSphere Distributed Switch der Version 4.1.0 oder höher verfügt.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Ressourcenzuteilung** auf **Eigenschaften**.
- 4 Wählen Sie **Network I/O Control auf diesem vSphere Distributed Switch aktivieren** und klicken Sie auf **OK**.

Erstellen eines Netzwerkressourcenpools

Erstellen Sie benutzerdefinierte Netzwerkressourcenpools für die benutzerdefinierte Netzwerkressourcenverwaltung.

Benutzerdefinierte Netzwerkressourcenpools stehen nur auf vSphere Distributed Switches der Version 5.0.0 oder höher zur Verfügung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Ressourcenzuteilung** auf **Neuer Netzwerkressourcenpool**.
- 4 Geben Sie einen **Namen** für den Netzwerkressourcenpool ein.
- 5 (Optional) Geben Sie eine **Beschreibung** für den Netzwerkressourcenpool ein.
- 6 Wählen Sie die **Physischer Adapter - Anteile** für den Netzwerkressourcenpool aus.

Option	Beschreibung
Benutzerdefiniert	Geben Sie eine bestimmte Anzahl von Anteilen (von 1 bis 100) für diesen Netzwerkressourcenpool ein.
Hoch	Setzt die Anteile für diesen Ressourcenpool auf 100.
Normal	Setzt die Anteile für diesen Ressourcenpool auf 50.
Niedrig	Setzt die Anteile für diesen Ressourcenpool auf 25.

- 7 Geben Sie das **Hostlimit** für den Netzwerkressourcenpool in Megabits pro Sekunde an oder wählen Sie **Unbegrenzt** aus.
- 8 (Optional) Wählen Sie das **QoS-Prioritäts-Tag** für den Netzwerkressourcenpool aus.
- 9 Klicken Sie auf **OK**.

Der neue Ressourcenpool wird auf der Registerkarte **Ressourcenzuteilung** unter „Benutzerdefinierte Netzwerkressourcenpools“ angezeigt.

Weiter

Fügen Sie eine oder mehrere verteilte Portgruppen zum Netzwerkressourcenpool hinzu.

Hinzufügen oder Entfernen von verteilten Portgruppen von einem Netzwerkressourcenpool

Fügen Sie eine verteilte Portgruppe zu einem benutzerdefinierten Netzwerkressourcenpool hinzu, um den gesamten VM-Netzwerkdatenverkehr dieser verteilten Portgruppe in den Netzwerkressourcenpool aufzunehmen.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Erstellen Sie einen oder mehrere Netzwerkressourcenpools auf dem vSphere Distributed Switch.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Ressourcenzuteilung** auf **Portgruppen verwalten**.
- 4 (Optional) Wählen Sie aus dem Dropdown-Menü „Netzwerkressourcenpool“ den benutzerdefinierten Netzwerkressourcenpool aus, der mit einer einzelnen verteilten Portgruppe verknüpft werden soll, oder wählen Sie **Keiner**, um diese verteilte Portgruppe aus einem benutzerdefinierten Ressourcenpool zu entfernen.
- 5 (Optional) Wählen Sie den benutzerdefinierten Netzwerkressourcenpool aus, der mit mehreren verteilten Portgruppen verknüpft werden soll.
 - a Halten Sie die STRG-Taste gedrückt, um mehrere verteilte Portgruppen zum Ändern auszuwählen, und klicken Sie auf **Mehrere zuweisen**.
 - b Wählen Sie aus dem Dropdown-Menü „Netzwerkressourcenpool“ den benutzerdefinierten Netzwerkressourcenpool aus, der mit den verteilten Portgruppen verknüpft werden soll, oder wählen Sie **Keiner**, um die verteilten Portgruppen aus allen benutzerdefinierten Ressourcenpools zu entfernen.
- 6 Klicken Sie auf **OK**.

Bearbeiten von Einstellungen für den Netzwerkressourcenpool

Sie können für jeden Netzwerkressourcenpool Einstellungen, wie zugeteilte Anteile und Grenzwerte, ändern, um die Priorität des Netzwerkdatenverkehrs für den jeweiligen Netzwerkressourcenpool anzupassen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ressourcenzuteilung** auf den zu ändernden Ressourcenpool und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Wählen Sie die **Physischer Adapter - Anteile** für den Netzwerkressourcenpool aus.

Option	Beschreibung
Benutzerdefiniert	Geben Sie eine bestimmte Anzahl von Anteilen (von 1 bis 100) für diesen Netzwerkressourcenpool ein.
Hoch	Setzt die Anteile für diesen Ressourcenpool auf 100.
Normal	Setzt die Anteile für diesen Ressourcenpool auf 50.
Niedrig	Setzt die Anteile für diesen Ressourcenpool auf 25.

- 5 Geben Sie das **Hostlimit** für den Netzwerkressourcenpool in Megabits pro Sekunde an oder wählen Sie **Unbegrenzt** aus.
- 6 (Optional) Wählen Sie im Dropdown-Menü das **QoS-Prioritäts-Tag** aus.
Das QoS-Prioritäts-Tag definiert ein IEEE-802.1p-Tag, mit dem die Servicequalität auf der Ebene der Medienzugriffssteuerung ermöglicht wird
- 7 Klicken Sie auf **OK**.

Löschen eines Netzwerkressourcenpools

Sie können benutzerdefinierte Netzwerkressourcenpools löschen, die nicht mehr benötigt werden.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Entfernen aller verteilten Portgruppen aus einem Netzwerkressourcenpool

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie auf der Registerkarte **Ressourcenzuteilung** mit der rechten Maustaste auf den benutzerdefinierten Ressourcenpool, der gelöscht werden soll, und wählen Sie **Entfernen** aus.
- 4 Klicken Sie auf **Ja**.

TCP-Segmentierungs-Offload und Jumbo-Frames

Wenn Sie den TCP-Segmentierungs-Offload (TCP Segmentation Offload, TSO) auf einem VMkernel-Netzwerkadapter und auf virtuellen Maschinen sowie Jumbo-Frames auf einem vSphere Distributed Switch oder vSphere Standard-Switch verwenden, wird die Netzwerkleistung von virtuellen Maschinen und Infrastruktur-Workloads verbessert.

Aktivieren der TSO-Unterstützung für eine virtuelle Maschine

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

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

Aktivieren von Jumbo-Frames für eine VMkernel-Schnittstelle auf einem vSphere Standard-Switch

Jumbo-Frames reduzieren die CPU-Auslastung, die durch die Übertragung von Daten verursacht wird. Aktivieren Sie Jumbo-Frames auf einer VMkernel-Netzwerkschnittstelle, indem Sie die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der VMkernel-Schnittstelle ändern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Klicken Sie auf **Eigenschaften** für den vSphere Standard-Switch, der mit dem zu ändernden VMkernel verknüpft ist.
- 4 Wählen Sie auf der Registerkarte **Ports** die VMkernel-Schnittstelle aus und klicken Sie auf **Bearbeiten**.
- 5 Legen Sie **MTU** auf 9000 fest und klicken Sie auf **OK**.

Aktivieren von Jumbo-Frames auf einem vSphere Distributed Switch

Aktivieren Sie einen vSphere Distributed Switch für Jumbo-Frames, indem Sie die MTU-Größe für diesen Distributed Switch ändern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Eigenschaften** die Option **Erweitert** aus.
- 4 Legen Sie als **Maximalwert für MTU** den größten MTU-Wert der virtuellen Netzwerkadapter fest, die mit dem vSphere Distributed Switch verbunden sind, und klicken Sie auf **OK**.

Aktivieren der Jumbo Frame-Unterstützung auf einer virtuellen Maschine

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

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

DirectPath I/O

DirectPath-I/O ermöglicht den Zugriff virtueller Maschinen auf physische PCI-Funktionen auf Plattformen mit einer E/A-Arbeitsspeicherverwaltungseinheit.

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

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

Die folgenden Funktionen sind nur für virtuelle Maschinen verfügbar, die mit DirectPath I/O auf Cisco Unified Computing Systems (UCS) über Cisco Virtual Machine Fabric Extender (VM-FEX) Distributed Switches konfiguriert sind.

- vMotion
- Hinzufügen und Entfernen von virtuellen Geräten bei laufendem Betrieb
- Anhalten und Fortsetzen
- Hohe Verfügbarkeit

- DRS
- Snapshots

Detaillierte Informationen über unterstützte Switches und Switch-Konfigurationen finden Sie in der Dokumentation zu Cisco VM-FEX.

Konfigurieren von Passthrough-Geräten auf einem Host

Sie können Passthrough-Netzwerkgeräte auf einem Host konfigurieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Die Seite Passthrough-Konfiguration wird angezeigt. Auf ihr werden alle verfügbaren Passthrough-Geräte aufgelistet. Ein grünes Symbol bedeutet, dass ein Gerät aktiviert und aktiv ist. Ein orangefarbenes Symbol bedeutet, dass sich der Status des Geräts geändert hat und der Host neu gestartet werden muss, bevor das Gerät verwendet werden kann.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie die für das Passthrough zu verwendenden Geräte aus und klicken Sie auf **OK**.

Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

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

Aktivieren von DirectPath I/O mit vMotion auf einer virtuellen Maschine

Sie können DirectPath I/O mit vMotion für virtuelle Maschinen in einem Datencenter auf einem Cisco UCS-System aktivieren, das über mindestens einen unterstützten Cisco UCS Virtual Machine Fabric Extender (VM-FEX) Distributed Switch verfügt.

Voraussetzungen

- Aktivieren Sie Hochleistungsnetzwerk-E/A in mindestens einem Cisco UCS-Portprofil auf einem unterstützten Cisco VM-FEX Distributed Switch. Weitere Informationen über unterstützte Switches und Switch-Konfigurationen finden Sie in der Cisco-Dokumentation unter <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

- Schalten Sie die virtuelle Maschine aus.

Vorgehensweise

- 1 Melden Sie sich bei vSphere Client an und wählen Sie die Bestandslistenansicht „VMs und Vorlagen“.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Ressourcen** die Option **Arbeitsspeicher** aus.
- 4 Wählen Sie **Unbegrenzt**.
- 5 Wählen Sie auf der Registerkarte **Hardware** den zu konfigurierenden Netzwerkadapter als Passthrough-Gerät aus.
- 6 Wählen Sie ein Portprofil, bei dem Hochleistung aktiviert ist, aus dem Dropdown-Menü „Netzwerkbezeichnung“ aus und klicken Sie auf **OK**.
- 7 Schalten Sie die virtuelle Maschine ein.

Nachdem die virtuelle Maschine eingeschaltet wurde, erscheint DirectPath I/O auf der Registerkarte **Hardware** des Dialogfelds „Eigenschaften der virtuellen Maschine“ als „Aktiv“.

Single Root I/O Virtualization (SR-IOV)

vSphere 5.1 und höhere Releases unterstützen „Single Root I/O Virtualization“ (SR-IOV). Sie können SR-IOV für Netzwerke von virtuellen Maschinen verwenden, die latenzsensitiv sind oder weitere CPU-Ressourcen erfordern.

Überblick über SR-IOV

SR-IOV ist eine Spezifikation, wodurch ein einzelnes PCIe-Gerät (PCIe, Peripheral Component Interconnect Express) unter dem Root-Port dem Hypervisor oder dem Gastbetriebssystem als mehrere separate physische Geräte angezeigt wird.

SR-IOV verwendet physische Funktionen (PFs) und virtuelle Funktionen (VFs), um globale Funktionen für die SR-IOV-Geräte zu verwalten. PFs sind vollständige PCIe-Funktionen, die in der Lage sind, die SR-IOV-Funktion zu konfigurieren und zu verwalten. Es ist möglich, PCIe-Geräte unter Verwendung von PFs zu konfigurieren bzw. zu steuern, und die PF hat die Fähigkeit, Daten auf das und von dem Gerät zu verschieben. VFs sind leichtgewichtige PCIe-Funktionen, die Datenflüsse unterstützen, aber über einen eingeschränkten Satz Konfigurationsressourcen verfügen.

Die Anzahl der virtuellen Funktionen, die dem Hypervisor oder dem Gastbetriebssystem bereitgestellt werden, hängt vom Gerät ab. SR-IOV-aktivierte PCIe-Geräte erfordern entsprechende BIOS- und Hardwareunterstützung sowie SR-IOV-Unterstützung auf dem Treiber des Gastbetriebssystems oder der Hypervisor-Instanz. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Netzwerken*.

Verwenden von SR-IOV in vSphere

In vSphere kann eine virtuelle Maschine eine virtuelle SR-IOV-Funktion für Netzwerkfunktionen verwenden. Die virtuelle Maschine und der physische Adapter tauschen Daten direkt aus, ohne den VMkernel als Zwischenkomponente zu nutzen. Durch die Umgehung des VMkernel für Netzwerkfunktionen wird die Latenz reduziert und die CPU-Effizienz verbessert.

In vSphere 5.5 und höher verarbeitet zwar kein virtueller Switch (Standard-Switch oder Distributed Switch) den Netzwerkverkehr einer SR-IOV-aktivierten virtuellen Maschine, die mit dem Switch verbunden ist; Sie können aber die zugewiesenen virtuellen Funktionen steuern, indem Sie die Switch-Konfigurationsrichtlinien auf Portgruppen- oder Portebene nutzen.

Konfigurieren von SR-IOV in einem Hostprofil

Bevor Sie eine virtuelle Maschine mit einer virtuellen Funktion verknüpfen können, müssen Sie die virtuellen Funktionen der physischen Netzwerkkarte auf Ihrem Host mithilfe eines Hostprofils konfigurieren.

Sie können auch virtuelle SR-IOV-Funktionen auf dem Host aktivieren, indem Sie entsprechend der Treiberdokumentation den vCLI-Befehl `esxcli system module parameters set` im Netzwerkkarten-Treiberparameter für virtuelle Funktionen verwenden. Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Dokumentation zur vSphere-Befehlszeilenschnittstelle*.

Voraussetzungen

- Stellen Sie sicher, dass die Konfiguration Ihrer Umgebung SR-IOV unterstützt. Informationen hierzu finden Sie unter [SR-IOV-Unterstützung](#).
- Erstellen Sie ein Hostprofil unter Verwendung des SR-IOV-fähigen Hosts als Referenz. Weitere Informationen zu Hostprofilen finden Sie in der Dokumentation *vSphere-Hostprofile*.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere Client auf **Home** und wählen Sie die Hauptansicht **Hostprofile** aus.
- 2 Wählen Sie das Hostprofil aus der Liste aus und klicken Sie auf **Profil bearbeiten**.
- 3 Erweitern Sie Konfiguration des Kernelmoduls > Kernelmodul und wählen Sie das Kernelmodul für den physischen Funktionstreiber aus.
- 4 Erweitern Sie den **Kernelmodulparameter** und wählen Sie den Parameter des physischen Funktionstreibers zum Erstellen virtueller Funktionen aus.

Beispielsweise lautet der Parameter des physischen Funktionstreibers einer physischen Intel-Netzwerkkarte **max_vfs**.

- 5 Klicken Sie auf **Bearbeiten**.

- 6 Geben Sie im Textfeld **Wert** eine kommagetrennte Liste mit gültigen Anzahlwerten für virtuelle Funktionen ein.

Jeder Listeneintrag besteht aus der Anzahl der virtuellen Funktionen, die Sie für jede physische Funktion konfigurieren möchten. Der Wert 0 bedeutet, dass SR-IOV für diese physische Funktion nicht aktiviert wird.

Beispiel: Wenn Sie einen Dual Port haben, definieren Sie die Anzahl mit

x,y

wobei x oder y die Anzahl der virtuellen Funktionen ist, die Sie für einen einzelnen Port aktivieren möchten.

Wenn die Zielanzahl virtueller Funktionen auf einem einzelnen Host 30 ist, verfügen Sie möglicherweise über zwei Dual-Port-Karten, die auf 0,10,10,10 festgelegt sind.

HINWEIS Die Anzahl an virtuellen Funktionen, die für die Konfiguration unterstützt wird und verfügbar ist, hängt von der Systemkonfiguration ab.

- 7 Klicken Sie auf **OK**.
- 8 Standardisieren Sie das geänderte Hostprofil für den Zielhost.

Nachdem die virtuellen Funktionen auf dem Host aktiviert wurden, wird die physische Netzwerkkarte in der Liste **Netzwerkadapter** auf der Registerkarte **Konfiguration** für den Host nicht mehr als Hostnetzwerkadapter angezeigt. Sie wird in der Liste **Erweiterte Einstellungen** für den Host angezeigt.

Weiter

Verknüpfen Sie eine virtuelle Funktion mit einer virtuellen Maschine als PCI-Gerät für die Vernetzung über Direct Path I/O.

Zuweisen einer virtuellen Funktion zu einer virtuellen Maschine

Um sicherzustellen, dass eine virtuelle Maschine und eine physische Netzwerkkarte Daten austauschen können, müssen Sie eine virtuelle Maschine mit einer oder mehreren virtuellen Funktionen verknüpfen.

Nach der Aktivierung der virtuellen Funktionen auf dem Host steht jede Funktion als PCI-Gerät zur Verfügung.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Voraussetzungen

- Stellen Sie sicher, dass die Konfiguration Ihrer Umgebung SR-IOV unterstützt. Informationen hierzu finden Sie unter [SR-IOV-Unterstützung](#).
- Stellen Sie sicher, dass die virtuellen Funktionen auf dem Host vorhanden sind.
- Stellen Sie sicher, dass das Passthrough-Netzwerkgerät für die virtuelle Funktion auf dem Host aktiv ist.

Vorgehensweise

- 1 Wählen Sie eine virtuelle Maschine aus dem Bestandslistenbereich des vSphere-Clients aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie im Menü **Bestandsliste** den Befehl **Virtuelle Maschine > Einstellungen bearbeiten**.
- 4 Wählen Sie auf der Registerkarte **Ressourcen** die Option **Arbeitsspeicher** aus.
- 5 Wählen Sie **Unbegrenzt**.
- 6 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.

- 7 Wählen Sie **PCI-Gerät** und klicken Sie auf **Weiter**.
- 8 Wählen Sie im Dropdown-Menü die virtuelle Funktion aus.
- 9 Klicken Sie auf **Beenden**.
- 10 Schalten Sie die virtuelle Maschine ein.

Wird eine virtuelle Funktion als PCI-Gerät zu einer virtuellen Maschine hinzugefügt, wird die Größe der Arbeitsspeicherreservierung auf die Arbeitsspeichergröße der virtuellen Maschine festgelegt.

Konfigurieren des Passthrough-Geräts für eine virtuelle Funktion

Nachdem Sie eine virtuelle Maschine mit einer virtuellen Funktion als PCI-Gerät konfiguriert haben, können Sie die virtuelle Funktion mit einer statischen MAC-Adresse und einem Standard-VLAN mithilfe des vSphere Clients konfigurieren.

Sie können in der .vmx-Konfigurationsdatei der virtuellen Maschine der virtuellen Funktion eine statische MAC-Adresse und ein Standard-VLAN zuweisen.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Funktion der virtuellen Maschine als PCI-Gerät zugewiesen wurde.

Vorgehensweise

- 1 Wählen Sie eine virtuelle Maschine aus dem Bestandslistenbereich des vSphere-Clients aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie im Menü **Bestandsliste** den Befehl **Virtuelle Maschine > Einstellungen bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie unter **Erweitert** die Option **Allgemein** aus.
- 5 Klicken Sie auf **Konfiguration**.
- 6 Um eine statische MAC-Adresse zuzuweisen, fügen Sie die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Parameter	Wert
pciPassthruX.MACAddressType	statisch
pciPassthruX.MACAddress	<i>MAC_address_of_the_virtual_function</i>

Das X neben pciPassthru steht für die fortlaufende Nummer des PCI-Geräts in der virtuellen Maschine. Beispielsweise steht die 0 in pciPassthru0 für die Einstellungen des PCI-Geräts, das zuerst zur virtuellen Maschine hinzugefügt wurde.

- 7 Um ein Standard-VLAN zuzuweisen, fügen Sie den Parameter pciPassthruX.defaultVlan entsprechend den folgenden Werterichtlinien hinzu bzw. bearbeiten Sie ihn. Das X neben pciPassthru steht für die fortlaufende Nummer des PCI-Geräts in der virtuellen Maschine.

Option	Beschreibung
0	Kein VLAN und kein Gast-VLAN-Tagging zulassen. Auf diese Weise wird das Gast-VLAN-Tagging administrativ verhindert.
1 -4095	Nur Gekennzeichnete, aber kein Gast-VLAN-Tagging zulassen.
Kein Eintrag	Nur Nicht-Gekennzeichnete und Gast-VLAN-Tagging zulassen.

- 8 Klicken Sie auf **OK**.
- 9 Schalten Sie die virtuelle Maschine ein.

Netzwerkrichtlinien

Richtlinien, die auf der Ebene der Standard-Switches oder der verteilten Portgruppen festgelegt werden, gelten für alle Portgruppen auf dem Standard-Switch bzw. für alle Ports in der verteilten Portgruppe. Ausnahmen bilden die Konfigurationsoptionen, die auf der Ebene der Standard-Portgruppe oder der verteilten Ports außer Kraft gesetzt werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch“, auf Seite 291
- „Teaming- und Failover-Richtlinie“, auf Seite 293
- „VLAN-Richtlinie“, auf Seite 302
- „Sicherheitsrichtlinie“, auf Seite 305
- „Traffic-Shaping-Richtlinie“, auf Seite 309
- „Ressourcenzuteilungsrichtlinie“, auf Seite 313
- „Überwachungsrichtlinie“, auf Seite 314
- „Portblockierungsrichtlinien“, auf Seite 315
- „Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch“, auf Seite 316

Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch

Netzwerkrichtlinien werden auf vSphere Standard Switches und vSphere Distributed Switches unterschiedlich angewandt. Nicht alle für einen vSphere Distributed Switch verfügbaren Richtlinien sind auch für einen vSphere Standard Switch verfügbar.

Tabelle 22-1. Virtual Switch-Objekte, für die Richtlinien gelten

Virtueller Switch	Virtual Switch-Objekt	Beschreibung
vSphere Standard-Switch	Gesamter Switch	Wenn Sie Richtlinien auf den gesamten Standard-Switch anwenden, werden die Richtlinien auf alle Standardportgruppen auf dem Switch ausgeweitet.
	Standard-Portgruppe	Sie können unterschiedliche Richtlinien auf einzelne Portgruppen anwenden, indem Sie die vom Switch vererbten Richtlinien außer Kraft setzen.

Tabelle 22-1. Virtual Switch-Objekte, für die Richtlinien gelten (Fortsetzung)

Virtueller Switch	Virtual Switch-Objekt	Beschreibung
vSphere Distributed Switch	Verteilte Portgruppe	Wenn Sie Richtlinien auf eine verteilte Portgruppe anwenden, werden die Richtlinien an alle Ports in der Gruppe weitergegeben.
	Verteilter Port	Sie können unterschiedliche Richtlinien auf einzelne verteilte Ports anwenden, indem Sie die von der verteilten Portgruppe vererbten Richtlinien außer Kraft setzen.
	Uplink-Portgruppe	Sie können Richtlinien auf der Ebene der Uplink-Portgruppe anwenden, und die Richtlinien werden an alle Ports in der Gruppe weitergegeben.
	Uplink-Port	Sie können unterschiedliche Richtlinien auf einzelne Uplink-Ports anwenden, indem Sie die von der Uplink-Portgruppe vererbten Richtlinien außer Kraft setzen.

Tabelle 22-2. Verfügbare Richtlinien für einen vSphere Standard Switch und vSphere Distributed Switch

Richtlinie	Standard-Switch	Distributed Switch	Beschreibung
Teaming und Failover	Ja	Ja	Damit können Sie die physischen Netzwerkkarten konfigurieren, die den Netzwerkverkehr für einen Standard-Switch, eine Standard-Portgruppe, eine verteilte Portgruppe oder einen verteilten Port bearbeiten. Sie ordnen die physischen Netzwerkkarten in einer Failover-Reihenfolge an und wenden unterschiedliche Lastausgleichsrichtlinien darauf an.
Sicherheit	Ja	Ja	Bietet Schutz des Datenverkehrs vor der Imitation von MAC-Adressen und unerwünschten Portprüfungen. Die Netzwerksicherheitsrichtlinie ist in Schicht 2 des Netzwerk-Protokoll-Stacks implementiert.
Traffic-Shaping	Ja	Ja	Damit beschränken Sie die Netzwerkbandbreite, die Ports zur Verfügung steht, ermöglichen aber auch Datenverkehr-Bursts mit höherer Geschwindigkeit. ESXi steuert den ausgehenden Netzwerkverkehr auf Standard-Switches sowie den ein- und ausgehenden Datenverkehr auf Distributed Switches.
VLAN	Ja	Ja	Damit können Sie VLAN-Tagging für einen Standard- oder Distributed Switch konfigurieren. Sie können External Switch Tagging (EST), Virtual Switch Tagging (VST) und Virtual Guest Tagging (VGT) konfigurieren.
Überwachen	Nein	Ja	Aktiviert und deaktiviert die NetFlow-Überwachung an einem verteilten Port oder einer Portgruppe.
Filtern und Markieren des Datenverkehrs	Nein	Ja	Ermöglicht den Schutz des virtuellen Netzwerks vor unerwünschtem Datenverkehr und Sicherheitsangriffen bzw. die Anwendung eines QoS-Tag auf einen bestimmten Datenverkehrstyp.
Ressourcenzuteilung	Nein	Ja	Ermöglicht die Zuordnung eines verteilten Ports oder einer Portgruppe zu einem benutzerdefinierten Netzwerkressourcenpool. So können Sie die für den Port oder die Portgruppe verfügbare Bandbreite besser kontrollieren. Die Ressourcenzuteilungsrichtlinie kann für vSphere Network I/O Control Version 2 und 3 verwendet werden.
Portblockierung	Nein	Ja	Ermöglicht die selektive Blockierung von Ports für das Senden und Empfangen von Daten.

Teaming- und Failover-Richtlinie

Anhand der NIC-Gruppierung können Sie die Netzwerkkapazität eines virtuellen Switch erhöhen, indem Sie zwei oder mehr physische Netzwerkkarten in einer Gruppe zusammenfassen. Um zu bestimmen, wie der Datenverkehr im Fall eines Adapterfehlers umgeleitet wird, schließen Sie physische Netzwerkkarten in einer Failover-Reihenfolge ein. Um zu bestimmen, wie der virtuelle Switch den Netzwerkdatenverkehr zwischen den physischen Netzwerkkarten in einer Gruppe verteilt, wählen Sie Lastausgleichsalgorithmen aus, die sich für die Bedürfnisse und Kapazitäten Ihrer Umgebung eignen.

NIC-Gruppierungsrichtlinien

Anhand der NIC-Gruppierung können Sie einen virtuellen Switch mit mehreren physischen Netzwerkkarten auf einem Host verbinden, um die Netzwerkbandbreite des Switch zu erhöhen und Redundanz bereitzustellen. Eine NIC-Gruppe kann den Datenverkehr zwischen ihren Mitgliedern verteilen und bei einem Adapterfehler oder einem Netzerkausfall passives Failover bereitstellen. NIC-Gruppierungsrichtlinien werden für einen vSphere Standard Switch auf der Ebene des virtuellen Switch oder der Portgruppe und für einen vSphere Distributed Switch auf der Ebene des Ports oder der Portgruppe festgelegt.

HINWEIS Alle Ports am physischen Switch in der gleichen Gruppe müssen sich in der gleichen Broadcast-Domäne der Ebene 2 befinden.

Lastausgleichsrichtlinie

Die Lastausgleichsrichtlinie bestimmt, wie der Netzwerkdatenverkehr zwischen den Netzwerkadaptern in einer NIC-Gruppe verteilt wird. Bei virtuellen vSphere-Switches erfolgt der Lastausgleich nur für den ausgehenden Datenverkehr. Der eingehende Datenverkehr wird durch die Lastausgleichsrichtlinie auf dem physischen Switch gesteuert.

Weitere Informationen zu den einzelnen Lastausgleichsalgorithmen finden Sie in der Dokumentation zu *vSphere-Netzwerken*.

Richtlinie für die Netzerkausfallerkennung

Sie können eine der folgenden Methoden festlegen, die von einem virtuellen Switch für die Ausfallerkennung verwendet werden.

Nur Verbindungsstatus

Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Ermittelt Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches. Der Verbindungsstatus ermittelt jedoch nicht die folgenden Konfigurationsfehler:

- Die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN.
- Nicht angeschlossene Kabel zwischen einem physischen Switch und einem anderen Netzwerkgerät, z. B. einem Upstream-Switch.

Signalprüfung

Sendet Ethernet-Broadcast-Frames und hört diese ab (Signalprüfung), welche von physischen Netzwerkkarten gesendet werden, um Verbindungsfehler in allen physischen Netzwerkkarten in einer Gruppe zu ermitteln. ESXi-Hosts senden jede Sekunde Signalkpakete. Die Signalprüfung eignet sich am besten zur Fehlerermittlung in dem physischen Switch, der dem ESXi-Host am nächsten liegt, bei dem der Fehler kein „Link deaktiviert“-Ereignis für den Host verursacht.

Verwenden Sie die Signalprüfung bei mindestens drei Netzwerkkarten in einer Gruppe, da ESXi Fehler eines einzelnen Adapters erkennen kann. Wenn nur zwei Netzwerkkarten zugewiesen sind und für eine der Netzwerkkarten die Verbindung getrennt wird, kann der Switch nicht ermitteln, welche Netzwerkkarte außer Betrieb genommen werden muss, da beide Netzwerkkarten keine Signale empfangen und demzufolge alle Pakete an beide Uplinks gesendet werden. Die Verwendung von mindestens drei Netzwerkkarten in einer solchen Gruppe erlaubt $n-2$ Fehler, wobei n für die Anzahl der Netzwerkkarten in der Gruppe steht, bevor eine unklare Situation eintritt.

Failback-Richtlinie

Standardmäßig ist für eine NIC-Gruppe eine Failback-Richtlinie aktiviert. Wenn eine ausgefallene physische Netzwerkkarte wieder online geht, legt der virtuelle Switch die Netzwerkkarte wieder als aktiv fest, indem die Standby-Netzwerkkarte ersetzt wird, die deren Steckplatz übernommen hatte.

Wenn die physische Netzwerkkarte, die in der Failover-Reihenfolge an erster Stelle steht, immer wieder ausfällt, kann die Failback-Richtlinie häufige Änderungen der verwendeten Netzwerkkarte verursachen. Der physische Switch stellt häufige Änderungen der MAC-Adressen fest, und möglicherweise akzeptiert der Port des physischen Switch nicht sofort Datenverkehr, wenn der Adapter online geschaltet wird. Um diese Verzögerungen zu minimieren, können die folgenden Einstellungen des physischen Switch geändert werden:

- Deaktivieren Sie das Spanning-Tree-Protocol (STP) für physische Netzwerkkarten, die mit den ESXi-Hosts verbunden sind.
- Aktivieren Sie für Cisco-basierte Netzwerke den PortFast-Modus für Zugriffsschnittstellen oder den PortFast-Trunk-Modus für Trunk-Schnittstellen. Dadurch können ca. 30 Sekunden während der Initialisierung des Ports des physischen Switches eingespart werden.
- Deaktivieren Sie die Trunking-Aushandlung.

Richtlinie zur Switch-Benachrichtigung

Wenn Sie die Richtlinie zur Switch-Benachrichtigung verwenden, können Sie festlegen, wie der ESXi-Host über Failover-Ereignisse benachrichtigt. Wenn eine physische Netzwerkkarte eine Verbindung zum virtuellen Switch herstellt oder wenn der Datenverkehr zu einer anderen physischen Netzwerkkarte in der Gruppe umgeleitet wird, sendet der virtuelle Switch Benachrichtigungen über das Netzwerk, um die Lookup-Tabellen der physischen Switches zu aktualisieren. Durch das Benachrichtigen des physischen Switches wird die geringste Latenz bei Eintreten eines Failovers oder einer Migration mit vSphere vMotion erreicht.

Bearbeiten der Failover- und Lastausgleichsrichtlinie für einen vSphere Standard-Switch

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

Die Failover- und Lastausgleichs-Richtlinien beinhalten folgende Parameter:

- Lastausgleichsrichtlinie: Die Lastausgleichsrichtlinie legt fest, wie der ausgehende Datenverkehr über die Netzwerkadapter verteilt wird, die einem Standard-Switch zugewiesen wurden. Der eingehende Datenverkehr wird durch die Lastausgleichsrichtlinie auf dem physischen Switch gesteuert.
- Failover-Ermittlung: Verbindungsstatus/Signalprüfung
- Reihenfolge der Netzwerkadapter (Aktiv/Standby)

In manchen Fällen kann bei einem Failover oder Failback die Verbindung zum Standard-Switch unterbrochen werden. Dies führt dazu, dass die MAC-Adressen, die von diesem Standard-Switch zugeordneten virtuellen Maschinen verwendet werden, auf einem anderen Switch-Port als zuvor erscheinen. Um dieses Problem zu vermeiden, setzen Sie Ihren physischen Switch auf den Portfast- oder Portfast-Trunk-Modus.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie einen Standard-Switch aus und klicken Sie auf **Eigenschaften**.
- 4 Klicken Sie auf die Registerkarte **Ports (Ports)**.
- 5 Zum Bearbeiten der Einstellungen für **Failover- und Lastausgleich** wählen Sie das Standard-Switch-Element und klicken auf **Bearbeiten**.
- 6 Klicken Sie auf die Registerkarte **NIC-Gruppierung**.

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

- 7 Wählen Sie in der Liste **Lastausgleich** eine Option für die Art der Auswahl eines Uplinks.

Option	Beschreibung
Anhand der Quelle der Port-ID routen	Wählen Sie einen Uplink basierend auf dem virtuellen Port aus, durch den der Datenverkehr in den Standard-Switch gelangt ist.
Anhand des IP-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist.
Anhand des Quell-MAC-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs des Quell-Ethernets aus.
Ausdrückliche Failover-Reihenfolge verwenden	Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungskriterien erfüllt.

- 8 Wählen Sie in der Liste Netzwerk-Failover-Ermittlung die Option, die für die Failover-Ermittlung verwendet werden soll.

Option	Beschreibung
Nur Verbindungsstatus	Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, jedoch keine Konfigurationsfehler, wie z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches.
Signalprüfung	Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Durch diese Option können zahlreiche der oben genannten Ausfälle ermittelt werden, die durch den Verbindungsstatus allein nicht ermittelt werden können. HINWEIS Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.

- 9 Wählen Sie **Ja** oder **Nein**, um Switches bei einem Failover zu benachrichtigen.

Wenn Sie „Ja“ wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen Standard-Switch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte im Team geleitet wird, über das Netzwerk eine Benachrichtigung gesendet, um die Verweistabellen auf den physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Latenzzeiten für Failover-Ereignisse und Migrationen mit vMotion zu minimieren.

Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.

- 10 Wählen Sie **Ja** oder **Nein**, um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.

Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Failback-Funktion auf **Ja** (Standardeinstellung) gesetzt wird, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert; er ersetzt in diesem Fall den ggf. vorhandenen Standby-Adapter, der seinen Platz eingenommen hatte. Wenn diese Option auf **Nein** gesetzt wird, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.

- 11 **Failover-Reihenfolge** – Gibt an, wie die Arbeitslast für die Adapter verteilt wird.

Sie können diese Bedingung mithilfe des Dropdown-Menüs einstellen und die Adapter in zwei Gruppen aufteilen, um bestimmte Adapter zu verwenden und andere für Notfälle zu reservieren.

Option	Beschreibung
Aktive Adapter	Dieser Adapter wird weiter verwendet, wenn die Verbindung zum Netzwerkadapter verfügbar und aktiv ist.
Standby-Adapter	Dieser Adapter wird verwendet, wenn mindestens eine Verbindung zum aktiven Adapter nicht verfügbar ist.
Nicht verwendete Adapter	Verwenden Sie diesen Adapter nicht.

Wenn Sie iSCSI-Multipathing einsetzen, muss Ihre VMkernel-Schnittstelle über einen aktiven Adapter verfügen und darf keine Standby-Adapter aufweisen. Informationen finden Sie in der Dokumentation *vSphere-Speicher*.

HINWEIS Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.

Bearbeiten der Failover- und Lastausgleichsrichtlinie für eine Standard-Portgruppe

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie einen Standard-Switch aus und klicken Sie auf **Eigenschaften**.
- 4 Wählen Sie auf der Registerkarte **Ports** eine Portgruppe aus und klicken Sie auf **Bearbeiten**.

5 Klicken Sie auf die Registerkarte **NIC-Gruppierung**.

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

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

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

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

7 Klicken Sie auf **OK**.

Bearbeiten der Teaming-und-Failover-Richtlinie für eine verteilte Portgruppe

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.

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

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

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

- 5 Klicken Sie auf **OK**.

Bearbeiten von Gruppierungs- und Failover-Richtlinien für verteilte Ports

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Richtlinien**, um Port-Netzwerkrichtlinien anzuzeigen und zu ändern.

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

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

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

6 Klicken Sie auf **OK**.

VLAN-Richtlinie

Die VLAN-Richtlinien legen fest, wie VLANs in Ihrer Netzwerkumgebung funktionieren.

Ein virtuelles lokales Netzwerk (VLAN) ist eine Gruppe von Hosts mit einer gemeinsamen Gruppe von Anforderungen, die so kommunizieren, als wären sie an dieselbe Broadcast-Domäne angeschlossen, unabhängig von ihrem physischen Standort. Ein VLAN hat dieselben Attribute wie ein physisches lokales Netzwerk (LAN), ermöglicht aber das Gruppieren der Endstationen, auch wenn sie nicht an demselben Netzwerk-Switch angeschlossen sind.

Die VLAN-Richtlinien können verteilte Portgruppen und Ports sowie Uplink-Portgruppen und Ports umfassen.

Bearbeiten der VLAN-Richtlinie für eine verteilte Portgruppe

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.

- 4 Wählen Sie den Typ des VLAN-Filters und der Markierung aus dem Dropdown-Menü **VLAN-Typ** aus.

Option	Beschreibung
Keine	Verwenden Sie VLAN nicht. Verwenden Sie diese Option im Falle von External Switch Tagging.
VLAN	Kennzeichnen Sie den Datenverkehr mit der ID aus dem Feld VLAN-ID . Geben Sie eine Zahl zwischen 1 und 4094 für Virtual Switch Tagging ein.
VLAN-Trunking	Übergeben Sie den VLAN-Datenverkehr mit einer ID innerhalb des VLAN-Trunk-Bereichs an das Gastbetriebssystem. Sie können mithilfe einer kommagetrennten Liste mehrere Bereiche und individuelle VLANs festlegen. Verwenden Sie diese Option für Virtual Guest Tagging.
Privates VLAN	Ordnen Sie den Datenverkehr einem privaten VLAN zu, das auf dem Distributed Switch erstellt wurde.

- 5 Klicken Sie auf **OK**.

Bearbeiten von VLAN-Richtlinien für verteilte Ports oder Uplink-Ports

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Richtlinien**.
- 5 Wählen Sie den zu verwendenden **VLAN-Typ** aus.

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

- 6 Klicken Sie auf **OK**.

Bearbeiten der VLAN-Richtlinie für eine Uplink-Portgruppe

Legen Sie die VLAN-Richtlinie für eine Uplink-Portgruppe mit dem vSphere Client fest, um die Verarbeitung des VLAN-Datenverkehrs für alle Mitglieder-Uplinks zu konfigurieren.

Verwenden Sie die VLAN-Richtlinie auf Uplink-Portebene, um zum Filtern des Datenverkehrs einen Trunk-Bereich von VLAN-IDs an die physischen Netzwerkadapter weiterzuleiten. Die physischen Netzwerkadapter werfen die Pakete von anderen VLANs, sofern die Adapter das Filtern nach VLAN unterstützen. Das Festlegen eines Trunk-Bereichs optimiert die Netzwerkleistung, da physische Netzwerkadapter den Datenverkehr anstelle der Uplink-Ports in der Gruppe filtern.

Wenn Sie über einen physischen Netzwerkadapter verfügen, der den VLAN-Filter nicht unterstützt, sind die VLANs möglicherweise immer noch nicht blockiert. Konfigurieren Sie in diesem Fall den VLAN-Filter auf einer verteilten Portgruppe oder einem verteilten Port.

Weitere Informationen zur Unterstützung von VLAN-Filtern finden Sie in der technischen Dokumentation der Adapteranbieter.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die Uplink-Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie unter **Richtlinien** auf **VLAN** und geben Sie einen **VLAN-Trunk-Bereich** ein, der an die physischen Netzwerkadapter weitergeleitet werden soll.

Trennen Sie die Einträge beim Trunking mehrerer Bereiche und individueller VLANs durch Kommas.

- 4 Klicken Sie auf **OK**.

Bearbeiten der VLAN-Richtlinie für einen Uplink-Port

Legen Sie die VLAN-Richtlinie für einen Uplink-Port mit dem vSphere Client so fest, dass der VLAN-Datenverkehr über den Port anders als bei der übergeordneten Uplink-Portgruppe abgewickelt wird.

Verwenden Sie die VLAN-Richtlinie für den Uplink-Port, um zum Filtern des Datenverkehrs einen Trunk-Bereich von VLAN-IDs an den physischen Netzwerkadapter weiterzuleiten. Der physische Netzwerkadapter verwirft Pakete von anderen VLANs, sofern der Adapter das Filtern nach VLAN unterstützt. Das Festlegen eines Trunk-Bereichs optimiert die Netzwerkleistung, da der physische Netzwerkadapter den Datenverkehr anstelle des Uplink-Ports filtert.

Wenn Sie über einen physischen Netzwerkadapter verfügen, der den VLAN-Filter nicht unterstützt, sind die VLANs möglicherweise immer noch nicht blockiert. Konfigurieren Sie in diesem Fall den VLAN-Filter auf einer verteilten Portgruppe oder einem verteilten Port.

Weitere Informationen zur Unterstützung von VLAN-Filtern finden Sie in der technischen Dokumentation des Adapteranbieters.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Voraussetzungen

Aktivieren Sie die Außerkraftsetzungen auf Portebene, um die VLAN-Richtlinie auf Portebene außer Kraft zu setzen. Siehe [„Bearbeiten der erweiterten Einstellungen von verteilten Portgruppen“](#), auf Seite 47.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Wählen Sie unter **Richtlinien** die Option **VLAN** aus und klicken Sie auf **Außer Kraft setzen**.
- 5 Geben Sie einen **VLAN-Trunk-Bereich** ein, der an den physischen Netzwerkadapter weitergeleitet werden soll.

Trennen Sie die Einträge beim Trunking mehrerer Bereiche und individueller VLANs durch Kommas.

- 6 Klicken Sie auf **OK**.

Sicherheitsrichtlinie

Die Netzwerksicherheitsrichtlinie bietet Schutz des Datenverkehrs vor der Imitation von MAC-Adressen und unerwünschten Portprüfungen.

Die Sicherheitsrichtlinie eines Standard-Switches oder eines Distributed Switch ist auf Schicht 2 (Sicherungsschicht) des Netzwerkprotokoll-Stacks implementiert. Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen. Weitere Informationen zu möglichen Netzwerkbedrohungen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Bearbeiten der Sicherheitsrichtlinie für einen vSphere Standard-Switch

Sie können für einen vSphere Standard-Switch die die Schicht 2-Sicherheitsrichtlinie bearbeiten, wie z. B. MAC-Adressänderungen und gefälschte Übertragungen.

Schicht 2 ist die Sicherungsschicht. Die drei Elemente der Sicherheitsrichtlinie für Schicht 2 sind der Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen. Wenn der Promiscuous-Modus nicht aktiviert wurde, überwacht der Gastadapter nur Datenverkehr auf seiner eigenen MAC-Adresse. Im Promiscuous-Modus kann dieser alle Datenpakete überwachen. Standardmäßig ist der Promiscuous-Modus für die Gastadapter deaktiviert.

Für einzelne Standard-Portgruppen können die Einstellungen auf Switch-Ebene außer Kraft gesetzt werden, indem Sie die Einstellungen für die Portgruppe bearbeiten.

Weitere Informationen zur Sicherheit finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Klicken Sie für den Standard-Switch, dessen Sicherheitsrichtlinie für Schicht 2 Sie bearbeiten möchten, auf **Eigenschaften**.
- 4 Klicken Sie im Eigenschaftendialogfeld des Standard-Switches auf die Registerkarte **Ports**.
- 5 Wählen Sie das Standard-Switch-Element aus und klicken Sie auf **Bearbeiten**.
- 6 Klicken Sie auf die Registerkarte **Sicherheit**.

- 7 Im Bereich „Richtlinienausnahmen“ können Sie auswählen, ob die Ausnahmen für die Schicht 2-Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen – Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden. ■ Akzeptieren – Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSphere Standard-Switch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressenänderungen	<ul style="list-style-type: none"> ■ Ablehnen – Wenn die Option MAC-Adressenänderungen auf Ablehnen festgelegt ist und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der .vmx-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der .vmx-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet. ■ Akzeptieren – Die Änderung der MAC-Adresse des Gastbetriebssystems hat den gewünschten Effekt: Frames an die neue MAC-Adresse werden empfangen.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen – Alle ausgehenden Frames, bei denen sich die MAC-Quelladresse von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen. ■ Akzeptieren – Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 8 Klicken Sie auf **OK**.

Bearbeiten der Ausnahme der Sicherheitsrichtlinie für Schicht 2 für eine Standard-Portgruppe

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Standard-Switch“ und klicken Sie für die zu bearbeitende Portgruppe auf **Eigenschaften**.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **Ports**.
- 5 Wählen Sie das Portgruppenelement aus und klicken Sie auf **Bearbeiten**.
- 6 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **Sicherheit**.

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

Diese Richtlinienausnahme setzt jede Richtlinie, die auf der Standard-Switch-Ebene gesetzt wurde, außer Kraft.

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

Tabelle 22-3. Richtlinienausnahmen

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

- 8 Klicken Sie auf **OK**.

Bearbeiten der Sicherheitsrichtlinie für eine verteilte Portgruppe

Sie können eine Sicherheitsrichtlinie für eine verteilte Portgruppe festlegen, um die Richtlinie, die für den Distributed Switch festgelegt wurde, außer Kraft zu setzen.

Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen.

Im Nicht-Promiscuous-Modus überwacht der Gastadapter nur Datenverkehr an seiner eigenen MAC-Adresse. Im Promiscuous-Modus kann dieser alle Datenpakete überwachen. Standardmäßig ist der Promiscuous-Modus für die Gastadapter deaktiviert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.

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

- 4 Sie können in der Gruppe **Sicherheit** auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen – Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden. ■ Akzeptieren – Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSphere Standard-Switch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen – Wenn die Option MAC-Adressenänderungen auf Ablehnen festgelegt ist und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der .vmx-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der .vmx-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet. ■ Akzeptieren – Die Änderung der MAC-Adresse des Gastbetriebssystems hat den gewünschten Effekt: Frames an die neue MAC-Adresse werden empfangen.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen – Alle ausgehenden Frames, bei denen sich die MAC-Quelle von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen. ■ Akzeptieren – Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 5 Klicken Sie auf **OK**.

Bearbeiten von Sicherheitsrichtlinien für verteilte Ports

Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen.

Im Nicht-Promiscuous-Modus überwacht der Gastadapter nur Datenverkehr an seiner eigenen MAC-Adresse. Im Promiscuous-Modus kann dieser alle Datenpakete überwachen. Standardmäßig ist der Promiscuous-Modus für die Gastadapter deaktiviert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Richtlinien**.

Standardmäßig ist für den **Promiscuous-Modus** **Ablehnen** festgelegt, und für **MAC-Adressänderungen** und **Gefälschte Übertragungen** ist **Akzeptieren** festgelegt.

- 5 Sie können in der Gruppe **Sicherheit** auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen – Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden. ■ Akzeptieren – Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames erkannt, die über den vSphere Distributed Switch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen – Wenn die Option MAC-Adressenänderungen auf Ablehnen festgelegt ist und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der .vmx-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der .vmx-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet. ■ Akzeptieren – Die Änderung der MAC-Adresse des Gastbetriebssystems hat den gewünschten Effekt: Frames an die neue MAC-Adresse werden empfangen.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen – Alle ausgehenden Frames, bei denen sich die MAC-Quelladresse von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen. ■ Akzeptieren – Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 6 Klicken Sie auf **OK**.

Traffic-Shaping-Richtlinie

Eine Traffic-Shaping-Richtlinie wird anhand der durchschnittlichen Bandbreite, der Spitzenbandbreite und der Burstgröße definiert. Sie können für jede Portgruppe sowie jede verteilte Portgruppe und jeden verteilten Port eine Traffic-Shaping-Richtlinie erstellen.

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

Durchschnittsbandbreite	Legt fest, wie viele Bit pro Sekunde im Durchschnitt einen Port durchlaufen dürfen. Bei diesem Wert handelt es sich um die zulässige durchschnittliche Last.
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dieser Wert begrenzt die Bandbreite, die ein Port nutzt, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Wenn dieser Port mehr Bandbreite benötigt als von der durchschnittlichen Bandbreite angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt wurden, und überträgt den Datenverkehr mit einer höheren Geschwindigkeit.

Bearbeiten der Traffic-Shaping-Richtlinie für einen vSphere Standard-Switch

ESXi ermöglicht Ihnen das Traffic-Shaping des ausgehenden Datenverkehrs auf Standard-Switches. Der Traffic-Shaper beschränkt die verfügbare Netzwerkbandbreite für jeden Port, kann aber auch so konfiguriert werden, dass er vorübergehende Datenverkehr-Bursts mit höherer Geschwindigkeit für einen Port zulässt.

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

Durchschnittliche Bandbreite	Legt die zulässige Zahl der Bit pro Sekunde fest, die einen Port im Durchschnitt durchlaufen darf, d. h. die zulässige durchschnittliche Datenlast.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte Bandbreite nutzt, die ihm zugeteilt wurde. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung Durchschnittliche Bandbreite angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt werden und somit mit einer höheren Geschwindigkeit übertragen werden können.
Spitzenbandbreite	Die maximale Anzahl an Bits pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet. Dieser Parameter kann niemals kleiner als die durchschnittliche Bandbreite sein.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie einen Standard-Switch aus und klicken Sie auf **Eigenschaften**.
- 4 Klicken Sie auf die Registerkarte **Ports (Ports)**.
- 5 Wählen Sie einen Standard-Switch aus und klicken Sie auf **Bearbeiten**.
- 6 Klicken Sie auf die Registerkarte **Traffic-Shaping**.
- 7 Wählen Sie zum Aktivieren der Traffic-Shaping-Richtlinienausnahmen im Dropdown-Menü **Status** die Option **Aktiviert** aus.

Die Statusrichtlinie wird in diesem Fall auf alle virtuellen Adapter angewendet, die an der Portgruppe angeschlossen sind, jedoch nicht auf den gesamten Standard-Switch. Wenn Sie die Richtlinienausnahmen im Feld **Status** aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.
- 8 Geben Sie für jede Traffic-Shaping-Richtlinie eine Bandbreite ein.

Bearbeiten der Traffic-Shaping-Richtlinie für eine Standard-Portgruppe

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Netzwerk**.
- 3 Wählen Sie die Ansicht „vSphere Standard-Switch“ und klicken Sie für die zu bearbeitende Portgruppe auf **Eigenschaften**.
- 4 Wählen Sie im Dialogfeld „Eigenschaften“ die Registerkarte **Ports**.
- 5 Wählen Sie das Portgruppenelement aus und klicken Sie auf **Bearbeiten**.
- 6 Klicken Sie im Eigenschaftendialogfeld der Portgruppe auf die Registerkarte **Traffic-Shaping**.

Bei deaktiviertem Traffic-Shaping werden die Optionen abgeblendet dargestellt.

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

Bearbeiten der Traffic-Shaping-Richtlinie für eine verteilte Portgruppe

ESXi ermöglicht Ihnen das Traffic-Shaping auf vSphere Distributed Switches, sowohl bei eingehendem als auch bei ausgehendem Datenverkehr. Der Traffic-Shaper beschränkt die verfügbare Netzwerkbandbreite für jeden Port, kann aber auch so konfiguriert werden, dass er vorübergehende Datenverkehr-Bursts mit höherer Geschwindigkeit für einen Port zulässt.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.

- 4 Sie können in der Gruppe **Traffic-Shaping** sowohl **Ingress-Traffic-Shaping** als auch **Egress-Traffic-Shaping** konfigurieren.

Wenn Traffic-Shaping deaktiviert ist, werden die einstellbaren Funktionen abgeblendet dargestellt.

Status – Wenn Sie die Richtlinienausnahmen für **Ingress-Traffic-Shaping** oder **Egress-Traffic-Shaping** im Feld **Status** aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für jeden mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.

- 5 Festlegen der Netzwerkparameter.

Option	Beschreibung
Durchschnittliche Bandbreite	Legt die zulässige Zahl der Bit pro Sekunde fest, die einen Port im Durchschnitt durchlaufen darf, d. h. die zulässige durchschnittliche Datenlast.
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte Bandbreite nutzt, die ihm zugeteilt wurde. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung Durchschnittliche Bandbreite angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt werden und somit mit einer höheren Geschwindigkeit übertragen werden können.

- 6 Klicken Sie auf **OK**.

Bearbeiten von Traffic-Shaping-Richtlinien für verteilte Ports oder Uplink-Ports

ESXi ermöglicht Ihnen das Traffic-Shaping auf vSphere Distributed Switches, sowohl bei eingehendem als auch bei ausgehendem Datenverkehr. Der Traffic-Shaper beschränkt die verfügbare Netzwerkbandbreite für jeden Port, kann aber auch so konfiguriert werden, dass er vorübergehende Datenverkehr-Bursts mit höherer Geschwindigkeit für einen Port zulässt.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Richtlinien**.
- 5 Sie können in der Gruppe **Traffic-Shaping** sowohl **Ingress-Traffic-Shaping** als auch **Egress-Traffic-Shaping** konfigurieren.

Wenn Traffic-Shaping deaktiviert ist, werden die einstellbaren Funktionen abgeblendet dargestellt.

Status – Wenn Sie die Richtlinienausnahmen für **Ingress-Traffic-Shaping** oder **Egress-Traffic-Shaping** im Feld **Status** aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für jeden mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.

6 Festlegen der Netzwerkparameter.

- **Durchschnittliche Bandbreite** – Legt die zulässige Anzahl der Bits pro Sekunde fest, die im Durchschnitt über einen Port geleitet werden kann, d. h. die zulässige durchschnittliche Datenlast.
- **Spitzenbandbreite** – Die maximale Anzahl an Bits pro Sekunde, die über einen Port geleitet werden kann, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
- **Burstgröße** – Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte Bandbreite nutzt, die ihm zugeteilt wurde. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung **Durchschnittliche Bandbreite** angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt werden und somit mit einer höheren Geschwindigkeit übertragen werden können.

7 Klicken Sie auf **OK**.

Ressourcenzuteilungsrichtlinie

Mit der Ressourcenzuteilungsrichtlinie können Sie einen verteilten Port oder eine verteilte Portgruppe zu einem von einem Benutzer erstellten Netzwerkressourcenpool zuordnen. Mit dieser Richtlinie lässt sich die Bandbreite für den Port oder die Portgruppe besser steuern.

Weitere Informationen zum Erstellen und Konfigurieren von Netzwerkressourcenpools finden Sie unter „[vSphere Network I/O Control](#)“, auf Seite 279.

Bearbeiten der Ressourcenzuteilungsrichtlinie für eine verteilte Portgruppe

Ordnen Sie eine verteilte Portgruppe einem Netzwerkressourcenpool zu, um mehr Kontrolle über die Bandbreite zu haben, die der verteilten Portgruppe zugeteilt wird.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Aktivieren Sie Network I/O Control auf dem Host und erstellen Sie einen oder mehrere benutzerdefinierte Netzwerkressourcenpools.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.
- 4 Wählen Sie in der Gruppe „Ressourcenzuteilung“ im Dropdown-Menü den **Netzwerkressourcenpool** aus, der mit der verteilten Portgruppe verknüpft werden soll.
- 5 Klicken Sie auf **OK**.

Bearbeiten der Ressourcenzuteilungsrichtlinie für verteilte Ports

Ordnen Sie einen verteilten Port einem Netzwerkressourcenpool zu, um mehr Kontrolle über die Bandbreite zu haben, die dem Port zugeteilt wird.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Aktivieren Sie Network I/O Control auf dem Host und erstellen Sie einen oder mehrere benutzerdefinierte Netzwerkressourcenpools.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Wählen Sie **Richtlinien**.
- 5 Wählen Sie in der Gruppe „Ressourcenzuteilung“ im Dropdown-Menü den **Netzwerkressourcenpool** aus, der mit der verteilten Portgruppe verknüpft werden soll.
- 6 Klicken Sie auf **OK**.

Überwachungsrichtlinie

Die Überwachungsrichtlinie aktiviert oder deaktiviert die NetFlow-Überwachung auf einem verteilten Port oder einer Portgruppe.

NetFlow-Einstellungen können auf der Ebene der vSphere Distributed Switches konfiguriert werden. Siehe [„Konfigurieren der NetFlow-Einstellungen“](#), auf Seite 329.

Bearbeiten der Überwachungsrichtlinie für eine verteilte Portgruppe

Mithilfe der Überwachungsrichtlinie können Sie die NetFlow-Überwachung auf einer verteilten Portgruppe aktivieren oder deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.
- 4 Wählen Sie in der Gruppe „Überwachung“ den **NetFlow-Status** aus.

Option	Beschreibung
Deaktiviert	NetFlow ist für die verteilte Portgruppe deaktiviert.
Aktiviert	NetFlow ist für die verteilte Portgruppe aktiviert. Sie können auf der vSphere Distributed Switch-Ebene NetFlow-Einstellungen konfigurieren. Siehe „Konfigurieren der NetFlow-Einstellungen“ , auf Seite 329.

- 5 Klicken Sie auf **OK**.

Bearbeiten der Überwachungsrichtlinie für einen verteilten Port

Mithilfe der Überwachungsrichtlinie können Sie die NetFlow-Überwachung auf einem verteilter Port aktivieren oder deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Wählen Sie **Richtlinien**.
- 5 Wählen Sie in der Gruppe „Überwachung“ den **NetFlow-Status** aus.

Option	Beschreibung
Deaktiviert	NetFlow ist auf dem Port deaktiviert.
Aktiviert	NetFlow ist auf dem Port aktiviert. Sie können auf der Distributed Switch-Ebene NetFlow-Einstellungen konfigurieren. Siehe „ Konfigurieren der NetFlow-Einstellungen “, auf Seite 329.

- 6 Klicken Sie auf **OK**.

Portblockierungsrichtlinien

Mit Portblockierungsrichtlinien können Sie ausgewählte Ports daran hindern, Daten zu senden oder zu empfangen.

Bearbeiten der Portblockierungsrichtlinie für eine verteilte Portgruppe

Das Dialogfeld „Verschiedene Richtlinien“ ermöglicht Ihnen das Konfigurieren verschiedener Richtlinien für verteilte Portgruppen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Richtlinien**.
- 4 Wählen Sie in der Gruppe **Verschiedenes** die Option **Alle Ports blockieren** aus, wenn alle Ports in dieser verteilten Portgruppe blockiert werden sollen.
- 5 Klicken Sie auf **OK**.

Bearbeiten von Blockierungsrichtlinien für verteilte Ports oder Uplink-Ports

Im Dialogfeld „Verschiedene Richtlinien“ können Sie Blockierungsrichtlinien für verteilte Ports oder Uplink-Ports konfigurieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Wählen Sie den vSphere Distributed Switch im Bestandslistenbereich aus.
- 3 Klicken Sie mit der rechten Maustaste auf der Registerkarte **Ports** auf den zu ändernden Port und wählen Sie die Option **Einstellungen bearbeiten** aus.
- 4 Klicken Sie auf **Richtlinien**.
- 5 Wählen Sie in der Gruppe **Verschiedenes** mithilfe der Option **Diesen Port blockieren** aus, ob dieser Port blockiert werden soll.
- 6 Klicken Sie auf **OK**.

Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch

Sie können die Netzwerkrichtlinien für mehrere Portgruppen auf einem Distributed Switch ändern.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Erstellen Sie einen vSphere Distributed Switch mit einer oder mehreren Portgruppen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Portgruppen verwalten**.
- 3 Wählen Sie die zu ändernden Richtlinienkategorien aus.

Option	Beschreibung
Sicherheit	Nehmen Sie Einstellungen zu MAC-Adressänderungen, zu gefälschten Übertragungen und zum Promiscuous-Modus für die ausgewählten Portgruppen vor.
Traffic-Shaping	Legen Sie die durchschnittliche Bandbreite, die Spitzenbandbreite und die Burstgröße für den ein- und ausgehenden Datenverkehr auf den ausgewählten Portgruppen fest.
VLAN	Konfigurieren Sie die Art der Verbindung der ausgewählten Portgruppen zu physischen VLANs.
Teaming und Failover	Legen Sie den Lastausgleich, die Failover-Erkennung, die Switch-Benachrichtigung und die Failover-Reihenfolge für die ausgewählten Portgruppen fest.
Ressourcenzuteilung	Legen Sie die Zuordnung des Netzwerkressourcenpools für die ausgewählten Portgruppen fest. Diese Option ist nur für vSphere Distributed Switch Version 5.0.0 und höher verfügbar.

Option	Beschreibung
Überwachen	Aktivieren oder deaktivieren Sie NetFlow auf den ausgewählten Portgruppen. Diese Option ist nur für vSphere Distributed Switch Version 5.0.0 und höher verfügbar.
Sonstiges	Aktivieren oder deaktivieren Sie die Portblockierung auf den ausgewählten Portgruppen.

- 4 Klicken Sie auf **Weiter**.

- 5 Wählen Sie eine oder mehrere Portgruppen zum Ändern aus und klicken Sie auf **Weiter**.

Die Seite zum Konfigurieren der Richtlinien wird angezeigt. Es werden nur die Richtlinienkategorien angezeigt, die Sie zuvor ausgewählt haben.

- 6 (Optional) Sie können in der Gruppe „Sicherheit“ auswählen, ob die Ausnahmen für die Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen – Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden. ■ Akzeptieren – Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames erkannt, die über den vSphere Distributed Switch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen – Wenn die Option MAC-Adressenänderungen auf Ablehnen festgelegt ist und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der .vmx-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der .vmx-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet. ■ Akzeptieren – Die Änderung der MAC-Adresse des Gastbetriebssystems hat den gewünschten Effekt: Frames an die neue MAC-Adresse werden empfangen.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen – Alle ausgehenden Frames, bei denen sich die MAC-Quelladresse von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen. ■ Akzeptieren – Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

- 7 (Optional) Sie können in der Gruppe „Traffic-Shaping“ sowohl **Ingress-Traffic-Shaping** als auch **Egress-Traffic-Shaping** konfigurieren.

Wenn Traffic-Shaping deaktiviert ist, werden die einstellbaren Funktionen abgeblendet dargestellt.

Status – Wenn Sie die Richtlinienausnahmen für **Ingress-Traffic-Shaping** oder **Egress-Traffic-Shaping** im Feld **Status** aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für jeden mit den ausgewählten Portgruppen verknüpften verteilten Port. Wenn Sie die Richtlinie deaktivieren, ist die Netzwerkbandbreite nicht begrenzt, bevor sie das physische Netzwerk erreicht.

8 (Optional) Festlegen der Netzwerkparameter.

Option	Beschreibung
Durchschnittliche Bandbreite	Legt die zulässige Zahl der Bit pro Sekunde fest, die einen Port im Durchschnitt durchlaufen darf, d. h. die zulässige durchschnittliche Datenlast.
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte Bandbreite nutzt, die ihm zugeteilt wurde. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung Durchschnittliche Bandbreite angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt werden und somit mit einer höheren Geschwindigkeit übertragen werden können.

9 (Optional) Wählen Sie den zu verwendenden VLAN-Typ aus.

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

10 (Optional) Geben Sie in der Gruppe „Teaming und Failover“ Folgendes an.

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

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

- 11 (Optional) Wählen Sie in der Gruppe „Ressourcenzuteilung“ im Dropdown-Menü den **Netzwerkressourcenpool** aus, der mit der verteilten Portgruppe verknüpft werden soll.
- 12 (Optional) Wählen Sie in der Gruppe „Überwachung“ den **NetFlow-Status** aus.

Option	Beschreibung
Deaktiviert	NetFlow ist für die verteilte Portgruppe deaktiviert.
Aktiviert	NetFlow ist für die verteilte Portgruppe aktiviert. NetFlow-Einstellungen können auf der Ebene der vSphere Distributed Switches konfiguriert werden.

- 13 (Optional) Wählen Sie in der Gruppe **Verschiedenes** die Option **Alle Ports blockieren** aus, wenn alle Ports in dieser verteilten Portgruppe blockiert werden sollen.
- 14 Klicken Sie auf **Weiter**.

Alle angezeigten Richtlinien werden auf alle ausgewählten Portgruppen angewendet, einschließlich der Richtlinien, die unverändert geblieben sind.
- 15 (Optional) Wenn Sie Änderungen vornehmen müssen, klicken Sie auf **Zurück**, um zu dem gewünschten Bildschirm zu gelangen.
- 16 Überprüfen Sie die Einstellungen für die Portgruppe und klicken Sie auf **Beenden**.

Erweiterte Netzwerkthemen

Erweiterte Netzwerkkonfigurationsoptionen bieten Ihnen mehr Kontrolle über Ihre vSphere-Netzwerkumgebung.

Dieses Kapitel behandelt die folgenden Themen:

- „Unterstützung für Internet Protocol Version 6 (IPv6)“, auf Seite 321
- „VLAN-Konfiguration“, auf Seite 322
- „Arbeiten mit der Portspiegelung“, auf Seite 322
- „Konfigurieren der NetFlow-Einstellungen“, auf Seite 329
- „Switch-Discovery-Protokoll“, auf Seite 330
- „Ändern der DNS- und Routing-Konfiguration“, auf Seite 332
- „Verwaltung von MAC-Adressen“, auf Seite 333

Unterstützung für Internet Protocol Version 6 (IPv6)

Die Unterstützung für Internet Protocol Version 6 (IPv6) in ESXi bietet die Möglichkeit, Funktionen der virtuellen Infrastruktur, wie etwa NFS, in einer IPv6-Umgebung zu verwenden. Verwenden Sie das Dialogfeld „Netzwerkeigenschaften“ zum Aktivieren oder Deaktivieren der IPv6-Unterstützung auf dem Host.

IPv6 wurde von der Internet Engineering Task Force als Nachfolger von IPv4 bestimmt. Der offensichtlichste Unterschied ist die Adresslänge. IPv6 verwendet 128-Bit-Adressen statt die 32-Bit-Adressen, die IPv4 verwendet. Diese Erweiterung löst das Problem der Adressknappheit und macht die Netzwerkadressübersetzung überflüssig. Weitere Unterschiede sind Link-Local-Adressen, die beim Initialisieren der Schnittstelle erscheinen, Adressen, die über eine Router-Ankündigung festgelegt werden, und die Fähigkeit, mehrere IPv6-Adressen auf einer Schnittstelle zu haben.

Unter VMware ESXi 5.1 ist IPv6 standardmäßig aktiviert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Host.Konfiguration.Netzwerkkonfiguration**

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere Clients auf **Hosts und Cluster**.
- 2 Wählen Sie einen Host, und klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie unter **Hardware** auf den Link **Netzwerk**.
- 4 Klicken Sie in der Ansicht **vSphere Standard-Switch** auf den Link **Eigenschaften**.

- 5 Wählen Sie **IPv6-Unterstützung auf diesem Host aktivieren** und klicken Sie auf **OK**.
- 6 Starten Sie den Host neu.

VLAN-Konfiguration

Mit virtuellen LANs (VLANs) kann ein einzelnes physisches LAN-Segment weiter isoliert werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten.

Aus den folgenden Gründen wird empfohlen, ESXi mit VLANs zu konfigurieren.

- Der Host wird in eine bereits vorhandene Umgebung integriert.
- Der Netzwerkdatenverkehr wird isoliert und gesichert.
- Die Überlastung durch Netzwerkdatenverkehr wird verringert.

Sie können VLANs in ESXi mithilfe von drei Methoden konfigurieren: External Switch Tagging (EST), Virtual Switch Tagging (VST) und Virtual Guest Tagging (VGT).

Beim EST wird das gesamte VLAN-Tagging der Pakete auf dem physischen Switch durchgeführt. Host-Netzwerkadapter sind mit Zugriffs-Ports auf dem physischen Switch verbunden. Bei Portgruppen, die mit dem virtuellen Switch verbunden sind, muss die VLAN-ID auf 0 gesetzt sein.

Beim VST wird das gesamte VLAN-Tagging der Pakete vor dem Verlassen des Hosts vom virtuellen Switch durchgeführt. Host-Netzwerkadapter müssen mit Trunk-Ports auf dem physischen Switch verbunden sein. Für Portgruppen, die mit dem virtuellen Switch verbunden sind, ist eine VLAN-ID zwischen 1 und 4094 erforderlich.

Beim VGT wird das gesamte VLAN-Tagging von der virtuellen Maschine durchgeführt. VLAN-Tags werden zwischen dem VM-Netzwerkstapel und dem externen Switch beibehalten, wenn Frames zu und von virtuellen Switches übertragen werden. Host-Netzwerkadapter müssen mit Trunk-Ports auf dem physischen Switch verbunden sein. Für einen Standard-Switch muss die VLAN-ID von Portgruppen mit VGT auf 4095 gesetzt sein. Für einen Distributed Switch muss die VLAN-Trunking-Richtlinie den Bereich der VLANs umfassen, mit denen virtuelle Maschinen verbunden sind.

HINWEIS Bei Verwendung von VGT muss ein 802.1Q-VLAN-Trunking-Treiber auf der virtuellen Maschine installiert sein.

Arbeiten mit der Portspiegelung

Die Portspiegelung ermöglicht Ihnen, den Datenverkehr von einem verteilten Port an andere verteilte Ports oder bestimmte physische Switch-Ports zu spiegeln.

Die Portspiegelungsfunktion wird auf einem Switch verwendet, um eine Kopie von Paketen, die auf einem Switch-Port (oder einem kompletten VLAN) angezeigt werden, an einen überwachenden Anschluss an einem anderen Switch-Port zu senden. Die Portspiegelungsfunktion verwendet, um Daten zu analysieren und zu reparieren oder Fehler in einem Netzwerk zu diagnostizieren.

Portspiegelung - Versionskompatibilität

Bestimmte Portspiegelungsfunktionen in vSphere 5.1 und höher sind abhängig von der Version von vCenter Server, dem vSphere Distributed Switch und dem Host, die Sie einsetzen, sowie davon, wie Sie diese Aspekte von vSphere zusammen verwenden.

Tabelle 23-1. Portspiegelungskompatibilität

vCenter Server-Version	Version des vSphere Distributed Switch	Hostversion	vSphere 5.1-Portspiegelungsfunktionalität
vSphere 5.1 und höher	vSphere 5.1 und höher	vSphere 5.1 und höher	Die Portspiegelung von vSphere 5.1 kann verwendet werden. Funktionen für die Portspiegelung von vSphere 5.0 und vorherigen Versionen stehen nicht zur Verfügung.
vSphere 5.1 und höher	vSphere 5.1 und höher	vSphere 5.0 und früher	vSphere 5.0 und frühere Hosts können zu vSphere 5.1 vCenter Server hinzugefügt werden, zu Distributed Switches der Version 5.1 und höher können sie jedoch nicht hinzugefügt werden.
vSphere 5.1 und höher	vSphere 5.0	vSphere 5.0	vSphere vCenter Server 5.1 und höher kann die Portspiegelung auf einem vSphere 5.0 Distributed Switch konfigurieren.
vSphere 5.1 und höher	vSphere 5.0	vSphere 5.1 und höher	Hosts, auf denen vSphere 5.1 ausgeführt wird, können zu vSphere 5.0 Distributed Switches hinzugefügt werden und die vSphere 5.0 Portspiegelung unterstützen.
vSphere 5.1 und höher	Vor vSphere 5.0	vSphere 5.5 und früher	Portspiegelung wird nicht unterstützt.
vSphere 5.0 und früher	vSphere 5.0 und früher	vSphere 5.1	Ein vSphere 5.1-Host kann nicht zu vCenter Server 5.0 und früher hinzugefügt werden.

Wenn Sie ein Hostprofil mit Portspiegelungseinstellungen verwenden, muss das Hostprofil an die neue Version der Portspiegelung in vSphere 5.1 und höher angepasst werden.

Portspiegelung - Interoperabilität

Einige Interoperabilitätsprobleme müssen berücksichtigt werden, wenn Sie die vSphere 5.1-Portspiegelung zusammen mit anderen Funktionen von vSphere verwenden.

vMotion

Abhängig von dem von Ihnen ausgewählten Typ der vSphere 5.1-Portspiegelungssitzung funktioniert vMotion unterschiedlich. Bei vMotion wird möglicherweise ein Spiegelungspfad vorübergehend ungültig. Er wird jedoch wiederhergestellt, wenn der vMotion-Vorgang abgeschlossen ist.

Tabelle 23-2. vMotion-Interoperabilität mit der Portspiegelung

Typ der Portspiegelungssitzung	Quelle und Ziel	Interoperabilität mit vMotion	Funktionalität
Spiegelung verteilter Ports	Quelle und Ziel eines verteilten Nicht-Uplink-Ports	Ja	Die Portspiegelung zwischen verteilten Ports kann nur lokal sein. Wenn sich aufgrund von vMotion die Quelle und das Ziel auf unterschiedlichen Hosts befinden, funktioniert die Spiegelung zwischen ihnen nicht. Wenn jedoch die Quelle und das Ziel auf denselben Host verschoben werden, funktioniert die Portspiegelung.
Remotespiegelungsquelle	Quelle eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Quelle dient, von Host A auf Host B verschoben wird, wird der ursprüngliche Spiegelungspfad vom Quellport zum Uplink von Host A auf Host A entfernt und ein neuer Spiegelungspfad vom Quellport zum Uplink von Host B wird auf Host B erstellt. Der Uplink, der schließlich verwendet wird, wird vom in der Sitzung angegebenen Uplink-Namen bestimmt.
	Uplink-Port-Ziele	Nein	Uplinks können nicht von vMotion verschoben werden.
Remotespiegelungsziel	VLAN-Quelle	Nein	
	Ziel eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Ziel dient, von Host A auf Host B verschoben wird, werden alle ursprünglichen Spiegelungspfade von Quell-VLANs zum Zielport von Host A auf Host B verschoben.
Gekapselte Remotespiegelungsquelle (L3)	Quelle eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Quelle dient, von Host A auf Host B verschoben wird, werden alle ursprünglichen Spiegelungspfade vom Quellport auf die Ziel-IP-Adressen von Host A auf Host B verschoben.
	IP-Ziel	Nein	

Tabelle 23-2. vMotion-Interoperabilität mit der Portspiegelung (Fortsetzung)

Typ der Portspiegelungssitzung	Quelle und Ziel	Interoperabilität mit vMotion	Funktionalität
Spiegelung verteilter Ports (Legacy)	IP-Quelle	Nein	
	Ziel eines verteilten Nicht-Uplink-Ports	Nein	Wenn ein verteilter Port, der als Ziel dient, von Host A auf Host B verschoben wird, sind alle ursprünglichen Spiegelungspfade von den Quell-IP-Adressen auf den Zielport ungültig, da die Quelle der Portspiegelungssitzung nach wie vor das Ziel auf Host A sieht.

TSO und LRO

TSO (TCP Segmentation Offload) und LRO (Large Receive Offload) sorgen möglicherweise dafür, dass die Anzahl der Spiegelungspakete nicht mit der Anzahl der gespiegelten Pakete übereinstimmt.

Wenn TSO auf einer vNIC aktiviert ist, sendet die vNIC möglicherweise ein umfangreiches Paket an einen Distributed Switch. Wenn LRO auf einer vNIC aktiviert ist, werden kleine Pakete, die an die vNIC gesendet werden, möglicherweise in einem großen Paket zusammengefasst.

Quelle	Ziel	Beschreibung
TSO	LRO	Pakete von der Quell-vNIC sind möglicherweise große Pakete. Ob sie aufgeteilt werden, hängt davon ab, ob ihre Größen den LRO-Grenzwert der Ziel-vNIC überschreiten.
TSO	Beliebiges Ziel	Pakete von der Quell-vNIC sind möglicherweise große Pakete und werden an der Ziel-vNIC in Standardpakete aufgeteilt.
Beliebige Quelle	LRO	Pakete von der Quell-vNIC sind Standardpakete und werden möglicherweise an der Ziel-vNIC in größere Pakete zusammengefasst.

Erstellen einer Portspiegelungssitzung mit dem vSphere-Client

Erstellen Sie eine Portspiegelungssitzung, um den Datenverkehr eines vSphere Distributed Switch auf bestimmten physischen Switch-Ports zu spiegeln.

Voraussetzungen

Erstellen Sie einen vSphere Distributed Switch Version 5.0.0 oder höher.

Vorgehensweise

- 1 [Festlegen des Portspiegelungsnamens und von Sitzungsdetails](#) auf Seite 326
Geben Sie den Namen, die Beschreibung und die Sitzungsdetails für die neue Portspiegelungssitzung an.
- 2 [Auswählen von Portspiegelungsquellen](#) auf Seite 326
Wählen Sie Quellen und die Datenverkehrsrichtung für die neue Portspiegelungssitzung aus.
- 3 [Auswählen von Portspiegelungszielen](#) auf Seite 326
Wählen Sie Ports oder Uplinks als Ziele für die Portspiegelungssitzung aus.
- 4 [Überprüfen der neuen Portspiegelungseinstellungen](#) auf Seite 327
Überprüfen Sie die Einstellungen und aktivieren Sie die neue Portspiegelungssitzung.

Festlegen des Portspiegelungsnamens und von Sitzungsdetails

Geben Sie den Namen, die Beschreibung und die Sitzungsdetails für die neue Portspiegelungssitzung an.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie auf die Registerkarte „Portspiegelung“ auf **Hinzufügen**.
- 4 Geben Sie einen **Namen** und eine **Beschreibung** für die Portspiegelungssitzung ein.
- 5 (Optional) Wählen Sie **Normale E/A auf Zielports zulassen**, um normalen E/A-Datenverkehr auf den Zielports zuzulassen.
Wenn Sie diese Option nicht auswählen, wird ausgehender gespiegelter Datenverkehr auf den Zielports zugelassen, aber eingehender Datenverkehr nicht.
- 6 (Optional) Wählen Sie **Kapselungs-VLAN**, um eine VLAN-ID zu erstellen, die alle Frames an den Zielports kapselt.
Wenn die ursprünglichen Frames über ein VLAN verfügen und **Ursprüngliches VLAN beibehalten** nicht ausgewählt ist, wird das ursprüngliche VLAN durch das Kapselungs-VLAN ersetzt.
- 7 (Optional) Wählen Sie **Ursprüngliches VLAN beibehalten**, um das ursprüngliche VLAN in einem inneren Tag zu behalten, damit gespiegelte Frames doppelt eingekapselt sind.
Diese Option ist nur dann verfügbar, wenn Sie **Kapselungs-VLAN** auswählen.
- 8 (Optional) Wählen Sie **Länge des gespiegelten Pakets**, um die Größe der gespiegelten Frames zu beschränken.
Wenn diese Option ausgewählt ist, werden alle gespiegelten Frames auf die angegebene Länge gekürzt.
- 9 Klicken Sie auf **Weiter**.

Auswählen von Portspiegelungsquellen

Wählen Sie Quellen und die Datenverkehrsrichtung für die neue Portspiegelungssitzung aus.

Vorgehensweise

- 1 Wählen Sie, ob diese Quelle für den **Ingress**- oder **Egress**-Datenverkehr verwendet werden soll, oder wählen Sie **Ingress/Egress**, um diese Quelle für beide Datenverkehrstypen zu verwenden.
- 2 Geben Sie die IDs der Quellports ein und klicken Sie auf >>, um die Quellen zur Portspiegelungssitzung hinzuzufügen.
Trennen Sie mehrere Port-IDs durch ein Komma voneinander.
- 3 Klicken Sie auf **Weiter**.

Auswählen von Portspiegelungszielen

Wählen Sie Ports oder Uplinks als Ziele für die Portspiegelungssitzung aus.

Die Portspiegelung wird anhand der VLAN-Weiterleitungsrichtlinie überprüft. Wenn das VLAN der ursprünglichen Frames nicht gleich dem Zielport ist oder von ihm getrunkt wird, werden die Frames nicht gespiegelt.

Vorgehensweise

- 1 Wählen Sie den **Zieltyp**.

Option	Beschreibung
Port	Geben Sie eine oder mehrere Port-IDs ein, die als Ziel für die Portspiegelungssitzung verwendet werden sollen. Trennen Sie mehrere IDs durch ein Komma voneinander.
Uplink	Wählen Sie einen oder mehrere Uplinks aus, die als Ziel für die Portspiegelungssitzung verwendet werden sollen.

- 2 Klicken Sie auf >>, um die ausgewählten Ziele zur Portspiegelungssitzung hinzuzufügen.
- 3 (Optional) Wiederholen Sie die oben aufgeführten Schritte, um mehrere Ziele hinzuzufügen.
- 4 Klicken Sie auf **Weiter**.

Überprüfen der neuen Portspiegelungseinstellungen

Überprüfen Sie die Einstellungen und aktivieren Sie die neue Portspiegelungssitzung.

Vorgehensweise

- 1 Überprüfen Sie, ob der angegebene Name und die Einstellungen für die neue Portspiegelungssitzung richtig sind.
- 2 (Optional) Klicken Sie auf **Zurück (Back)**, um Änderungen vorzunehmen.
- 3 (Optional) Klicken Sie auf **Diese Portspiegelungssitzung aktivieren**, um die Portspiegelungssitzung umgehend zu starten.
- 4 Klicken Sie auf **Beenden**.

Anzeigen von Details zu einer Portspiegelungssitzung

Zeigen Sie Details zu einer Portspiegelungssitzung an, wie Status, Quellen und Ziele.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Portspiegelung** die Portspiegelungssitzung aus, die angezeigt werden soll.

Detailinformationen zu der ausgewählten Spiegelungssitzung werden unter **Details der Portspiegelungssitzung** angezeigt.
- 4 (Optional) Klicken Sie auf **Bearbeiten**, um die Details der ausgewählten Portspiegelungssitzung zu bearbeiten.
- 5 (Optional) Klicken Sie auf **Löschen**, um die ausgewählte Portspiegelungssitzung zu löschen.
- 6 (Optional) Klicken Sie auf **Hinzufügen**, um eine neue Portspiegelungssitzung hinzuzufügen.

Bearbeiten von Portspiegelungsnamen und Sitzungsdetails

Bearbeiten Sie die Details einer Portspiegelungssitzung, zu denen Name, Beschreibung und Status gehören.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Portspiegelung** die zu ändernde Portspiegelungssitzung aus und klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Eigenschaften (Properties)**.
- 5 (Optional) Geben Sie einen neuen **Namen** für die Portspiegelungssitzung ein.
- 6 (Optional) Geben Sie eine neue **Beschreibung** für die Portspiegelungssitzung ein.
- 7 Wählen Sie aus, ob die Portspiegelungssitzung **Aktiviert** oder **Deaktiviert** sein soll.
- 8 (Optional) Wählen Sie **Normale E/A auf Zielports zulassen**, um normalen E/A-Datenverkehr auf den Zielports zuzulassen.
Wenn Sie diese Option nicht auswählen, wird ausgehender gespiegelter Datenverkehr auf den Zielports zugelassen, aber eingehender Datenverkehr nicht.
- 9 (Optional) Wählen Sie **Kapselungs-VLAN**, um eine VLAN-ID zu erstellen, die alle Frames an den Zielports kapselt.
Wenn die ursprünglichen Frames über ein VLAN verfügen und **Ursprüngliches VLAN beibehalten** nicht ausgewählt ist, wird das ursprüngliche VLAN durch das Kapselungs-VLAN ersetzt.
- 10 (Optional) Wählen Sie **Ursprüngliches VLAN beibehalten**, um das ursprüngliche VLAN in einem inneren Tag zu behalten, damit gespiegelte Frames doppelt eingekapselt sind.
Diese Option ist nur dann verfügbar, wenn Sie **Kapselungs-VLAN** auswählen.
- 11 (Optional) Wählen Sie **Länge des gespiegelten Pakets**, um die Größe der gespiegelten Frames zu beschränken.
Wenn diese Option ausgewählt ist, werden alle gespiegelten Frames auf die angegebene Länge gekürzt.
- 12 Klicken Sie auf **OK**.

Bearbeiten von Portspiegelungsquellen

Bearbeiten Sie die Quellen und die Datenverkehrsrichtung für die Portspiegelungssitzung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.

- 3 Wählen Sie auf der Registerkarte **Portspiegelung** die zu ändernde Portspiegelungssitzung aus und klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Quellen**.
- 5 (Optional) Wählen Sie, ob diese Quelle für den **Ingress**- oder den **Egress**-Datenverkehr verwendet werden soll, oder wählen Sie **Ingress/Egress**, um diese Quelle für beide Datenverkehrstypen zu verwenden.
- 6 (Optional) Geben Sie eine oder mehrere Port-IDs bzw. Port-ID-Bereiche ein, die als Quelle für die Portspiegelungssitzung hinzugefügt werden sollen, und klicken Sie auf >>.

Trennen Sie mehrere IDs durch Kommas.
- 7 (Optional) Wählen Sie eine Quelle aus der rechten Liste aus und klicken Sie auf <<, um die Quelle aus der Portspiegelungssitzung zu entfernen.
- 8 Klicken Sie auf **OK**.

Bearbeiten von Portspiegelungszielen

Bearbeiten Sie die Zielports und -Uplinks für eine Portspiegelungssitzung, um den Speicherort zu ändern, an dem der Datenverkehr für die Sitzung gespiegelt wird.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Portspiegelung** die zu ändernde Portspiegelungssitzung aus und klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Ziele**.
- 5 (Optional) Wählen Sie den **Zieltyp** für das Ziel aus, das Sie hinzufügen möchten.

Option	Beschreibung
Port	Geben Sie eine oder mehrere Port-IDs ein, die als Ziel für die Portspiegelungssitzung verwendet werden sollen. Trennen Sie mehrere IDs durch ein Komma voneinander.
Uplink	Wählen Sie einen oder mehrere Uplinks aus, die als Ziel für die Portspiegelungssitzung verwendet werden sollen.

- 6 (Optional) Geben Sie eine oder mehrere Port-IDs bzw. Port-ID-Bereiche ein, die als Ziel für die Portspiegelungssitzung verwendet werden sollen, und klicken Sie auf >>.

Trennen Sie mehrere IDs durch Kommas.
- 7 (Optional) Wählen Sie ein Ziel aus der rechten Spalte aus und klicken Sie auf <<, um das Ziel aus der Portspiegelungssitzung zu entfernen.
- 8 Klicken Sie auf **OK**.

Konfigurieren der NetFlow-Einstellungen

NetFlow ist ein Tool für die Netzwerkanalyse, das Sie zum Überwachen der Netzwerküberwachung und des VM-Datenverkehrs verwenden können.

NetFlow steht in vSphere Distributed Switch Version 5.0.0 und höher zur Verfügung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Navigieren Sie zur Registerkarte **NetFlow**.
- 4 Geben Sie die **IP-Adresse** und den **Port** des NetFlow-Collectors ein.
- 5 Geben Sie die **vDS-IP-Adresse** ein.

Mithilfe einer IP-Adresse für den vSphere Distributed Switch kann der NetFlow-Collector mit dem vSphere Distributed Switch als einem einzelnen Switch interagieren, anstatt mit einem separaten, unabhängigen Switch für jeden zugewiesenen Host.
- 6 (Optional) Verwenden Sie die Menüfeile nach oben und nach unten, um die Einstellungen **Zeitüberschreitung bei aktivem Flow-Export** und **Zeitüberschreitung bei Flow-Export im Leerlauf** festzulegen.
- 7 (Optional) Verwenden Sie die Menüfeile nach oben und nach unten, um die **Sampling-Rate** festzulegen.

Die Sampling-Rate definiert, welcher Datenanteil von NetFlow erfasst wird, während die Sampling-Raten-Anzahl definiert, wie oft NetFlow die Pakete erfasst. Ein Collector mit einer Sampling-Rate von 2 erfasst Daten von jedem zweiten Paket. Ein Collector mit einer Sampling-Rate von 5 erfasst Daten von jedem fünften Paket.
- 8 (Optional) Wählen Sie **Nur interne Flows verarbeiten**, wenn Daten nur bei Netzwerkaktivität zwischen virtuellen Maschinen auf demselben Host erfasst werden sollen.
- 9 Klicken Sie auf **OK**.

Switch-Discovery-Protokoll

Switch-Discovery-Protokolle helfen vSphere-Administratoren zu ermitteln, welcher Port des physischen Switch mit einem vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist.

vSphere 5.0 und höher unterstützt das Cisco Discovery Protocol (CDP) und das Link Layer Discovery Protocol (LLDP). CDP ist verfügbar für vSphere Standard-Switches und vSphere Distributed Switches, die mit physischen Cisco-Switches verbunden sind. LLDP ist verfügbar für vSphere Distributed Switches der Version 5.0.0 und höher.

Wenn CDP oder LLDP für einen bestimmten vSphere Distributed Switch oder vSphere Standard-Switch aktiviert ist, können Sie die Eigenschaften des physischen Peer-Switches wie z. B. Geräte-ID, Softwareversion und Zeitüberschreitung vom vSphere Web Client aus anzeigen.

Aktivieren des Cisco Discovery-Protokolls auf einem vSphere Distributed Switch

Cisco Discovery-Protokolle (CDP) ermöglichen es vSphere-Administratoren, zu ermitteln, welcher Cisco-Switch-Port mit einem bestimmten vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist. Wenn CDP für einen bestimmten vSphere Distributed Switch aktiviert ist, können Sie in vSphere Client Eigenschaften des Cisco-Switches anzeigen (z. B. Geräte-ID, Softwareversion und Zeitlimit).

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Eigenschaften** die Option **Erweitert** aus.
- 4 Wählen Sie **Aktiviert** aus dem Dropdown-Menü **Status**.
- 5 Wählen Sie **Cisco Discovery-Protokoll** aus dem Dropdown-Menü **Typ**.
- 6 Wählen Sie den CDP-Modus aus dem Dropdown-Menü **Vorgang**.

Option	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften Cisco-Switchport an, jedoch stehen dem Administrator des Cisco-Switches keine Informationen über den vSphere Distributed Switch zur Verfügung.
Anzeigen	ESXi stellt dem Cisco-Switch-Administrator Informationen zum vSphere Distributed Switch zur Verfügung, ohne jedoch Informationen zum Cisco-Switch zu erkennen und anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften Cisco-Switch an und stellt dem Administrator des Cisco-Switches Informationen über den vSphere Distributed Switch zur Verfügung.

- 7 Klicken Sie auf **OK**.

Aktivieren des Link Layer Discovery Protocol (LLDP) auf einem vSphere Distributed Switch

vSphere-Administratoren können mithilfe des Link-Layer Discovery Protocol (LLDP) den physischen Switch-Port ermitteln, mit dem ein angegebener vSphere Distributed Switch verbunden ist. Wenn LLDP für einen bestimmten Distributed Switch aktiviert ist, können Sie die Eigenschaften des physischen Switches, wie z. B. Chassis-ID, Systemnamen und -beschreibung sowie Gerätefunktionen, vom vSphere Client aus anzeigen.

LLDP steht nur in vSphere Distributed Switch Version 5.0.0 und höher zur Verfügung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und wählen Sie die Bestandslistenansicht **Netzwerk**.
- 2 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich auf den vSphere Distributed Switch und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie auf der Registerkarte **Eigenschaften** die Option **Erweitert** aus.
- 4 Wählen Sie **Aktiviert** aus dem Dropdown-Menü **Status**.
- 5 Wählen Sie **Link-Layer Discovery Protocol (LLDP)** aus dem Dropdown-Menü **Typ**.

- 6 Wählen Sie den LLDP-Modus aus dem Dropdown-Menü **Vorgang**.

Option	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switchport an, jedoch stehen dem Switch-Administrator keine Informationen über den vSphere Distributed Switch zur Verfügung.
Anzeigen	ESXi stellt dem Switch-Administrator Informationen zum vSphere Distributed Switch zur Verfügung, ohne jedoch Informationen über den physischen Switch zu erkennen oder anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch an und stellt dem Switch-Administrator Informationen über den vSphere Distributed Switch zur Verfügung.

- 7 Klicken Sie auf **OK**.

Anzeigen von Switchinformationen auf dem vSphere Client

Wenn CDP oder LLDP auf **Überwachen** oder **Beides** festgelegt ist, können Sie Informationen zu physischen Switches vom vSphere Client aus ansehen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf das Informationssymbol rechts neben dem vSphere Standard-Switch bzw. dem vSphere Distributed Switch, um Informationen über den jeweiligen Switch zu erhalten.

Informationen zu dem ausgewählten Switch werden angezeigt.

Ändern der DNS- und Routing-Konfiguration

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Verwaltung von MAC-Adressen

MAC-Adressen werden auf Schicht 2 (Sicherheitsschicht) des Netzwerkprotokoll-Stacks zum Übertragen von Frames an den Empfänger verwendet. In vSphere generiert vCenter Server MAC-Adressen für Adapter der virtuellen Maschine und für VMkernel-Adapter. Sie können aber auch manuell Adressen zuweisen.

Jedem Hersteller von Netzwerkadaptern wird ein eindeutiges, drei Byte großes Präfix zugewiesen, das als OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) genannt wird und das der Hersteller zur Generierung eindeutiger MAC-Adressen verwenden kann.

VMware unterstützt mehrere Adresszuteilungsmechanismen mit jeweils einem separaten OUI:

- Generierte MAC-Adressen
 - Von vCenter Server zugewiesen
 - Vom ESXi-Host zugewiesen
- Manuell festgelegte MAC-Adressen
- Für ältere virtuelle Maschinen generiert (wird jedoch bei ESXi nicht mehr verwendet)

Wenn Sie den Netzwerkadapter einer ausgeschalteten virtuellen Maschine neu konfigurieren, zum Beispiel durch das Ändern des automatischen MAC-Adressen-Zuteilungstyps oder durch das Festlegen einer statischen MAC-Adresse, löst vCenter Server alle MAC-Adressenkonflikte, bevor die Adapterneukonfiguration übernommen wird.

Hinzufügen oder Anpassen von bereichs- oder präfixbasierten Zuteilungen im vSphere Client

Wenn Sie eine bereichs- oder präfixbasierte Zuteilung verwenden, können Sie mit dem vSphere Client die Parameter für die Zuteilung anpassen.

Um die Zuteilungsschemen von VMware OUI in eine bereichs- oder präfixbasierte Zuteilung zu ändern, müssen Sie unter „Erweiterte Einstellungen“ einen Schlüssel und einen Standardwert hinzufügen. Wenn Sie bereits den Schlüssel und die Standardwerte hinzugefügt haben, können Sie unter **Erweiterte Einstellungen** die Parameter für jeden Schlüssel anpassen.

Eine Änderung von einer bereichs- oder präfixbasierten Zuteilung zur VMware OUI-Zuteilung ist mit dem vSphere Client nicht möglich. Sie müssen die Datei `vpxd.cfg` manuell bearbeiten. Es wird empfohlen, die Zuteilungstypen über den vSphere Client zu ändern, weil es bei der Bearbeitung von Dateien zu Fehlern kommen kann. Weitere Informationen zur Bearbeitung der Datei `vpxd.cfg` finden Sie in der Dokumentation zu *vSphere-Netzwerken*.



VORSICHT Die präfixbasierte Zuteilung von MAC-Adressen wird nur von vCenter Server 5.1 und 5.1-Hosts unterstützt. Wenn Sie Hosts vor 5.1 zu vCenter Server 5.1 hinzufügen und etwas anderes als die VMware OUI-präfixbasierte Zuteilung von MAC-Adressen verwenden, können virtuelle Maschinen mit Nicht-VMware OUI-MAC-Adressen mit Präfix auf Hosts vor 5.1 nicht eingeschaltet werden.

Die präfixbasierten Zuteilungsschemen von MAC-Adressen werden auf Hosts vor 5.1 nicht unterstützt, weil Hosts vor 5.1 explizit validieren, ob eine zugeteilte MAC-Adresse den Präfix VMware OUI 00:50:56 verwendet. Wenn die MAC-Adresse nicht den Präfix 00:50:56 aufweist, kann der Host vor 5.1 der virtuellen Maschine nicht eingeschaltet werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere Client **Verwaltung > Servereinstellungen**.

- 2 Klicken Sie auf **Erweiterte Einstellungen**.
- 3 Fügen Sie eine der folgenden Zuteilungstypen hinzu oder passen Sie diese an.

HINWEIS Verwenden Sie nur einen Zuteilungstyp.

◆ Präfixbasierte Zuteilung

Schlüssel	Standardwert
config.vpxd.macAllocScheme.prefixScheme.prefix	005026
config.vpxd.macAllocScheme.prefixScheme.prefixLength	23

Ändern Sie die Standardwerte entsprechend Ihrer Wahl des Präfixes und der Präfixlänge.

◆ Bereichsbasierte Zuteilung

Schlüssel	Standardwert
config.vpxd.macAllocScheme.rangeScheme.range[0].begin	005067000000
config.vpxd.macAllocScheme.rangeScheme.range[0].end	005067ffff

Ändern Sie die Standardwerte auf den Zuteilungsbereich Ihrer Wahl. Ersetzen Sie [0] durch die Bereichs-ID Ihrer Wahl.

- 4 Klicken Sie auf **OK**.

Zuweisen von statischen MAC-Adressen im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht** auf **Einstellungen bearbeiten**.
- 3 Wählen Sie in der Liste Hardware (Hardware) den Netzwerkadapter aus.
- 4 Wählen Sie unter MAC-Adresse (MAC Address) die Option **Manuell (Manual)** aus.
- 5 Geben Sie die statische MAC-Adresse ein und klicken Sie auf **OK**.

Wenn Sie mithilfe des vSphere Client eine Verbindung mit einem Host oder einem vCenter Server-System herstellen, können Sie eine Reihe von Speicherverwaltungsaufgaben durchführen, beispielsweise Konfigurieren von Adaptern, Erstellen von Datenspeichern und Anzeigen von Informationen zu Speichergeräten.

Dieses Kapitel behandelt die folgenden Themen:

- „Speichereinschränkungen im vSphere Client“, auf Seite 336
- „Anzeigen von Speichergeräten für einen Host im vSphere Client“, auf Seite 336
- „Anzeigen von Speichergeräten für einen Adapter im vSphere Client“, auf Seite 337
- „Anzeigen von Informationen zu Speicheradaptern im vSphere Client“, auf Seite 337
- „Überprüfen der Informationen zu Datenspeichern im vSphere Client“, auf Seite 337
- „Zuweisen von WWNs zu virtuellen Maschinen“, auf Seite 338
- „Ändern von WWN-Zuweisungen“, auf Seite 339
- „Einrichten des Netzwerks für Software-FCoE“, auf Seite 339
- „Hinzufügen von Software-FCoE-Adaptern“, auf Seite 340
- „Deaktivieren der automatischen Hostregistrierung“, auf Seite 341
- „Einrichten von unabhängigen Hardware-iSCSI-Adaptern“, auf Seite 341
- „Konfigurieren von abhängigen Hardware-iSCSI-Adaptern“, auf Seite 343
- „Konfigurieren von Software-iSCSI-Adaptern“, auf Seite 345
- „Einrichten des iSCSI-Netzwerks“, auf Seite 347
- „Verwenden von Jumbo-Frames mit iSCSI“, auf Seite 352
- „Konfigurieren von Erkennungsadressen für iSCSI-Adapter“, auf Seite 353
- „Konfigurieren von CHAP-Parametern für iSCSI-Adapter“, auf Seite 355
- „Konfigurieren erweiterter Parameter für iSCSI im vSphere Client“, auf Seite 359
- „Verwalten von Speichergeräten“, auf Seite 359
- „Arbeiten mit Datenspeichern“, auf Seite 361
- „Raw-Gerätezuordnung“, auf Seite 372
- „Grundlegendes zu Multipathing und Failover“, auf Seite 374
- „Speicherhardware-Beschleunigung“, auf Seite 377

- „Thin Provisioning von Speicher“, auf Seite 377
- „Verwenden von Speicher-Anbieter-Providern“, auf Seite 380

Speichereinschränkungen im vSphere Client

Die Speicheraufgaben, die Sie bei einer direkten Verbindung mit einem ESXi-Host oder einem vCenter Server-System mit dem vSphere Client ausführen können, sind eingeschränkt.

Die folgenden Speicherfunktionen sind im vSphere Client nicht verfügbar bzw. schreibgeschützt:

- AHCI SATA-Geräte
- NFS-Client 4.1 mit Kerberos
- Storage DRS mit vSphere Replication
- Interoperabilität zwischen Storage DRS und vCenter Site Recovery Manager
- E/A-Filter für Speicherrichtlinien
- Verwaltung von Virtual SAN-Festplattengruppen
- Fehler- und Warnmeldungen für Virtual SAN-Profilkompatibilität
- Auf Virtual SAN-Speicherrichtlinien basierte Verwaltung
- Virtual SAN-Standardprofile
- Nutzung von Virtual SAN-Festplatten
- Isolierung von Fault Domains in Virtual SAN
- Virtuelle Volumes
- vSphere-Flash-Lesecache
- vSphere Flash Read Cache DRS-Interoperabilität

Über den vSphere Web Client stehen Ihnen hingegen alle Speicherfunktionen Ihrer vSphere 6.0-Umgebung zur Verfügung.

Anzeigen von Speichergeräten für einen Host im vSphere Client

Verwenden Sie den vSphere Client, um alle einem Host zur Verfügung stehenden Speichergeräte oder LUNs anzuzeigen. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Anzeigen von Speichergeräten für einen Adapter im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Anzeigen von Informationen zu Speicheradaptern im vSphere Client

Verwenden Sie den vSphere Client zum Anzeigen der von Ihrem Host verwendeten Speicheradapter und zum Überprüfen ihrer Informationen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Überprüfen der Informationen zu Datenspeichern im vSphere Client

Verwenden Sie den vSphere Client, um alle auf den Hosts verfügbaren Datenspeicher anzuzeigen und deren Eigenschaften zu analysieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Zuweisen von WWNs zu virtuellen Maschinen

Sie können einer neuen virtuellen Maschine mit einer RDM-Festplatte einen WWN zuweisen, wenn Sie die virtuelle Maschine erstellen.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Öffnen Sie den Assistenten Neue virtuelle Maschine.
- 2 Wählen Sie **Benutzerdefiniert** aus, und klicken Sie auf **Weiter**.
- 3 Befolgen Sie sämtliche Anweisungen zum Erstellen einer benutzerdefinierten virtuellen Maschine.
- 4 Wählen Sie auf der Seite „Festplatte auswählen“ die Option **Zuordnungen für Raw-Geräte** und klicken Sie auf **Weiter**.
- 5 Wählen Sie in der Liste der SAN-Festplatten bzw. LUNs eine Raw-LUN, auf welche die virtuelle Maschine direkt zugreifen soll.
- 6 Wählen Sie einen Datenspeicher für die Raw-Gerätezuordnungsdatei aus.

Sie können die Raw-Gerätezuordnungsdatei im selben Datenspeicher ablegen, in dem sich die Datei der virtuellen Maschine befindet, oder einen anderen Datenspeicher auswählen.

HINWEIS Wenn Sie VMotion für eine virtuelle Maschine mit aktivierter NPIV verwenden möchten, stellen Sie sicher, dass sich die Raw-Gerätezuordnungsdatei auf demselben Datenspeicher wie die Konfigurationsdateien der virtuellen Maschine befindet.

- 7 Führen Sie die Schritte zum Erstellen einer virtuellen Maschine mit dem RDM aus.
- 8 Aktivieren Sie auf der Seite „Bereit zum Abschließen“ das Kontrollkästchen **Einstellungen der virtuellen Maschine vor Fertigstellung bearbeiten** und klicken Sie auf **Weiter**.

Das Dialogfeld Eigenschaften der virtuellen Maschinen wird geöffnet.

- 9 Weist WWNs zur virtuellen Maschine hinzu.
 - a Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **Fibre-Channel-NPIV**.
 - b Wählen Sie **Neue WWNs generieren**.
 - c 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.

- 10 Klicken Sie auf **Beenden**.

Der Host erstellt WWN-Zuweisungen für die virtuelle Maschine.

Weiter

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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

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.

Vorgehensweise

- 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
NPIV für diese virtuelle Maschine vorübergehend deaktivieren	Deaktivieren Sie die WWN-Zuweisungen für die virtuelle Maschine.
Unverändert lassen	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.
Neue WWNs generieren	Neue WWNs werden generiert und der virtuellen Maschine zugewiesen, wobei vorhandene WWNs überschrieben werden (dies betrifft nicht die HBA-WWNs).
WWN-Zuweisung entfernen	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.

Einrichten des Netzwerks für Software-FCoE

Bevor Sie die Software-FCoE-Adapter aktivieren, müssen Sie den VMkernel mit den physischen FCoE-Netzwerkkarten verbinden, die auf dem Host installiert sind.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

- 3 Klicken Sie in der Ansicht „vSphere Standard-Switch“ auf **Netzwerk hinzufügen**.
- 4 Wählen Sie **VMkernel (VMkernel)** aus, und klicken Sie auf **Weiter**.
- 5 Wählen Sie **vSphere Standard-Switch erstellen**, um einen neuen vSphere Standard-Switch zu erstellen.
- 6 Wählen Sie den Netzwerkkadapter aus (vmnic#), der FCoE unterstützt, und klicken Sie auf **Weiter**.

Wenn Ihr Host über mehrere Netzwerkkadapter oder mehrere Ports auf dem Adapter verfügt, können Sie alle diese zu einem einzelnen vSphere Standard-Switch hinzufügen. Als Alternative kann jede FCoE-Netzwerkkarte mit einem separaten Standard-Switch verbunden werden.

HINWEIS ESXi unterstützt maximal vier Netzwerkkadapter-Ports, die für Software-FCoE verwendet werden.

- 7 Geben Sie eine Netzwerkbezeichnung ein.

Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. „FCoE“.
- 8 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*.
- 9 Geben Sie die IP-Einstellungen an und klicken Sie auf **Weiter**.
- 10 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

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

HINWEIS Um Störungen im FCoE-Datenverkehr zu vermeiden, sollten Sie den FCoE-Netzwerkkadapter (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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

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

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicheradapter**.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie **Software-FCoE-Adapter** aus und klicken Sie auf **OK**.

- 4 Wählen Sie im Dialogfeld „Hinzufügen von Software-FCoE-Adaptoren“ 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.

- 5 Klicken Sie auf **OK**.

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

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.

Deaktivieren der automatischen Hostregistrierung

Wenn Sie EMC CLARiiON- oder Invista-Arrays verwenden, müssen sich die Hosts bei den Arrays registrieren. 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.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere Clients den gewünschten Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und dann unter „Software“ auf **Erweiterte Einstellungen (Advanced Settings)**.
- 3 Klicken Sie im linken Bedienfeld auf **Festplatte** und scrollen Sie nach unten bis „Disk.EnableNaviReg“ (rechts).
- 4 Ändern Sie den Standardwert in 0.

Die standardmäßig aktivierte automatische Hostregistrierungsfunktion wird dadurch deaktiviert.

Einrichten von unabhängigen Hardware-iSCSI-Adaptoren

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.

Wenn Sie den vSphere Client direkt mit einem Host verbinden, umfasst der Installations- und Konfigurationsprozess für die unabhängigen Hardware-iSCSI-Adapter die folgenden Schritte:

- 1 Prüfen Sie, ob der Adapter lizenziert werden muss.
Informationen finden Sie in der Dokumentation des Anbieters.
- 2 Installieren Sie den Adapter.
Informationen zur Installation sowie zu Firmware-Updates finden Sie in der Herstellerdokumentation.
- 3 Stellen Sie sicher, dass der Adapter ordnungsgemäß installiert wurde.
Weitere Informationen hierzu finden Sie unter [„Anzeigen von unabhängigen Hardware-iSCSI-Adaptoren im vSphere Client“](#), auf Seite 342.
- 4 Konfigurieren Sie die Erkennungsinformationen.
Weitere Informationen hierzu finden Sie unter [„Konfigurieren von Erkennungsadressen für iSCSI-Adapter“](#), auf Seite 353.

- 5 (Optional) CHAP-Parameter konfigurieren.

Weitere Informationen hierzu finden Sie unter „[Konfigurieren von CHAP-Parametern für iSCSI-Adapter](#)“, auf Seite 355.

- 6 (Optional) Aktivieren Sie Jumbo-Frames.

Weitere Informationen hierzu finden Sie unter „[Verwenden von Jumbo-Frames mit iSCSI](#)“, auf Seite 352.

Anzeigen von unabhängigen Hardware-iSCSI-Adaptern im vSphere Client

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 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**

Vorgehensweise

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

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

- 3 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.

- 4 Klicken Sie auf **Eigenschaften**.

Das Dialogfeld iSCSI-Initiator-Eigenschaften wird angezeigt. Auf der Registerkarte **Allgemein** werden zusätzliche Merkmale des Adapters angezeigt.

Sie können den unabhängigen Hardwareadapter jetzt konfigurieren oder seine Standardmerkmale ändern.

Ändern des Namens und der IP-Adresse für unabhängige Hardware-iSCSI-Adapter

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.
- 2 Klicken Sie auf **Konfigurieren**.
- 3 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.

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

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

- 5 Ändern Sie die Standard-IP-Einstellungen.

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

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

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.

Konfigurieren von 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.

Der gesamte Installations- und Konfigurationsprozess für die abhängigen Hardware-iSCSI-Adapter besteht aus diesen Schritten:

- 1 Zeigen Sie die abhängigen Hardware-Adapter an.

Weitere Informationen hierzu finden Sie unter „[Abhängige Hardware-iSCSI-Adapter anzeigen](#)“, auf Seite 344.

Falls Ihre abhängigen Hardware-Adapter nicht in der Liste der Speicheradapter angezeigt werden, vergewissern Sie sich, dass sie lizenziert werden müssen. Informationen finden Sie in der Dokumentation des Anbieters.

- 2 Ermitteln Sie, welchen physischen Netzwerkkarten die abhängigen Hardware-Adapter zugeordnet sind.

Weitere Informationen hierzu finden Sie unter „[Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkkartentypen](#)“, auf Seite 344.

Notieren Sie sich die Namen der zugehörigen physischen Netzwerkkarten. Beispielsweise gehört der Adapter „vmhba33“ zu „vmnic1“ und „vmhba34“ zu „vmnic2“.

- 3 Konfigurieren Sie das Netzwerk für iSCSI.

Weitere Informationen hierzu finden Sie unter „[Einrichten des iSCSI-Netzwerks](#)“, auf Seite 347.

Im Rahmen der Konfiguration des Netzwerks muss eine VMkernel-Schnittstelle für jeden physischen Netzwerkadapter erstellt und die Schnittstelle mit einem entsprechenden iSCSI-Adapter verknüpft werden.

- 4 (Optional) Aktivieren Sie Jumbo-Frames.
Weitere Informationen hierzu finden Sie unter „[Verwenden von Jumbo-Frames mit iSCSI](#)“, auf Seite 352.
- 5 Konfigurieren Sie die Erkennungsinformationen.
Weitere Informationen hierzu finden Sie unter „[Konfigurieren von Erkennungsadressen für iSCSI-Adapter](#)“, auf Seite 353.
- 6 (Optional) CHAP-Parameter konfigurieren.
Weitere Informationen hierzu finden Sie unter „[Konfigurieren von CHAP-Parametern für iSCSI-Adapter](#)“, auf Seite 355.

Abhängige Hardware-iSCSI-Adapter anzeigen

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

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.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

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

Falls installiert, werden die abhängigen Hardware-iSCSI-Adapter in der Liste der Speicheradapter unter Kategorien wie z. B. „Broadcom iSCSI Adapter“ angezeigt.
- 3 Wählen Sie den Adapter aus, der angezeigt werden soll, und klicken Sie auf **Eigenschaften**.

Das Dialogfeld „Eigenschaften des iSCSI-Initiators“ wird angezeigt. Es enthält die standardmäßigen Detailinformationen zu dem Adapter, wie iSCSI-Namen, iSCSI-Alias und Status.
- 4 (Optional) Soll der Standard-iSCSI-Name geändert werden, klicken Sie auf **Konfigurieren**.

Weiter

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.

Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern

Netzwerkverbindungen dienen dazu, abhängige iSCSI- und 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

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

Vorgehensweise

- 1 Klicken Sie im Dialogfeld „iSCSI-Initiator-Eigenschaften“ auf die Registerkarte **Netzwerkkonfiguration**.

- 2 Klicken Sie auf **Hinzufügen**.

Der Netzwerkadapter, beispielsweise vmnic2, der dem abhängigen iSCSI-Adapter entspricht, wird aufgelistet.

Weiter

Sie müssen die zugewiesenen abhängigen Hardware-iSCSI- und Netzwerkadapter anhand von Netzwerkverbindungen binden.

Konfigurieren von Software-iSCSI-Adaptern

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 Netzwerkstack 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 Netzwerkadapter für iSCSI fest. Verwenden Sie iSCSI nicht bei Adaptern mit 100 MBit/s oder weniger.

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

- 1 Aktivieren Sie den Software-iSCSI-Adapter.

Weitere Informationen hierzu finden Sie unter „[Aktivieren des Software-iSCSI-Adapters im vSphere Client](#)“, auf Seite 345.

- 2 Konfigurieren Sie das Netzwerk für iSCSI.

Weitere Informationen hierzu finden Sie unter „[Einrichten des iSCSI-Netzwerks](#)“, auf Seite 347.

Im Rahmen der Konfiguration des Netzwerks muss für jeden physischen Netzwerkadapter, den Sie für iSCSI verwenden, eine VMkernel-Schnittstelle erstellt und alle Schnittstellen müssen mit dem Software-iSCSI-Adapter müssen verknüpft werden.

- 3 (Optional) Aktivieren Sie Jumbo-Frames.

Weitere Informationen hierzu finden Sie unter „[Verwenden von Jumbo-Frames mit iSCSI](#)“, auf Seite 352.

- 4 Konfigurieren Sie die Erkennungsinformationen.

Weitere Informationen hierzu finden Sie unter „[Konfigurieren von Erkennungsadressen für iSCSI-Adapter](#)“, auf Seite 353.

- 5 (Optional) CHAP-Parameter konfigurieren.

Weitere Informationen hierzu finden Sie unter „[Konfigurieren von CHAP-Parametern für iSCSI-Adapter](#)“, auf Seite 355.

Aktivieren des Software-iSCSI-Adapters im vSphere Client

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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicheradapter**.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie **Software-iSCSI-Adapter**.
Der Software-iSCSI-Adapter wird in der Liste der Speicheradapter angezeigt.
- 4 Wählen Sie den iSCSI-Adapter aus der Liste aus und klicken Sie auf **Eigenschaften**.
- 5 Klicken Sie auf **Konfigurieren**.
- 6 Stellen Sie sicher, dass der Adapter aktiviert ist, und klicken Sie auf **OK**.

Nachdem Sie den Adapter aktiviert haben, weist ihm der Host den Standard-iSCSI-Namen zu. Falls Sie den Standardnamen ändern möchten, befolgen Sie die iSCSI-Namenskonventionen.

Deaktivieren des Software-iSCSI-Adapters im vSphere Client

Verwenden Sie den vSphere Client, um den Software-iSCSI-Adapter zu deaktivieren, wenn Sie ihn nicht benötigen.

HINWEIS Wenn Sie den für den Software-iSCSI-Start verwendeten Adapter deaktivieren, wird dieser jedesmal, wenn Sie den Host starten, reaktiviert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter Hardware auf **Speicheradapter**.
- 3 Wählen Sie den Software-iSCSI-Adapter aus der Liste der Speicheradapter aus und klicken Sie auf **Eigenschaften**.
- 4 Klicken Sie auf **Konfigurieren**.
- 5 Um den Adapter zu deaktivieren, heben Sie die Auswahl der Option **Aktiviert** auf und klicken auf **OK**.
- 6 Starten Sie den Host neu.

Nach dem Neustart wird der Adapter nicht mehr in der Liste der Speicheradapter angezeigt.

Der Status zeigt an, dass der Adapter deaktiviert wurde.

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>.

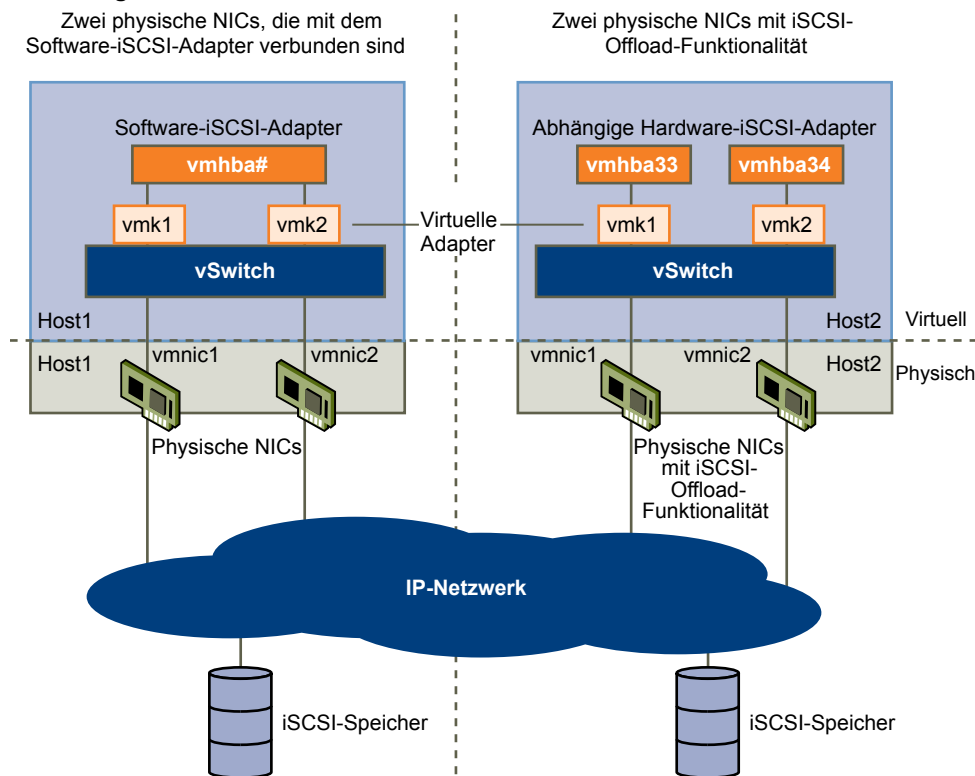
Mehrere Netzwerkadapter in der iSCSI-Konfiguration

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 24-1. Netzwerk mit iSCSI



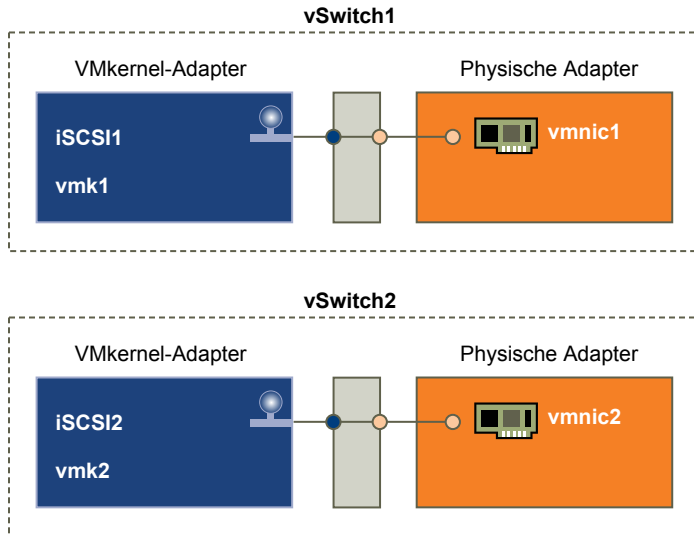
Der iSCSI-Adapter und die physische Netzwerkkarte werden über einen virtuellen VMkernel-Adapter verbunden, der auch als virtueller Netzwerkadapter oder VMkernel-Port bezeichnet wird. Sie erstellen einen VMkernel-Adapter (vmk) auf einem vSphere-Switch (vSwitch) mithilfe einer 1:1-Zuordnung zwischen jedem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

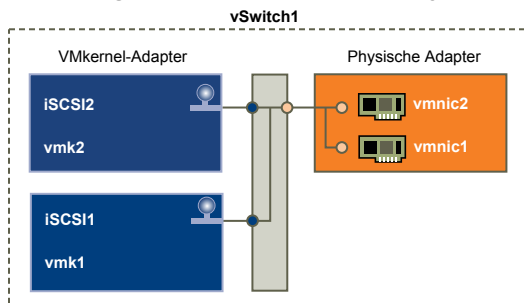
Abbildung 24-2. 1:1-Adapterzuordnung auf separaten vSphere Standard-Switches



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 24-3. 1:1-Adapterzuordnung auf einem einzelnen vSphere Standard-Switch



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

Tabelle 24-1. Netzwerkkonfiguration für iSCSI

iSCSI-Adapter	VMkernel-Adapter (Ports)	Physische Adapter (NICs)
Software-iSCSI		
vmhba32	vmk1	vmnic1

Tabelle 24-1. Netzwerkkonfiguration für iSCSI (Fortsetzung)

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

Erstellen von Netzwerkverbindungen für iSCSI im vSphere-Client

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*.

Erstellen eines einzelnen VMkernel-Adapters für iSCSI

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Klicken Sie in der Ansicht „vSphere Standard-Switch“ auf **Netzwerk hinzufügen**.
- 4 Wählen Sie **VMkernel (VMkernel)** aus, und klicken Sie auf **Weiter**.
- 5 Wählen Sie **vSphere Standard-Switch erstellen** aus, um einen neuen vSphere Standard-Switch zu erstellen.
- 6 Wählen Sie eine Netzwerkkarte aus, die Sie für iSCSI-Datenverkehr verwenden möchten.

WICHTIG Wenn Sie eine VMkernel-Schnittstelle für den abhängigen Hardware-iSCSI-Adapter erstellen, wählen Sie die Netzwerkkarte aus, die zu der iSCSI-Komponente gehört. Siehe [„Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptem“](#), auf Seite 344.

- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie eine Netzwerkbezeichnung ein.
Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. iSCSI.
- 9 Klicken Sie auf **Weiter**.
- 10 Geben Sie die IP-Einstellungen an und klicken Sie auf **Weiter**.
- 11 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

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

Weiter

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 Netzwerkkarten mit einem einzigen vSphere Standard-Switch verbinden möchten. Mit diesem Verfahren fügen Sie Netzwerkkarten und VMkernel-Adapter zu einem vorhandenen vSphere Standard-Switch hinzu.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Sie müssen einen vSphere Standard-Switch erstellen, der einen VMkernel-iSCSI-Adapter einer einzelnen physischen Netzwerkkarte zuordnet, die für den iSCSI-Datenverkehr vorgesehen ist.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie den vSphere Standard-Switch aus, den Sie für iSCSI verwenden, und klicken Sie auf **Eigenschaften**.
- 4 Verbinden Sie zusätzliche Netzwerkadapter mit dem Standard-Switch.
 - a Klicken Sie im Dialogfeld „Eigenschaften des Standard-Switches“ auf die Registerkarte **Netzwerkadapter** und klicken Sie auf **Hinzufügen**.
 - b Wählen Sie mindestens eine Netzwerkkarte in der Liste aus und klicken Sie auf **Weiter**.
Wählen Sie für abhängige Hardware-iSCSI-Adapter nur die Netzwerkkarten aus, die eine entsprechende iSCSI-Komponente besitzen.
 - c Überprüfen Sie die Informationen auf der Seite Adapterübersicht und klicken Sie auf **Beenden**.
Die Liste der Netzwerkadapter mit den nun dem vSphere Standard-Switch zugewiesenen Netzwerkadaptern wird erneut angezeigt.
- 5 Erstellen Sie iSCSI-VMkernel-Adapter für alle hinzugefügten Netzwerkkarten.
Die Anzahl an VMkernel-Schnittstellen muss mit der Anzahl an Netzwerkkarten auf dem vSphere Standard-Switch übereinstimmen.
 - a Klicken Sie im Dialogfeld „Eigenschaften des Standard-Switches“ auf die Registerkarte **Ports** und anschließend auf **Hinzufügen**.
 - b Wählen Sie **VMkernel (VMkernel)** aus, und klicken Sie auf **Weiter**.
 - c Geben Sie unter **Portgruppeneigenschaften** eine Netzwerkbezeichnung ein, z. B. „iSCSI“, und klicken Sie auf **Weiter**.

- d Geben Sie die IP-Einstellungen an und klicken Sie auf **Weiter**.

Wenn Sie die Subnetzmaske eingeben, stellen Sie sicher, dass die Netzwerkkarte auf das Subnetz des Speichersystems eingestellt ist, mit dem sie verbunden wird.

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



VORSICHT Wenn sich die Netzwerkkarte, die Sie mit Ihrem Software- oder abhängigen Hardware-iSCSI-Adapter verwenden, nicht im selben Subnetz befindet wie Ihr iSCSI-Ziel, können Sie keine Sitzungen von diesen Netzwerkadap-tern zum Ziel einrichten.

Weiter

Ändern Sie die Netzwerkkarte für alle VMkernel-Adapter, damit sie mit den Anforderungen an die Netzwerkbindung kompatibel ist. Sie können dann die iSCSI-VMkernel-Adapter an die Software-iSCSI- oder an die abhängigen Hardware-iSCSI-Adapter binden.

Ändern der Portgruppenrichtlinie für iSCSI-VMkernel-Adapter

Wenn Sie einen einzelnen vSphere Standard-Switch zum Verbinden von VMkernel mit mehreren Netzwerkadap-tern verwenden, ändern Sie die Portgruppenrichtlinie, damit sie mit den Anforderungen für iSCSI-Netzwerke kompatibel ist.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Wählen Sie den vSphere Standard-Switch aus, den Sie für iSCSI verwenden, und klicken Sie auf **Eigenschaften**.
- 4 Wählen Sie auf der Registerkarte **Ports** einen iSCSI-VMkernel-Adapter aus und klicken Sie auf **Bearbeiten**.
- 5 Klicken Sie auf die Registerkarte **NIC-Gruppierung** und wählen Sie **Switch-Failover-Reihenfolge 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.

Weiter

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

Binden von iSCSI-Adaptern mit VMkernel-Adaptern im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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**

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicheradapter**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Wählen Sie den zu konfigurierenden Software- oder abhängigen iSCSI-Adapter aus und klicken Sie auf **Eigenschaften**.
- 4 Klicken Sie im Dialogfeld „iSCSI-Initiator-Eigenschaften“ auf die Registerkarte **Netzwerkkonfiguration**.
- 5 Klicken Sie auf **Hinzufügen** und wählen Sie einen VMkernel-Adapter aus, der an den iSCSI-Adapter gebunden werden soll.
Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter ist nur eine VMkernel-Schnittstelle verfügbar, die mit der richtigen physischen Netzwerkkarte verknüpft ist.
- 6 Klicken Sie auf **OK**.
Die Netzwerkverbindung wird in der Liste der VMkernel-Portbindungen für den iSCSI-Adapter angezeigt.
- 7 Stellen Sie sicher, dass die Netzwerkrichtlinie für die Verbindung die Anforderungen für das Binden erfüllt.

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 24-2. 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 iSCSI

Verwenden Sie den vSphere Client, um Jumbo Frames für jeden vSphere Standard-Switch und VMkernel-Adapter zu aktivieren, die für den iSCSI-Datenverkehr vorgesehen sind.

Sie aktivieren Jumbo-Frames auf dem Standard-Switch und dem VMkernel-Adapter, indem Sie den MTU-Parameter entsprechend ändern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Netzwerk**.
- 3 Klicken Sie auf **Eigenschaften** für den Standard-Switch, den Sie für den iSCSI-Datenverkehr verwenden.
- 4 Wählen Sie auf der Registerkarte „Ports“ den Standard-Switch aus und klicken Sie auf **Bearbeiten**.
- 5 Legen Sie den MTU-Parameter für den Standard-Switch fest und klicken Sie auf **OK**.
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.
- 6 Wählen Sie auf der Registerkarte „Ports“ den VMkernel-Adapter aus und klicken Sie auf **Bearbeiten**.
- 7 Legen Sie den Wert der MTU so fest, dass er mit dem auf dem Standard-Switch konfigurierten Wert übereinstimmt, und klicken Sie auf **OK**.

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 Erkennung im vSphere Client

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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Wenn Sie die dynamische Erkennung einrichten, können Sie nur ein neues iSCSI-System hinzufügen. Sie können die IP-Adresse, den DNS-Namen oder die Portnummer eines vorhandenen iSCSI-Systems nicht ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene System und fügen Sie ein neues hinzu.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicheradapter**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 3 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicheradapter**.
Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.
- 4 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **Eigenschaften**.
- 5 Klicken Sie auf die Registerkarte **Dynamische Erkennung**.
- 6 Um der „SendTargets“-Erkennungsmethode eine Adresse hinzuzufügen, klicken Sie auf **Hinzufügen**.
- 7 Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf **OK**.
Nachdem der Host die „SendTargets“-Sitzung mit diesem System gestartet hat, werden in der Liste „Statische Erkennung“ alle neu erkannten Ziele angezeigt.

- 8 Sie können einen bestimmten „SendTargets“-Server löschen, indem Sie ihn auswählen und auf **Entfernen** klicken.

Nachdem Sie einen „SendTargets“-Server entfernt haben, wird er möglicherweise immer noch im Feld „Vererbung“ als übergeordnetes Element von statischen Zielen angezeigt. Dieser Eintrag zeigt an, wo die statischen Ziele ermittelt wurden, und wirkt sich nicht auf die Funktionsweise aus.

Weiter

Nachdem Sie die dynamische Erkennung für Ihren iSCSI-Adapter eingerichtet haben, prüfen Sie den Adapter erneut.

Einrichten der statischen Erkennung im vSphere Client

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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

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

Vorgehensweise

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

Weiter

Nachdem Sie die statische Erkennung für Ihren iSCSI-Adapter eingerichtet haben, prüfen Sie den Adapter erneut.

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.

Einrichten von CHAP für iSCSI-Adapter im vSphere Client

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

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

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

- Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI oder abhängige Hardware-iSCSI fest, ob unidirektionales oder beiderseitiges CHAP konfiguriert werden soll. Abhängige Hardware-iSCSI-Adapter unterstützen das beiderseitige CHAP nicht.
 - Bei unidirektionalem CHAP authentifiziert das Ziel den Initiator.
 - Bei beiderseitigem CHAP authentifizieren sich das Ziel und der Initiator gegenseitig. Verwenden Sie für CHAP und beiderseitiges CHAP verschiedene Schlüssel.

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

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

Vorgehensweise

- 1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.
- 2 Klicken Sie auf der Registerkarte **Allgemein** auf **CHAP**.
- 3 Wenn Sie das unidirektionale CHAP konfigurieren möchten, geben Sie unter CHAP Folgendes an:
 - a Wählen Sie die CHAP-Sicherheitsstufe.
 - CHAP nicht verwenden, sofern nicht vom Ziel benötigt (nur Software- und abhängige Hardware-iSCSI)
 - CHAP verwenden, es sei denn, das Ziel verbietet dies
 - CHAP verwenden (nur Software- und abhängige Hardware-iSCSI). Um beiderseitiges CHAP zu konfigurieren, müssen Sie diese Option auswählen.

- b Geben Sie den CHAP-Namen an.

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

- Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiator-Name verwenden**.
 - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Textfeld **Name** ein.
 - c Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.

- 4 Wenn Sie beiderseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter [Schritt 3](#) befolgen.

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

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

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

Einrichten von CHAP für Ziele im vSphere Client

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

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

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

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

Vorgehensweise

- 1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.
- 2 Wählen Sie die Registerkarte **Dynamische Erkennung** oder **Statische Erkennung** aus.
- 3 Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Einstellungen > CHAP**.
- 4 Konfigurieren Sie unidirektionales CHAP im Bereich „CHAP“.
 - a Deaktivieren Sie **Vom übergeordneten Element übernehmen**.
 - b Wählen Sie eine der folgenden Optionen aus:
 - CHAP nicht verwenden, sofern nicht vom Ziel benötigt
 - CHAP verwenden, es sei denn, das Ziel verbietet dies
 - CHAP verwenden. Um beiderseitiges CHAP konfigurieren zu können, müssen Sie diese Option auswählen.

- c Geben Sie den CHAP-Namen an.
Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.
 - Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiator-Name verwenden**.
 - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Feld **Name** ein.
 - d Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Stellen Sie sicher, dass Sie denselben Schlüssel verwenden, den Sie auf der Speicherseite eingeben.
- 5 Wenn Sie beiderseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter [Schritt 4](#) befolgen.
- Stellen Sie sicher, dass Sie als Option für unidirektionales CHAP **CHAP verwenden** auswählen. Geben Sie anschließend im Bereich „Beiderseitiges CHAP“ Folgendes an:
- a Deaktivieren Sie **Vom übergeordneten Element übernehmen**.
 - b Wählen Sie die Option **CHAP verwenden** aus.
 - c Geben Sie den Namen für beiderseitiges CHAP an.
 - d Geben Sie den Schlüssel für beiderseitiges CHAP an. Stellen Sie sicher, dass Sie für unidirektionales CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.
- 6 Klicken Sie auf **OK**.
- 7 Prüfen Sie den Initiator erneut.

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

Deaktivieren von CHAP

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

Wenn Sie CHAP auf einem System deaktivieren, das die CHAP-Authentifizierung benötigt, bleiben bestehende iSCSI-Sitzungen so lange aktiv, bis Sie Ihren 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.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 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 im vSphere Client

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



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

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.
- 2 Klicken Sie zum Konfigurieren von erweiterten Parametern auf der Initiatorebene auf der Registerkarte „Allgemein“ auf **Erweitert**. Fahren Sie mit [Schritt 4](#) fort.
- 3 Konfigurieren Sie erweiterte Parameter auf der Zielebene.
Auf der Zielebene können erweiterte Parameter nur für Software- und abhängige Hardware-iSCSI-Adapter konfiguriert werden.
 - a Wählen Sie die Registerkarte **Dynamische Erkennung** oder **Statische Erkennung** aus.
 - b Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Einstellungen > Erweitert**.
- 4 Geben Sie die erforderlichen Werte für die erweiterten Parameter ein, die Sie ändern möchten, und klicken Sie zum Speichern Ihrer Änderungen auf **OK**.

Verwalten von Speichergeräten

Verwalten des lokalen und vernetzten Speichergeräts, auf das Ihr ESXi-Host zugreifen kann.

Umbenennen von Speichergeräten im vSphere Client

Sie können den Anzeigenamen eines Speichergeräts ändern. Der Anzeigename wird vom ESXi-Host basierend auf dem Speichertyp und Hersteller zugewiesen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Host aus der Bestandsliste des vSphere Clients aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie auf **Speicher** und dann auf **Geräte**.
- 4 Klicken Sie mit der rechten Maustaste auf das Gerät, um es umzubenennen, und wählen Sie die Option **Umbenennen** aus.
- 5 Ändern Sie den Gerätenamen auf einen aussagekräftigen Namen.

Durchführen einer erneuten Speicherprüfung im vSphere Client

Wenn Sie Änderungen an Ihrer Host- oder SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut prüfen. Sie können alle Speicher erneut prüfen, die Ihrem Host zur Verfügung stehen. Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, auf die über einen bestimmten Adapter zugegriffen wird, führen Sie eine erneute Prüfung nur dieses Adapters durch.

Führen Sie die folgenden Schritte aus, wenn Sie die erneute Prüfung des Speichers, der einem bestimmten Host zur Verfügung steht oder auf den über einen bestimmten Adapter auf den Host zugegriffen wird, beschränken möchten. Wenn Sie den Speicher, der allen Hosts zur Verfügung steht, die von Ihrem vCenter Server-System verwaltet werden, erneut prüfen möchten, können Sie dies tun, indem Sie mit der rechten Maustaste auf ein Datacenter, einen Cluster oder einen Ordner klicken, in dem sich die Hosts befinden, und die Option **Erneut auf Datenspeicher prüfen** wählen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere Client einen Host und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie eine Option für eine erneute Prüfung aus.

Option	Beschreibung
Speicher	Klicken Sie im Fenster „Hardware“ auf Speicher und klicken Sie über dem Fenster „Datenspeicher“ oder „Geräte“ auf Alle erneut prüfen .
Speicheradapter	Klicken Sie im Fenster „Hardware“ auf Speicheradapter und klicken Sie über dem Fenster „Speicheradapter“ auf Alle erneut prüfen . HINWEIS Sie können auch mit der rechten Maustaste auf einzelne Adapter klicken und auf Erneut prüfen klicken, wenn Sie nur diesen Adapter erneut prüfen möchten.

- 3 Geben Sie den Umfang der erneuten Prüfung an.

Option	Beschreibung
Auf neue Speichergeräte prüfen	Prüfen Sie alle Adapter erneut auf neu hinzugefügte Speichergeräte. Wenn neue Geräte erkannt werden, werden sie in der Geräteliste angezeigt.
Auf neue VMFS-Volumes prüfen	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.

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.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere Client den Host, klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter "Software" auf **Erweiterte Einstellungen**.
- 2 Wählen Sie **Festplatte**.
- 3 Führen Sie einen Bildlauf zu **Disk.MaxLUN** durch.
- 4 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“.

Arbeiten mit Datenspeichern

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

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

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

- Virtual Machine File System (VMFS)
- Network File System (NFS)

Nach dem Erstellen von Datenspeichern können Sie diese auf unterschiedliche Weise 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 Alarme 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 über Datenspeichercluster finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Erstellen eines VMFS-Datenspeichers im vSphere Client

VMFS-Datenspeicher dienen als Repositories für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.

- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicher**.
- 3 Klicken Sie auf **Datenspeicher** und anschließend auf **Speicher hinzufügen**.
- 4 Markieren Sie den Speichertyp **Festplatte/LUN**, und klicken Sie auf **Weiter**.
- 5 Wählen Sie ein Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **Weiter**.

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

- 6 Wählen Sie die **Dateisystemversion** und klicken Sie auf **Weiter**.

WICHTIG Wenn Sie VMFS3 auswählen, müssen Sie unter **Formatierung** die maximale Dateigröße definieren.

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

Option	Beschreibung
Alle verfügbaren Partitionen verwenden	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.
Freien Speicherplatz verwenden	Stellt einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereit.

Wenn die zu formatierende Festplatte leer ist, zeigt die Seite **Aktuelles Festplattenlayout** den gesamten, für die Speicherkonfiguration verfügbaren Festplattenspeicher an.

- 8 Klicken Sie auf **Weiter**.
- 9 Geben Sie auf der Seite **Eigenschaften** einen Datenspeichernamen ein und klicken Sie auf **Weiter**.
- 10 Wenn der angegebene Speicherplatz für Ihre Zwecke zu groß ist, können Sie die Kapazität entsprechend anpassen.
Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.
- 11 Klicken Sie auf **Weiter**.
- 12 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **Beenden**.

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

Erstellen eines NFS-Datenspeichers im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicher**.
- 3 Klicken Sie auf **Datenspeicher** und anschließend auf **Speicher hinzufügen**.
- 4 Wählen Sie **Network File System (NFS)** als Speichertyp aus, und klicken Sie auf **Weiter**.
- 5 Geben Sie den Server-, den Mount-Punkt-Ordner- und den Datenspeichernamen ein.

Geben Sie für den Servernamen eine IP-Adresse, einen DNS-Namen oder eine NFS-UUID ein.

HINWEIS Wenn Sie das gleiche NFS-Volume auf verschiedenen Hosts mounten, müssen Sie sicherstellen, dass Server- und Ordnernamen auf allen Hosts identisch sind. Wenn die Namen nicht genau übereinstimmen, betrachten die Hosts dasselbe NFS-Volume als zwei unterschiedliche Datenspeicher. Bei Funktionen wie vMotion kann dies zu einem Fehler führen. Ein Beispiel für eine solche Diskrepanz wäre, wenn Sie **filer** als Servernamen auf einem Host und **filer.domain.com** auf dem anderen Host eingeben.

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

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-Client oder dem 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 im vSphere Client

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.

WICHTIG Sie können eine VMFS-Datenspeicherkopie nur mounten, wenn sie nicht mit dem ursprünglichen VMFS-Datenspeicher, der über dieselbe UUID verfügt, kollidiert. Zum Mounten der Kopie muss der ursprüngliche VMFS-Datenspeicher offline sein.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

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

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

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

Weiter

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

Neusignieren einer VMFS-Datenspeicherkopie im vSphere Client

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

Beim Neusignieren einer VMFS-Kopie weist ESXi der Kopie eine neue UUID und eine neue Bezeichnung zu und mountet die Kopie als einen vom Original unabhängigen Datenspeicher.

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

Beachten Sie bei der Datenspeicher-Neusignierung Folgendes:

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

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

Vorgehensweise

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

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

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

Weiter

Nach der erneuten Signierung sind möglicherweise die folgenden Schritte erforderlich:

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

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 6.0-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 24-3. 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 zu den VMFS-Sperrungsmechanismen und der Aktualisierung auf Nur-ATS finden Sie in der Dokumentation zum *vSphere-Speicher*.

Upgrade von VMFS2-Datenspeichern auf VMFS3

Wenn der Datenspeicher mit VMFS2 formatiert ist, müssen Sie zunächst ein Upgrade auf VMFS3 durchführen. Da ESXi 5.x-Hosts nicht auf VMFS2-Datenspeicher zugreifen können, verwenden Sie einen Legacy-Host (ESX/ESXi 4.x oder früher), um auf den VMFS2-Datenspeicher zuzugreifen, und führen Sie dann das Upgrade von VMFS2 auf VMFS3 durch.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Akzeptieren oder verwerfen Sie alle Änderungen an virtuellen Festplatten auf dem VMFS2-Datenspeicher, für das ein Upgrade durchgeführt werden soll.
- Sichern Sie den VMFS2-Datenspeicher.
- Stellen Sie sicher, dass der VMFS2-Datenspeicher nicht von aktiven virtuellen Maschinen verwendet wird.

- Stellen Sie sicher, dass kein anderer ESXi-Host auf den VMFS2-Datenspeicher zugreift.
- Beim Upgrade des Dateisystems VMFS2 darf die Dateiblockgröße 8 MB nicht übersteigen.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Speicher**.
- 3 Wählen Sie den Datenspeicher, der das VMFS2-Format verwendet.
- 4 Klicken Sie auf **Upgrade auf VMFS3**.
- 5 Führen Sie auf allen Hosts, auf denen der Datenspeicher angezeigt wird, eine erneute Prüfung durch.

Weiter

Nach dem Upgrade des VMFS2-Datenspeichers auf VMFS3 steht der Datenspeicher auf dem ESXi 5.x-Host zur Verfügung. Sie können jetzt den ESXi 5.x-Host verwenden, um das Upgrade auf VMFS5 abzuschließen.

Durchführen eines Upgrades von VMFS3-Datenspeichern auf VMFS5 im vSphere Client

VMFS5 ist eine neue Version des VMware-Clusterdateisystems mit Verbesserungen der Leistung und Skalierbarkeit.

Voraussetzungen

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Wenn Sie einen VMFS2-Datenspeicher verwenden, müssen Sie zunächst ein Upgrade auf VMFS3 durchführen. Befolgen Sie die unter „[Upgrade von VMFS2-Datenspeichern auf VMFS3](#)“, auf Seite 366 beschriebenen Schritte.
- Alle Hosts, die auf den Datenspeicher zugreifen, müssen VMFS5 unterstützen.
- Stellen Sie sicher, dass das Volume, das aktualisiert werden soll, mindestens über 2 MB an verfügbaren freien Blöcken und einen freien Dateideskriptor verfügt.

Vorgehensweise

- 1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Speicher**.
- 3 Wählen Sie den VMFS3-Datenspeicher aus.
- 4 Klicken Sie auf **Upgrade auf VMFS5**.
Eine Warnmeldung bezüglich der Unterstützung der Hostversion wird angezeigt.
- 5 Klicken Sie auf **OK**, um das Upgrade zu starten
Die Aufgabe VMFS aktualisieren wird in der Liste **Aktuelle Aufgaben** angezeigt.
- 6 Führen Sie auf allen Hosts, die dem Datenspeicher zugewiesen sind, eine erneute Prüfung durch.

Erhöhen der VMFS-Datenspeicherkapazität im vSphere Client

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

Verwenden Sie zum Vergrößern eines VMFS-Datenspeichers eine der folgenden Methoden:

- Fügen Sie eine neue Erweiterung hinzu. Eine Erweiterung ist eine Partition auf einem Speichergerät. Sie können einem vorhandenen VMFS-Datenspeicher bis zu 32 Erweiterungen desselben Speichertyps hinzufügen. 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.
- Vergrößern Sie eine Erweiterung in einem vorhandenen VMFS-Datenspeicher, sodass sie die verfügbare angrenzende Kapazität ausfüllt. Nur Erweiterungen mit nachfolgendem freiem Speicherplatz sind erweiterbar.

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Speicher**.
- 3 Wählen Sie in der Ansicht „Datenspeicher“ den zu erhöhenden Datenspeicher aus und klicken Sie auf **Eigenschaften**.
- 4 Klicken Sie auf **Erhöhen**.
- 5 Wählen Sie ein Gerät aus der Liste der Speichergeräte aus und klicken Sie auf **Weiter**.

Option	Beschreibung
So fügen Sie eine neue Erweiterung hinzu	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Nein“ hat.
So vergrößern Sie eine vorhandene Erweiterung	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Ja“ hat.

- 6 Prüfen Sie das **aktuelle Festplattenlayout** auf die verfügbaren Konfigurationen und klicken Sie auf **Weiter**.

- 7 Wählen Sie eine Konfigurationsoption im unteren Fenster aus.

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

Option	Beschreibung
Freien Speicherplatz nutzen, um eine neue Erweiterung hinzuzufügen	Fügt den freien Speicherplatz auf dieser Festplatte als neue Erweiterung hinzu.
Freien Speicherplatz nutzen, um eine vorhandene Erweiterung zu erweitern	Vergrößert eine vorhandene Erweiterung auf die erforderliche Kapazität.
Freien Speicherplatz verwenden	Stellt eine Erweiterung im verbleibenden freien Speicherplatz auf der Festplatte bereit. Diese Option ist nur verfügbar, wenn Sie eine Erweiterung hinzufügen.
Alle verfügbaren Partitionen verwenden	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.

- 8 Geben Sie die Kapazität der Erweiterung an.

Die Mindesterweiterungsgröße ist 1,3 GB. Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

- 9 Klicken Sie auf **Weiter**.

- 10 Überprüfen Sie das vorgeschlagene Layout und die neue Konfiguration des Datenspeichers, und klicken Sie anschließend auf **Beenden**.

Weiter

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

Umbenennen von VMFS- oder NFS-Datenspeichern im vSphere Client

Der Name eines vorhandenen Datenspeichers kann geändert werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

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

Gruppieren von VMFS- oder NFS-Datenspeichern im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

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

Löschen von VMFS-Datenspeichern im vSphere Client

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

- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.
- Entfernen Sie alle virtuelle Maschinen aus dem Datenspeicher.
- Stellen Sie sicher, dass kein anderer Host auf den Datenspeicher zugreift.

Vorgehensweise

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

Erstellen einer Diagnosepartition im vSphere Client

Sie können eine Diagnosepartition für Ihren Host erstellen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.

- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicher**.
- 3 Klicken Sie auf **Datenspeicher** und anschließend auf **Speicher hinzufügen**.
- 4 Wählen Sie **Diagnose (Diagnostic)** aus, und klicken Sie auf **Weiter**.

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

- 5 Legen Sie den Diagnosepartitionstyp fest.

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

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

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.

Wenden Sie sich an den VMware-Support, bevor Sie Änderungen an den Gerätefiltern vornehmen. Sie können die Filter nur dann deaktivieren, wenn Sie über andere Methoden zum Verhindern von Gerätebeschädigungen verfügen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere Client **Verwaltung > vCenter Server-Einstellungen**.
- 2 Wählen Sie in der Liste „Einstellungen“ den Eintrag **Erweiterte Einstellungen** aus.
- 3 Geben Sie einen Schlüssel im Feld **Schlüssel** ein.

Schlüssel	Filtername
config.vpxd.filter.vmfsFilter	VMFS-Filter
config.vpxd.filter.rdmFilter	RDM-Filter
config.vpxd.filter.SameHostAndTransportsFilter	Filter für denselben Host und dieselben Transports
config.vpxd.filter.hostRescanFilter	Filter für das erneute Prüfen eines Hosts HINWEIS Wenn Sie den Filter für das erneute Prüfen eines Hosts deaktivieren, führen Ihre Hosts weiterhin eine erneute Prüfung durch, sobald Sie für einen Host oder Cluster eine neue LUN bereitstellen.

- 4 Geben Sie im Textfeld **Wert** für den angegebenen Schlüssel **False** ein.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Klicken Sie auf **OK**.

Es ist nicht erforderlich, dass Sie das vCenter Server-System neu starten.

Raw-Gerätezuordnung

Die Raw-Gerätezuordnung bietet virtuellen Maschinen einen Mechanismus für den direkten Zugriff auf eine LUN im physischen Speichersubsystem (nur Fibre-Channel oder iSCSI).

Die folgenden Themen enthalten Informationen über RDMs und bieten Anleitungen zum Erstellen und Verwalten von RDMs.

Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen

Wenn Sie eine virtuelle Maschine mit einem Direktzugriff auf eine Raw-SAN-LUN versehen, erstellen Sie eine Zuordnungsdatei (Raw-Gerätezuordnung), die sich in einem VMFS-Datenspeicher befindet und auf die LUN verweist. Wenngleich die Zuordnungsdatei dieselbe `.vmdk`-Erweiterung wie eine herkömmliche virtuelle Festplattendatei hat, enthält die Raw-Gerätezuordnungsdatei nur Zuordnungsinformationen. Die eigentlichen virtuellen Festplattendaten werden direkt in der LUN gespeichert.

Sie können die Raw-Gerätezuordnung als Ausgangsfestplatte für eine neue virtuelle Maschine erstellen oder sie einer vorhandenen virtuellen Maschine hinzufügen. Beim Erstellen der Raw-Gerätezuordnung geben Sie die zuzuordnende LUN und den Datenspeicher an, in dem die Raw-Gerätezuordnung abgelegt werden soll.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Befolgen Sie sämtliche Anweisungen zum Erstellen einer benutzerdefinierten virtuellen Maschine.
- 2 Wählen Sie auf der Seite **Festplatte auswählen (Select a Disk)** die Option **Raw-Gerätezuordnung (Raw Device Mapping)** aus, und klicken Sie anschließend auf **Weiter**.
- 3 Wählen Sie in der Liste der SAN-Festplatten bzw. LUNs eine Raw-LUN aus, auf welche die virtuelle Maschine direkt zugreifen soll.
- 4 Wählen Sie einen Datenspeicher für die Raw-Gerätezuordnungsdatei aus.

Sie können die Raw-Gerätezuordnungsdatei im selben Datenspeicher ablegen, in dem sich die Konfigurationsdatei der virtuellen Maschine befindet, oder einen anderen Datenspeicher auswählen.

HINWEIS Um VMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die RDM-Dateien der virtuellen Maschinen im selben Datenspeicher befinden. Sie können Storage vMotion nicht durchführen, wenn NPIV aktiviert ist.

- 5 Wählen Sie den Kompatibilitätsmodus aus.

Option	Beschreibung
Physisch	Ermöglicht es dem Gastbetriebssystem, auf die Hardware direkt zuzugreifen. Der physische Kompatibilitätsmodus bietet sich an, wenn Sie SAN-fähige Anwendungen in der virtuellen Maschine einsetzen. Eingeschaltete virtuelle Maschinen mit RDMS, die für die physische Kompatibilität konfiguriert sind, können jedoch nicht migriert werden, wenn für die Migration die Festplatte kopiert werden muss. Diese virtuellen Maschinen können auch nicht geklont oder in eine Vorlage umgewandelt werden.
Virtuell	Ermöglicht es der RDM, sich wie eine virtuelle Festplatte zu verhalten, so dass Sie Funktionen wie Snapshots, Klonen usw. verwenden können.

- 6 Wählen Sie den Knoten des virtuellen Geräts aus.
- 7 Wenn Sie den unabhängigen Modus wählen, aktivieren Sie eine der folgenden Optionen.

Option	Beschreibung
Dauerhaft	Änderungen werden sofort wirksam und dauerhaft auf die Festplatte geschrieben.
Nicht dauerhaft	Änderungen auf der Festplatte werden beim Herunterfahren oder Wiederherstellen eines Snapshots verworfen.

- 8 Klicken Sie auf **Weiter**.
- 9 Überprüfen Sie auf der Seite **Bereit zum Abschließen der neuen virtuellen Maschine (Ready to Complete New Virtual Machine)** Ihre Angaben.
- 10 Klicken Sie auf **Beenden**, um die virtuelle Maschine zu erstellen.

Verwalten von Pfaden für eine zugeordnete Raw-LUN

Sie können die Pfade für zugeordnete Raw-LUNs verwalten.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Melden Sie sich als Administrator oder als Besitzer der virtuellen Maschine an, zu der die zugeordnete Festplatte gehören soll.
- 2 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.
- 3 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
- 4 Wählen Sie auf der Registerkarte **Hardware** die Option **Festplatte (Hard Disk)** aus, und klicken Sie auf **Pfade verwalten (Manage Paths)**.
- 5 Im Dialogfeld **Pfade verwalten** können Sie Ihre Pfade aktivieren oder deaktivieren, eine Multipathing-Richtlinie festlegen und den bevorzugten Pfad angeben.

Weitere Informationen zur Verwaltung von Pfaden finden Sie unter „[Grundlegendes zu Multipathing und Failover](#)“, auf Seite 374.

Grundlegendes zu Multipathing und Failover

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.

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 Mehrfachpfad-Plug-Ins (MPP) die Pfade zu einem bestimmten Gerät beanspruchen sollten und somit für das Verwalten der Unterstützung von Mehrfachpfaden 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-Mehrfachpfad-Plug-Ins oder das native Mehrfachpfad-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-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 in der Dokumentation *vSphere-Speicher*.

Weitere Informationen zu den verfügbaren Befehlen zum Verwalten von PSA finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Eine vollständige Liste der Speicher-Arrays und der entsprechenden SATPs und PSPs finden Sie in der SAN-Array-Modellreferenz von *vSphere Compatibility Guide*.

Anzeigen von Datenspeicherpfaden im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenbereich auf den Host.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicher**.
- 3 Klicken Sie unter „Ansicht“ auf **Datenspeicher**.
- 4 Wählen Sie in der Liste der konfigurierten Datenspeicher den Datenspeicher aus, dessen Pfade Sie anzeigen möchten, und klicken Sie auf **Eigenschaften**.
- 5 Wählen Sie unter „Erweiterungen“ das Speichergerät aus, dessen Pfade Sie anzeigen möchten, und klicken Sie auf **Pfade verwalten**.
- 6 Wählen Sie im Bereich „Pfade“ den Pfad aus, den Sie anzeigen möchten.
Im darunter befindlichen Bereich wird der Name des Pfads angezeigt. Der Name enthält Parameter, die den Pfad beschreiben: Adapter-ID, Ziel-ID und Geräte-ID.
- 7 (Optional) Klicken Sie mit der rechten Maustaste auf den Pfad und wählen Sie **Pfad in die Zwischenablage kopieren**, um die Parameter des Pfads zu extrahieren.

Anzeigen von Speichergerätepfaden im vSphere Client

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

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Melden Sie sich am vSphere Client an, und klicken Sie im Bestandslistenfenster auf den Server.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend unter „Hardware“ auf **Speicher**.
- 3 Klicken Sie unter „Ansicht“ auf **Geräte**.
- 4 Wählen Sie das Speichergerät aus, dessen Pfade Sie anzeigen möchten, und klicken Sie auf **Pfade verwalten**.
- 5 Wählen Sie im Bereich „Pfade“ den Pfad aus, den Sie anzeigen möchten.
Im darunter befindlichen Bereich wird der Name des Pfads angezeigt. Der Name enthält Parameter, die den Pfad beschreiben: Adapter-ID, Ziel-ID und Geräte-ID.
- 6 (Optional) Klicken Sie mit der rechten Maustaste auf den Pfad und wählen Sie **Pfad in die Zwischenablage kopieren**, um die Parameter des Pfads zu extrahieren.

Ändern der Pfadauswahl-Richtlinie im vSphere Client

In der Regel müssen Sie die standardmäßigen Multipathing-Einstellungen, die Ihr Host für ein bestimmtes Speichergerät verwendet, nicht ändern. Falls Sie jedoch Änderungen vornehmen möchten, können Sie im Dialogfeld „Pfade verwalten“ eine Pfadauswahl-Richtlinie ändern und den bevorzugten Pfad für die Richtlinie „Fest“ angeben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.
- 2 Wählen Sie eine Pfadauswahlrichtlinie aus.

Standardmäßig unterstützt VMware die folgenden Pfadauswahlrichtlinien: Wenn Sie die PSP eines Drittanbieters auf Ihrem Host installiert haben, wird die zugehörige Richtlinie ebenfalls in der Liste aufgeführt.

- Fest (VMware)
- Zuletzt verwendet (VMware)
- Round-Robin (VMware)

- 3 Geben Sie für die Richtlinie „Fest“ den bevorzugten Pfad an, indem Sie mit der rechten Maustaste auf den Pfad klicken, den Sie als bevorzugten Pfad zuweisen möchten, und die Option **Bevorzugt** auswählen.
- 4 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Deaktivieren von Pfaden im vSphere Client

Pfade können zu Wartungszwecken oder aus anderen Gründen vorübergehend deaktiviert werden. Diese Aufgabe kann über den vSphere Client ausgeführt werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.
- 2 Klicken Sie im Fenster „Pfade“ mit der rechten Maustaste auf den zu deaktivierenden Pfad und wählen Sie **Deaktivieren**.
- 3 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Sie können einen Pfad auch aus der Ansicht „Pfade“ des Adapters deaktivieren, indem Sie in der Liste mit der rechten Maustaste auf den Pfad klicken und **Deaktivieren** wählen.

Speicherhardware-Beschleunigung

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>.

Deaktivieren der Hardwarebeschleunigung für Blockspeichergeräte

Auf Ihrem Host ist die Hardwarebeschleunigung für Blockspeichergeräte standardmäßig aktiviert. Sie können die erweiterten Einstellungen des vSphere Clients verwenden, um die Hardwarebeschleunigungsvorgänge zu deaktivieren.

Wenden Sie sich, wie bei allen erweiterten Einstellungen, an den VMware-Support, bevor Sie die Hardwarebeschleunigung deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere Clients den Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und dann unter **Software** auf **Erweiterte Einstellungen**.
- 3 Ändern Sie den Wert für eine beliebige Option auf 0 (deaktiviert):
 - VMFS3.HardwareAcceleratedLocking
 - DataMover.HardwareAcceleratedMove
 - DataMover.HardwareAcceleratedInit

Thin Provisioning von Speicher

Mit ESXi können Sie zwei Modelle des Thin Provisioning verwenden: Thin Provisioning auf Array-Ebene und Thin Provisioning auf der Ebene der virtuellen Festplatte.

Thin Provisioning ist eine Methode, die die Speichernutzung optimiert, indem Speicherplatz auf flexible Weise nach Bedarf zugeteilt wird. Thin Provisioning unterscheidet sich vom herkömmlichen Modell, dem Thick Provisioning. 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.

Die Thin Provisioning-Funktionen von VMware helfen Ihnen dabei, Probleme hinsichtlich einer zu geringen Speichernutzung auf Datenspeicher- und Speicher-Array-Ebene zu vermeiden.

Erstellen von virtuellen Thin-bereitgestellten Festplatten

Wenn Sie Speicherplatz sparen müssen, können Sie eine virtuelle Festplatte im Thin-bereitgestellten Format erstellen. Die Größe der virtuellen Thin-bereitgestellten Festplatte ist zunächst gering und steigt an, sobald mehr virtueller Festplattenspeicher erforderlich ist.

Für dieses Verfahren wird vorausgesetzt, dass Sie mit dem Assistenten für neue virtuelle Maschinen eine standardmäßige oder benutzerdefinierte virtuelle Maschine erstellen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Sie können Thin-Festplatten nur auf Datenspeichern erstellen, die Thin Provisioning auf Festplattenebene unterstützen.

Vorgehensweise

- ◆ Wählen Sie im Dialogfeld „Festplatte erstellen“ **Thin Provisioning**.

Es wird eine virtuelle Festplatte im Thin-Format erstellt.

Weiter

Wenn die virtuelle Festplatte das Thin-Format aufweist, können Sie sie später auf ihre volle Größe vergrößern.

Anzeigen von Speicherressourcen virtueller Maschinen

Sie können anzeigen, wie Speicherplatz von Datenspeichern Ihren virtuellen Maschinen zugeteilt ist.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste die gewünschte virtuelle Maschine aus.
- 2 Klicken Sie auf die Registerkarte **Übersicht (Summary)**.
- 3 Überprüfen Sie die Informationen zur Speicherplatzzuteilung im Abschnitt „Ressourcen“.
 - Bereitgestellter Speicher – Zeigt den für die virtuelle Maschine zugeteilten Speicherplatz. Wenn die virtuelle Maschine über Festplatten im Thin-bereitgestellten Format verfügt, kann möglicherweise nicht der gesamte Speicherplatz genutzt werden. Andere virtuelle Maschinen können nicht genutzten Speicherplatz in Anspruch nehmen.
 - Nicht gemeinsam genutzter Speicher - Zeigt den Datenspeicherplatz, der von der virtuellen Maschine beansprucht und nicht gemeinsam mit anderen virtuellen Maschinen genutzt wird.
 - Verwendeter Speicher – Zeigt Datenspeicherplatz, der tatsächlich von den Dateien der virtuellen Maschine, z. B. Konfigurations- und Protokolldateien, Snapshots, virtuellen Festplatten usw., beansprucht wird. Wenn die virtuelle Maschine läuft, werden im verwendeten Speicherplatz auch die Auslagerungsdateien berücksichtigt.

Festlegen des Festplattenformats für eine virtuelle Maschine

Sie können festlegen, ob Ihre virtuelle Festplatte im Thick- oder im Schnell-Format vorliegen soll.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste die gewünschte virtuelle Maschine aus.
- 2 Klicken Sie auf **Einstellungen bearbeiten**, um das Dialogfeld „Eigenschaften virtueller Maschinen“ anzuzeigen.
- 3 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie die entsprechende Festplatte aus der Hardwareliste aus.

Der Typ der virtuellen Festplatte wird rechts im Abschnitt „Festplattenbereitstellung“ angezeigt.

- 4 Klicken Sie auf **OK**.

Weiter

Wenn die virtuelle Festplatte das Format „Schnell“ aufweist, können Sie sie auf ihre volle Größe vergrößern.

Vergrößern virtueller Thin-Festplatten

Wenn die virtuelle Festplatte das Thin-Provisioning-Format aufweist, können Sie sie auf ihre volle Größe vergrößern.

Mit diesem Verfahren wird eine Thin-Festplatte in eine virtuelle Festplatte im Thick-Provision-Format konvertiert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste die gewünschte virtuelle Maschine aus.
- 2 Klicken Sie zum Öffnen des Dialogfelds „Datenspeicherbrowser“ auf die Registerkarte **Übersicht** und doppelklicken Sie unter „Ressourcen“ auf den Datenspeicher für die virtuelle Maschine.
- 3 Klicken Sie zum Auffinden der virtuellen Festplattendatei, die Sie konvertieren möchten, auf den VM-Ordner. Die Datei weist die Erweiterung `.vmdk` auf.
- 4 Klicken Sie mit der rechten Maustaste auf die virtuelle Festplattendatei und wählen Sie **Vergrößern**.

Die vergrößerte virtuelle Festplatte belegt den ganzen Datenspeicherplatz, der ursprünglich für sie bereitgestellt wurde.

Verwenden von Speicher-Anbieter-Providern

Bei der Verwendung von Anbieter-Provider-Komponenten kann vCenter Server mit externem Speicher (sowohl Block- als auch NFS-Speicher) integriert werden, damit Sie sich einen besseren Einblick in die Ressourcen verschaffen sowie umfassende und aussagekräftige Speicherdaten erhalten können.

Der Anbieter-Provider ist ein Software-Plug-In, das von einem Drittanbieter über die Speicher-APIs für Storage Awareness entwickelt wurde. In der Regel wird die Anbieter-Provider-Komponente auf der Speicher-Array-Seite installiert und dient als Server in der vSphere-Umgebung. vCenter Server verwendet Anbieter-Provider zum Abrufen von Informationen über die Speichertopologie, Funktionen und den Status.

Weitere Informationen darüber, ob Ihr Speicher die Anbieter-Provider-Plug-Ins unterstützt, erhalten Sie von Ihrem Speicheranbieter.

Sofern Ihr Speicher Anbieter-Provider unterstützt, verwenden Sie die Menüoption **Speicheranbieter** im vSphere Client oder im vSphere Web Client zum Registrieren und Verwalten der Anbieter-Providerkomponenten.

Registrieren der Anbieter-Provider im vSphere Client

Sie müssen zum Herstellen einer Verbindung zwischen dem vCenter Server und einem Anbieter-Provider den Anbieter-Provider registrieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Stellen Sie sicher, dass die Anbieter-Provider-Komponente auf der Speicherseite installiert ist, und fragen Sie Ihren Speicheradministrator nach den Anmeldedaten.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Verwaltung > Speicheranbieter**.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Geben Sie im Dialogfeld **Anbieter-Provider hinzufügen** die Verbindungsinformationen für den Anbieter-Provider ein, d. h. den Namen, die URL und die Anmeldedaten.
- 4 (Optional) Wählen Sie die Option **Zertifikat des Anbieter-Providers verwenden** und geben Sie den Speicherort des Zertifikats an, um das Zertifikat des Anbieter-Providers dem vCenter Server zuzuordnen.

Wenn Sie diese Option nicht auswählen, zeigt der vSphere Client einen Fingerabdruck des Zertifikats an. Sie können den Fingerabdruck überprüfen und ihn genehmigen.

- 5 Klicken Sie auf **OK**, um die Registrierung abzuschließen.

Der vCenter Server hat den Anbieter-Provider registriert und eine sichere SSL-Verbindung mit ihm hergestellt.

Anzeigen von Anbieterinformationen

Nachdem Sie mit dem vCenter Server eine Anbieter-Provider-Komponente registriert haben, wird der Anbieter-Provider im vSphere Client in der Liste der Anbieter-Provider aufgeführt.

Anzeigen der allgemeinen Informationen zum Anbieter-Provider und der Details für jede Anbieter-Komponente.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Verwaltung > Speicheranbieter**.
- 2 Zeigen Sie in der Liste „Anbieter-Provider“ die mit dem vCenter Server registrierten Provider-Komponenten an.

Die Liste enthält allgemeine Anbieterinformationen, wie den Namen, die URL sowie den Zeitpunkt der letzten Ansichtsaktualisierung.
- 3 Wenn Sie weitere Details ansehen möchten, wählen Sie einen bestimmten Anbieter-Provider aus der Liste aus.

Zu den Detailinformationen gehören Speicher-Array-Anbieter sowie die vom Anbieter-Provider unterstützten Array-Modelle.

HINWEIS Ein einzelner Anbieter-Provider kann Speicher-Arrays vieler verschiedener Anbieter unterstützen.

Aufheben der Registrierung von Anbietern

Heben Sie die Registrierung für nicht benötigte Anbieter-Provider auf.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Verwaltung > Speicheranbieter**.
- 2 Wählen Sie aus der Liste der Anbieter-Provider den Anbieter-Provider aus, für den Sie die Registrierung aufheben möchten, und klicken Sie auf **Entfernen**.

vCenter Server beendet die Verbindung und entfernt den Anbieter-Provider aus seiner Konfiguration.

Aktualisieren von Anbietern

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.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie **Ansicht > Verwaltung > Speicheranbieter**.
- 2 Wählen Sie aus der Liste den Anbieter-Provider aus, den Sie synchronisieren möchten, und klicken Sie auf **Synchronisieren**.

Der vSphere Client aktualisiert die Speicherdaten für den Anbieter.

Wenn Sie den vSphere-Client direkt mit einem Host verbinden, können Sie auf eine begrenzte Anzahl an Einstellungen für die Ressourcenverwaltung zugreifen, beispielsweise auf Einstellungen für Hyper-Threading, auf die Energieverwaltungskonfiguration und auf Eigenschaften der Auslagerungsdatei.

Dieses Kapitel behandelt die folgenden Themen:

- [„Konfigurieren von Einstellungen für die Ressourcenzuteilung“](#), auf Seite 383
- [„Verwalten von CPU-Ressourcen“](#), auf Seite 385
- [„Verwalten von Arbeitsspeicherressourcen“](#), auf Seite 388
- [„Verwalten von Speicher-E/A-Ressourcen“](#), auf Seite 393
- [„Verwalten von Ressourcenpools“](#), auf Seite 397
- [„Verwenden des DRS-Clusters zur Ressourcenverwaltung“](#), auf Seite 401
- [„Erstellen eines Datenspeicher-Clusters“](#), auf Seite 415
- [„Verwenden des Datenspeicher-Clusters zur Verwaltung von Speicherressourcen“](#), auf Seite 419
- [„Verwenden von NUMA-Systemen mit ESXi“](#), auf Seite 428
- [„Erweiterte Attribute“](#), auf Seite 430

Konfigurieren von Einstellungen für die Ressourcenzuteilung

Wenn die verfügbare Ressourcenkapazität die Erfordernisse der Ressourcenverbraucher (und des Virtualisierungs-Overheads) nicht erfüllt, müssen Administratoren möglicherweise die Menge der Ressourcen anpassen, die virtuellen Maschinen oder sind Ressourcenpools zugeteilt.

Verwenden Sie die Einstellungen für die Ressourcenzuteilung (Anteile, Reservierung und Grenzwert) zum Bestimmen der CPU-, Arbeitsspeicher- und Speicherressourcen, die einer virtuellen Maschine zur Verfügung gestellt werden. Vor allen Administratoren stehen mehrere Optionen für die Zuteilung von Ressourcen zur Verfügung.

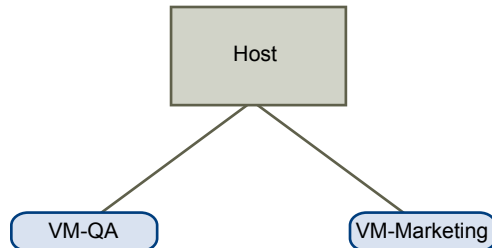
- Reservieren der physischen Ressourcen des Hosts oder Clusters.
- Festlegen einer Obergrenze für die Ressourcen, die einer virtuellen Maschine zugeteilt werden können.
- Sicherstellen, dass eine bestimmte virtuelle Maschine immer einen höheren Prozentsatz der physischen Ressourcen erhält als andere virtuelle Maschinen.

Beispiel für das Ändern von Einstellungen für die Ressourcenzuteilung

Das folgende Beispiel zeigt, wie Sie die Einstellungen für die Ressourcenzuteilung ändern können, um die Leistung der virtuellen Maschine zu optimieren.

Angenommen, dass Sie zwei neue virtuelle Maschinen auf einem ESXi-Host erstellt haben, jeweils eine für die Qualitätssicherung (VM-QA) und das Marketing (VM-Marketing).

Abbildung 25-1. Einzelhost mit zwei virtuellen Maschinen



Im folgenden Beispiel wird angenommen, dass VM-QA arbeitsspeicherintensiv ist und Sie dementsprechend die Einstellungen für die Ressourcenzuteilung für die zwei virtuellen Maschinen ändern möchten:

- Legen Sie fest, dass die VM-QA im Falle einer Mehrfachvergabe des Systemarbeitsspeichers doppelt so viele Arbeitsspeicher- und CPU-Ressourcen nutzen kann wie die virtuelle Maschine der Marketingabteilung. Legen Sie die Arbeitsspeicher- und CPU-Anteile für VM-QA auf **Hoch** und für VM-Marketing auf **Normal** fest.
- Stellen Sie sicher, dass die virtuelle Maschine der Marketingabteilung über eine bestimmte Menge an garantierten CPU-Ressourcen verfügt. Dies können Sie über eine Reservierungseinstellung erreichen.

Vorgehensweise

- 1 Starten Sie den vSphere-Client und verbinden Sie ihn mit einem vCenter Server-System.
- 2 Klicken Sie mit der rechten Maustaste auf **VM-QA**, die virtuelle Maschine, deren Anteile Sie ändern möchten, und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie die Registerkarte **Ressourcen** aus und wählen Sie anschließend im CPU-Bereich **Hoch** aus dem Dropdown-Menü **Anteile** aus.
- 4 Wählen Sie im Fenster „Arbeitsspeicher“ im Dropdown-Menü **Anteile** die Option **Hoch** aus.
- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine der Marketing-Abteilung (**VM-Marketing**) und wählen Sie **Einstellungen bearbeiten**.
- 7 Ändern Sie im Bereich „CPU“ den Wert im Feld **Reservierung** in die gewünschte Nummer.
- 8 Klicken Sie auf **OK**.

Wenn Sie die Registerkarte **Ressourcenzuteilung** des Clusters auswählen und auf **CPU** klicken, sehen Sie, dass die Anteile für die **VM-QA** doppelt so hoch sind wie die der anderen virtuellen Maschine. Beachten Sie auch, dass sich die Felder **Verwendete Reservierung** nicht verändert haben, da die virtuellen Maschinen nicht eingeschaltet wurden.

Verwalten von CPU-Ressourcen

Sie haben die Möglichkeit, virtuelle Maschinen mit mindestens einem virtuellen Prozessor zu konfigurieren, wobei jeder über einen eigenen Register und Steuerungsstrukturen verfügt.

Bei der Planung einer virtuellen Maschine wird festgelegt, dass die virtuellen Prozessoren auf physischen Prozessoren ausgeführt werden. Über den Ressourcen-Manager des VMkernels werden die virtuellen CPUs physischen CPUs zugeordnet, sodass der Zugriff der virtuellen Maschine auf physische CPU-Ressourcen gesteuert werden kann. ESXi unterstützt virtuelle Maschinen mit bis zu 128 virtuellen CPUs.

Anzeigen von Prozessorinformationen

Sie können entweder über den vSphere-Client oder über die vSphere-SDK auf Informationen über die aktuelle CPU-Konfiguration zugreifen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client den Host, und klicken Sie anschließend auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie auf **Prozessoren (Processors)**

Sie können nun die Informationen über die Anzahl und den Typ der physischen Prozessoren sowie die Anzahl der logischen Prozessoren anzeigen.

HINWEIS Bei Systemen mit aktivierter Hyper-Threading-Funktion ist jeder Hardware-Thread ein logischer Prozessor. Beispielsweise verfügt ein Dual-Core-Prozessor mit aktivierter Hyper-Threading-Funktion über zwei Cores und vier logische Prozessoren.

- 3 (Optional) Zudem haben Sie die Möglichkeit, Hyper-Threading zu deaktivieren oder zu aktivieren, indem Sie auf **Eigenschaften (Properties)** klicken.

Aktivieren von Hyper Threading

Zum Aktivieren von Hyper-Threading müssen Sie es zuerst in den BIOS-Einstellungen Ihres Systems aktivieren und es dann im vSphere-Client einschalten. Hyper-Threading ist standardmäßig aktiviert.

Lesen Sie Ihre Systemdokumentation, um festzustellen, ob Ihre CPU Hyper-Threading unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Hyper-Threading-Technologie unterstützt.
- Aktivieren Sie Hyper-Threading im System-BIOS. Einige Hersteller bezeichnen diese Option als **Logischer Prozessor**, andere als **Hyper-Threading aktivieren**.
- Öffnen Sie eine vSphere Client-Verbindung mit einem vCenter Server.

Vorgehensweise

- ◆ Aktivieren Sie die Hyper-Threading-Funktion für den ESXi-Host.
 - a Wählen Sie im vSphere-Client den Host, und klicken Sie anschließend auf die Registerkarte **Konfiguration**.
 - b Wählen Sie die Option **Prozessoren (Processors)**, und klicken Sie auf **Eigenschaften (Properties)**.
 - c Im Dialogfeld können Sie den Hyper-Threading-Status anzeigen und deaktivieren bzw. aktivieren (Standardeinstellung).

Hyper-Threading ist aktiviert.

Festlegen der Optionen für den gemeinsamen Zugriff auf Hyper-Threading für eine virtuelle Maschine

Sie können festlegen, wie die virtuellen CPUs einer virtuellen Maschine physische Kerne auf einem System mit Hyper-Threading gemeinsam verwenden können.

Ein Kern wird von zwei virtuellen CPUs gemeinsam verwendet, wenn sie gleichzeitig auf logischen CPUs des Kerns ausgeführt werden. Diese Eigenschaft kann für einzelne virtuelle Maschinen festgelegt werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Ressourcen (Resources)** und anschließend Sie auf **Erweiterte CPU (Advanced CPU)**.
- 3 Wählen Sie einen Hyper-Threading-Modus für diese Virtuelle Maschine aus dem Dropdown-Menü **Modus** aus.

Zuweisen einer virtuellen Maschine zu einem bestimmten Prozessor

Unter Verwendung der CPU-Affinität können Sie eine virtuelle Maschine einem bestimmten Prozessor zuweisen. Dadurch können Sie die Zuweisung von virtuellen Maschinen auf einen bestimmten verfügbaren Prozessor in Systemen mit mehreren Prozessoren beschränken.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere-Clients eine virtuelle Maschine aus und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Ressourcen** und anschließend **Erweiterte CPU**.
- 3 Klicken Sie auf die Schaltfläche **Auf folgenden Prozessoren ausführen (Run on processor(s))**.
- 4 Wählen Sie die Prozessoren, auf denen die virtuelle Maschine ausgeführt werden soll, und klicken Sie auf **OK**.

Auswahl einer CPU-Energieverwaltungsrichtlinie

Sie legen die CPU-Energieverwaltungsrichtlinie für einen Host mithilfe des vSphere-Clients fest.

Voraussetzungen

ESX/ESXi unterstützt die Enhanced Intel SpeedStep- und Enhanced AMD PowerNow! Technologien für die CPU-Energieverwaltung. Damit der VMkernel die Energieverwaltungsfunktionen, die diese Technologien bieten, nutzen kann, müssen Sie die Energieverwaltung, die manchmal auch DBS (Demand-Based Switching) genannt wird, im BIOS aktivieren.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere-Clients einen Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie unter „Hardware“ die Option **Energieverwaltung** und klicken Sie auf **Eigenschaften**.
- 3 Wählen Sie eine Energieverwaltungsrichtlinie für den Host aus und klicken Sie auf **OK**.

Die ausgewählte Richtlinie wird in der Hostkonfiguration gespeichert und kann beim Starten erneut verwendet werden. Sie können sie jederzeit ändern. Zum Aktivieren ist kein Neustart des Servers erforderlich.

Konfigurieren von benutzerdefinierten Richtlinienparametern für die Energieverwaltung des Hosts

Wenn Sie die Richtlinie „Benutzerdefiniert“ für die Energieverwaltung des Hosts verwenden, basiert ESXi seine Energieverwaltungsrichtlinie auf den Werten mehrerer erweiterter Konfigurationsparameter.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Wählen Sie **Benutzerdefiniert** als Energieverwaltungsrichtlinie, wie unter [„Auswahl einer CPU-Energieverwaltungsrichtlinie“](#), auf Seite 387 beschrieben.

Vorgehensweise

- 1 Wählen Sie im Bestandslistenbereich des vSphere-Client den Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Wählen Sie unter „Software“ die Option **Erweiterte Einstellungen**.
- 3 Klicken Sie im linken Fenster auf **Energieverwaltung (Power)**.

- 4 Sie können im rechten Bereich die Energieverwaltungsparameter bearbeiten, die Ihre benutzerdefinierte Richtlinie beeinflussen.

Energieverwaltungsparameter, die die Richtlinie „Benutzerdefiniert“ beeinflussen, haben Beschreibungen, die mit **In benutzerdefinierter Richtlinie** beginnen. Alle anderen Energieparameter betreffen alle Energieverwaltungsrichtlinien.

HINWEIS Die Standardwerte der Parameter für die Energieverwaltung stimmen mit der Richtlinie „Ausgeglichen“ überein.

Parameter	Beschreibung
Power.UsePStates	Verwenden Sie ACPI P-Statuszustände zur Energieeinsparung, wenn der Prozessor beschäftigt ist.
Power.MaxCpuLoad	Verwenden Sie P-States zur Einsparung von Energie nur dann, wenn eine CPU für weniger als den angegebenen Prozentsatz der Echtzeit beschäftigt ist.
Power.MinFreqPct	Verwenden Sie keine P-Statuszustände, die langsamer als der angegebene Prozentsatz der vollen CPU-Geschwindigkeit sind.
Power.UseStallCtr	Verwenden Sie einen tieferen P-State, wenn der Prozessor beim Warten auf Ereignisse häufig ins Stocken gerät, wie z. B. bei Cache-Misses.
Power.TimerHz	Steuert, wie oft in der Sekunde ESXi den P-State neu auswertet, den jede CPU aufweisen muss.
Power.UseCStates	Verwenden Sie tiefe ACPI C-Status (C2 oder niedriger), wenn sich der Prozessor im Leerlauf befindet.
Power.CStateMaxLatency	Verwenden Sie keine C-Status, deren Latenz größer als dieser Wert ist.
Power.CStateResidencyCoef	Wenn sich eine CPU im Leerlauf befindet, wählen Sie den niedrigsten C-Status aus, dessen Latenz multipliziert mit diesem Wert weniger als die Vorhersage des Hosts über die Dauer des Leerlaufs ist. Größere Werte führen dazu, dass ESXi tiefe C-Status eher konservativ verwendet, wobei kleinere Werte aggressiver sind.
Power.CStatePredictionCoef	Ein Parameter im ESXi-Algorithmus für die Vorhersage, wie lange eine CPU, die sich im Leerlauf befindet, im Leerlauf bleiben wird. Es wird nicht empfohlen, diesen Wert zu ändern.
Power.PerfBias	Performance Energy Bias Hint (nur Intel). Legt ein MSR auf Intel-Prozessoren auf einen von Intel empfohlenen Wert fest. Intel empfiehlt 0 für Hochleistung, 6 für ausgeglichen und 15 für geringen Energieverbrauch. Andere Werte sind nicht definiert.

Verwalten von Arbeitsspeicherressourcen

Mithilfe des vSphere-Clients können Sie Informationen zu Einstellungen für die Arbeitsspeicherzuteilung anzeigen und Änderungen an diesen Einstellungen vornehmen. Damit Sie Ihre Arbeitsspeicherressourcen effektiv verwalten können, müssen Sie auch mit dem Arbeitsspeicher-Overhead, der Leerlaufbelastung für Arbeitsspeicher und dem Prozess der Rückgewinnung von Arbeitsspeicher durch ESXi-Hosts vertraut sein.

Beim Verwalten von Arbeitsspeicherressourcen können Sie die Arbeitsspeicherzuteilung festlegen. Falls Sie die Arbeitsspeicherzuteilung nicht anpassen, verwendet der ESXi-Host Standardwerte, die in den meisten Situationen zu zufriedenstellenden Ergebnissen führen.

Sie können die Arbeitsspeicherzuteilung auf verschiedene Weisen festlegen.

- Verwenden Sie die Attribute und speziellen Funktionen, die über den vSphere-Client verfügbar sind. Mithilfe der Benutzerschnittstelle des vSphere-Clients können Sie eine Verbindung mit dem ESXi-Host oder dem vCenter Server-System herstellen.
- Verwenden Sie die erweiterten Einstellungen.
- Verwenden Sie für die Skript-Arbeitsspeicherzuteilung das vSphere-SDK.

Aktivieren der lokalen Auslagerung auf einem Host für einen DRS-Cluster

Die lokale Auslagerung auf einem Host ermöglicht Ihnen, einen lokal auf dem Host gespeicherten Datenspeicher als Speicherort für die Auslagerungsdatei anzugeben. Sie können die lokale Auslagerung für einen DRS-Cluster aktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie im linken Fenster des Dialogfelds „Einstellungen“ des Clusters auf **Speicherort der Auslagerungsdatei**.
- 3 Aktivieren Sie die Option **Speichern Sie die Auslagerungsdatei in dem Datenspeicher, der durch den Host angegeben wird**, und klicken Sie auf **OK**.
- 4 Wählen Sie in der Bestandsliste des vSphere-Clients einen Host aus dem Cluster aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 5 Wählen Sie unter „Software“ **Speicherort der VM-Auslagerungsdatei**.
- 6 Wählen Sie den zu verwendenden lokalen Datenspeicher und klicken Sie auf **OK**.
- 7 Wiederholen Sie die Schritte [Schritt 4](#) bis [Schritt 6](#) für jeden Host im Cluster.

Die lokale Auslagerung auf einem Host ist jetzt für den DRS-Cluster aktiviert.

Aktivieren der lokalen Auslagerung für einen eigenständigen Host

Die lokale Auslagerung auf einem Host ermöglicht Ihnen, einen lokal auf dem Host gespeicherten Datenspeicher als Speicherort für die Auslagerungsdatei anzugeben. Sie können die lokale Auslagerung für einen eigenständigen Host aktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf **Konfiguration**.
- 3 Wählen Sie unter „Software“ die Option **Speicherort der VM-Auslagerungsdatei** und klicken Sie auf **Bearbeiten..**
- 4 Wählen Sie **Die Auslagerungsdatei in dem Datenspeicher speichern, der durch den Host angegeben ist**.
- 5 Wählen Sie einen lokalen Datenspeicher aus der Liste aus und klicken Sie auf **OK**.

Die lokale Auslagerung ist jetzt für den eigenständigen Host aktiviert.

Konfigurieren der Eigenschaften von VM-Auslagerungsdateien für den Host

Konfigurieren Sie einen Speicherort der Auslagerungsdatei für den Host, um den Standardspeicherort der Auslagerungsdateien für virtuelle Maschinen festzulegen.

Standardmäßig befinden sich die Auslagerungsdateien für eine virtuelle Maschine in einem VMFS3-Datenspeicher in dem Ordner, in dem sich auch die anderen Dateien der virtuellen Maschine befinden. Sie können jedoch den Host so konfigurieren, dass die Auslagerungsdateien der virtuellen Maschine in einem anderen Datenspeicher gespeichert werden.

Mithilfe dieser Option können Sie VM-Auslagerungsdateien in einem kosteneffizienteren oder leistungsfähigeren Speicher ablegen. Zudem haben Sie die Möglichkeit, diese Einstellung für einzelne virtuelle Maschinen auf Hostebene außer Kraft zu setzen.

Die Festlegung eines alternativen Speicherortes für die Auslagerungsdateien kann dazu führen, dass mit vMotion durchgeführte Migrationen langsamer abgeschlossen werden. Zum Erzielen der besten vMotion-Leistung sollten Sie die VM-Auslagerungsdateien in dem selben Verzeichnis wie die virtuellen Maschinen speichern.

Wird der Host von vCenter Server verwaltet, können Sie den Speicherort der Auslagerungsdatei nicht ändern, wenn Sie direkt über den vSphere-Client eine Verbindung mit dem Host herstellen. Sie müssen den vSphere-Client mit dem vCenter Server-System verbinden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

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

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie auf den Link **Speicherort der VM-Auslagerungsdatei**.

Auf der Registerkarte **Konfiguration** wird der ausgewählte Speicherort für die Auslagerungsdateien angezeigt. Falls die Konfiguration des Speicherorts für die Auslagerungsdateien auf dem ausgewählten Host nicht unterstützt wird, wird auf der Registerkarte eine entsprechende Meldung angezeigt.

Gehört der Host zu einem Cluster und legen die Clustereinstellungen fest, dass die Auslagerungsdateien im selben Verzeichnis wie Dateien der virtuellen Maschine gespeichert werden, kann der Speicherort für die Auslagerungsdateien nicht über die Registerkarte für die Hostkonfiguration bearbeitet werden. Den Speicherort der Auslagerungsdateien für einen solchen Host können Sie über das Dialogfeld Clustereinstellungen ändern.

- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie entweder **Auslagerungsdatei im selben Verzeichnis wie VM speichern** oder **Auslagerungsdatei in einem unten ausgewählten Datenspeicher für Auslagerungsdateien speichern**.

Wenn Sie die Option **Speichern Sie die Auslagerungsdatei in einem der unten ausgewählten Datenspeicher für Auslagerungsdateien** auswählen, wählen Sie einen Datenspeicher aus der Liste.

- 6 Klicken Sie auf **OK**.

Die VM-Auslagerungsdatei wird an dem von Ihnen ausgewählten Speicherort gespeichert.

Konfigurieren des Speicherorts der VM-Auslagerungsdatei für einen Cluster

Standardmäßig befinden sich die Auslagerungsdateien für eine virtuelle Maschine in einem VMFS-Datenspeicher in dem Ordner, in dem sich auch die anderen Dateien der virtuellen Maschine befinden. Sie können die Hosts in Ihrem Cluster jedoch stattdessen so konfigurieren, dass die VM-Auslagerungsdateien in einem anderen Datenspeicher Ihrer Wahl abgelegt werden.

Sie können einen alternativen Speicherort der Auslagerungsdatei konfigurieren, um die VM-Auslagerungsdateien je nach Bedarf entweder in einem kosteneffizienteren Speicher oder einem leistungsfähigeren Speicher abzulegen.

HINWEIS Die Festlegung eines alternativen Speicherortes für die Auslagerungsdateien kann dazu führen, dass mit vMotion durchgeführte Migrationen langsamer abgeschlossen werden. Zum Erzielen der besten vMotion-Leistung sollten Sie die VM-Auslagerungsdateien in dem selben Verzeichnis wie die virtuellen Maschinen speichern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Bevor Sie den Speicherort der Auslagerungsdatei einer virtuellen Maschine für einen Cluster konfigurieren, müssen Sie die Speicherorte der VM-Auslagerungsdateien der Hosts im Cluster konfigurieren, wie unter [„Konfigurieren der Eigenschaften von VM-Auslagerungsdateien für den Host“](#), auf Seite 390 beschrieben.

Vorgehensweise

- 1 Zeigen Sie den Cluster in der Bestandsliste an.
- 2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 3 Klicken Sie in der Liste „Einstellungen“ auf **Speicherort der Auslagerungsdatei**.
- 4 Wählen Sie unter „Auslagerungsdatei-Richtlinie für virtuelle Maschinen“ aus, wo die Auslagerungsdatei der virtuellen Maschine gespeichert werden soll.

Option	Beschreibung
Die Auslagerungsdatei im selben Verzeichnis wie die virtuelle Maschine speichern	Speichert die Auslagerungsdatei im selben Verzeichnis wie die Konfigurationsdatei der virtuellen Maschine.
Die Auslagerungsdatei in dem Datenspeicher speichern, der durch den Host angegeben ist	Speichert die Auslagerungsdatei am Speicherort, der in der Hostkonfiguration angegeben wurde. Wenn die Auslagerungsdatei nicht in dem vom Host angegebenen Datenspeicher gespeichert werden kann, wird die Auslagerungsdatei im selben Verzeichnis wie die virtuelle Maschine gespeichert.

- 5 Klicken Sie auf **OK**.

Löschen von Auslagerungsdateien

Wenn ein Host ausfällt, auf dem virtuelle Maschinen ausgeführt werden, die Auslagerungsdateien verwenden, bestehen die Auslagerungsdateien nach wie vor und verbrauchen mehrere Gigabyte an Speicherplatz. Sie können die Auslagerungsdateien löschen, um dieses Problem zu beheben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System oder einem ESXi-Host an.

Vorgehensweise

- 1 Starten Sie die virtuelle Maschine neu, die sich auf dem ausgefallenen Host befand.
- 2 Halten Sie die virtuelle Maschine an.

Die Auslagerungsdatei für die virtuelle Maschine wird gelöscht.

Konfigurieren des Host-Caches

Sie können den Prozentsatz des zugeteilten Speicherplatzes für den Host-Cache ändern oder die Fähigkeit des Hosts zur Auslagerung auf den Host-Cache deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Sie benötigen einen SSD-gestützten Datenspeicher in Ihrer Bestandsliste.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie unter „Software“ auf **Host-Cache-Konfiguration**.
- 4 Wählen Sie den Datenspeicher in der Liste aus und klicken Sie auf **Eigenschaften**.
- 5 Wählen Sie eine Größe für die Host-Cache-Zuteilung auf dem Laufwerk aus.
- 6 Deaktivieren Sie das Kontrollkästchen **Speicher für Host-Cache zuteilen**, wenn Sie die Fähigkeit des Hosts zur Auslagerung nach Host-Cache datenspeicherweise deaktivieren möchten.
- 7 Klicken Sie auf **OK**.

Aktivieren bzw. Deaktivieren des Cachespeichers für die Arbeitsspeicherkomprimierung

Die Arbeitsspeicherkomprimierung ist standardmäßig aktiviert. Mithilfe des Dialogfelds „Erweiterte Einstellungen“ im vSphere-Client können Sie die Arbeitsspeicherkomprimierung für einen Host aktivieren oder deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Wählen Sie unter „Software“ die Option **Erweiterte Einstellungen**.
- 4 Wählen Sie im linken Fensterbereich **Mem** und suchen Sie nach „Mem.MemZipEnable“.
- 5 Geben Sie zum Aktivieren des Cachespeichers für die Arbeitsspeicherkomprimierung 1 oder zum Deaktivieren 0 ein.
- 6 Klicken Sie auf **OK**.

Festlegen der maximalen Größe des Cachespeichers für die Arbeitsspeicherkomprimierung

Sie können die maximale Größe des Cachespeichers für die Arbeitsspeicherkomprimierung für die virtuellen Maschinen des Hosts festlegen.

Sie legen die Größe des Cachespeichers für die Arbeitsspeicherkomprimierung als Prozentsatz der Arbeitsspeichergöße der virtuellen Maschine fest. Wenn Sie beispielsweise „20“ eingeben und die Größe des Arbeitsspeichers einer virtuellen Maschine 1.000 MB beträgt, kann ESXi bis zu 200 MB Hostspeicher verwenden, um die komprimierten Seiten der virtuellen Maschine zu speichern.

Wenn Sie die Größe des Cachespeichers für die Arbeitsspeicherkomprimierung nicht festlegen, verwendet ESXi den Standardwert von 10 Prozent.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Wählen Sie unter „Software“ die Option **Erweiterte Einstellungen**.
- 4 Wählen Sie im linken Fensterbereich **Mem** und suchen Sie nach „Mem.MemZipMaxPct“.
Der Wert dieses Attributs bestimmt die maximale Größe des Cachespeichers für die Arbeitsspeicherkomprimierung der virtuellen Maschine.
- 5 Geben Sie die maximale Größe des Cachespeichers für die Arbeitsspeicherkomprimierung ein.
Der Wert ist ein Prozentsatz der Größe der virtuellen Maschine und muss zwischen 5 und 100 Prozent liegen.
- 6 Klicken Sie auf **OK**.

Verwalten von Speicher-E/A-Ressourcen

vSphere Storage I/O Control ermöglicht die clusterweite Priorisierung der Speicher-E/A, die zu einer besseren Arbeitslastkonsolidierung führt und durch Überbelegungen verursachte Kosten verringern hilft.

Storage I/O Control erweitert die Konstrukte von Anteilen und Grenzwerten, um Speicher-E/A-Ressourcen zu behandeln. Sie können die Menge an Speicher-E/A steuern, die virtuellen Maschinen bei E/A-Überlastung zugeteilt wird. Dies sorgt dafür, dass bei der Zuteilung von E/A-Ressourcen die wichtigeren virtuellen Maschinen bevorzugt werden.

Wenn Sie Storage I/O Control für einen Datenspeicher aktivieren, beginnt ESXi die Gerätelatenz zu überwachen, die Hosts beim Kommunizieren mit dem Datenspeicher beobachten. Wenn die Gerätelatenz einen Schwellenwert überschreitet, gilt der Datenspeicher als überlastet und jeder virtuellen Maschine, die auf den Datenspeicher zugreift, werden E/A-Ressourcen im Verhältnis zu ihren Anteilen zugeteilt. Sie legen Anteile pro virtueller Maschine fest. Sie können die Anteile für jede Maschine bei Bedarf anpassen.

Das Konfigurieren von Storage I/O Control erfolgt in zwei Schritten:

- 1 Aktivieren von Storage I/O Control für den Datenspeicher.
- 2 Festlegen der Anzahl an Speicher-E/A-Anteilen und des oberen Grenzwerts der E/A-Vorgänge pro Sekunde (IOPS), der für jede virtuelle Maschine zulässig ist.

Standardmäßig werden die VM-Anteile auf „Normal“ (1000) mit unbegrenzten IOPS festgelegt.

HINWEIS Storage I/O Control wird standardmäßig auf Speicher-DRS-aktivierten Datenspeicher-Clustern aktiviert.

Ressourcenanteile und Grenzwerte für Storage I/O Control

Sie teilen die Anzahl der Speicher-E/A-Anteile und den oberen Grenzwert für die E/A-Vorgänge pro Sekunde (IOPS) zu, die für jede virtuelle Maschine zulässig ist. Wenn für einen Datenspeicher eine Speicher-E/A-Überlastung erkannt wird, werden die E/A-Workloads der virtuellen Maschinen, die auf den Datenspeicher zugreifen, gemäß der Proportion der VM-Anteile angepasst, die jede virtuelle Maschine besitzt.

Speicher-E/A-Anteile entsprechen den für die Ressourcenzuteilung bei Arbeitsspeicher und CPU verwendeten Anteilen, die in der Dokumentation zur *vSphere-Ressourcenverwaltung* beschrieben sind. Diese Anteile repräsentieren die relative Wichtigkeit einer virtuellen Maschine im Hinblick auf die Verteilung von Speicher-E/A-Ressourcen. Bei Ressourcenkonflikten haben virtuelle Maschinen mit höheren Anteilswerten mehr Zugriff auf das Speicher-Array, was in der Regel einen höheren Durchsatz und niedrige Latenz mit sich bringt.

Wenn Sie Speicher-E/A-Ressourcen zuteilen, können Sie die IOPS begrenzen, die für eine virtuelle Maschine zulässig sind. Standardmäßig sind sie unbegrenzt. Wenn eine virtuelle Maschine über mehr als eine virtuelle Festplatte verfügt, müssen Sie den Grenzwert für alle ihre virtuellen Festplatten festlegen. Anderenfalls wird der Grenzwert für die virtuelle Maschine nicht wirksam. In diesem Fall ist der Grenzwert für die virtuelle Maschine die Summierung der Grenzwerte für alle virtuellen Festplatten.

Die Vor- und Nachteile des Festlegens von Ressourcengrenzwerten sind in der Dokumentation zur *vSphere-Ressourcenverwaltung* beschrieben. Wenn der Grenzwert, den Sie für eine virtuelle Maschine festlegen möchten, in Form von MB pro Sekunde anstatt in IOPS vorliegt, können Sie auf Basis der Standard-E/A-Größe für diese virtuelle Maschine die MB pro Sekunde in IOPS konvertieren. Wenn Sie beispielsweise eine Sicherungsanwendung mit E/A-Vorgängen von 64 KB auf 10MB pro Sekunde beschränken möchten, legen Sie einen Grenzwert von 160 IOPS fest.

Anzeigen von Ressourcenanteilen und Grenzwerten für Storage I/O Control

Sie können die Anteile und Grenzwerte aller virtuellen Maschinen einsehen, die auf einem Datenspeicher ausgeführt werden. Anhand dieser Informationen können Sie ungeachtet des Clusters, auf dem sie ausgeführt werden, die Einstellungen aller virtuellen Maschinen vergleichen, die auf den Datenspeicher zugreifen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Datenspeicher in der Bestandsliste des vSphere-Clients aus.
- 2 Klicken Sie auf die Registerkarte **Virtuelle Maschinen (Virtual Machines)**.

Die Registerkarte zeigt jede virtuelle Maschine an, die auf dem Datenspeicher ausgeführt wird, sowie die zugewiesenen Anteilswerte, den IOPS-Grenzwert und den Prozentsatz der Datenspeicheranteile.

Überwachen der Anteile von Storage I/O Control

Anhand der Datenspeicher-Registerkarte **Leistung** können Sie überwachen, wie Storage I/O Control die E/A-Arbeitslasten der virtuellen Maschinen verarbeitet, die auf Basis ihrer Anteile auf einen Datenspeicher zugreifen.

Die Leistungsdiagramme des Datenspeichers ermöglichen Ihnen die Überwachung der folgenden Informationen:

- Durchschnittliche Latenz und aggregierte IOPS auf dem Datenspeicher

- Latenz für Hosts
- Warteschlangentiefe für Hosts
- Lese/Schreib-IOPS für Hosts
- Latenz für Lese-/Schreibvorgänge für Festplatten virtueller Maschinen
- Lese/Schreib-IOPS für Festplatten virtueller Maschinen

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients den Datenspeicher aus und klicken Sie auf die Registerkarte **Leistung**.
- 2 Wählen Sie im Dropdown-Menü **Ansicht** die Option **Leistung**.

Weitere Informationen finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*.

Festlegen von Ressourcenanteilen und Grenzwerten für Storage I/O Control

Teilen Sie den virtuellen Maschinen Speicher-E/A-Ressourcen basierend auf der Wichtigkeit zu, indem Sie der virtuellen Maschine eine relative Menge an Anteilen zuweisen.

Freigaben schreiben nicht unbedingt die Zuteilung in Form von E/A-Vorgängen oder MB pro Sekunde vor, es sei denn, die Arbeitslasten der virtuellen Maschine sind sehr ähnlich. Höhere Anteile erlauben einer virtuellen Maschine, am Speichergerät oder Datenspeicher mehr gleichzeitige E/A-Vorgänge bereitzuhalten als einer virtuellen Maschine mit niedrigeren Anteilen. Die beiden virtuellen Maschinen haben je nach Arbeitslast möglicherweise einen unterschiedlichen Durchsatz.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie eine virtuellen Maschine aus der Bestandsliste des vSphere-Clients aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht** auf **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Ressourcen** und wählen Sie **Festplatte**.
- 4 Wählen Sie eine virtuelle Festplatte aus der Liste aus.
- 5 Klicken Sie auf die Spalte **Anteile**, um die relative Menge an Anteilen („Niedrig“, „Normal“ oder „Hoch“) auszuwählen, die der virtuellen Maschine zugeteilt werden soll.

Sie können die Option **Benutzerdefiniert** auswählen und eigene Anteilswerte angeben.

- 6 Klicken Sie auf die Spalte **Grenzwert - IOPs** und geben Sie den oberen Grenzwert für Speicherressourcen an, die der virtuellen Maschine zugeteilt werden sollen.

Unter IOPs versteht man die Anzahl an E/A-Vorgängen pro Sekunde. Standardmäßig sind IOPs nicht begrenzt. Sie wählen „Niedrig“ (500), „Normal“ (1000) oder „Hoch“ (2000), oder sie können „Benutzerdefiniert“ wählen, um eine benutzerdefinierte Anzahl an Anteilen einzugeben.

- 7 Klicken Sie auf **OK**.

Anteile und Grenzwerte sind auf der Registerkarte **Ressourcenzuteilung** für den Host und den Cluster wiedergegeben.

Storage I/O Control aktivieren

Wenn Sie Storage I/O Control aktivieren, überwacht ESXi die Datenspeicherlatenz und passt die an den Datenspeicher gesendete E/A-Last an, wenn die durchschnittliche Latenz des Datenspeichers den Schwellenwert überschreitet.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients einen Datenspeicher aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie auf **Eigenschaften**.
- 3 Wählen Sie unter „Storage I/O Control“ das Kontrollkästchen **Aktiviert**.
- 4 Klicken Sie auf **Schließen**.

In der Spalte „Speicher-E/A-Steuerung“ der Registerkarte „Datenspeicher“ wird angezeigt, dass die Speicher-E/A-Steuerung für den Datenspeicher aktiviert ist.

Einstellen des Schwellenwerts für Storage I/O Control

Der Überlastungsschwellenwert eines Datenspeichers ist die für den Datenspeicher maximal zulässige Latenz, die erreicht werden kann, bevor Storage I/O Control damit beginnt, den VM-Arbeitslasten ihren Anteil entsprechend eine Wichtigkeit zuzuweisen.

In den meisten Umgebungen kann die Einstellung des Schwellenwerts beibehalten werden.



VORSICHT Damit Storage I/O Control ordnungsgemäß arbeiten kann, müssen für alle Datenspeicher, die dieselben Spindel im Array verwenden, derselbe Überlastungsschwellenwert eingestellt sein.

Falls Sie die Einstellung für den Überlastungsschwellenwert ändern möchten, ziehen Sie dabei Folgendes in Betracht.

- Ein höherer Wert führt in der Regel zu einem höheren Aggregatdurchsatz und zu einer schwächeren Isolation. Eine Drosselung tritt erst dann ein, wenn die durchschnittliche Latenz den Schwellenwert überschreitet.
- Falls der Durchsatz eine größerer Bedeutung als die Latenz hat, stellen Sie den Wert nicht zu niedrig ein. Für Fibre-Channel-Festplatten kann beispielsweise ein Wert unter 20 ms den Spitzendurchsatz bei Festplatten beeinträchtigen. Ein sehr hoher Wert (mehr als 50 ms) lässt eine sehr hohe Latenz zu, möglicherweise jedoch ohne signifikanten Nutzen für den Gesamtdurchsatz.
- Ein niedrigerer Wert führt zu kürzerer Gerätelatenz und zu stärkerer E/A-Leistungsisolation bei der virtuellen Maschine. Stärkere Isolation bedeutet, dass die Anteilsteuerung häufiger durchgeführt wird. Eine geringere Gerätelatenz bewirkt bei virtuellen Maschinen mit den höchsten Anteilen eine geringere E/A-Latenz. Dabei muss bei den virtuellen Maschinen mit geringeren Anteilen eine höhere E/A-Latenz in Kauf genommen werden.
- Wenn die Latenz wichtiger ist, führt ein sehr niedriger Wert (niedriger als 20 ms) zu niedrigerer Gerätelatenz und besserer Isolation der I/Os auf Kosten einer Verringerung des Gesamtdatenspeicherdurchsatzes.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Überprüfen Sie, ob Storage I/O Control aktiviert ist.

Vorgehensweise

- 1 Wählen Sie in der Bestandsliste des vSphere-Clients einen Datenspeicher aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie auf **Eigenschaften**.
- 3 Wählen Sie unter „Storage I/O Control“ das Kontrollkästchen **Aktiviert**.
- 4 (Optional) Klicken Sie auf **Erweitert**, wenn Sie den Überlastungsschwellenwert für den Datenspeicher bearbeiten möchten.
Der Wert muss zwischen 10 ms und 100 ms liegen.
- 5 (Optional) Klicken Sie auf **Zurücksetzen**, um den Überlastungsschwellenwert auf den Standardwert (30 ms) zurückzusetzen.
- 6 Klicken Sie auf **OK** und klicken Sie dann auf **Schließen**.

Verwalten von Ressourcenpools

Ein Ressourcenpool ist eine logische Abstraktion für eine flexible Verwaltung von Ressourcen. Ressourcenpools können in Hierarchien angeordnet und zur hierarchischen Partitionierung verfügbarer CPU- und Arbeitsspeicherressourcen verwendet werden.

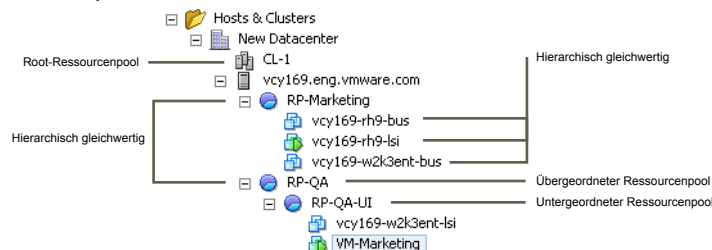
Jeder eigenständige Host und jeder DRS-Cluster verfügt über einen (nicht sichtbaren) Root-Ressourcenpool, der die Ressourcen des Hosts oder Clusters gruppiert. Der Root-Ressourcenpool erscheint deshalb nicht, weil er stets mit den Ressourcen des Hosts (oder Clusters) identisch ist.

Der Benutzer hat die Möglichkeit, auf Basis des Root-Ressourcenpools oder anderer, durch Benutzer erstellter, untergeordneter Ressourcenpools weitere untergeordnete Ressourcenpools zu erstellen. Jeder untergeordnete Ressourcenpool besitzt einen gewissen Anteil der übergeordneten Ressourcen und kann seinerseits selbst über eine Hierarchie untergeordneter Ressourcenpools verfügen, um immer kleinere Einheiten der Rechenfähigkeit abzubilden.

In einem Ressourcenpool können untergeordnete Ressourcenpools, virtuelle Maschinen oder beides enthalten sein. So entsteht eine hierarchische Ordnung gemeinsam genutzter Ressourcen. Die Ressourcenpools einer höheren Ebene werden als übergeordnete Ressourcenpools bezeichnet. Ressourcenpools und virtuelle Maschinen derselben Ebene werden als hierarchisch gleichwertig bezeichnet. Der Cluster selbst stellt den Root-Ressourcenpool dar. Falls Sie keine untergeordneten Ressourcenpools erstellen, gibt es lediglich die Root-Ressourcenpools.

Im folgenden Beispiel ist RP-QA der übergeordnete Ressourcenpool für RP-QA-UI. RP-Marketing und RP-QA sind hierarchisch gleichwertige Ressourcenpools. Die drei virtuelle Maschinen direkt unter RP-Marketing sind ebenfalls hierarchisch gleichwertig.

Abbildung 25-2. Übergeordnete, untergeordnete und hierarchisch gleichwertige Ressourcenpools in der Ressourcenpoolhierarchie



Für jeden Ressourcenpool können Werte für Reservierung, Grenze und Anteile festgelegt und bestimmt werden, ob die Reservierung erweiterbar sein soll. Die Ressourcen des Ressourcenpools sind anschließend für untergeordnete Ressourcenpools und virtuelle Maschinen verfügbar.

Erstellen eines Ressourcenpools

Sie können für jeden ESXi-Host, Ressourcenpool oder DRS-Cluster einen untergeordneten Ressourcenpool erstellen.

HINWEIS Wenn ein Host zu einem Cluster hinzugefügt wurde, ist es nicht möglich, untergeordnete Ressourcenpools dieses Hosts zu erstellen. Wenn der Cluster für DRS aktiviert ist, können Sie untergeordnete Ressourcenpools des Clusters erstellen.

Im Rahmen der Erstellung eines untergeordneten Ressourcenpools werden Sie aufgefordert, Attributinformationen für den Ressourcenpool einzugeben. Das System verwendet eine Zugangssteuerung, um sicherzustellen, dass nicht verfügbare Ressourcen auch nicht zugeteilt werden.

Voraussetzungen

Der vSphere-Client ist mit dem vCenter Server-System verbunden. Wenn Sie den vSphere-Client direkt mit einem Host verbinden, können Sie keinen Ressourcenpool erstellen.

Vorgehensweise

- 1 Wählen Sie in der vSphere-Client-Bestandsliste ein übergeordnetes Objekt für den Ressourcenpool aus (einen Host, einen anderen Ressourcenpool oder einen DRS-Cluster).
- 2 Wählen Sie **Datei > Neu > Ressourcenpool**.
- 3 Geben Sie einen Namen zur Identifikation des Ressourcenpools ein.
- 4 Geben Sie an, wie die CPU- und Arbeitsspeicherressourcen zugeteilt werden sollen.

Die CPU-Ressourcen Ihres Ressourcenpools sind die garantierten physischen Ressourcen, die der Host für einen Ressourcenpool reserviert. In der Regel sollten Sie die Voreinstellung übernehmen, und dem Host die Zuteilung der Ressourcen überlassen.

Option	Beschreibung
Anteile	<p>Geben Sie den Anteil der Ressourcen dieses Ressourcenpools an den Gesamtressourcen des übergeordneten Ressourcenpools an. Hierarchisch gleichwertige Ressourcenpools teilen sich Ressourcen auf der Basis ihrer relativen Anteilswerte, die an die Reservierung und die Grenzwerte geknüpft sind.</p> <ul style="list-style-type: none"> ■ Wählen Sie Niedrig, Normal oder Hoch. Dadurch werden die Anteilswerte im Verhältnis 1:2:4 festgelegt. ■ Wählen Sie die Einstellung Benutzerdefiniert, um jeder virtuellen Maschine einen bestimmten Anteil zuzuweisen, der einer proportionalen Gewichtung entspricht.
Reservierung	<p>Geben Sie eine garantierte CPU- oder Arbeitsspeicherzuteilung für diesen Ressourcenpool an. Die Standardeinstellung lautet 0.</p> <p>Eine Reservierung ungleich Null wird von den nicht reservierten Ressourcen des übergeordneten Hosts oder Ressourcenpools subtrahiert. Die Ressourcen werden als reserviert betrachtet, auch wenn keine virtuellen Maschinen mit dem Ressourcenpool verknüpft sein sollten.</p>

Option	Beschreibung
Erweiterbare Reservierung	Wenn das Kontrollkästchen ausgewählt ist (Standardeinstellung), werden erweiterbare Reservierungen bei der Zugangssteuerung berücksichtigt. Wenn Sie eine virtuelle Maschine in diesem Ressourcenpool einschalten und die gesamten Reservierungen der virtuellen Maschinen größer als die Reservierung des Ressourcenpools sind, kann der Ressourcenpool Ressourcen vom übergeordneten Pool verwenden.
Grenzwert	Geben Sie die Obergrenze der Zuteilung von CPU- oder Arbeitsspeicheranteilen für diesen Ressourcenpool an. In der Regel können Sie die Voreinstellung übernehmen (Unbegrenzt). Deaktivieren Sie das Kontrollkästchen Unbegrenzt , um einen Grenzwert festzulegen.

5 Klicken Sie auf **OK**.

Nachdem Sie einen Ressourcenpool erstellt haben, können Sie ihm virtuelle Maschinen hinzufügen. Die Anteile einer virtuellen Maschine sind relativ zu anderen virtuellen Maschinen (oder Ressourcenpools) mit demselben übergeordneten Ressourcenpool.

Beispiel: Erstellen von Ressourcenpools

Angenommen, Sie haben einen Host, der 6 GHz an CPU und 3 GB an Arbeitsspeicher liefert und von Ihrer Marketing- und Ihrer QA-Abteilung gemeinsam verwendet werden muss. Sie möchten die Ressourcen außerdem ungleichmäßig verteilen und der einen Abteilung (QA) eine höhere Priorität einräumen. Dies lässt sich erreichen, indem man einen Ressourcenpool für jede Abteilung erstellt und das Attribut **Anteile** verwendet, um die Ressourcenzuteilung zu priorisieren.

In dem Beispiel wird gezeigt, wie Sie mit dem ESXi-Host als übergeordneter Ressource einen Ressourcenpool erstellen.

- 1 Geben Sie im Dialogfeld „Ressourcenpool erstellen“ einen Namen für den Ressourcenpool der QA-Abteilung ein (z. B. „RP-QA“).
- 2 Legen Sie für die **Anteile (Shares)** die Option **Hoch (High)** fest, und zwar sowohl für die CPU- als auch die Arbeitsspeicherressourcen von RP-QS.
- 3 Erstellen Sie einen zweiten Ressourcenpool namens „RP-Marketing“.
Übernehmen Sie die Anteilseinstellung **Normal** für CPU- und Arbeitsspeicherressourcen.
- 4 Klicken Sie auf **OK**.

Wenn Ressourcenkonflikte auftreten, erhält „RP-QA“ 4GHz an Taktfrequenz und 2GB an Arbeitsspeicher und „RP-Marketing“ 2GHz und 1GB. Anderenfalls können sie mehr als diesen Anteil erhalten. Diese Ressourcen sind anschließend für die virtuellen Maschinen im jeweiligen Ressourcenpool verfügbar.

Bearbeiten eines Ressourcenpools

Nachdem Sie den Ressourcenpool erstellt haben, können Sie seine Einstellungen für die Speicherressourcen und die CPU bearbeiten.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie in der Bestandsliste des vSphere-Clients mit der rechten Maustaste auf den Ressourcenpool und wählen Sie **Einstellungen bearbeiten**.
- 2 Im Dialogfeld „Einstellungen bearbeiten“ können Sie sämtliche Attribute des ausgewählten Ressourcenpools ändern, wie unter [„Erstellen eines Ressourcenpools“](#), auf Seite 398 beschrieben.

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

Hinzufügen einer virtuellen Maschine zu einem Ressourcenpool

Wenn Sie eine virtuelle Maschine erstellen, können Sie mithilfe des Assistenten zum Erstellen neuer virtuellen Maschinen im Rahmen des Erstellungsprozesses einen Speicherort für den Ressourcenpool angeben. Darüber hinaus können Sie eine vorhandene virtuelle Maschine zu einem Ressourcenpool hinzufügen.

Folgendes geschieht, wenn Sie eine virtuelle Maschine in einen neuen Ressourcenpool verschieben:

- Reservierung und Grenzwert der virtuellen Maschine ändern sich nicht.
- Wenn die Anteile der virtuellen Maschine hoch, mittel oder gering sind, gibt % Anteile (%Shares) die Gesamtzahl der im neuen Ressourcenpool genutzten Anteile wieder.
- Wurden der virtuellen Maschine benutzerdefinierte Anteile zugewiesen, bleibt der Anteilswert unverändert.

HINWEIS Da sich Anteilszuordnungen stets auf einen Ressourcenpool beziehen, müssen Sie die Anteile einer virtuellen Maschine möglicherweise beim Verschieben in einen Ressourcenpool manuell ändern, damit diese mit den relativen Werten im neuen Ressourcenpool konsistent sind. Es wird eine Meldung angezeigt, falls eine virtuelle Maschine einen sehr hohen (oder sehr geringen) Prozentsatz der gesamten Anteile erhalten würde.

- Die in der Registerkarte Ressourcenzuteilung angezeigten Informationen zu reservierten und nicht reservierten CPU- und Arbeitsspeicherressourcen des Ressourcenpools ändern sich, um (ggf.) die mit der virtuellen Maschine verknüpften Reservierungen wiederzugeben.

HINWEIS Falls die virtuelle Maschine ausgeschaltet oder angehalten wurde, kann sie zwar verschoben werden, die insgesamt verfügbaren Ressourcen (wie reservierte und nicht reservierte CPU- und Arbeitsspeicheranteile) des Ressourcenpools werden dadurch jedoch nicht beeinträchtigt.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Clients die gewünschte virtuelle Maschine in der Bestandsliste aus.
Die virtuelle Maschine kann mit einem eigenständigen Host, einem Cluster, oder einem anderen Ressourcenpool verknüpft sein.
- 2 Ziehen Sie die virtuelle(n) Maschine(n) in den Ressourcenpool.

Wenn eine virtuelle Maschine eingeschaltet ist und der Zielressourcenpool nicht über ausreichende CPU- oder Arbeitsspeicheranteile verfügt, um die Reservierung der virtuellen Maschine zu garantieren, wird die Verschiebung durch die Zugangssteuerung unterbunden. In einem Fehlerdialogfeld werden die verfügbaren und angeforderten Ressourcen angezeigt, sodass Sie abwägen können, ob das Problem durch eine entsprechende Anpassung behoben werden könnte.

Entfernen einer virtuellen Maschine aus einem Ressourcenpool

Sie können eine virtuelle Maschine aus einem Ressourcenpool entfernen, indem Sie die virtuelle Maschine entweder in einen anderen Ressourcenpool verschieben oder löschen.

Wenn Sie eine virtuelle Maschine aus einem Ressourcenpool entfernen, sinkt die Gesamtzahl der mit dem Ressourcenpool verknüpften Anteile, sodass jeder verbleibende Anteil nun mehr Ressourcen darstellt. Angenommen, Sie verfügen über einen Pool mit einer Berechtigung von 6 GHz, in dem drei virtuelle Maschinen enthalten sind, für deren Anteile die Einstellung auf **Normal** gesetzt wurde. Nehmen wir weiter an, die virtuellen Maschinen sind CPU-gebunden und verfügen über eine gleiche Zuteilung von je 2 GHz. Falls nun eine der drei Maschinen in einen anderen Ressourcenpool verschoben wird, erhalten die beiden verbleibenden virtuellen Maschinen eine gleiche Zuteilung von je 3 GHz.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie eine der folgenden Methoden zum Entfernen der virtuellen Maschine aus dem Ressourcenpool aus.
 - Ziehen Sie die virtuelle Maschine in einen anderen Ressourcenpool.
Die virtuelle Maschine muss nicht ausgeschaltet werden, wenn Sie sie verschieben möchten.
 - Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Aus Bestandsliste entfernen** oder **Von Festplatte löschen**.
Die virtuelle Maschine muss ausgeschaltet sein, damit sie vollständig entfernt werden kann.

Entfernen eines Ressourcenpools

Sie können einen Ressourcenpool aus der Bestandsliste entfernen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf den Ressourcenpool und wählen Sie **Entfernen**.
Ein Bestätigungsdialogfeld wird angezeigt.
- 2 Klicken Sie auf **Ja**, um den Ressourcenpool zu entfernen.

Verwenden des DRS-Clusters zur Ressourcenverwaltung

Nachdem Sie einen DRS-Cluster erstellt haben, können Sie ihn anpassen und zur Ressourcenverwaltung verwenden.

Um Ihren DRS-Cluster und die enthaltenen Ressourcen anzupassen, können Sie Affinitätsregeln konfigurieren sowie Hosts und virtuelle Maschinen hinzufügen und entfernen. Wenn die Einstellungen und Ressourcen eines Clusters definiert wurden, sollten Sie sicherstellen, dass es sich um einen gültigen Cluster handelt und dies so bleibt. Mit einem gültigen DRS-Cluster können Sie zudem Betriebsressourcen verwalten und mit vSphere HA interoperieren.

Erstellen eines DRS-Clusters

Ein Cluster ist eine Sammlung von ESXi-Hosts und verknüpften virtuellen Maschinen mit gemeinsam genutzten Ressourcen und einer gemeinsamen Verwaltungsoberfläche. Sie müssen einen Cluster erstellen und DRS aktivieren, um die Vorteile der Ressourcenverwaltung auf Clusterebene ausnutzen zu können.

Je nachdem, ob Enhanced vMotion Compatibility (EVC) aktiviert ist, verhält sich DRS anders, wenn Sie virtuelle vSphere Fault Tolerance (vSphere FT)-Maschinen im Cluster verwenden.

Tabelle 25-1. DRS-Verhalten mit virtuellen vSphere FT-Maschinen und EVC

EVC	DRS (Lastenausgleich)	DRS (anfängliche Platzierung)
Aktiviert	Aktiviert (primäre und sekundäre virtuelle Maschinen)	Aktiviert (primäre und sekundäre virtuelle Maschinen)
Deaktiviert	Deaktiviert (primäre und sekundäre virtuelle Maschinen)	Deaktiviert (primäre virtuelle Maschine) Vollautomatisiert (sekundäre virtuelle Maschinen)

Erstellen eines DRS-Clusters

Erstellen Sie ein DRS-Cluster unter Verwendung des Assistenten für Neuer Cluster im vSphere-Client.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Sie können einen Cluster zwar ohne zusätzliche Lizenz erstellen, Sie benötigen jedoch eine Lizenz zur Aktivierung von vSphere DRS (oder vSphere HA) für einen Cluster.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf ein Datacenter oder einen Ordner im vSphere Client und wählen Sie **Neuer Cluster**.
- 2 Benennen Sie den Cluster im Textfeld **Name**.
Dieser Name wird im Bestandslistenbereich des vSphere-Clients angezeigt.
- 3 Aktivieren Sie die DRS-Funktion, indem Sie auf **vSphere DRS** klicken.
Sie können die vSphere HA-Funktion auch aktivieren, indem Sie auf **vSphere HA** klicken.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie eine Standard-Automatisierungsebene für DRS.

Automatisierungsebene	Aktion
Manuell	<ul style="list-style-type: none"> ■ Anfängliche Platzierung: Die empfohlenen Hosts werden angezeigt. ■ Migration: Empfehlung wird angezeigt.
Teilautomatisiert	<ul style="list-style-type: none"> ■ Anfängliche Platzierung: Automatisch. ■ Migration: Empfehlung wird angezeigt.
Vollautomatisiert	<ul style="list-style-type: none"> ■ Anfängliche Platzierung: Automatisch. ■ Migration: Die Empfehlung wird automatisch umgesetzt.

- 6 Legen Sie den Migrationsschwellenwert für DRS fest.
- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie die Standard-Energieverwaltungseinstellung für den Cluster an.
Wählen Sie beim Aktivieren der Energieverwaltung eine vSphere DPM-Schwellenwerteinstellung aus.

- 9 Klicken Sie auf **Weiter**.
- 10 Aktivieren Sie ggf. Enhanced vMotion Compatibility (EVC) und wählen Sie den entsprechenden Betriebsmodus aus.
- 11 Klicken Sie auf **Weiter**.
- 12 Wählen Sie einen Speicherort für die Auslagerungsdateien Ihrer virtuellen Maschinen aus.
 Sie können die Auslagerungsdatei entweder im selben Verzeichnis wie die virtuelle Maschine speichern oder in einen Datenspeicher, der vom Host festgelegt wird (lokale Auslagerung durch Host).
- 13 Klicken Sie auf **Weiter**.
- 14 Überprüfen Sie die von Ihnen ausgewählten Optionen auf der Übersichtsseite.
- 15 Klicken Sie auf **Beenden (Finish)**, um die Clustererstellung abzuschließen bzw. auf **Zurück (Back)**, um im Assistenten seitenweise zurückzugehen und Änderungen an der Clustereinrichtung vorzunehmen.

Ein neuer Cluster enthält keine Hosts oder virtuellen Maschinen.

Informationen zum Hinzufügen von Hosts und virtuellen Maschinen zum Cluster finden Sie unter „[Hinzufügen von Hosts zu einem Cluster](#)“, auf Seite 405 und „[Entfernen virtueller Maschinen aus einem Cluster](#)“, auf Seite 406.

Festlegen einer benutzerdefinierten Automatisierungsebene für eine virtuelle Maschine

Nachdem Sie einen DRS-Cluster erstellt haben, können Sie die Automatisierungsebene für einzelne virtuelle Maschinen anpassen, um den standardmäßigen Automatisierungsmodus des Clusters außer Kraft zu setzen.

So können Sie zum Beispiel für bestimmte virtuelle Maschinen in einem vollautomatisierten Cluster **Manuell** oder für bestimmte virtuelle Maschinen in einem manuellen Cluster **Teilautomatisiert** auswählen.

Wenn eine virtuelle Maschine auf **Deaktiviert** gesetzt ist, führt vCenter Server keine Migration dieser virtuellen Maschine durch bzw. bietet keine entsprechenden Migrationsempfehlungen an. Dies wird als Binden der virtuellen Maschine an ihren registrierten Host bezeichnet.

HINWEIS Wenn Sie EVC (Enhanced vMotion Compatibility) nicht für den Cluster aktiviert haben, wird bei fehlertoleranten virtuellen Maschinen „DRS deaktiviert“ eingestellt. Sie werden auf diesem Bildschirm angezeigt, aber Sie können ihnen keinen Automatisierungsmodus zuweisen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Fenster unter „vSphere DRS“ die Option **Optionen für virtuelle Maschinen**.
- 3 Aktivieren Sie das Kontrollkästchen **Automatisierungsebenen von individuellen virtuellen Maschinen aktivieren**.
- 4 (Optional) Heben Sie die Auswahl der Einstellung **Automatisierungsebenen von individuellen virtuellen Maschinen aktivieren** auf, um alle einzeln festgelegten VM-Außerkraftsetzungen vorübergehend zu deaktivieren.

Wenn das Kontrollkästchen wieder aktiviert wird, werden die Einstellungen der virtuellen Maschine wiederhergestellt.

- 5 (Optional) Um vorübergehend alle vMotion-Aktivitäten in einem Cluster anzuhalten, versetzen Sie den Cluster in den manuellen Modus und heben die Auswahl des Kontrollkästchens **Automatisierungsebenen von individuellen virtuellen Maschinen aktivieren** auf.
- 6 Wählen Sie eine oder mehrere virtuelle Maschinen aus.
- 7 Klicken Sie auf die Spalte **Automatisierungsebene** und wählen Sie eine Automatisierungsebene aus dem Dropdown-Menü aus.

Option	Beschreibung
Manuell	Die Empfehlungen zur Platzierung und zur Migration werden angezeigt, jedoch erst ausgeführt, wenn Sie die Empfehlungen manuell übernommen haben.
Vollautomatisiert	Die Empfehlungen zur Platzierung und zur Migration werden automatisch ausgeführt.
Teilautomatisiert	Die anfängliche Platzierung wird automatisch durchgeführt. Die Migrationsempfehlungen werden angezeigt, aber nicht ausgeführt.
Deaktiviert	vCenter Server migriert die virtuelle Maschine nicht und gibt auch keine Migrationsempfehlungen für sie.

- 8 Klicken Sie auf **OK**.

HINWEIS Andere VMware-Produkte oder Funktionen, z. B. vSphere vApp und vSphere Fault Tolerance, können die Automatisierungsebenen von virtuellen Maschinen in einem DRS-Cluster möglicherweise außer Kraft setzen. Weitere Informationen finden Sie in der produktspezifischen Dokumentation.

Deaktivieren von DRS

Sie können DRS für ein Cluster deaktivieren.

Beim Deaktivieren von DRS werden die Ressourcenpoolhierarchie und die Affinitätsregeln des Clusters nicht wiederhergestellt, wenn DRS wieder eingeschaltet wird. Wenn Sie DRS deaktivieren, werden die Ressourcenpools aus dem Cluster entfernt. Wenn Sie die Ressourcenpools nicht durch das Deaktivieren von DRS verlieren möchten, müssen Sie DRS anhalten, indem Sie die DRS-Automatisierungsebene in „Manuell“ ändern (und alle Außerkraftsetzungen für virtuelle Maschinen deaktivieren). Dies verhindert automatische DRS-Aktionen, erhält jedoch die Ressourcenpoolhierarchien.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Cluster in der Bestandsliste des vSphere-Clients aus.
- 2 Klicken Sie mit der rechten Maustaste und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie im linken Fenster die Option **Allgemein** und deaktivieren Sie das Kontrollkästchen **vSphere DRS einschalten**.
- 4 Klicken Sie auf **OK**, um DRS zu deaktivieren.

Hinzufügen von Hosts zu einem Cluster

Die Vorgehensweise für das Hinzufügen von Hosts zu einem Cluster unterscheidet sich für Hosts, die durch denselben vCenter Server (verwaltete Hosts) verwaltet werden, im Vergleich zu Hosts, die derzeit nicht durch diesen Server verwaltet werden.

Nach dem Hinzufügen eines Hosts werden die virtuellen Maschinen, die für den Host bereitgestellt wurden, Bestandteil des Clusters und DRS kann das Migrieren von einigen virtuellen Maschinen auf andere Hosts in dem Cluster empfehlen.

Hinzufügen eines verwalteten Hosts zu einem Cluster

Wenn Sie einen eigenständigen Host, der bereits von vCenter Server verwaltet wird, zu einem DRS-Cluster hinzufügen, werden dem Cluster die Ressourcen des Hosts zugeordnet.

Sie können auswählen, ob vorhandene virtuelle Maschinen und Ressourcenpools dem Root-Ressourcenpool des Clusters zugeordnet oder die Ressourcenpoolhierarchie übertragen werden soll.

HINWEIS Falls ein Host über keine untergeordneten Ressourcenpools oder virtuellen Maschinen verfügt, werden dem Cluster die Host-Ressourcen hinzugefügt, es wird jedoch keine Ressourcenpool-Hierarchie mit einem Ressourcenpool oberster Ebene erstellt.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Host entweder über die Bestandsliste oder die Listenanzeige aus.
- 2 Ziehen Sie den Host in das Zielclusterobjekt.
- 3 Geben Sie die weitere Verfahrensweise mit den virtuellen Maschinen und Ressourcenpools des Hosts an.
 - **Alle virtuellen Maschinen dieses Hosts im Root-Ressourcenpool des Clusters platzieren**
vCenter Server entfernt alle vorhandenen Ressourcenpools des Hosts und die virtuellen Maschinen in der Hierarchie des Hosts werden alle Root zugeordnet. Da Anteilszuordnungen stets relativ zu einem Ressourcenpool sind, müssen Sie die Anteile einer virtuellen Maschine möglicherweise manuell ändern, nachdem Sie diese Option ausgewählt haben, die die Ressourcenpoolhierarchie zerstört.
 - **Einen Ressourcenpool für die virtuellen Maschinen und Ressourcenpools dieses Hosts erstellen**
vCenter Server erstellt einen Ressourcenpool auf oberster Ebene, der zu einem dem Cluster direkt untergeordneten Element wird, und fügt alle untergeordneten Elemente des Hosts zu diesem neuen Ressourcenpool hinzu. Für diesen neuen Ressourcenpool der obersten Ebene können Sie einen Namen vergeben. Der Standard ist **Übertragen von <host_name>**.

Der Host wurde zum Cluster hinzugefügt.

Hinzufügen eines nicht verwalteten Hosts zu einem Cluster

Sie können einen nicht verwalteten Host zu einem Cluster hinzufügen. Ein solcher Host wird derzeit nicht durch dasselbe vCenter Server-System wie der Cluster verwaltet und ist im vSphere-Client nicht sichtbar.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Cluster, zu dem der Host hinzugefügt werden soll, und klicken Sie im Kontextmenü auf **Host hinzufügen**.
- 2 Geben Sie den Hostnamen, den Benutzernamen und das Kennwort ein und klicken Sie auf **Weiter**.
- 3 Zeigen Sie die Informationsübersicht an, und klicken Sie auf **Weiter (Next)**.
- 4 Geben Sie die weitere Verfahrensweise mit den virtuellen Maschinen und Ressourcenpools des Hosts an.

- **Alle virtuellen Maschinen dieses Hosts im Root-Ressourcenpool des Clusters platzieren**

vCenter Server entfernt alle vorhandenen Ressourcenpools des Hosts und die virtuellen Maschinen in der Hierarchie des Hosts werden alle Root zugeordnet. Da Anteilszuordnungen stets relativ zu einem Ressourcenpool sind, müssen Sie die Anteile einer virtuellen Maschine möglicherweise manuell ändern, nachdem Sie diese Option ausgewählt haben, die die Ressourcenpoolhierarchie zerstört.

- **Einen Ressourcenpool für die virtuellen Maschinen und Ressourcenpools dieses Hosts erstellen**

vCenter Server erstellt einen Ressourcenpool auf oberster Ebene, der zu einem dem Cluster direkt untergeordneten Element wird, und fügt alle untergeordneten Elemente des Hosts zu diesem neuen Ressourcenpool hinzu. Für diesen neuen Ressourcenpool der obersten Ebene können Sie einen Namen vergeben. Der Standard ist **Übertragen von <host_name>**.

Der Host wurde zum Cluster hinzugefügt.

Hinzufügen virtueller Maschinen zu einem Cluster

Es gibt drei Möglichkeiten, eine virtuelle Maschine zu einem Cluster hinzuzufügen.

- Wird ein Host zu einem Cluster hinzugefügt, werden alle auf dem Host befindlichen virtuellen Maschinen ebenfalls zum Cluster hinzugefügt.
- Bei der Erstellung einer virtuellen Maschine werden Sie durch den Assistenten zum Erstellen neuer virtueller Maschinen aufgefordert, den Speicherort der virtuellen Maschine festzulegen. Sie können einen eigenständigen Host oder einen Cluster auswählen und jeden Ressourcenpool in dem Host oder Cluster auswählen.
- Sie können mithilfe des Assistenten für das Migrieren einer virtuellen Maschine eine virtuelle Maschine von einem eigenständigen Host oder von einem Cluster auf einen anderen Cluster migrieren. Ziehen Sie zum Starten dieses Assistenten das Objekt der virtuellen Maschine auf das Clusterobjekt oder klicken Sie mit der rechten Maustaste auf den Namen der virtuellen Maschine und wählen Sie **Migrieren**.

HINWEIS Eine virtuelle Maschine kann unmittelbar in den Ressourcenpool innerhalb eines Clusters verschoben werden. In diesem Fall wird der Assistent für das Migrieren einer virtuellen Maschine gestartet, aber die Auswahlseite für den Ressourcenpool erscheint nicht. Das direkte Migrieren auf einen Host innerhalb eines Clusters ist nicht zulässig, da die Ressourcen über den Ressourcenpool gesteuert werden.

Entfernen virtueller Maschinen aus einem Cluster

Sie können virtuelle Maschine aus einem Cluster entfernen.

Sie haben zwei Möglichkeiten, um eine virtuelle Maschine aus einem Cluster zu entfernen.

- Wenn Sie einen Host aus einem Cluster entfernen, werden alle ausgeschalteten virtuellen Maschinen, die nicht auf andere Hosts migriert werden, ebenfalls entfernt. Ein Host kann nur entfernt werden, wenn er sich im Wartungsmodus befindet oder nicht verbunden ist. Wird ein Host aus einem DRS-Cluster entfernt, wird der Cluster möglicherweise aufgrund einer Überbelegung gelb gekennzeichnet.

- Sie können mithilfe des Assistenten für das Migrieren einer virtuellen Maschine eine virtuelle Maschine von einem eigenständigen Host oder von einem Cluster auf einen anderen Cluster migrieren. Um diesen Assistenten zu starten, klicken Sie mit der rechten Maustaste auf den Namen der virtuellen Maschine und wählen Sie **Migrieren**.

Entfernen eines Hosts aus einem Cluster

Wenn Sie einen Host aus einem DRS-Cluster entfernen, wirkt sich dies auf die Ressourcenpoolhierarchien und die virtuellen Maschinen aus und Sie erstellen möglicherweise ungültige Cluster. Berücksichtigen Sie die Auswirkungen auf die betroffenen Objekte, bevor Sie den Host entfernen.

- Ressourcenpoolhierarchien – Nach dem Entfernen eines Hosts aus einem Cluster behält der Host nur noch den Root-Ressourcenpool bei, selbst wenn Sie einen DRS-Cluster verwendet haben und beim Hinzufügen des Hosts zum Cluster die Option gewählt haben, den Ressourcenpool des Hosts zu übertragen. In diesem Fall bleibt die Hierarchie im Cluster erhalten. Sie können eine hostspezifische Ressourcenpoolhierarchie erstellen.

HINWEIS Stellen Sie sicher, dass Sie den Host aus dem Cluster entfernen, indem Sie ihn zuerst in den Wartungsmodus versetzen. Wenn Sie stattdessen die Verbindung des Hosts trennen, bevor Sie ihn aus dem Cluster entfernen, behält der Host den Ressourcenpool bei, der die Clusterhierarchie wiedergibt.

- Virtuelle Maschinen – Ein Host muss sich im Wartungsmodus befinden, damit Sie ihn aus dem Cluster entfernen können, und alle eingeschalteten virtuellen Maschinen müssen von dem Host migriert werden, damit der Host in den Wartungsmodus versetzt werden kann. Wenn Sie angeben, dass ein Host in den Wartungsmodus versetzt wird, werden Sie gefragt, ob alle ausgeschalteten virtuellen Maschinen auf dem Host auf andere Hosts im Cluster migriert werden sollen.
- Ungültige Cluster – Wird ein Host aus einem Cluster entfernt, nimmt auch die Zahl der für den Cluster verfügbaren Ressourcen ab. Falls der Cluster über ausreichende Ressourcen verfügt, um den Reservierungsanforderungen aller virtuellen Maschinen und Ressourcenpools des Clusters gerecht zu werden, passt der Cluster die Ressourcenzuteilung an, um den verringerten Umfang an Ressourcen anzuzeigen. Falls der Cluster nicht über ausreichende Ressourcen verfügt, um den Reservierungsanforderungen aller Ressourcenpools, jedoch denen der virtuellen Maschinen des Clusters gerecht zu werden, wird eine Alarmmeldung ausgegeben und der Cluster gelb gekennzeichnet. DRS wird weiterhin ausgeführt.

Versetzen eines Hosts in den Wartungsmodus

Sie sollten einen Host in den Wartungsmodus versetzen, wenn Sie Wartungstätigkeiten ausführen müssen, beispielsweise das Installieren von zusätzlichem Arbeitsspeicher. Ein Host wird in den Wartungsmodus nur auf Benutzeranforderung versetzt bzw. verlässt diesen nur dann.

Virtuelle Maschinen, die auf einem Host ausgeführt werden, der in den Wartungsmodus wechselt, müssen auf einen anderen Host migriert (manuell oder automatisch durch DRS) oder heruntergefahren werden. Der Host befindet sich so lange im Status **Wechsel in den Wartungsmodus**, bis alle ausgeführten virtuellen Maschinen ausgeschaltet oder auf andere Hosts migriert wurden. Sie können auf einem Host, der gerade in den Wartungsmodus wechselt, keine virtuellen Maschinen einschalten oder eine Migration virtueller Maschinen auf diesen Host durchführen.

Wenn sich auf dem Host keine ausgeführten virtuellen Maschinen mehr befinden, ändert sich das Hostsymbol in Wartungsphase und der neue Betriebszustand wird im Fenster **Übersicht (Summary)** des Hosts angezeigt. Während sich der Host im Wartungsmodus befindet, können virtuelle Maschinen weder bereitgestellt noch eingeschaltet werden.

HINWEIS Die Migration virtueller Maschinen von einem Host, der in den Wartungs- oder Standby-Modus versetzt wird, wird von DRS nicht empfohlen (und im Fall des vollautomatisierten Modus nicht durchgeführt), wenn nach dem Übergang in den angeforderten Modus gegen die vSphere HA-Failover-Ebene verstoßen würde.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie in der vSphere-Client-Bestandsliste mit der rechten Maustaste auf einen Host und wählen Sie **In den Wartungsmodus wechseln**.
 - Wenn der Host Teil eines automatisierten oder manuellen DRS-Clusters ist, wird eine Liste der Migrationsempfehlungen für virtuelle Maschinen angezeigt, die auf dem Host ausgeführt werden.
 - Wenn der Host Teil eines automatisierten DRS-Clusters ist, werden virtuelle Maschinen auf unterschiedliche Hosts migriert, wenn der Host in den Wartungsmodus wechselt.
- 2 Klicken Sie, sofern zutreffend, auf **Empfehlungen übernehmen**.

Der Host befindet sich im Wartungsmodus, bis Sie **Wartungsmodus beenden** auswählen.

Entfernen eines Hosts aus einem Cluster

Sie können Hosts aus einem Cluster entfernen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf den Host in der Bestandsliste und wählen Sie **In den Wartungsmodus wechseln**.
- 2 Im Wartungsmodus kann der Host an einen anderen Bestandslistenspeicherort verschoben werden – entweder in das Datacenter der obersten Ebene oder in einen anderen Cluster.

Nachdem Sie einen Host aus einem Cluster entfernt haben, können Sie die folgenden Aufgaben ausführen.

- Entfernen des Hosts aus vCenter Server: Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Entfernen**.
- Führen Sie den Host unter vCenter Server als eigenständigen Host aus: Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus beenden**.
- Ziehen Sie den Host in einen anderen Cluster.

Beim Verschieben des Hosts werden seine Ressourcen aus dem Cluster entfernt. Wenn Sie die Ressourcenpoolhierarchie des Hosts in den Cluster übertragen haben, bleibt diese Hierarchie im Cluster erhalten.

Verwendung des Standby-Modus

Beim Versetzen eines Hosts in den Standby-Modus wird dieser ausgeschaltet.

Normalerweise werden Hosts durch die vSphere DPM-Funktion in den Standby-Modus versetzt, um die Betriebszeiten zu optimieren. Sie können einen Host auch manuell in den Standby-Modus versetzen. Allerdings macht DRS beim nächsten Start möglicherweise Ihre Änderung rückgängig (oder empfiehlt das Rückgängigmachen). Damit ein Host ausgeschaltet bleibt, versetzen Sie diesen in den Wartungsmodus und schalten Sie ihn aus.

Verwalten von Energieressourcen

Die vSphere Distributed Power Management-Funktion (DPM) ermöglicht die Senkung des Energieverbrauchs eines DRS-Clusters, indem Hosts auf Basis der Clusterressourcennutzung ein- und ausgeschaltet werden.

vSphere DPM überwacht den kumulativen Bedarf aller virtuellen Maschinen im Cluster nach Arbeitsspeicher- und CPU-Ressourcen und vergleicht ihn mit der Gesamtkapazität der verfügbaren Ressourcen aller Hosts im Cluster. Wenn eine ausreichende Überkapazität ermittelt wird, versetzt vSphere DPM einen oder mehrere Hosts in den Standby-Modus und migriert dabei alle virtuellen Maschinen, die auf diesen Hosts ausgeführt werden, auf andere Hosts und schaltet sie anschließend aus. Wenn umgekehrt die Kapazität als nicht ausreichend angesehen wird, holt DRS Hosts aus dem Standby-Modus (schaltet sie ein) und migriert mithilfe von vMotion virtuelle Maschinen auf diese Hosts. Beim Durchführen dieser Berechnungen berücksichtigt vSphere DPM nicht nur den aktuellen Bedarf, sondern auch alle vom Benutzer angegebenen VM-Ressourcenreservierungen.

HINWEIS ESXi-Hosts können nur dann automatisch aus dem Standby-Modus geholt werden, wenn sie in einem von vCenter Server verwalteten Cluster ausgeführt werden.

vSphere DPM kann eines von drei Energieverwaltungsprotokollen verwenden, um einen Host aus dem Standby-Modus zu versetzen: Intelligent Platform Management Interface (IPMI), Hewlett-Packard Integrated Lights-Out (iLO) oder Wake-On-LAN (WOL). Jedes Protokoll benötigt eine eigene Hardwareunterstützung und -konfiguration. Sofern ein Host keines dieser Protokolle unterstützt, kann er nicht von vSphere DPM in den Standby-Modus versetzt werden. Falls ein Host mehrere Protokolle unterstützt, werden sie in der folgenden Reihenfolge verwendet: IPMI, iLO, WOL.

HINWEIS Ein Host im Standby-Modus darf weder getrennt noch aus dem DRS-Cluster verschoben werden, ohne ihn erst einzuschalten. Anderenfalls kann vCenter Server den Host nicht mehr einschalten.

Konfigurieren von IPMI- oder iLO-Einstellungen für vSphere DPM

IPMI ist eine Hardwarespezifikation und Hewlett-Packard iLO ist eine eingebettete Servermanagementtechnologie. Beide definieren eine Schnittstelle für die Remoteüberwachung und -steuerung von Computern und stellen diese zur Verfügung.

Sie müssen den folgenden Vorgang auf jedem Host durchführen.

Voraussetzungen

Sowohl IPMI als auch iLO benötigen einen Baseboard Management Controller (BMC), um ein Gateway zum Zugriff auf Hardwaresteuerungsfunktionen bereitzustellen und zu ermöglichen, dass von einem Remotesystem mit einer seriellen oder LAN-Verbindung auf die Schnittstelle zugegriffen werden kann. Der BMC wird auch dann eingeschaltet, selbst wenn der Host ausgeschaltet wird. Sofern ordnungsgemäß aktiviert, reagiert der BMC auf Befehle zum Einschalten.

Wenn Sie IPMI oder iLO als Wake-Protokoll verwenden möchten, müssen Sie den BMC konfigurieren. Die BMC-Konfiguration variiert je nach Modell. Weitere Informationen finden Sie in der Dokumentation Ihres Anbieters. Mit IPMI müssen Sie zudem sicherstellen, dass der BMC LAN-Kanal so konfiguriert ist, dass er immer verfügbar ist und Operatorbefehle zulässig sind. Wenn Sie auf einigen IPMI-Systemen "IPMI über LAN" aktivieren, müssen Sie dies im BIOS konfigurieren und ein bestimmtes IPMI-Konto angeben.

vSphere DPM nur mit IPMI unterstützt die MD5- und textbasierte Authentifizierung, die MD2-basierte Authentifizierung wird dagegen nicht unterstützt. vCenter Server verwendet MD5, wenn der BMC eines Hosts meldet, dass er unterstützt wird und für die Operatorrolle aktiviert ist. Anderenfalls wird die textbasierte Authentifizierung verwendet, wenn BMC meldet, dass sie unterstützt wird und aktiviert ist. Falls weder die MD5- noch die textbasierte Authentifizierung aktiviert ist, kann IPMI nicht mit dem Host verwendet werden. In diesem Fall versucht vCenter Server, Wake-on-LAN zu verwenden.

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Host aus der Bestandsliste des vSphere Clients aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie auf **Energieverwaltung**.
- 4 Klicken Sie auf **Eigenschaften**.
- 5 Geben Sie die folgenden Informationen ein.
 - Benutzername und Kennwort für ein BMC-Konto. (Der Benutzername muss die Berechtigung haben, den Host remote einzuschalten.)
 - IP-Adresse der dem BMC zugewiesenen Netzwerkkarte im Unterschied zur IP-Adresse des Hosts. Die IP-Adresse sollte statisch oder eine DHCP-Adresse mit unbegrenzter Lease sein.
 - MAC-Adresse der dem BMC zugeordneten Netzwerkkarte.
- 6 Klicken Sie auf **OK**.

Testen von Wake-on-LAN für vSphere DPM

Die Verwendung von Wake-on-LAN (WOL) für die vSphere DPM-Funktion wird vollständig unterstützt, sofern Sie sie konfigurieren und gemäß den VMware-Richtlinien erfolgreich testen. Sie müssen diese Schritte durchführen, bevor Sie vSphere DPM zum ersten Mal für ein Cluster aktivieren, bzw. diese auf jedem Host durchführen, der zu einem Cluster hinzugefügt wird, der vSphere DPM verwendet.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Stellen Sie sicher, dass der Cluster alle Voraussetzungen erfüllt, bevor Sie WOL testen.

- Der Cluster muss mindestens zwei ESX-Hosts der Version 3.5 (oder ESX 3i Version 3.5) oder höher enthalten.
- Der VMotion-Netzwerk-Link muss auf jeden Host ordnungsgemäß funktionieren. Das VMotion-Netzwerk sollte auch ein Einzel-IP-Subnetz sein, nicht mehrere, durch Router getrennte Subnetze.
- Die VMotion-Netzwerkkarte muss auf jedem Host WOL unterstützen. Ermitteln Sie zum Prüfen auf WOL-Unterstützung zunächst den Namen des physischen Netzwerkkadapters, der dem VMkernel-Port zugewiesen ist, indem Sie im Bestandslistenbereich des vSphere-Clients den Host auswählen, dann die Registerkarte **Konfiguration** auswählen und auf **Netzwerk** klicken. Nachdem Sie die Informationen gesammelt haben, klicken Sie auf **Netzwerkkadapter** und suchen Sie den für den Netzwerkkadapter entsprechenden Eintrag. In der Spalte **Wake-on-LAN unterstützt** des entsprechenden Adapters sollte „Ja“ stehen.
- Zur Anzeige des WOL-Kompatibilitätsstatus der einzelnen Netzwerkkarten auf dem Host wählen Sie im Bestandslistenbereich des vSphere-Clients den Host, klicken Sie auf die Registerkarte **Konfiguration** und klicken Sie anschließend auf **Netzwerkkadapter**. Für die Netzwerkkarte muss in der Spalte **Wake-on-LAN unterstützt** „Ja“ angezeigt werden.

- Der Switch-Port, in dem jede WOL-unterstützende VMotion-Netzwerkkarte eingesteckt ist, sollte so eingestellt sein, dass die Linkgeschwindigkeit automatisch ausgehandelt wird. Legen Sie keine feste Geschwindigkeit fest (z. B. 1000 Mb/s). Viele Netzwerkkarten unterstützen WOL nur dann, wenn sie auf eine Geschwindigkeit von 100 Mb/s oder weniger umschalten können, wenn der Host ausgeschaltet wird.

Nachdem Sie diese Voraussetzungen verifiziert haben, testen Sie jeden ESXi-Host, der WOL zum Unterstützen von vSphere DPM verwenden wird. Wenn Sie diese Hosts testen, stellen Sie sicher, dass für den Cluster die vSphere DPM-Funktion von VMware deaktiviert ist.



VORSICHT Vergewissern Sie sich, dass jeder zu einem vSphere-DPM-Cluster hinzugefügte Host, der WOL als Wake-Protokoll verwendet, getestet und von der Verwendung der Energieverwaltung deaktiviert wird, wenn er den Test nicht besteht. Wird dies nicht durchgeführt, schaltet vSphere DPM möglicherweise Hosts aus, die es anschließend nicht mehr einschalten kann.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client auf den Befehl **In den Standby-Modus wechseln** auf der Registerkarte **Übersicht** des Hosts.
Diese Aktion fährt den Host herunter.
- 2 Versuchen Sie, den Host aus dem Standby-Modus zu holen, indem Sie auf den Befehl **Einschalten** auf der Registerkarte **Übersicht** des Hosts klicken.
- 3 Achten Sie darauf, dass der Host wieder erfolgreich eingeschaltet wird.
- 4 Wählen Sie jeden Host, der den Standby-Modus nicht erfolgreich verlässt, auf der Seite Hostoptionen des Dialogfelds „Clustereinstellungen“ aus und ändern Sie dessen Einstellung für **Energieverwaltung** in „Deaktiviert“.

Nach Durchführung dieser Schritte hält vSphere DPM den Host nicht für einen Kandidaten, der ausgeschaltet werden soll.

Verwenden von DRS-Affinitätsregeln

Durch die Verwendung von Affinitätsregeln können Sie die Platzierung von virtuellen Maschinen auf Hosts innerhalb eines Clusters steuern.

Sie können zwei Typen von Regeln erstellen.

- Werden verwendet, um die Affinität oder Anti-Affinität zwischen einer Gruppe virtueller Maschinen und einer Gruppe von Hosts anzugeben. Eine Affinitätsregel legt fest, dass die Mitglieder einer ausgewählten VM-DRS-Gruppe auf den Mitgliedern einer bestimmten Host-DRS-Gruppe ausgeführt werden können bzw. müssen. Eine Anti-Affinitätsregel legt fest, dass die Mitglieder einer ausgewählten VM-DRS-Gruppe nicht auf den Mitgliedern einer bestimmten Host-DRS-Gruppe ausgeführt werden können.

Weitere Informationen über das Erstellen und Verwenden dieses Regeltyps finden Sie unter „[VM-Host-Affinitätsregeln](#)“, auf Seite 414.

- Werden verwendet, um die Affinität bzw. die Anti-Affinität zwischen individuellen virtuellen Maschinen anzugeben. Eine Regel, die die Affinität angibt, führt dazu, dass DRS versucht, die angegebenen virtuellen Maschinen auf demselben Host zusammenzuhalten, z. B. aus Leistungsgründen. Mit einer Anti-Affinitätsregel versucht DRS, die angegebenen virtuellen Maschinen voneinander zu trennen, damit beispielsweise beim Auftreten eines Problems auf einem Host nicht beide virtuellen Maschinen verloren gehen.

Weitere Informationen über das Erstellen und Verwenden dieses Regeltyps finden Sie unter „[VM-VM-Affinitätsregeln](#)“, auf Seite 413.

Wird eine Affinitätsregel hinzugefügt oder bearbeitet und der aktuelle Status des Clusters steht in Widerspruch zur Regel, wird das System weiterhin ausgeführt und versuchen, die Regelverletzung zu korrigieren. Bei manuellen und teilautomatisierten DRS-Clustern werden die Migrationsempfehlungen, die sowohl auf die Erfüllung der Regel als auch auf dem Lastausgleich basieren, zur Genehmigung präsentiert. Sie müssen die Regeln zwar nicht erfüllen, jedoch bleiben die zugehörigen Empfehlungen solange bestehen, bis die Regeln erfüllt sind.

Um zu prüfen, ob gegen aktivierte Affinitätsregeln verstoßen wird und dies nicht von DRS korrigiert werden kann, wählen Sie die Registerkarte **DRS** des Clusters aus und klicken Sie auf **Fehler**. Alle Regeln, die verletzt werden, weisen einen entsprechenden Fehler auf dieser Seite auf. Der Fehler gibt an, warum DRS die jeweilige Regel nicht einhalten kann. Regelverletzungen generieren auch Protokollierungsereignisse.

HINWEIS VM-VM- und VM-Host-Affinitätsregeln unterscheiden sich von den CPU-Affinitätsregeln eines einzelnen Hosts.

Erstellen einer Host-DRS-Gruppe

Eine VM-Host-Affinitätsregel stellt eine Affinitäts- bzw. eine Anti-Affinitätsbeziehung zwischen einer VM-DRS-Gruppe und einer Host-DRS-Gruppe her. Sie müssen zunächst beide Gruppen erstellen, bevor Sie eine Regel erstellen können, die auf diese Gruppen verweist.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Fenster des Dialogfelds „Clustereinstellungen“ unter **vSphere DRS** die Option **DRS-Gruppenmanager** aus.
- 3 Klicken Sie im Abschnitt „Host-DRS-Gruppen“ auf **Hinzufügen**.
- 4 Geben Sie in das Dialogfeld „DRS-Gruppe“ einen Namen für die Gruppe ein.
- 5 Wählen Sie im linken Fenster einen Host aus und klicken Sie auf >>, um ihn der Gruppe hinzuzufügen. Wiederholen Sie diesen Vorgang, bis alle gewünschten Hosts hinzugefügt wurden.

Sie können Hosts aus der Gruppe entfernen, indem Sie sie im rechten Fenster auswählen und auf << klicken.

- 6 Klicken Sie auf **OK**.

Weiter

Mithilfe dieser Host-DRS-Gruppe können Sie eine VM-Host-Affinitätsregel erstellen, die eine Affinitäts- oder eine Anti-Affinitätsbeziehung zwischen dieser Gruppe und einer geeigneten VM-DRS-Gruppe herstellt.

[„Erstellen einer VM-DRS-Gruppe“](#), auf Seite 413

[„Erstellen einer VM-Host-Affinitätsregel“](#), auf Seite 414

Erstellen einer VM-DRS-Gruppe

Affinitätsregeln stellen eine Affinitätsbeziehung (oder eine Anti-Affinitätsbeziehung) zwischen DRS-Gruppen her. Sie müssen zunächst DRS-Gruppen erstellen, bevor Sie eine Regel erstellen können, die auf diese Gruppen verweist.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Fenster des Dialogfelds „Clustereinstellungen“ unter **vSphere DRS** die Option **DRS-Gruppenmanager** aus.
- 3 Klicken Sie im Abschnitt zu „VM-DRS-Gruppen“ auf **Hinzufügen**.
- 4 Geben Sie in das Dialogfeld „DRS-Gruppe“ einen Namen für die Gruppe ein.
- 5 Wählen Sie im linken Fenster einen Host aus und klicken Sie auf >>, um ihn der Gruppe hinzuzufügen. Wiederholen Sie diesen Vorgang, bis alle gewünschten Hosts hinzugefügt wurden.
Sie können Hosts aus der Gruppe entfernen, indem Sie sie im rechten Fenster auswählen und auf << klicken.
- 6 Klicken Sie auf **OK**.

Weiter

[„Erstellen einer Host-DRS-Gruppe“](#), auf Seite 412

[„Erstellen einer VM-Host-Affinitätsregel“](#), auf Seite 414

[„Erstellen einer VM-VM-Affinitätsregel“](#), auf Seite 413

VM-VM-Affinitätsregeln

Eine VM-VM-Affinitätsregel gibt an, ob ausgewählte virtuelle Maschinen auf demselben oder verschiedenen Hosts ausgeführt werden sollen. Dieser Regeltyp wird zum Erstellen der Affinität oder Anti-Affinität zwischen einzelnen, von Ihnen ausgewählten virtuellen Maschinen verwendet.

Wenn eine Affinitätsregel erstellt wird, versucht DRS, die angegebenen virtuellen Maschinen auf einem Host zusammenzuhalten. Dies ist z. B. sinnvoll, um die Leistung zu verbessern.

Bei einer Anti-Affinitätsregel versucht DRS, die angegebenen virtuellen Maschinen auseinanderzuhalten. Sie könnten eine solche Regel verwenden, wenn Sie sichergehen möchten, dass sich bestimmte virtuelle Maschinen immer auf unterschiedlichen physischen Hosts befinden. In diesem Fall riskieren Sie nicht den Ausfall aller virtuellen Maschinen, falls es Probleme mit dem Host gibt.

Erstellen einer VM-VM-Affinitätsregel

Sie können im Dialogfeld „Clustereinstellungen“ VM-VM-Affinitätsregeln erstellen, um anzugeben, ob einzelne ausgewählte virtuelle Maschinen auf demselben Host ausgeführt werden oder auf separaten Hosts verbleiben sollen.

HINWEIS Wenn Sie in vSphere HA die Zugangssteuerungsrichtlinie „Failover-Hosts angeben“ verwenden und dabei mehrere Failover-Hosts auswählen, werden VM-VM-Affinitätsregeln nicht unterstützt.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Fenster des Dialogfelds Clustereinstellungen unter **vSphere DRS** die Option **Regeln** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie in das Dialogfeld „Regeln“ einen Namen für die Regel ein.
- 5 Wählen Sie im Menü **Typ** entweder **Virtuelle Maschinen zusammenhalten** oder **Separate virtuelle Maschinen** aus.
- 6 Klicken Sie auf **Hinzufügen**.
- 7 Wählen Sie mindestens zwei virtuelle Maschinen aus, auf die die Regel angewendet werden soll, und klicken Sie auf **OK**.
- 8 Klicken Sie auf **OK**.

VM-Host-Affinitätsregeln

Eine VM-Host-Affinitätsregel legt fest, ob die Mitglieder einer ausgewählten VM-DRS-Gruppe auf den Mitgliedern einer bestimmten Host-DRS-Gruppe ausgeführt werden können.

Im Unterschied zu einer VM/VM-Affinitätsregel, die die Affinität (oder Anti-Affinität) zwischen einzelnen virtuellen Maschinen angibt, gibt eine VM/Host-Affinitätsregel die Affinität zwischen einer Gruppe virtueller Maschinen und einer Gruppe von Hosts an. Es gibt „erforderliche“ Regeln („muss“) und „bevorzugte“ Regeln („sollte“).

Eine VM-Host-Affinitätsregel umfasst die folgenden Komponenten.

- Eine VM-DRS-Gruppe.
- Eine Host-DRS-Gruppe.
- Eine Festlegung, ob es sich bei der Regel um eine Voraussetzung („muss“) oder eine Präferenz („sollte“) sowie um eine Affinität („wird ausgeführt auf“) oder eine Anti-Affinität („wird nicht ausgeführt auf“) handelt.

Weil VM-Host-Affinitätsregeln clusterbasiert sind, müssen sich alle in die Regel aufgenommenen virtuellen Maschinen und Hosts in demselben Cluster befinden. Wenn eine virtuelle Maschine aus dem Cluster entfernt wird, verliert sie auch dann ihre DRS-Gruppenzugehörigkeit, wenn sie später erneut in den Cluster aufgenommen wird.

Erstellen einer VM-Host-Affinitätsregel

Sie können im Dialogfeld „Clustereinstellungen“ Host-VM-Affinitätsregeln erstellen, um anzugeben, ob die Mitglieder einer ausgewählten VM-DRS-Gruppe auf den Mitgliedern einer bestimmten Host-DRS-Gruppe ausgeführt werden können.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erstellen Sie für die virtuelle Maschine und den Host die DRS-Gruppen, für die die VM-Host-Affinitätsregel gilt.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste im Bestandslistenbereich des vSphere-Clients auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Fenster des Dialogfelds „Clustereinstellungen“ unter vSphere DRS die Option **Regeln** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie in das Dialogfeld „Regeln“ einen Namen für die Regel ein.
- 5 Wählen Sie im Menü **Typ** die Option **Virtuelle Maschinen zu Hosts** aus.
- 6 Wählen Sie die VM-DRS-Gruppe und die Host-DRS-Gruppe aus, auf die die Regel angewendet werden soll.
- 7 Wählen Sie eine Spezifikation für die Regel aus.
 - **Muss auf Hosts in der Gruppe ausgeführt werden** Virtuelle Maschinen in VM-Gruppe 1 müssen auf Hosts in Hostgruppe A ausgeführt werden.
 - **Sollte auf Hosts in der Gruppe ausgeführt werden.** Virtuelle Maschinen in VM-Gruppe 1 sollten, müssen aber nicht auf Hosts in Hostgruppe A ausgeführt werden.
 - **Darf nicht auf Hosts in der Gruppe ausgeführt werden.** Virtuelle Maschinen in VM-Gruppe 1 dürfen niemals auf Hosts in Hostgruppe A ausgeführt werden.
 - **Sollte nicht auf Hosts in der Gruppe ausgeführt werden.** Virtuelle Maschinen in VM-Gruppe 1 sollten nicht, können aber auf Hosts in Hostgruppe A ausgeführt werden.
- 8 Klicken Sie auf **OK**.

Erstellen eines Datenspeicher-Clusters

Ein Datenspeicher-Cluster ist eine Sammlung von Datenspeichern mit gemeinsam genutzten Ressourcen und einer gemeinsamen Verwaltungsoberfläche. Datenspeicher-Cluster sind für Datenspeicher dasselbe wie Cluster für Hosts. Wenn Sie einen Datenspeicher-Cluster erstellen, können Sie vSphere Storage DRS zum Verwalten von Speicherressourcen verwenden.

HINWEIS Datenspeicher-Cluster werden in der vSphere-API als Speicher-Pods bezeichnet.

Wenn Sie einen Datenspeicher zu einem Datenspeicher-Cluster hinzufügen, werden die Ressourcen des Datenspeichers Teil der Ressourcen des Datenspeicher-Clusters. Ebenso wie bei Host-Clustern werden Datenspeicher-Cluster dazu verwendet, Speicherressourcen zu vereinen, was Ihnen ermöglicht, Ressourcenzuteilungsrichtlinien auf Datenspeicher-Cluster-Ebene zu unterstützen. Die folgenden Ressourcenverwaltungsfunktionen sind ebenfalls pro Datenspeicher-Cluster verfügbar.

Lastausgleich für die Speicherplatznutzung

Sie können einen Schwellenwert für die Speicherplatznutzung festlegen. Wenn die Speicherplatznutzung in einem Datenspeicher den Schwellenwert überschreitet, generiert Speicher-DRS Empfehlungen oder führt Storage vMotion-Migrationen durch, um die Speicherplatznutzung innerhalb des Datenspeicher-Clusters zu verteilen.

Lastausgleich für die E/A-Latenz

Sie können einen E/A-Latenz-Schwellenwert festlegen, um Engpässe zu vermeiden. Wenn die E/A-Latenz in einem Datenspeicher den Schwellenwert überschreitet, generiert Speicher-DRS Empfehlungen oder führt Storage vMotion-Migrationen durch, damit eine hohe E/A-Last vermieden wird.

Anti-Affinitätsregeln

Sie können Anti-Affinitätsregeln für Festplatten virtueller Maschinen erstellen. Beispielsweise müssen die virtuellen Festplatten einer bestimmten virtuellen Maschine auf unterschiedlichen Datenspeichern gehalten werden. Standardmäßig werden alle virtuellen Festplatten für eine virtuelle Maschine im selben Datenspeicher platziert.

Datenspeicher-Cluster erstellen

Sie können Datenspeicher-Cluster-Ressourcen mithilfe von Speicher-DRS verwalten.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie in der Ansicht „Datenspeicher und Datenspeicher-Cluster“ der vSphere-Client-Bestandsliste mit der rechten Maustaste auf das Datencenterobjekt und wählen Sie **Neuer Datenspeicher-Cluster**.
- 2 Befolgen Sie die Eingabeaufforderungen, um den Assistenten zum Erstellen eines Datenspeicher-Clusters abzuschließen.

Speicher-DRS aktivieren und deaktivieren

Sie können mithilfe von Speicher-DRS die aggregierten Ressourcen eines Datenspeicher-Clusters verwalten. Wenn Speicher-DRS aktiviert ist, werden Empfehlungen für die Platzierung von VM-Festplatten sowie zur Migration von virtuellen Maschinen ausgesprochen, damit Speicherplatz- und E/A-Ressourcen über alle Datenspeicher im Datenspeicher-Cluster hinweg ausgeglichen werden.

Wenn Sie Speicher-DRS aktivieren, aktivieren Sie die folgenden Funktionen.

- Speicherplatz-Lastausgleich zwischen Datenspeichern innerhalb eines Datenspeicher-Clusters.
- E/A-Lastausgleich zwischen Datenspeichern innerhalb eines Datenspeicher-Clusters.
- Anfängliche Platzierung für virtuelle Festplatten auf Basis von Speicherplatz und E/A-Arbeitslast.

Durch Aktivieren des Kontrollkästchens „Speicher-DRS aktivieren“ im Dialogfeld „Datenspeicher-Cluster-einstellungen“ werden alle diese Komponenten gleichzeitig aktiviert bzw. deaktiviert. Falls erforderlich, können Sie die E/A-bezogenen Funktionen von Speicher-DRS unabhängig von den Speicherplatzverteilungsfunktionen deaktivieren.

Wenn Sie Speicher-DRS auf einem Datenspeicher-Cluster deaktivieren, werden die Speicher-DRS-Einstellungen beibehalten. Wenn Sie Speicher-DRS aktivieren, werden die Einstellungen für den Datenspeicher-Cluster bis zu dem Zeitpunkt wiederhergestellt, zu dem Speicher-DRS deaktiviert wurde.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf **Allgemein**.
- 3 Wählen Sie **Speicher-DRS einschalten** und klicken Sie auf **OK**.
- 4 (Optional) Führen Sie die folgenden Schritte aus, um nur die E/A-bezogenen Funktionen von Speicher-DRS zu deaktivieren, ohne auch die Speicherplatzverteilungsfunktionen zu deaktivieren.
 - a Wählen Sie **SDRS-Laufzeitregeln**.
 - b Heben Sie die Aktivierung des Kontrollkästchens **E/A-Metrik für SDRS-Empfehlungen aktivieren** auf.
- 5 Klicken Sie auf **OK**.

Festlegen der Automatisierungsebene für Datenspeicher-Cluster

Die Automatisierungsebene für einen Datenspeicher-Cluster legt fest, ob Platzierungs- und Migrationsempfehlungen aus Speicher-DRS automatisch angewendet werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Option **SDRS-Automatisierung** aus.
- 3 Wählen Sie eine Automatisierungsebene.
„Manuell“ ist die Standardautomatisierungsebene.

Option	Beschreibung
Keine Automatisierung (Manueller Modus)	Die Empfehlungen zur Platzierung und zur Migration werden angezeigt, jedoch erst ausgeführt, wenn Sie die Empfehlungen manuell übernommen haben.
Vollautomatisiert	Die Empfehlungen zur Platzierung und zur Migration werden automatisch ausgeführt.

- 4 Klicken Sie auf **OK**.

Festlegen von Speicher-DRS-Laufzeitregeln

Mit der Option „Speicher-DRS festlegen“ werden erweiterte Optionen für den Datenspeicher-Cluster ausgelöst und konfiguriert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 (Optional) Aktivieren Sie das Kontrollkästchen **E/A-Metrik für SDRS-Empfehlungen aktivieren**, um die Berücksichtigung von E/A-Metriken zu aktivieren, bzw. heben Sie die Auswahl auf, um sie zu deaktivieren.

Wenn Sie diese Option deaktivieren, berücksichtigt vCenter Server keine E/A-Metriken beim Abgeben von Speicher-DRS-Empfehlungen. Wenn Sie daher diese Option deaktivieren, deaktivieren Sie auch die folgenden Speicher-DRS-Elemente:

- E/A-Lastausgleich zwischen Datenspeichern innerhalb eines Datenspeicher-Clusters.
- Anfängliche Platzierung für virtuelle Festplatten basierend auf der E/A-Arbeitslast. Die anfängliche Platzierung berücksichtigt lediglich den Speicherplatz.

- 2 (Optional) Legen Sie die Speicher-DRS-Schwellenwerte fest.

Sie legen die Aggressivität von Speicher-DRS fest, indem Sie Schwellenwerte für den genutzten Speicherplatz und die E/A-Latenz festlegen.

- Verwenden Sie den Schieberegler für den verwendeten Speicherplatz, um den maximal zulässigen Prozentsatz an belegtem Speicherplatz festzulegen, ab dem Speicher-DRS ausgelöst wird. Speicher-DRS gibt Empfehlungen und führt Migrationen durch, wenn die Speicherplatznutzung auf den Datenspeichern über dem Schwellenwert liegt.
- Verwenden Sie den Schieberegler für die E/A-Latenz, um die maximal zulässige E/A-Latenz festzulegen, ab der Speicher-DRS ausgelöst wird. Speicher-DRS gibt Empfehlungen und führt Migrationen durch, wenn die Latenz über dem Schwellenwert liegt.

HINWEIS Der E/A-Latenz-Schwellenwert für Speicher-DRS für den Datenspeicher-Cluster sollte niedriger oder gleich dem Überlastungsschwellenwert von Storage I/O Control sein.

- 3 (Optional) Konfigurieren Sie erweiterte Optionen.

- Keine Empfehlungen, bis der Nutzungsunterschied zwischen Quelle und Ziel folgenden Wert erreicht: Verwenden Sie den Schieberegler, um den Schwellenwert für den Unterschied im Speicherplatzauslastung festzulegen. Auslastung ist gleich Nutzung * 100/Kapazität.

Dieser Schwellenwert stellt sicher, dass es irgendeinen minimalen Unterschied zwischen dem Speicherplatzauslastung der Quelle und des Ziels gibt. Wenn beispielsweise auf Datenspeicher A 82 % des Speicherplatzes genutzt werden und auf Datenspeicher B 79 %, beträgt die Differenz 3. Wenn der Schwellenwert 5 ist, gibt Speicher-DRS keine Empfehlungen für die Migration von Datenspeicher A nach Datenspeicher B.

- E/A-Last auswerten alle: Geben Sie an, wie oft Speicher-DRS den Lastausgleich für die Speicherplatznutzung und den E/A-Lastausgleich prüfen soll.
- E/A-Ungleichgewichtsschwellenwert: Verwenden Sie den Schieberegler, um die Aggressivität des E/A-Lastausgleichs festzulegen. Das Herabsetzen dieses Werts sorgt für einen weniger aggressiven Lastausgleich. Speicher-DRS berechnet eine E/A-Fairness-Metrik zwischen 0 und 1, wobei 1 die gerechteste Verteilung darstellt. Die E/A-Lastverteilung läuft nur, wenn die berechnete Metrik kleiner als 1 ist - (E/A-Ungleichgewichtsschwellenwert/100).

- 4 Klicken Sie auf **Weiter**.

Hinzufügen und Entfernen von Datenspeichern aus einem Datenspeicher-Cluster

Sie können Datenspeicher zu einem vorhandenen Datenspeicher-Cluster hinzufügen bzw. sie daraus entfernen, indem Sie sie in der vSphere-Client-Bestandsliste ziehen.

Sie können zu einem Datenspeicher-Cluster jeden Datenspeicher hinzufügen, der auf einem Host in der vSphere-Client-Bestandsliste gemountet ist. Es gelten die folgenden Ausnahmen:

- Alle mit dem Datenspeicher verbundenen Hosts müssen ESXi 5.0 und höher sein.
- Der Datenspeicher kann sich nicht in mehr als einem Datencenter in derselben Instanz des vSphere-Client befinden.

Wenn Sie einen Datenspeicher aus einem Datenspeicher-Cluster entfernen, verbleibt der Datenspeicher in der vSphere-Client-Bestandsliste und es wird kein Unmount vom Host für ihn durchgeführt.

Verwenden des Datenspeicher-Clusters zur Verwaltung von Speicherressourcen

Nachdem Sie einen Datenspeicher-Cluster erstellt haben, können Sie ihn anpassen und zum Verwalten der Speicher-E/A und der Speichernutzungsressourcen verwenden.

Verwenden des Speicher-DRS-Wartungsmodus

Sie versetzen einen Datenspeicher in den Wartungsmodus, wenn er zwecks Wartung vorübergehend nicht benutzt werden soll. Ein Datenspeicher wird in den Wartungsmodus nur auf Benutzeranforderung versetzt bzw. verlässt diesen nur dann.

Der Wartungsmodus ist für Datenspeicher in einem Speicher-DRS-fähigen Datenspeicher-Cluster verfügbar. Eigenständige Datenspeicher können nicht in den Wartungsmodus versetzt werden.

Virtuelle Festplatten, die sich in einem Datenspeicher befinden, der in den Wartungsmodus versetzt wird, müssen in einen anderen Datenspeicher migriert werden. Dies kann manuell oder mithilfe von Speicher-DRS durchgeführt werden. Wenn Sie versuchen, einen Datenspeicher in den Wartungsmodus zu versetzen, wird auf der Registerkarte **Platzierungsempfehlungen** eine Liste mit Migrationsempfehlungen angezeigt. Dabei handelt es sich um Datenspeicher im selben Datenspeicher-Cluster, in die virtuelle Festplatten migriert werden können. Auf der Registerkarte **Fehler** zeigt vCenter Server eine Liste der Festplatten an, die nicht migriert werden können, sowie die Gründe dafür. Wenn durch Affinitäts- oder Anti-Affinitätsregeln von Speicher-DRS das Migrieren von Festplatten verhindert wird, können Sie die Option zum Ignorieren der Affinitätsregeln für die Wartung aktivieren.

Der Datenspeicher befindet sich so lange im Zustand „Wechsel in den Wartungsmodus“, bis alle virtuellen Festplatten migriert wurden.

Versetzen eines Datenspeichers in den Wartungsmodus

Wenn Sie einen Datenspeicher außer Betrieb stellen müssen, können Sie den Datenspeicher in den Speicher-DRS-Wartungsmodus versetzen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Speicher-DRS ist auf dem Datenspeicher-Cluster aktiviert, der den Datenspeicher enthält, der in den Wartungsmodus wechselt.

Es sind keine CD-ROM-Image-Dateien auf dem Datenspeicher gespeichert.

Es gibt mindestens zwei Datenspeicher im Datenspeicher-Cluster.

Vorgehensweise

- 1 Klicken Sie in der Bestandsliste des vSphere-Clients mit der rechten Maustaste auf einen Datenspeicher in einem Datenspeicher-Cluster und wählen Sie **In den SDRS-Wartungsmodus wechseln**.

Eine Liste von Datenspeicher-Wartungsmodus-Migrationsempfehlungen erscheint.

- 2 (Optional) Deaktivieren Sie auf der Registerkarte „Platzierungsempfehlungen“ alle Empfehlungen, die Sie nicht übernehmen möchten.

HINWEIS Der Datenspeicher kann erst in den Wartungsmodus versetzt werden, nachdem alle Festplatten entfernt wurden. Wenn Sie die Empfehlungen deaktivieren, müssen Sie die betroffenen virtuellen Maschinen manuell verschieben.

- 3 Klicken Sie, falls erforderlich, auf **Empfehlungen übernehmen**.

vCenter Server verwendet Storage vMotion, um die virtuellen Festplatten vom Quell- zum Zieldatenspeicher zu migrieren, und der Datenspeicher wechselt in den Wartungsmodus.

Möglicherweise wird das Datenspeichersymbol nicht sofort aktualisiert, um den aktuellen Status des Datenspeichers wiederzugeben. Wenn Sie das Symbol sofort aktualisieren möchten, klicken Sie auf **Aktualisieren**.

Ignorieren von Speicher-DRS-Affinitätsregeln für den Wartungsmodus

Affinitäts- oder Anti-Affinitätsregeln für Speicher-DRS verhindern möglicherweise den Wechsel eines Datenspeichers in den Wartungsmodus. Sie können diese Regeln ignorieren, wenn Sie einen Datenspeicher in den Wartungsmodus versetzen.

Wenn Sie für einen Datenspeicher-Cluster die Option zum Ignorieren der Affinitätsregeln für die Wartung aktivieren, ignoriert vCenter Server die Speicher-DRS-Affinitäts- und -Anti-Affinitätsregeln, die verhindern, dass ein Datenspeicher in den Wartungsmodus versetzt wird.

Speicher-DRS-Regeln werden nur im Falle von Entfernungsempfehlungen ignoriert. vCenter Server verstößt nicht gegen die Regeln beim Erteilen von Speicherplatz- und Lastausgleichsempfehlungen oder Empfehlungen für die anfängliche Platzierung.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im rechten Bereich des Dialogfelds „Datenspeicher-Cluster bearbeiten“ die Option **SDRS-Automatisierung** aus.
- 3 Klicken Sie auf **Erweiterte Optionen**.
- 4 Wählen Sie die Option **IgnoreAffinityRulesForMaintenance** aus.
- 5 Geben Sie in der Spalte „Wert“ **1** ein, um die Option zu aktivieren.
Geben Sie **0** ein, um die Option zu deaktivieren.
- 6 Klicken Sie auf **OK**.

Die Option zum Ignorieren der Affinitätsregeln für die Wartung wird auf den Datenspeicher-Cluster angewendet.

Übernehmen von Speicher-DRS-Empfehlungen

Speicher-DRS erfasst Ressourcenverwendungsinformationen für alle Datenspeicher in einem Datenspeicher-Cluster. Speicher-DRS generiert mit diesen Informationen Empfehlungen für die Platzierung virtueller Maschinen auf Datenspeicher in einem Datenspeicher-Cluster.

Speicher-DRS-Empfehlungen werden auf der Registerkarte **Speicher-DRS** in der Datenspeicheransicht des vSphere-Client angezeigt. Empfehlungen werden außerdem angezeigt, wenn Sie versuchen, einen Datenspeicher in den Speicher-DRS-Wartungsmodus zu versetzen. Wenn Sie Speicher-DRS-Empfehlungen übernehmen, verwendet vCenter Server Storage vMotion, um die Festplatten virtueller Maschinen in andere Datenspeicher im Datenspeicher-Cluster zu migrieren und somit einen Ressourcenausgleich zu schaffen.

Wenn Sie eine Untermenge an Empfehlungen übernehmen möchten, aktivieren Sie das Kontrollkästchen „Angewählte DRS-Empfehlungen außer Kraft setzen“ und wählen Sie die zu übernehmenden Empfehlungen aus.

Tabelle 25-2. Speicher-DRS-Empfehlungen

Bezeichnung	Beschreibung
Priorität	Prioritätsstufe (1-5) der Empfehlung. (Standardmäßig verborgen.)
Empfehlung	Von Speicher-DRS empfohlene Aktion.
Grund	Warum die Aktion erforderlich ist.
Speicherplatznutzung % vorher (Quelle) und (Ziel)	Prozentsatz des verwendeten Speicherplatzes im Quell- und Zieldatenspeicher vor der Migration.
Speicherplatznutzung % nachher (Quelle) und (Ziel)	Prozentsatz des verwendeten Speicherplatzes im Quell- und Zieldatenspeicher nach der Migration.
E/A-Latenz vorher (Quelle)	Wert der E/A-Latenz im Quelldatenspeicher vor der Migration.
E/A-Latenz vorher (Ziel)	Wert der E/A-Latenz im Zieldatenspeicher vor der Migration.

Speicher-DRS-Empfehlung aktualisieren

Migrationsempfehlungen für Speicher-DRS werden auf der Registerkarte **Speicher-DRS** im vSphere-Client angezeigt. Sie können diese Empfehlungen durch die Ausführung von Speicher-DRS aktualisieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Mindestens ein Datenspeicher-Cluster muss sich in der Bestandsliste des vSphere-Client befinden.

Aktivieren Sie Speicher-DRS für den Datenspeicher-Cluster. Die Registerkarte **Speicher-DRS** wird nur angezeigt, wenn Speicher-DRS aktiviert ist.

Vorgehensweise

- 1 Wählen Sie in der Datenspeicheransicht des vSphere-Client den Datenspeicher-Cluster aus und klicken Sie auf die Registerkarte **Speicher-DRS**.
- 2 Wählen Sie die Ansicht **Empfehlungen** aus und klicken Sie in der oberen rechten Ecke auf den Link **Speicher-DRS ausführen**.

Die Empfehlungen werden aktualisiert. Der Zeitstempel des letzten Updates zeigt das Datum und die Uhrzeit des letzten Updates der Speicher-DRS-Empfehlungen an.

Ändern der Speicher-DRS-Automatisierungsebene für eine virtuelle Maschine

Sie können für einzelne virtuelle Maschinen die für den Datenspeicher-Cluster geltende Automatisierungsebene außer Kraft setzen. Sie können zudem die Standard-Affinitätsregel für virtuelle Festplatten außer Kraft setzen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie **Einstellungen der VM**.
- 3 Wählen Sie eine virtuelle Maschine aus.
- 4 Wählen Sie in der Spalte „Automatisierungsebene“ eine Automatisierungsebene für die virtuelle Maschine aus.

Option	Beschreibung
Standard (Manuell)	Die Empfehlungen zur Platzierung und zur Migration werden angezeigt, jedoch erst ausgeführt, wenn Sie die Empfehlungen manuell übernommen haben.
Vollautomatisiert	Die Empfehlungen zur Platzierung und zur Migration werden automatisch ausgeführt.
Deaktiviert	vCenter Server migriert die virtuelle Maschine nicht und gibt auch keine Migrationsempfehlungen für sie.

- 5 Heben Sie in der Spalte **VMDKs zusammenhalten** die Aktivierung des Kontrollkästchens auf, um die Standard-VMDK-Affinität außer Kraft zu setzen.

Siehe „[Außerkräftsetzen der VMDK-Affinitätsregeln](#)“, auf Seite 426.

- 6 Klicken Sie auf **OK**.

Einrichten von Zeitplänen außerhalb der Geschäftszeiten für Speicher-DRS

Sie können eine geplante Aufgabe erstellen, um die Speicher-DRS-Einstellungen für einen Datenspeicher-Cluster zu ändern, damit Migrationen für vollautomatisierte Datenspeicher-Cluster vorwiegend außerhalb der Geschäftszeiten durchgeführt werden.

Sie können eine geplante Aufgabe erstellen, um die Automatisierungsebene und die Aggressivitätsebene für einen Datenspeicher-Cluster zu ändern. Beispielsweise können Sie Speicher-DRS so konfigurieren, dass er in Spitzenzeiten – wenn die Leistung oberste Priorität hat – weniger aggressiv ausgeführt wird, um die Anzahl an Speichermigrationen zu minimieren. Außerhalb der Spitzenzeiten kann Speicher-DRS in einem aggressiveren Modus ausgeführt und häufiger aufgerufen werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Aktivieren Sie Speicher-DRS.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.

- 2 Klicken Sie im Dialogfeld „Datenspeicher-Cluster bearbeiten“ auf **SDRS-Zeitplan**.
 - 3 Klicken Sie auf **Hinzufügen**.
 - 4 Geben Sie die Uhrzeit ein und wählen Sie die Tage aus, an denen die Aufgabe ausgeführt werden soll.
 - 5 Klicken Sie auf **Weiter**.
 - 6 Geben Sie die Starteinstellungen für die Aufgabe an.
 - a Geben Sie eine Beschreibung für die Starteinstellungen ein.
Beispiel: **SDRS-Konfiguration ändern**.
 - b Wählen Sie eine Automatisierungsebene.
 - c Markieren Sie zum Deaktivieren der E/A-Metriken für Speicher-DRS-Empfehlungen das Kontrollkästchen aus.

Wenn Sie E/A-Metriken für Speicher-DRS-Empfehlungen deaktivieren, werden E/A-Metriken nicht als Teil der Speicher-DRS-Empfehlungen oder automatisierten Migrationen für den Datenspeicher-Cluster angesehen.
 - d Legen Sie den Schwellenwert für genutzten Speicherplatz fest.

Verwenden Sie den Schieberegler für den verwendeten Speicherplatz, um den maximal zulässigen Prozentsatz an belegtem Speicherplatz festzulegen, ab dem Speicher-DRS ausgelöst wird. Speicher-DRS gibt Empfehlungen und führt Migrationen durch, wenn die Speicherplatznutzung auf den Datenspeichern über dem Schwellenwert liegt.
 - e Legen Sie den E/A-Latenz-Schwellenwert fest.

Verwenden Sie den Schieberegler für die E/A-Latenz, um die maximal zulässige E/A-Latenz festzulegen, ab der Speicher-DRS ausgelöst wird. Speicher-DRS gibt Empfehlungen und führt Migrationen durch, wenn die Latenz über dem Schwellenwert liegt.

HINWEIS Der E/A-Latenz-Schwellenwert für Speicher-DRS für den Datenspeicher-Cluster sollte niedriger oder gleich dem Überlastungsschwellenwert von Storage I/O Control sein.

 - f Legen Sie den E/A-Ungleichgewichts-Schwellenwert fest.

Verwenden Sie den Schieberegler für den Schwellenwert des E/A-Ungleichgewichts, um die Aggressivität des E/A-Lastausgleichs festzulegen. Speicher-DRS gibt Empfehlungen und führt Migrationen durch, wenn das E/A-Lasten-Ungleichgewicht über dem Schwellenwert liegt.
- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie die Ende-Einstellungen für die Aufgabe an.
 - Aktivieren Sie zum Wiederherstellen der Vor-Aufgaben-Konfiguration der Speicher-DRS-Einstellungen das Kontrollkästchen **Einstellungen wiederherstellen**.
 - Wenn Sie andere Einstellungen als die Vor-Aufgaben-Konfiguration angeben möchten, deaktivieren Sie das Kontrollkästchen **Einstellungen wiederherstellen**.
- 9 Überprüfen Sie Ihre Auswahl auf der Seite „Bereit zum Abschließen“, und klicken Sie auf **Beenden**.

Die geplante Aufgabe wird zum festgelegten Zeitpunkt ausgeführt.

Speicher-DRS-Anti-Affinitätsregeln

Sie können Speicher-DRS-Anti-Affinitätsregeln erstellen, um zu kontrollieren, welche virtuellen Festplatten nicht auf demselben Datenspeicher innerhalb eines Datenspeicher-Clusters platziert werden sollen. Standardmäßig werden die virtuellen Festplatten einer virtuellen Maschine auf demselben Datenspeicher zusammengehalten.

Wenn Sie eine Anti-Affinitätsregel erstellen, gilt sie für alle relevanten virtuellen Festplatten im Datenspeicher-Cluster. Anti-Affinitätsregeln werden während der anfänglichen Platzierung und während der von Speicher-DRS empfohlenen Migrationen durchgesetzt. Sie werden jedoch nicht durchgesetzt, wenn eine Migration von einem Benutzer initiiert wird.

HINWEIS Anti-Affinitätsregeln gelten nicht für CD-ROM-ISO-Imagedateien, die auf einem Datenspeicher in einem Datenspeicher-Cluster gespeichert sind. Sie gelten auch nicht für Auslagerungsdateien, die in benutzerdefinierten Speicherorten gespeichert sind.

Inter-VM-Anti-Affinitätsregeln	Geben Sie an, welche virtuellen Maschinen nie auf demselben Datenspeicher gespeichert werden sollen. Siehe „ Erstellen von Inter-VM-Anti-Affinitätsregeln “, auf Seite 425.
Intra-VM-Anti-Affinitätsregeln	Geben Sie mit einer bestimmten virtuellen Maschine verknüpfte virtuelle Festplatten an, die auf unterschiedlichen Datenspeichern gehalten werden müssen. Siehe „ Erstellen von Intra-VM-Anti-Affinitätsregeln “, auf Seite 425.

Wenn Sie eine virtuelle Festplatte aus einem Datenspeicher-Cluster verschieben, gilt die Affinitäts- bzw. Anti-Affinitätsregel nicht mehr für diese Festplatte.

Wenn Sie virtuelle Festplattendateien auf einen Datenspeicher-Cluster verschieben, der über Affinitäts- und Anti-Affinitätsregeln verfügt, gilt das folgende Verhalten:

- Datenspeicher-Cluster B verfügt über eine Intra-VM-Affinitätsregel. Wenn Sie eine virtuelle Festplatte von Datenspeicher-Cluster A auf Datenspeicher-Cluster B verschieben, gelten alle Regeln nicht mehr, die für die virtuelle Festplatte einer bestimmten virtuellen Maschine in Datenspeicher-Cluster A galten. Die virtuelle Festplatte unterliegt jetzt der Intra-VM-Affinitätsregel im Datenspeicher-Cluster B.
- Datenspeicher-Cluster B verfügt über eine Inter-VM-Anti-Affinitätsregel. Wenn Sie eine virtuelle Festplatte von Datenspeicher-Cluster A auf Datenspeicher-Cluster B verschieben, gelten alle Regeln nicht mehr, die für die virtuelle Festplatte einer bestimmten virtuellen Maschine in Datenspeicher-Cluster A galten. Die virtuelle Festplatte unterliegt jetzt der Inter-VM-Anti-Affinitätsregel im Datenspeicher-Cluster B.
- Datenspeicher-Cluster B verfügt über eine Intra-VM-Anti-Affinitätsregel. Wenn Sie eine virtuelle Festplatte von Datenspeicher-Cluster A auf Datenspeicher-Cluster B verschieben, gilt die Intra-VM-Anti-Affinitätsregel für die virtuelle Festplatte einer bestimmten Virtuellen Maschine nicht, da sich die Regel nur auf bestimmte virtuelle Festplatten im Datenspeicher-Cluster B beschränkt.

HINWEIS Speicher-DRS verhindert möglicherweise den Wechsel eines Datenspeichers in den Wartungsmodus. Sie können auswählen, die Speicher-DRS-Regeln für den Wartungsmodus zu ignorieren, indem Sie die Option zum Ignorieren der Affinitätsregeln für die Wartung aktivieren.

Erstellen von Inter-VM-Anti-Affinitätsregeln

Sie können eine Anti-Affinitätsregel erstellen, um anzugeben, dass sich alle virtuellen Festplatten bestimmter virtueller Maschinen auf unterschiedlichen Datenspeichern befinden müssen. Diese Regel gilt für einzelne Datenspeicher-Cluster.

Virtuelle Maschinen, für die eine Inter-VM-Anti-Affinitätsregel in einem Datenspeicher-Cluster gilt, müssen einer Intra-VM-Affinitätsregel im Datenspeicher-Cluster zugewiesen sein. Die virtuellen Maschinen müssen zudem der Intra-VM-Affinitätsregel entsprechen.

Wenn eine virtuelle Maschine einer Inter-VM-Anti-Affinitätsregel unterliegt, trifft folgendes Verhalten zu:

- Speicher-DRS platziert die virtuellen Festplatten der virtuellen Maschine entsprechend der festgelegten Regel.
- Speicher-DRS migriert die virtuellen Festplatten mit vMotion auch dann der Regel entsprechend, wenn die Migration aus einem obligatorischen Grund stattfindet, z. B. wenn der Datenspeicher in den Wartungsmodus versetzt wird.
- Wenn die virtuelle Festplatte der virtuellen Maschine gegen die Regel verstößt, gibt Speicher-DRS Migrationsempfehlungen, um den Fehler zu beheben, oder meldet den Verstoß als Fehler, falls keine Empfehlung gegeben werden kann, die den Fehler beheben würde.

Inter-VM-Anti-Affinitätsregeln sind standardmäßig nicht definiert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Bereich des Dialogfelds „Datenspeicher-Cluster bearbeiten“ die Option **Regeln** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen für die Regel ein.
- 5 Wählen Sie im Menü „Typ“ die Option **VM-Anti-Affinität**.
- 6 Klicken Sie auf **Hinzufügen**.
- 7 Klicken Sie auf **Virtuelle Maschine auswählen**.
- 8 Wählen Sie mindestens zwei virtuelle Maschinen aus und klicken Sie auf **OK**.
- 9 Klicken Sie auf **OK**, um die Regel zu speichern.

Erstellen von Intra-VM-Anti-Affinitätsregeln

Sie können eine VMDK-Anti-Affinitätsregel für eine virtuelle Maschine erstellen, die vorschreibt, welche ihrer virtuellen Festplatten sich auf unterschiedlichen Datenspeichern befinden müssen.

VMDK-Anti-Affinitätsregeln gelten für die virtuelle Maschine, für die die Regel definiert ist, und nicht für alle virtuellen Maschinen. Die Regel wird als eine Liste der virtuellen Festplatten angegeben, die voneinander getrennt werden müssen.

Wenn Sie versuchen, eine Intra-VM-Anti-Affinitätsregel und eine Intra-VM-Affinitätsregel für eine virtuelle Maschine zu definieren, lehnt vCenter Server die zuletzt definierte Regel ab.

Wenn eine virtuelle Maschine einer VMDK-Anti-Affinitätsregel unterliegt, trifft folgendes Verhalten zu:

- Speicher-DRS platziert die virtuellen Festplatten der virtuellen Maschine entsprechend der festgelegten Regel.
- Speicher-DRS migriert die virtuellen Festplatten mit vMotion auch dann der Regel entsprechend, wenn die Migration aus einem obligatorischen Grund stattfindet, z. B. wenn der Datenspeicher in den Wartungsmodus versetzt wird.
- Wenn die virtuelle Festplatte der virtuellen Maschine gegen die Regel verstößt, gibt Speicher-DRS Migrationsempfehlungen, um den Fehler zu beheben, oder meldet den Verstoß als Fehler, falls keine Empfehlung gegeben werden kann, die den Fehler beheben würde.

Intra-VM-Anti-Affinitätsregeln sind standardmäßig nicht definiert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie im linken Bereich des Dialogfelds „Datenspeicher-Cluster bearbeiten“ die Option **Regeln** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen für die Regel ein.
- 5 Wählen Sie im Menü „Typ“ die Option **VMDK-Anti-Affinität**.
- 6 Klicken Sie auf **Hinzufügen**.
- 7 Klicken Sie auf **Virtuelle Maschine auswählen**.
- 8 Wählen Sie eine virtuelle Maschine aus und klicken Sie auf **OK**.
- 9 Wählen Sie mindestens zwei virtuelle Festplatten aus, auf die die Regel angewendet werden soll, und klicken Sie auf **OK**.
- 10 Klicken Sie auf **OK**, um die Regel zu speichern.

Außerkraftsetzen der VMDK-Affinitätsregeln

VMDK-Affinitätsregeln geben an, dass sich alle virtuellen Festplatten in einem Datenspeicher-Cluster, die einer bestimmten virtuellen Maschine zugewiesen wurden, in demselben Datenspeicher im Datenspeicher-Cluster befinden. Diese Regeln gelten für einzelne Datenspeicher-Cluster.

VMDK-Affinitätsregeln sind standardmäßig für alle virtuellen Maschinen eines Datenspeicher-Clusters aktiviert. Sie können die Standardeinstellung für den Datenspeicher-Cluster oder für einzelne virtuelle Maschinen außer Kraft setzen.

Virtuelle Maschinen, die VMDK-Affinitätsregeln unterliegen, haben folgendes Verhalten:

- Speicher-DRS platziert die virtuellen Festplatten der virtuellen Maschine entsprechend der festgelegten Regel.
- Speicher-DRS migriert die virtuellen Festplatten mit vMotion auch dann der Regel entsprechend, wenn die Migration aus einem obligatorischen Grund stattfindet, z. B. wenn der Datenspeicher in den Wartungsmodus versetzt wird.
- Wenn die virtuelle Festplatte der virtuellen Maschine gegen die Regel verstößt, gibt Speicher-DRS Migrationsempfehlungen, um den Fehler zu beheben, oder meldet den Verstoß als Fehler, falls keine Empfehlung gegeben werden kann, die den Fehler beheben würde.

Wenn Sie einem Datenspeicher-Cluster, der für Speicher-DRS aktiviert ist, einen Datenspeicher hinzufügen, wird die VMDK-Affinitätsregel für diejenigen virtuellen Maschinen deaktiviert, die in diesem Datenspeicher über virtuelle Festplatten verfügen, wenn diese auch über virtuelle Festplatten auf anderen Datenspeichern verfügen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste in der Bestandsliste des vSphere-Clients auf einen Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf **Einstellungen der virtuellen Maschine**.
- 3 Deaktivieren Sie das Kontrollkästchen **VMDKs zusammenhalten** für die virtuelle Maschine.
- 4 Klicken Sie auf **OK**.

Bereinigen der Speicher-DRS-Statistiken

Zur Diagnose von Problemen mit Speicher-DRS können Sie die Speicher-DRS-Statistiken löschen, bevor Sie Speicher-DRS manuell ausführen.

WICHTIG Wenn Sie die Option zum Löschen der Speicher-DRS-Statistiken aktivieren, werden die Statistiken bei jeder Ausführung von Speicher-DRS so lange gelöscht, bis Sie die Option deaktivieren. Deaktivieren Sie die Option immer, nachdem Sie das Speicher-DRS-Problem diagnostiziert haben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Aktivieren Sie Speicher-DRS für den Datenspeicher-Cluster.

Vorgehensweise

- 1 Aktivieren Sie die Option **ClearIoStatsOnSdrsRun**.
 - a Klicken Sie im vSphere-Client mit der rechten Maustaste auf den Datenspeicher-Cluster und wählen Sie **Einstellungen bearbeiten**.
 - b Wählen Sie **SDRS-Automatisierungsebene** und klicken Sie auf **Erweiterte Optionen**.
 - c Geben Sie im Textfeld „Option“ **ClearIoStatsOnSdrsRun** ein.
 - d Geben Sie im entsprechenden Textfeld „Wert“ **1** ein.
 - e Klicken Sie auf **OK** und anschließend wieder auf **OK**, um das Einstellungsdialogfeld zu beenden.
- 2 Wählen Sie aus der vSphere-Client-Bestandsliste einen Datenspeichercluster aus.
- 3 Klicken Sie auf die Registerkarte **Speicher-DRS** und wählen Sie in der oberen rechten Ecke der Seite **DRS ausführen** aus.

Die aktuelle Speicher-DRS-Statistik für alle Datenspeicher und virtuellen Festplatten in allen Datenspeicher-Clustern in der vSphere-Client-Bestandsliste werden gelöscht; es werden jedoch keine neuen Statistiken erfasst.
- 4 Ändern Sie den Wert von **ClearIoStatsOnSdrsRun** in **0**, um es zu deaktivieren.
- 5 Führen Sie Speicher-DRS erneut aus.

Speicher-DRS wird normal ausgeführt. Die neue Einstellung wird erst nach einigen Stunden wirksam.

Verwenden von NUMA-Systemen mit ESXi

ESXi unterstützt die Optimierung des Arbeitsspeicherzugriffs für Intel- und AMD Opteron-Prozessoren in Serverarchitekturen mit NUMA-Unterstützung (Non Uniform Memory Access).

Wenn Sie verstanden haben, wie das Planen von ESXi-NUMA durchgeführt wird und wie VMware-NUMA-Algorithmen funktionieren, können Sie NUMA-Steuerungen festlegen, um die Leistung Ihrer virtuellen Maschinen zu optimieren.

Ändern der Anzahl virtueller CPUs

Sie können eine virtuelle Maschine, die auf einem ESXi-Host ausgeführt wird, mit bis zu 64 virtuellen CPUs konfigurieren.

WICHTIG Wenn Sie Ihre virtuelle Maschine für Einstellungen für virtuelle CPUs mit mehreren Kernen konfigurieren, müssen Sie sicherstellen, dass Ihre Konfiguration den Anforderungen der Endbenutzer-Lizenzvereinbarung des Gastbetriebssystems entspricht.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie **CPUs**.
- 3 Wählen Sie im Dropdown-Menü **Anzahl der virtuellen Sockets** einen Wert aus.
- 4 Wählen Sie im Dropdown-Menü **Anzahl der Kerne pro Socket** einen Wert aus.
Die sich daraus ergebende Gesamtzahl der Kerne ist gleich oder geringer der Anzahl der logischen CPUs auf dem Host.
- 5 Klicken Sie auf **OK**.

Verknüpfen von virtuelle Maschinen mit bestimmten Prozessoren

Möglicherweise können Sie die Leistung der Anwendungen auf einer virtuellen Maschine verbessern, indem sie ihre virtuellen CPUs an feste Prozessoren binden. Dies ermöglicht Ihnen, die Migration der virtuellen CPUs über NUMA-Knoten hinweg zu verhindern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Ressourcen** und anschließend **Erweiterte CPU**.
- 3 Setzen Sie im Bereich „Planen von Affinität“ die CPU-Affinität auf die bevorzugten Prozessoren.

HINWEIS Sie müssen die Kontrollkästchen aller Prozessoren im NUMA-Knoten manuell aktivieren. Die CPU-Affinität wird pro Prozessor und nicht pro Knoten festgelegt.

Verknüpfen von Arbeitsspeicherzuweisungen mit einem NUMA-Knoten unter Verwendung der Arbeitsspeicheraffinität

Sie können festlegen, dass bei künftigen Arbeitsspeicherzuteilungen auf einer virtuellen Maschine die mit einem einzigen NUMA-Knoten verknüpften Seiten genutzt werden (auch bekannt als manuelle Arbeitsspeicheraffinität).

HINWEIS Sie sollten die für künftige Arbeitsspeicherzuteilungen zu verwendenden Knoten nur dann festlegen, wenn Sie auch die CPU-Affinität festgelegt haben. Wenn Sie lediglich an den Arbeitsspeicheraffinitäts-einstellungen manuelle Änderungen vornehmen, wird der automatische NUMA-Ausgleich beeinträchtigt.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie die Registerkarte **Ressourcen** und anschließend **Arbeitsspeicher**.
- 3 Legen Sie im Fenster NUMA-Arbeitsspeicheraffinität (NUMA Memory Affinity) die gewünschte Arbeitsspeicheraffinität fest.

Beispiel: Verknüpfen einer virtuellen Maschine mit einem einzigen NUMA-Knoten

Das folgende Beispiel zeigt, wie Sie die letzten vier physischen CPUs mit einem einzigen NUMA-Knoten für eine virtuelle 2-Wege-Maschine manuell auf einem 8-Wege-Server verknüpfen.

Die CPUs, z. B. 4, 5, 6 und 7, stellen die physischen CPU-Nummern dar.

- 1 Wählen Sie im Bestandslistenbereich des vSphere-Clients die virtuelle Maschine aus und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie **Optionen** und klicken Sie auf **Erweitert**.
- 3 Klicken Sie auf die Schaltfläche **Konfigurationsparameter**.
- 4 Aktivieren Sie im vSphere-Client die CPU-Affinität für die Prozessoren 4, 5, 6 und 7.

Diese virtuelle Maschine soll nur auf Knoten 1 ausgeführt werden.

- 1 Wählen Sie im Bestandslistenbereich des vSphere-Clients die virtuelle Maschine aus und wählen Sie **Einstellungen bearbeiten**.
- 2 Wählen Sie **Optionen** und klicken Sie auf **Erweitert**.
- 3 Klicken Sie auf die Schaltfläche **Konfigurationsparameter**.
- 4 Setzen Sie im vSphere-Client die Arbeitsspeicheraffinität für den NUMA-Knoten auf 1.

Durch Ausführen dieser beiden Aufgaben wird sichergestellt, dass die virtuelle Maschine ausschließlich auf Knoten 1 ausgeführt wird und möglichst Arbeitsspeicher dieses Knotens zuteilt.

Verknüpfen von virtuellen Maschinen mit angegebenen NUMA-Knoten

Wenn Sie einen NUMA-Knoten mit einer virtuellen Maschine verknüpfen, um die NUMA-Knotenaffinität anzugeben, beschränken Sie den Satz von NUMA-Knoten, auf denen NUMA die virtuelle CPU und den virtuellen Arbeitsspeicher einer virtuellen Maschine planen kann.

HINWEIS Wenn Sie NUMA-Knotennaffinitäten beschränken, kann dies die Fähigkeit des ESXi-NUMA-Schedulers zur ausgleichenden Neuverteilung von virtuellen Maschinen über NUMA-Knoten hinweg beeinträchtigen. Geben Sie die NUMA-Knoten-Affinität nur an, wenn Sie die Knotenneuverteilung bedacht haben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf die Registerkarte **Optionen**.
- 3 Wählen Sie **Erweitert > Allgemein**.
- 4 Klicken Sie auf **Konfigurationsparameter**.
- 5 Klicken Sie auf **Zeile hinzufügen**, um eine neue Option hinzuzufügen.
- 6 Geben Sie in der Spalte „Name“ **numa.nodeAffinity** ein.
- 7 Geben Sie in der Spalte „Wert“ die NUMA-Knoten ein, auf denen die virtuelle Maschine geplant werden kann.

Verwenden Sie für die Eingabe mehrerer Knoten eine kommasetrennte Liste. Geben Sie beispielsweise **0,1** ein, um die VM-Ressourcenplanung auf die NUMA-Knoten 0 und 1 zu beschränken.
- 8 Klicken Sie auf **OK**.
- 9 Klicken Sie auf **OK**, um das Eigenschaftendialogfeld der virtuellen Maschine zu schließen.

Erweiterte Attribute

Sie können erweiterte Attribute für Hosts oder individuelle virtuelle Maschinen festlegen, um die Ressourcenverwaltung besser anpassen zu können.

In den meisten Fällen führt das Anpassen der Basiseinstellungen für die Ressourcenzuteilung (Reservierung, Grenzwert, Anteile) oder das Annehmen der Standardeinstellungen zu der entsprechenden Ressourcenzuteilung. Sie können jedoch erweiterte Attribute zum Anpassen der Ressourcenverwaltung für einen Host oder eine bestimmte virtuelle Maschine verwenden.

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.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere Client den gewünschten Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie unter **Software** auf **Erweiterte Einstellungen**.
- 4 Wählen Sie im Dialogfeld „Erweiterte Einstellungen“ das entsprechende Element aus (z. B. **CPU** oder **Arbeitsspeicher**).
- 5 Suchen Sie im rechten Bereich das Attribut und bearbeiten Sie den Wert.
- 6 Klicken Sie auf **OK**.

Festlegen von erweiterten Attributen von virtuellen Maschinen

Sie können erweiterte Attribute für virtuelle Maschinen festlegen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf die virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten**.
- 2 Klicken Sie auf **Optionen** und anschließend auf **Erweitert > Allgemein**.
- 3 Klicken Sie auf **Konfigurationsparameter**.
- 4 Klicken Sie im angezeigten Dialogfeld auf **Zeile hinzufügen (Add Row)**, um einen neuen Parameter und den zugehörigen Wert einzugeben.
- 5 Klicken Sie auf **OK**.

Erstellen und Verwenden von vSphere HA-Clustern

26

vSphere HA-Cluster ermöglichen einer Sammlung von ESXi-Hosts das Zusammenarbeiten in einer Gruppe und bieten virtuellen Maschinen dadurch eine höhere Verfügbarkeit, als es einzelne ESXi-Hosts können. Wenn Sie planen, einen neuen vSphere HA-Cluster zu erstellen und zu verwenden, beeinflussen die ausgewählten Optionen, wie der Cluster auf Ausfälle von Hosts oder virtuellen Maschinen reagieren wird.

Vor dem Erstellen eines vSphere HA-Clusters sollten Sie wissen, wie vSphere HA Hostausfälle und -isolierung identifiziert und auf solche Situationen reagiert. Darüber hinaus sollten Sie wissen, wie die Zugangssteuerung funktioniert, damit Sie die für Ihre Failover-Anforderungen geeignete Richtlinie wählen können. Nach der Einrichtung eines Clusters können Sie mit erweiterten Optionen dessen Verhalten beeinflussen und seine Leistung optimieren, wenn Sie sich an die folgenden Best Practices halten.

HINWEIS Möglicherweise erhalten Sie eine Fehlermeldung, wenn Sie versuchen, vSphere HA zu verwenden. Informationen zu Fehlermeldungen im Zusammenhang mit vSphere HA finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1033634>.

Dieses Kapitel behandelt die folgenden Themen:

- „vSphere HA-Checkliste“, auf Seite 433
- „Erstellen und Konfigurieren eines vSphere HA-Clusters“, auf Seite 434
- „Anpassen einer einzelnen virtuellen Maschine im vSphere Web Client“, auf Seite 439

vSphere HA-Checkliste

In der vSphere HA-Checkliste sind die Voraussetzungen aufgeführt, die Ihnen bekannt sein müssen, bevor Sie einen vSphere HA-Cluster erstellen und verwenden.

Überprüfen Sie diese Liste, bevor Sie einen vSphere HA-Cluster einrichten. Weitere Informationen erhalten Sie in den entsprechenden Querverweisen.

- Alle Hosts müssen für vSphere HA lizenziert sein.
- Ein Cluster muss mindestens zwei Hosts enthalten.
- Alle Hosts müssen mit statischen IP-Adressen konfiguriert werden. Wenn Sie DHCP verwenden, müssen Sie sichergehen, dass nach jedem Neustart die Adresse eines jeden Hosts beibehalten wird.
- Alle Hosts müssen mindestens ein gemeinsames Verwaltungsnetzwerk haben. Es werden mindestens zwei gemeinsame Verwaltungsnetzwerke empfohlen. Verwenden Sie das VMkernel-Netzwerk mit aktiviertem Kontrollkästchen **Verwaltungsdatenverkehr**. Die Netzwerke müssen füreinander zugänglich sein, und vCenter Server und die Hosts müssen in den Verwaltungsnetzwerken füreinander zugänglich sein. In der Dokumentation zur *vSphere-Verfügbarkeit* finden Sie empfohlene Vorgehensweisen.

- Alle Hosts müssen auf dieselben VM-Netzwerke und -Datenspeicher zugreifen können, um sicherzustellen, dass jede virtuelle Maschine auf jedem Host im Cluster ausgeführt werden kann. In gleicher Weise müssen sich virtuelle Maschinen auf gemeinsam genutztem, nicht lokalem Speicher befinden. Anderenfalls kann im Falle eines Hostsausfalls kein Failover erfolgen.

HINWEIS vSphere HA verwendet Datenspeicher-Taktsignale, um zwischen partitionierten, isolierten und ausgefallenen Hosts zu unterscheiden. Sind also einige Datenspeicher in Ihrer Umgebung zuverlässiger, konfigurieren Sie vSphere HA so, dass diese Priorität haben.

- VMware Tools muss installiert sein, damit die VM-Überwachung funktionieren kann. Nähere Informationen zur Überwachung von virtuellen Maschinen und Anwendungen finden Sie in der Dokumentation zur *vSphere-Verfügbarkeit*.
- vSphere HA unterstützt sowohl IPv4 als auch IPv6. Nähere Informationen zur vSphere HA-Interoperabilität finden Sie in der Dokumentation zur *vSphere-Verfügbarkeit*.
- Der VM-Komponentenschutz funktioniert nur, wenn für die Hosts die Zeitüberschreitungsfunktion „Keine Pfade verfügbar“ (All Paths Down, ADP) aktiviert ist.
- Damit der VM-Komponentenschutz verwendet werden kann, müssen die Cluster ESXi 6.0-Hosts oder höher enthalten.
- Nur vSphere HA-Cluster, die Hosts der Version ESXi 6.0 oder höher enthalten, können zum Aktivieren des VM-Komponentenschutzes verwendet werden. Cluster, die Hosts einer früheren Version enthalten, können den VM-Komponentenschutz nicht aktivieren, und diese Hosts können einem Cluster mit aktiviertem VM-Komponentenschutz nicht hinzugefügt werden.
- Wenn der Cluster Datenspeicher mit virtuellen Volumes (vVol) verwendet, wird beim Aktivieren von vSphere HA von vCenter Server ein Konfigurations-vVol auf jedem vVol-Datenspeicher erstellt. In diesen Containern speichert vSphere HA die Dateien, die zum Schutz von virtuellen Maschinen verwendet werden. vSphere HA funktioniert nicht richtig, wenn Sie diese Container löschen. Pro vVol-Datenspeicher wird nur ein Container erstellt.

Erstellen und Konfigurieren eines vSphere HA-Clusters

vSphere HA arbeitet im Kontext eines Clusters von ESXi-Hosts (oder Legacy ESX-Hosts). Sie müssen ein Cluster erstellen, Hosts hinzufügen und vSphere HA-Einstellungen konfigurieren, bevor der Failover-Schutz eingerichtet werden kann.

Wenn Sie einen vSphere HA-Cluster erstellen, müssen Sie mehrere Einstellungen konfigurieren, die festlegen, wie die Funktion funktioniert. Identifizieren Sie zuvor die Knoten Ihres Clusters. Diese Knoten sind die ESXi-Hosts, die die Ressourcen für virtuelle Maschinen bereitstellen und von vSphere HA verwendet werden, um Failover-Schutz zu bieten. Legen Sie daraufhin fest, wie diese Knoten miteinander und mit dem gemeinsam genutzten Speicher verbunden werden sollen, auf dem sich die Daten Ihrer virtuellen Maschine befinden. Wenn sich diese Netzwerkarchitektur an Ort und Stelle befindet, können Sie die Hosts zum Cluster hinzufügen und das Konfigurieren von vSphere HA abschließen.

Sie können vSphere HA aktivieren und konfigurieren, bevor Sie Hostknoten zum Cluster hinzufügen. Ihr Cluster ist jedoch vor dem Hinzufügen der Hosts nicht voll funktionsfähig und manche Clustereinstellungen sind nicht verfügbar. Beispielsweise ist die Richtlinie für die Zugangssteuerung „Failover-Host angeben“ nicht verfügbar, bis es einen Host gibt, der als Failover-Host ausgewählt werden kann.

HINWEIS Die Funktion „Starten und Herunterfahren von virtuellen Maschinen“ (automatischer Start) ist für alle virtuellen Maschinen deaktiviert, die sich auf den in einem vSphere HA-Cluster verfügbaren Hosts befinden (oder dorthin verschoben werden). Der automatische Start wird bei Verwendung mit vSphere HA nicht unterstützt.

Erstellen eines vSphere HA-Clusters im vSphere Client

Wenn Sie Ihren Cluster für vSphere HA aktivieren möchten, erstellen Sie zuerst einen leeren Cluster. Nachdem Sie die Planung der Ressourcen und der Netzwerkarchitektur für Ihren Cluster abgeschlossen haben, können Sie mithilfe des vSphere-Clients Hosts zum Cluster hinzufügen und die Einstellungen für vSphere HA festlegen.

Öffnen Sie mithilfe eines Kontos mit Cluster-Administratorberechtigungen eine vSphere Client-Verbindung mit vCenter Server.

Voraussetzungen

Stellen Sie sicher, dass sich alle virtuellen Maschinen und deren Konfigurationsdateien auf gemeinsam genutztem Speicher befinden. Stellen Sie sicher, dass die Hosts so konfiguriert sind, dass sie Zugriff auf diesen gemeinsam genutzten Speicher haben, damit Sie die virtuellen Maschinen mithilfe verschiedener Hosts im Cluster einschalten können.

Stellen Sie sicher, dass Hosts für den Zugriff auf das Netzwerk virtueller Maschinen konfiguriert sind.

HINWEIS Verwenden Sie redundante Management-Netzwerkverbindungen für vSphere HA. Informationen zu den empfohlenen Vorgehensweisen hinsichtlich der Netzwerkredundanz finden Sie in der Dokumentation zur *vSphere-Verfügbarkeit*. Sie sollten außerdem Hosts mit mindestens zwei Datenspeichern konfigurieren, um Redundanz für Datenspeicher-Taktsignale von vSphere HA bereitzustellen.

Vorgehensweise

- 1 Wählen Sie die Ansicht „Hosts & Cluster“ aus.
- 2 Klicken Sie mit der rechten Maustaste auf ein Datacenter in der Bestandslistenstruktur und klicken Sie auf **Neuer Cluster**.
- 3 Führen Sie den Assistenten für Neue Cluster aus.
Aktivieren Sie vSphere HA (oder DRS) zu diesem Zeitpunkt nicht.
- 4 Klicken Sie auf **Beenden**, um den Assistenten zu schließen und den Cluster zu erstellen.
Sie haben einen leeren Cluster erstellt.
- 5 Fügen Sie basierend auf Ihrer Ressourcen- und Netzwerkarchitekturplanung mithilfe des vSphere-Clients Hosts zum Cluster hinzu.
- 6 Klicken Sie mit der rechten Maustaste auf den Cluster, und wählen Sie **Einstellungen bearbeiten**.
Im Dialogfeld „Einstellungen“ des Clusters können Sie die Einstellungen für vSphere HA und andere Clustereinstellungen ändern.
- 7 Wählen Sie auf der Seite „Clusterfunktionen“ **vSphere HA einschalten**.
- 8 Konfigurieren Sie dann die vSphere HA-Einstellungen gemäß den Anforderungen Ihres Clusters.
 - Hostüberwachungsstatus
 - Zugangssteuerung
 - Optionen für virtuelle Maschinen
 - VM-Überwachung
 - Datenspeicher-Taktsignale
- 9 Klicken Sie auf **OK**, um das Dialogfeld Einstellungen zu schließen.

Ein konfigurierter vSphere HA-Cluster mit den angegebenen Hosts steht zur Verfügung. Informationen zum Konfigurieren von Clustereinstellungen finden Sie unter „[Konfigurieren von vSphere HA-Clustereinstellungen im vSphere-Client](#)“, auf Seite 436.

HINWEIS Ein vSphere HA-aktivierter Cluster ist eine Voraussetzung zur Verwendung von Fault Tolerance.

Konfigurieren von vSphere HA-Clustereinstellungen im vSphere-Client

Wenn Sie einen vSphere HA-Cluster erstellen oder einen vorhandenen Cluster konfigurieren, müssen Sie die Einstellungen konfigurieren, die festlegen, wie die Funktion funktioniert.

Die folgenden vSphere HA-Einstellungen können Sie im vSphere-Client konfigurieren:

Hostüberwachung	Aktivieren Sie die Hostüberwachung, um Hosts im Cluster das Austauschen von Netzwerktaktsignalen zu ermöglichen und damit vSphere HA Maßnahmen ergreifen kann, wenn Fehler auftreten.
<hr/>	
HINWEIS Die Hostüberwachung ist erforderlich, damit der vSphere Fault Tolerance-Wiederherstellungsprozess ordnungsgemäß ausgeführt wird.	
<hr/>	
Zugangssteuerung	Aktivieren oder deaktivieren Sie die Zugangssteuerung für den vSphere HA-Cluster und wählen Sie eine Richtlinie dafür aus, wie diese erzwungen wird.
Optionen für virtuelle Maschinen	Legen Sie die VM-Neustartpriorität und Hostisolierungsreaktion fest.
VM-Überwachung	Aktivieren Sie die VM-Überwachung oder die VM- und Anwendungsüberwachung.
Datenspeicher-Taktsignale	Geben Sie die Voreinstellungen für die Datenspeicher an, die vSphere HA für Datenspeicher-Taktsignale verwendet.

Konfigurieren der Hostüberwachung und der Zugangssteuerung

Nachdem Sie einen Cluster erstellt haben, ermöglicht es die Hostüberwachung dem vSphere HA-Master-Host, auf Ausfälle des Hosts oder der virtuellen Maschine und die Isolierung des Verwaltungsnetzwerks zu reagieren. Über die Zugangssteuerung können Sie angeben, ob virtuelle Maschinen gestartet werden können, wenn sie gegen Verfügbarkeitsbedingungen verstoßen. Der Cluster reserviert Ressourcen, um für alle ausgeführten virtuellen Maschinen auf der angegebenen Anzahl von Hosts ein Failover zu ermöglichen.

Die Seite „Hostüberwachung“ und „Zugangssteuerung“ wird nur angezeigt, wenn Sie vSphere HA aktiviert haben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Zeigen Sie den Cluster in der Bestandsliste des vSphere-Clients an.
- 2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie im linken Fenster des Dialogfelds Clustereinstellungen die Option **vSphere HA** aus.
- 4 (Optional) Wählen Sie **Hostüberwachung aktivieren**.
- 5 Wählen Sie eine Zugangssteuerungsoption aus.
 - Aktivieren: VM-Einschaltvorgänge nicht zulassen, die gegen die Verfügbarkeitseinschränkungen verstoßen.

Durch die Aktivierung der Zugangssteuerung werden die Verfügbarkeitseinschränkungen erzwungen und die Failover-Kapazität beibehalten. Ein Vorgang auf einer virtuellen Maschine, der die nicht reservierten Ressourcen im Cluster reduziert und gegen Verfügbarkeitseinschränkungen verstößt, ist nicht zulässig.

- Deaktivieren: VM-Einschaltvorgänge zulassen, die gegen die Verfügbarkeitseinschränkungen verstoßen.

Das Deaktivieren der Zugangssteuerung ermöglicht, dass eine virtuelle Maschine selbst dann eingeschaltet werden kann, wenn dadurch die Failover-Kapazitäten nicht mehr ausreichend sind. Wenn dies geschieht, werden keine Warnungen angezeigt und der Cluster wird nicht rot gekennzeichnet. Wenn ein Cluster über eine ungenügende Failover-Kapazität verfügt, kann vSphere HA trotzdem Failover durchführen. High Availability verwendet die Einstellung „VM-Neustartpriorität“, um zu ermitteln, welche virtuellen Maschinen zuerst eingeschaltet werden sollen.

HINWEIS Wählen Sie diese Option, wenn Sie mehr virtuelle Maschinen einschalten möchten, als das vSphere HA-Failover-Level unterstützt. Wenn Sie diese Option auswählen, kann kein Failover garantiert werden.

- 6 Wählen Sie eine auf den Cluster anzuwendende Zugangssteuerungsrichtlinie.

Option	Beschreibung
Vom Cluster tolerierte Hostausfälle	Geben Sie an, wie viele Hosts maximal ausfallen dürfen, um noch wiederhergestellt werden zu können oder für die ein Failover garantiert werden kann.
Prozentsatz der Cluster-Ressourcen, der als Failover-Ersatzkapazität reserviert sind	Geben Sie einen Prozentsatz für die CPU- und Arbeitsspeicherressourcen des Clusters an, der zusätzlich reserviert werden soll, um Failover zu unterstützen.
Failover-Hosts angeben	Klicken Sie, um Hosts für Failover-Aktionen auszuwählen. Failover können immer noch von anderen Hosts im Cluster übernommen werden, wenn ein Standard-Failover-Host nicht über genügend Ressourcen verfügt.

- 7 (Optional) Wählen Sie **Erweiterte Optionen** aus, um die Optionen für den Automatisierungsmodus zu konfigurieren.

Nehmen Sie nur dann Änderungen an diesen Einstellungen vor, wenn Sie vom technischen Support von VMware dazu aufgefordert werden oder wenn Sie die entsprechenden Anweisungen in der VMware-Dokumentation befolgen.

- 8 Klicken Sie auf **OK**.

Failover-Hosts angeben

Wenn Sie die Richtlinie für die Zugangssteuerung „Failover-Hosts angeben“ auswählen, müssen Sie auch festlegen, welche Hosts für diese Funktion verwendet werden sollen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Öffnen Sie das Dialogfeld „Failover-Hosts angeben“ über den Bereich „vSphere HA“ des Dialogfelds „Clustereinstellungen“ des vSphere-Clients.
- 2 Wählen Sie im Bereich „Verfügbare Hosts“ einen verfügbaren Host aus, der als Failover-Host fungieren soll.
- 3 Klicken Sie auf die Schaltfläche >>, um den Hostnamen in den Bereich „Failover-Hosts“ zu verschieben.
- 4 Wiederholen Sie die Schritte 1 und 2 für jeden Host, den Sie als Failover-Host festlegen möchten.

- 5 Wählen Sie zum Entfernen eines Hosts aus der Liste der Failover-Hosts den Namen dieses Hosts im Bereich „Failover-Hosts“ aus.
- 6 Klicken Sie auf die Schaltfläche <<, um den Hostnamen in den Bereich „Verfügbare Hosts“ zu verschieben.

Sie können die Hosts, die Sie als Failover-Hosts festgelegt haben, zur Unterstützung des vSphere HA-Zugangssteuerungsprozesses verwenden.

Festlegen der Optionen für virtuelle Maschinen

Wenn Sie vSphere HA für einen Cluster aktiviert haben, können Sie die Neustartpriorität und die Hostisolierungsreaktion für virtuelle Maschinen im Cluster festlegen.

Die Seite „Optionen für virtuelle Maschinen“ wird nur angezeigt, wenn Sie vSphere HA aktiviert haben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie **VM-Neustartpriorität** für virtuelle Maschinen im Cluster aus.

Mithilfe der VM-Neustartpriorität legen Sie fest, in welcher Reihenfolge die virtuellen Maschinen nach einem Hostausfall neu gestartet werden. Virtuelle Maschinen mit einer höheren Priorität werden zuerst gestartet. Diese Priorität gilt nur bezogen auf den jeweiligen Host. Falls mehrere Hosts ausfallen, werden alle virtuellen Maschinen des ersten Hosts in der Reihenfolge der festgelegten Priorität migriert, anschließend werden alle virtuellen Maschinen des zweiten Hosts ebenfalls in der Reihenfolge der festgelegten Priorität migriert usw.

- 2 Wählen Sie **Hostisolierungsreaktion**.

Die Hostisolierungsreaktion legt fest, was geschieht, wenn die Netzwerkkonsolenverbindung eines Hosts innerhalb eines vSphere HA-Clusters unterbrochen wird, der Host aber weiterhin ausgeführt wird.

- 3 Klicken Sie auf **Weiter**.

Die Einstellungen für die Neustartpriorität und die Hostisolierungsreaktion Ihrer virtuellen Maschine sind jetzt wirksam.

Konfigurieren der VM- und Anwendungsüberwachung

Diese Funktion für die Überwachung virtueller Maschinen verwendet die Taktsignalinformationen, die von VMware Tools als Proxy für die Verfügbarkeit des Gastbetriebssystems ermittelt werden. Dadurch kann vSphere HA einzelne virtuelle Maschinen, die keine Taktsignale mehr senden können, automatisch zurücksetzen oder neu starten.

Die Seite „VM-Überwachung“ erscheint nur, wenn Sie vSphere HA aktiviert haben.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 (Optional) Wählen Sie **Nur VM-Überwachung**, um individuelle virtuelle Maschinen neu zu starten, wenn ihr Taktsignal nicht innerhalb einer festgelegten Zeit empfangen wird. Sie können **VM- und Anwendungsüberwachung** auswählen, wenn Sie auch die Anwendungsüberwachung aktivieren möchten.

- 2 Legen Sie die Überwachungsempfindlichkeit für virtuelle Maschinen fest, indem Sie den Schieberegler zwischen **Niedrig** und **Hoch** verschieben. Wählen Sie **Benutzerdefiniert** aus, um benutzerdefinierte Einstellungen bereitzustellen.
- 3 Klicken Sie auf **Weiter**.

Konfigurieren des Datenspeicher-Taktsignals

vSphere HA verwendet Datenspeicher-Taktsignale, um ausgefallene Hosts und Hosts, die sich auf einer Netzwerkpartition befinden, voneinander zu unterscheiden. Datenspeicher-Taktsignale ermöglichen vSphere HA, Hosts zu überwachen, wenn eine Verwaltungsnetzwerkpartition auftritt, und weiterhin auf Ausfälle zu reagieren.

Verwenden Sie das Dialogfeld zum Konfigurieren der Datenspeicher-Taktsignale, um die Datenspeicher anzugeben, die zu diesem Zweck verwendet werden sollen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Zeigen Sie den Cluster in der Bestandsliste des vSphere-Clients an.
- 2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Einstellungen bearbeiten**.
- 3 Wählen Sie im linken Bereich des Dialogfelds „Clustereinstellungen“ die Option **Datenspeicher-Taktsignal**.
- 4 Um vSphere HA anzuweisen, wie Datenspeicher auszuwählen und Ihre Voreinstellungen zu behandeln sind, wählen Sie aus den folgenden Optionen:

Tabelle 26-1.

Datenspeicher-Taktsignalooptionen

Nur aus den bevorzugten Datenspeichern auswählen

Beliebige Cluster-Datenspeicher auswählen

Unter Berücksichtigung meiner Voreinstellungen Cluster-Datenspeicher auswählen

- 5 Wählen Sie im Bereich **Für Taktsignale verfügbare Datenspeicher** die Datenspeicher aus, die Sie für Taktsignale verwenden möchten.

Die aufgelisteten Datenspeicher werden von mehreren Hosts im vSphere HA-Cluster gemeinsam verwendet. Wenn ein Datenspeicher ausgewählt wird, werden im unteren Bereich alle Hosts im vSphere HA-Cluster angezeigt, die auf diesen zugreifen können.

- 6 Klicken Sie auf **OK**.

Anpassen einer einzelnen virtuellen Maschine im vSphere Web Client

In einem vSphere HA-Cluster werden allen virtuellen Maschinen die Standard-Clustereinstellungen für die VM-Neustartpriorität, die Hostisolierungsreaktion und die VM-Überwachung zugewiesen. Sie können ein bestimmtes Verhalten für jede virtuelle Maschine festlegen, indem Sie diese Standardeinstellungen ändern. Wenn die virtuelle Maschine aus dem Cluster entfernt wird, gehen diese Einstellungen verloren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Cluster, und klicken Sie im Kontextmenü auf die Option **Einstellungen bearbeiten**.

- 2 Klicken Sie unter vSphere HA auf **Optionen für virtuelle Maschinen**.
- 3 Wählen Sie im Fenster „Einstellungen der virtuellen Maschine“ eine virtuelle Maschine aus und ändern Sie die Einstellung für die **VM-Neustartpriorität** oder die **Hostisolierungsreaktion**.
- 4 Wählen Sie **VM-Überwachung** unter „vSphere HA“ aus.
- 5 Wählen Sie im Fenster „Einstellungen der virtuellen Maschine“ eine virtuelle Maschine aus und ändern Sie die Einstellung für die **VM-Überwachung**.
- 6 Klicken Sie auf **OK**.

Das Verhalten der virtuellen Maschine wird jetzt gemäß den geänderten Einstellungen angepasst.

Aktivieren der Fault Tolerance für virtuelle Maschinen

27

Sie können vSphere Fault Tolerance für Ihre virtuellen Maschinen nutzen, um Business Continuity mit höherer Verfügbarkeit und besserem Datenschutz als bei vSphere HA sicherzustellen.

Fault Tolerance basiert auf der ESXi-Hostplattform und stellt unterbrechungsfreie Verfügbarkeit bereit, indem identische virtuelle Maschinen auf getrennten Hosts ausgeführt werden.

Um mit Fault Tolerance optimale Ergebnisse zu erzielen, sollten Sie mit ihrer Funktionsweise, dem Vorgang zu ihrer Aktivierung für Ihren Cluster und Ihre virtuellen Maschinen und den Best Practices für ihre Nutzung vertraut sein.

Dieses Kapitel behandelt die folgenden Themen:

- „Beispiele für die Nutzen der Fault Tolerance“, auf Seite 441
- „Fault Tolerance-Checkliste“, auf Seite 442
- „Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance“, auf Seite 443
- „Verwenden von Fault Tolerance“, auf Seite 447
- „Anzeigen von Daten über fehlertolerante virtuelle Maschinen im vSphere-Client“, auf Seite 450
- „Best Practices für Fault Tolerance“, auf Seite 451

Beispiele für die Nutzen der Fault Tolerance

Sie profitieren in mehreren typischen Situationen von der Verwendung von vSphere Fault Tolerance.

Fault Tolerance bietet einen höheren Level an Business Continuity als vSphere HA. Wenn eine sekundäre virtuelle Maschine aufgerufen wird, um die primäre virtuelle Maschine zu ersetzen, übernimmt sie sofort deren Rolle und der gesamte Zustand der primären virtuellen Maschine bleibt erhalten. Gestartete Anwendungen und im Arbeitsspeicher gespeicherte Daten müssen weder neu geladen noch erneut eingegeben werden. Dies unterscheidet sich von einem vSphere HA-Failover, das alle ausgefallenen virtuellen Maschinen neu startet.

Diese höhere Kontinuität und der zusätzliche Schutz von Zustandsinformationen und Daten wirken auf die Szenarien, in denen Sie möglicherweise die Fehlertoleranz bereitstellen möchten.

- Anwendungen, die immer bereit sein müssen vor allem diejenigen, die lang anhaltende Clientverbindungen benötigen, die Benutzer auch im Fall eines Hardwarefehlers aufrechterhalten möchten.
- Benutzerdefinierte Anwendungen, die keine Möglichkeit zur Clusterbildung haben.
- Fälle, in denen benutzerdefinierte Clusterlösungen High Availability bieten können, aber zu kompliziert sind, um konfiguriert und gewartet zu werden.

Ein weiterer bedeutender Verwendungszweck für den Schutz einer virtuellen Maschine mithilfe der Fehlertoleranz kann als „Fehlertoleranz bei Bedarf“ bezeichnet werden. In diesem Fall wird eine virtuelle Maschine im normalen Betrieb durch vSphere HA ausreichend geschützt. In bestimmten, kritischen Phasen erwägen Sie beispielsweise, den Schutz der virtuellen Maschine zu erhöhen. Beispielsweise erstellen Sie einen Bericht zum Quartalsende. Wenn Sie dabei unterbrochen werden, kann die Verfügbarkeit von unternehmenskritischen Informationen verzögert werden. Sie können diese virtuelle Maschine mithilfe von vSphere Fault Tolerance schützen, bevor Sie diesen Bericht ausführen, und die Fault Tolerance danach wieder deaktivieren oder aussetzen. Sie können die Fehlertoleranz bei Bedarf dazu verwenden, die virtuelle Maschine in einer kritischen Phase zu schützen und danach die Ressourcen für den unkritischen Betrieb in den Normalzustand zurückversetzen.

Fault Tolerance-Checkliste

In der folgenden Checkliste sind die Cluster-, Host- und VM-Anforderungen aufgeführt, die Ihnen bekannt sein müssen, bevor Sie vSphere Fault Tolerance verwenden.

Überprüfen Sie diese Liste, bevor Sie Fault Tolerance einrichten.

HINWEIS Das Failover von fehlertoleranten virtuellen Maschinen ist unabhängig von vCenter Server, allerdings müssen Sie vCenter Server verwenden, um Fault Tolerance-Cluster einzurichten.

Clusteranforderungen für Fault Tolerance

Die folgenden Clusteranforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Fehlertoleranz-Protokollierung und vMotion-Netzwerke sind konfiguriert. Siehe „[Konfigurieren von Netzwerken für Hostmaschinen im vSphere Client](#)“, auf Seite 444.
- vSphere HA-Cluster wurden erstellt und aktiviert. Weitere Informationen hierzu finden Sie unter „[Erstellen und Konfigurieren eines vSphere HA-Clusters](#)“, auf Seite 434. vSphere HA muss aktiviert sein, bevor Sie fehlertolerante virtuelle Maschinen einschalten oder einem Cluster einen Host hinzufügen können, der bereits fehlertolerante virtuelle Maschinen unterstützt.

Hostanforderungen für Fault Tolerance

Die folgenden Hostanforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Hosts müssen unterstützte Prozessoren verwenden.
- Hosts müssen für Fault Tolerance lizenziert sein.
- Hosts müssen für Fault Tolerance zertifiziert sein. Rufen Sie die Seite <http://www.vmware.com/resources/compatibility/search.php> auf und wählen Sie **Search by Fault Tolerant Compatible Sets**, um zu ermitteln, ob Ihre Hosts zertifiziert sind.
- Bei der Konfiguration für jeden Host muss im BIOS die Hardwarevirtualisierung (HV) aktiviert sein.

HINWEIS VMware empfiehlt, dass für die Hosts, die Sie zur Unterstützung von Fault Tolerance-VMs verwenden, die BIOS-Einstellungen zur Energieverwaltung auf maximale Leistung bzw. auf vom Betriebssystem verwaltete Leistung festgelegt sind.

Sie können auch Profilübereinstimmungsprüfungen ausführen, wie unter „[Erstellen von Clustern und Überprüfen der Übereinstimmung im vSphere Client](#)“, auf Seite 446 beschrieben sind, um die Kompatibilität der Hosts im Cluster zum Unterstützen von Fault Tolerance zu bestätigen.

VM-Anforderungen für Fault Tolerance

Die folgenden VM-Anforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Es dürfen keine nicht unterstützten Geräte mit den virtuellen Maschinen verbunden sein. Weitere Informationen zur Fault Tolerance-Interoperabilität finden Sie in der Dokumentation zur *vSphere-Verfügbarkeit*.
- Nicht kompatible Funktionen dürfen nicht mit den fehlertoleranten virtuellen Maschinen ausgeführt werden. Weitere Informationen zur Fault Tolerance-Interoperabilität finden Sie in der Dokumentation zur *vSphere-Verfügbarkeit*.
- Die Dateien der virtuellen Maschine müssen auf einem gemeinsam genutzten Speicher gespeichert sein. Zu den akzeptablen gemeinsam genutzten Speicherlösungen gehören Fibre-Channel, iSCSI (Hardware und Software), NFS und NAS.

Weitere Konfigurationsempfehlungen

Beim Konfigurieren von Fault Tolerance sollten Sie zudem die folgenden Richtlinien beachten.

- Falls Sie NFS für den Zugriff auf gemeinsam genutzten Speicher verwenden, sollten Sie dedizierte NAS-Hardware mit mindestens einer 1 Gbit Netzwerkkarte verwenden, um die für das ordnungsgemäße Funktionieren von Fault Tolerance erforderliche Netzwerkleistung zu erzielen.
- Die Arbeitsspeicherreservierung einer fehlertoleranten VM wird auf die Arbeitsspeichergröße der virtuellen Maschine festgelegt, wenn Fault Tolerance eingeschaltet wird. Stellen Sie sicher, dass ein Ressourcenpool, der fehlertolerante VMs enthält, eine größere Arbeitsspeichermenge als die für die virtuellen Maschinen erforderliche Menge besitzt. Ohne diesen Überschuss im Ressourcenpool ist es möglich, dass kein Arbeitsspeicher mehr zur Verfügung steht, der als Overhead-Arbeitsspeicher genutzt werden kann.
- Verwenden Sie maximal 16 virtuelle Festplatten pro fehlertoleranter virtueller Maschine.
- Um Redundanz und maximalen Fault Tolerance-Schutz zu gewährleisten, sollten sich mindestens drei Hosts im Cluster befinden. Auf diese Weise wird in einer Failover-Situation ein Host bereitgestellt, der die neu erstellte sekundäre virtuelle Maschine aufnehmen kann.

Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance

Zum Aktivieren von vSphere Fault Tolerance für Ihren Cluster müssen die Voraussetzungen der Funktion erfüllt sein. Anschließend müssen Sie bestimmte Konfigurationsschritte auf Ihren Hosts ausführen. Nachdem Sie diese Schritte ausgeführt haben und Ihr Cluster erstellt wurde, können Sie auch überprüfen, ob Ihre Konfiguration die Anforderungen für das Aktivieren der Fault Tolerance erfüllt.

Sie sollten die folgenden Aufgaben ausführen, bevor Sie versuchen, Fault Tolerance für Ihren Cluster zu aktivieren:

- Vergewissern Sie sich, dass Cluster, Hosts und virtuelle Maschinen die Voraussetzungen gemäß der Fault Tolerance-Checkliste erfüllen.
- Konfigurieren des Netzwerks für die einzelnen Hosts.
- Erstellen des vSphere HA-Clusters, Hinzufügen der Hosts und Prüfen der Übereinstimmung.

Nachdem Sie Ihren Cluster und Ihre Hosts für Fault Tolerance vorbereitet haben, können Sie sie für Ihre virtuellen Maschinen einschalten. Siehe [„Einschalten der Fault Tolerance für virtuelle Maschinen im vSphere Client“](#), auf Seite 447.

Konfigurieren von Netzwerken für Hostmaschinen im vSphere Client

Auf jedem Host, den Sie zu einem vSphere HA-Cluster hinzufügen möchten, müssen Sie zwei verschiedene Netzwerk-Switches konfigurieren, damit der Host auch vSphere Fault Tolerance unterstützen kann.

Sie müssen diesen Vorgang zweimal durchführen, um Fault Tolerance für einen Host zu aktivieren, je einmal pro Portgruppenoption. Dadurch wird sichergestellt, dass für die Protokollierung von Fault Tolerance genügend Bandbreite zur Verfügung steht. Wählen Sie eine Option, schließen Sie den Vorgang ab, führen Sie den Vorgang dann erneut durch und wählen Sie die andere Portgruppenoption.

Voraussetzungen

Mehrere Gigabit-Netzwerkkarten sind erforderlich. Sie benötigen für jeden Host, der Fault Tolerance unterstützt, mindestens zwei physische Gigabit-Netzwerkkarten. Sie benötigen beispielsweise eine für die Fault Tolerance-Protokollierung und eine für vMotion. Verwenden Sie mindestens drei Netzwerkkarten, um die Verfügbarkeit sicherzustellen.

HINWEIS Die Netzwerkkarten für vMotion und die Fault Tolerance-Protokollierung müssen sich auf unterschiedlichen Subnetzen befinden und IPv6 wird auf der Netzwerkkarte für die Fault Tolerance-Protokollierung nicht unterstützt.

Vorgehensweise

- 1 Melden Sie sich beim vSphere Client an und wählen Sie im Bestandslistenfenster einen Host aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Wählen Sie **Netzwerk** unter **Hardware** aus und klicken Sie auf den Link **Netzwerk hinzufügen**.
Der Assistent zum Hinzufügen von Netzwerk wird angezeigt.
- 4 Wählen Sie **VMkernel** unter **Verbindungstypen** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie **Einen virtuellen Switch erstellen** aus und klicken Sie auf **Weiter**.
- 6 Geben Sie eine Bezeichnung für den Switch an.
- 7 Wählen Sie entweder **Diese Portgruppe für vMotion verwenden** oder **Diese Portgruppe für die Fault Tolerance-Protokollierung verwenden** und klicken Sie auf **Weiter**.
- 8 Geben Sie eine IP-Adresse und Subnetzmaske ein und klicken Sie anschließend auf **Weiter**.
- 9 Klicken Sie auf **Beenden**.

Nachdem Sie sowohl einen virtuellen vMotion- als auch einen virtuellen Fault Tolerance-Protokollierungs-Switch erstellt haben, können Sie nach Bedarf weitere virtuelle Switches erstellen. Anschließend sollten Sie den Host zum Cluster hinzufügen und die Schritte zum Einschalten von Fault Tolerance ausführen.

Weiter

Zeigen Sie die Registerkarte **Übersicht** im vSphere-Client an, um zu bestätigen, dass Sie vMotion und Fault Tolerance erfolgreich auf dem Host installiert haben. In den Feldern **vMotion aktiviert** und **Host für die Fault Tolerance konfiguriert** im Fenster „Allgemein“ muss „Ja“ angezeigt werden..

HINWEIS Wenn Sie das Netzwerk für die Unterstützung von Fault Tolerance konfigurieren, daraufhin jedoch den Port für die Fault Tolerance-Protokollierung deaktivieren, bleiben die Paare von fehlertoleranten virtuellen Maschinen, die bereits eingeschaltet sind, immer noch eingeschaltet. Wenn dann jedoch ein Failover auftritt, wird keine neue sekundäre virtuelle Maschine gestartet, nachdem die primäre virtuelle Maschine durch ihre sekundäre virtuelle Maschine ersetzt wurde. Dadurch wird die neue primäre virtuelle Maschine mit dem Status „Nicht geschützt“ ausgeführt.

Fault Tolerance - Beispiel einer Hostnetzwerkconfiguration

In diesem Beispiel wird die Host-Netzwerkconfiguration für Fault Tolerance in einer Standardbereitstellung mit vier 1-GB-Netzwerkkarten beschrieben. Diese ist eine mögliche Bereitstellung, die ausreichenden Service für alle Datenverkehrstypen, die in diesem Beispiel erwähnt sind, gewährleistet und als „Best Practice“-Konfiguration gelten kann.

Fault Tolerance sorgt für eine durchgehende Betriebszeit während des Ausfalls eines physischen Hosts aufgrund eines Stromausfalls, einer Systempanik oder ähnlicher Ursachen. Netzwerk- oder Speicherpfadausfälle oder andere physische Serverkomponenten, die auf den betrieblichen Status des Hosts keine Auswirkung haben, dürfen kein Fault Tolerance-Failover auf die sekundäre virtuelle Maschine initiieren. Kunden wird deshalb dringend empfohlen, die entsprechende Redundanz (z. B. NIC-Gruppierung) zu verwenden, um die Chancen, die VM-Konnektivität mit Infrastrukturkomponenten (Netzwerken oder Speicher-Arrays) zu verlieren, zu reduzieren.

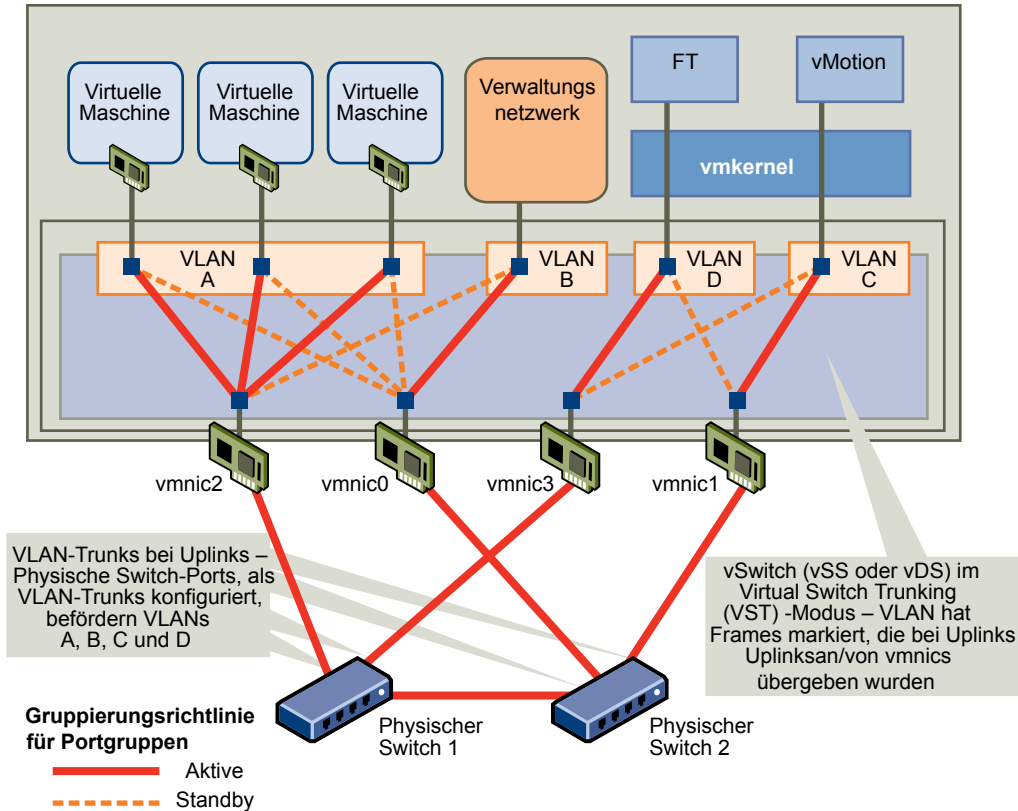
NIC-Gruppierungsrichtlinien werden auf den vSwitch-Portgruppen (bzw. auf verteilten virtuellen Portgruppen für vDS) konfiguriert und steuern, wie der vSwitch den Datenverkehr handhabt und ihn von den virtuellen Maschinen und VMkernel-Ports über die physischen Netzwerkkarten (vmnics) verteilt. Eine eindeutige Portgruppe wird in der Regel für jeden Datenverkehrstyp verwendet, wobei jeder Datenverkehrstyp einem anderen VLAN zugewiesen wird.

[Abbildung 27-1](#) wird die Netzwerkconfiguration für einen einzelnen ESXi-Host mit vier 1-GB-Netzwerkkarten dargestellt, die Fault Tolerance unterstützen. Andere Hosts im fehlertoleranten Cluster würden ähnlich konfiguriert.

In diesem Beispiel werden vier Portgruppen verwendet, die folgendermaßen konfiguriert sind:

- VLAN A: VM-Netzwerk-Portgruppe - Aktiv auf vmnic2 (zu physischem Switch 1); Standby auf vmnic0 (zu physischem Switch 2.)
- VLAN B: Verwaltungsnetzwerk-Portgruppe - Aktiv auf vmnic0 (zu physischem Switch 2); Standby auf vmnic2 (zu physischem Switch 1.)
- VLAN C: vMotion-Portgruppe - Aktiv auf vmnic1 (zu physischem Switch 2); Standby auf vmnic3 (zu physischem Switch 1.)
- VLAN D: Fault Tolerance-Protokollierung-Portgruppe - Aktiv auf vmnic3 (zu physischem Switch 1); Standby auf vmnic1 (zu physischem Switch 2.)

vMotion und die Fault Tolerance-Protokollierung können denselben VLAN gemeinsam nutzen (konfigurieren Sie hierfür dieselbe VLAN-Nummer für beide Portgruppen), aber sie benötigen ihre eigenen eindeutigen IP-Adressen, die sich in unterschiedlichen IP-Subnetzen befinden müssen. Separate VLANs werden möglicherweise bevorzugt, wenn auf dem physischen Netzwerk mit VLAN-basierendem QoS (Quality of Service) QoS-Einschränkungen gelten. QoS ist besonders in Situationen konkurrierender Datenströme nützlich, beispielsweise wenn mehrere physische Switch-Hops verwendet werden oder ein Failover erfolgt und mehrere Datenverkehrstypen um Netzwerkressourcen in Wettstreit treten.

Abbildung 27-1. Fault Tolerance - Beispiel einer Netzwerkkonfiguration

Erstellen von Clustern und Überprüfen der Übereinstimmung im vSphere Client

vSphere Fault Tolerance wird im Kontext eines vSphere HA-Clusters verwendet. Erstellen Sie den vSphere HA-Cluster und fügen Sie ihm die Hosts hinzu, nachdem Sie auf allen Hosts die Netzwerke konfiguriert haben. Sie können überprüfen, ob der Cluster richtig konfiguriert ist und den Anforderungen für die erfolgreiche Aktivierung von Fault Tolerance entspricht.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie den Cluster in der vCenter Server-Bestandsliste aus und klicken Sie auf die Registerkarte **Profil-Übereinstimmung**.
- 2 Klicken Sie auf **Jetzt auf Übereinstimmung prüfen**, um die Übereinstimmung zu überprüfen.
Klicken Sie auf **Beschreibung**, um die ausgeführten Tests anzuzeigen.

Die Ergebnisse der Überprüfung werden am unteren Rand des Bildschirms angezeigt. Ein Host erhält entweder den Status „Übereinstimmung“ oder „Nicht übereinstimmend“.

Verwenden von Fault Tolerance

Nachdem Sie alle erforderlichen Schritte zum Aktivieren von vSphere Fault Tolerance für Ihren Cluster ausgeführt haben, können Sie die Funktion nutzen, indem Sie sie für individuelle virtuelle Maschinen aktivieren.

Bevor Fault Tolerance eingeschaltet werden kann, werden auf einer virtuellen Maschine Validierungsprüfungen durchgeführt.

Wenn diese Prüfungen bestanden wurden und Sie vSphere Fault Tolerance für eine virtuelle Maschine aktivieren, werden neue Optionen zum Abschnitt „Fault Tolerance“ des Kontextmenüs hinzugefügt. Hierzu zählen Optionen zum Ausschalten oder Deaktivieren von Fault Tolerance, zum Migrieren der sekundären virtuellen Maschine, zum Testen des Failovers und zum Testen des Neustarts der sekundären virtuellen Maschine.

Einschalten der Fault Tolerance für virtuelle Maschinen im vSphere Client

Sie können vSphere Fault Tolerance über den vSphere Client einschalten.

Wenn die Fault Tolerance eingeschaltet wird, setzt vCenter Server den Grenzwert der virtuellen Maschine für den Arbeitsspeicher zurück und legt die Arbeitsspeicherreservierung auf die Arbeitsspeichergröße der virtuellen Maschine fest. Sie können die Arbeitsspeicherreservierung, -größe, -anteile oder den Arbeitsspeichergrenzwert nicht ändern, solange die Fault Tolerance eingeschaltet ist. Wenn die Fault Tolerance ausgeschaltet wird, werden geänderte Parameter nicht auf ihre ursprünglichen Werte zurückgesetzt.

Voraussetzungen

Öffnen Sie mithilfe eines Kontos mit Cluster-Administratorberechtigungen eine vSphere Client-Verbindung mit vCenter Server.

Vorgehensweise

- 1 Wählen Sie die Ansicht „Hosts & Cluster“ aus.
- 2 Klicken Sie mit der rechten Maustaste auf eine einzelne virtuelle Maschine und wählen Sie **Fehlertoleranz > Fehlertoleranz einschalten**.

Wenn Sie mehr als eine virtuelle Maschine auswählen, wird das Menü **Fault Tolerance** deaktiviert. Sie müssen die Fault Tolerance jeweils für eine virtuelle Maschine einschalten.

Die angegebene virtuelle Maschine wird als primäre virtuelle Maschine festgelegt und eine sekundäre virtuelle Maschine wird auf einem anderen Host eingerichtet. Die primäre virtuelle Maschine ist jetzt fehlertolerant.

Festlegen der Optionen für fehlertolerante virtuelle Maschinen im vSphere-Client

Wenn Sie die vSphere Fault Tolerance für eine virtuelle Maschine aktivieren, werden neue Optionen zum Abschnitt „Fault Tolerance“ ihres Kontextmenüs hinzugefügt.

Im vSphere-Client gibt es Optionen zum Ausschalten oder Deaktivieren von Fault Tolerance, zum Migrieren der sekundären virtuellen Maschine, zum Testen des Failovers und zum Testen des Neustarts der sekundären virtuellen Maschine.

Ausschalten der Fault Tolerance im vSphere Client

Das Ausschalten der vSphere Fault Tolerance löscht die sekundäre virtuelle Maschine, ihre Konfiguration und den Verlauf.

Verwenden Sie diese Option, wenn Sie nicht vorhaben, die Funktion wieder zu aktivieren. Verwenden Sie anderenfalls die Option **Fault Tolerance deaktivieren**.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Wenn sich die sekundäre virtuelle Maschine auf einem Host befindet, der im Wartungsmodus bzw. nicht verbunden ist oder nicht antwortet, können Sie die Option **Fault Tolerance ausschalten** nicht verwenden. In diesem Fall sollten Sie stattdessen Fault Tolerance deaktivieren und aktivieren.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Ansicht „**Hosts & Cluster**“.
- 2 Klicken Sie mit der rechten Maustaste auf die fehlertolerante virtuelle Maschine und wählen Sie **Fault Tolerance > Fault Tolerance ausschalten**.

Fault Tolerance wird für die ausgewählte virtuelle Maschine ausgeschaltet. Der Verlauf und die sekundäre virtuelle Maschine der ausgewählten virtuellen Maschine werden gelöscht.

Deaktivieren der Fault Tolerance im vSphere Client

Das Deaktivieren der vSphere Fault Tolerance für eine virtuelle Maschine hält ihren Fault Tolerance-Schutz an, behält jedoch die sekundäre virtuelle Maschine, ihre Konfiguration und den Verlauf bei. Verwenden Sie diese Option, wenn Sie den Fault Tolerance-Schutz möglicherweise später wieder aktivieren müssen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Ansicht „**Hosts & Cluster**“.
- 2 Klicken Sie mit der rechten Maustaste auf die fehlertolerante virtuelle Maschine und wählen Sie die Option **Fault Tolerance > Fault Tolerance deaktivieren**.

Fault Tolerance wird für die ausgewählte virtuelle Maschine deaktiviert. Der Verlauf und die sekundäre virtuelle Maschine für die ausgewählte virtuelle Maschine werden beibehalten und verwendet, falls die Funktion wieder aktiviert wird.

Weiter

Nachdem Sie Fault Tolerance deaktiviert haben, wird die Menüoption „Fault Tolerance deaktivieren“ in **Fault Tolerance aktivieren** umgestellt. Wählen Sie diese Option aus, um die Funktion zu reaktivieren.

Migrieren der sekundären virtuellen Maschine im vSphere Client

Nachdem die vSphere Fault Tolerance für eine Primäre Virtuelle Maschine eingeschaltet wurde, können Sie den Host ändern, auf dem sich ihre zugewiesene sekundäre virtuelle Maschine befindet, indem Sie sie migrieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Ansicht „**Hosts & Cluster**“.
- 2 Klicken Sie mit der rechten Maustaste auf die fehlertolerante virtuelle Maschine und wählen Sie die Option **Fault Tolerance > Sekundäre VM migrieren**.

Der Assistent für das Migrieren einer virtuellen Maschine wird geöffnet. Der Migrationstyp **Host ändern** ist ausgewählt.
- 3 Klicken Sie auf **Weiter**.
- 4 Wählen Sie den Zielhost für die sekundäre virtuelle Maschine aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie eine Migrationspriorität aus und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie Ihre Auswahl auf der Seite „Übersicht“ und klicken Sie auf **Beenden**.

Die sekundäre virtuelle Maschine, die der ausgewählten fehlertoleranten virtuellen Maschine zugewiesen ist, wird auf den angegebenen Host migriert. Beachten Sie, dass die primäre virtuelle Maschine mithilfe des Befehls **Migrieren** in ihrem Kontextmenü migriert werden kann.

Testen des Fault Tolerance-Failovers im vSphere Client

Sie können eine Failover-Situation für eine ausgewählte primäre virtuelle Maschine herbeiführen, um Ihren Fehlertoleranzschutz zu testen.

Diese Option ist nicht verfügbar, wenn die virtuelle Maschine ausgeschaltet ist.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Ansicht „**Hosts & Cluster**“.
- 2 Klicken Sie mit der rechten Maustaste auf die fehlertolerante virtuelle Maschine und wählen Sie die Option **Fehlertoleranz > Failover testen**.

Diese Aufgabe ruft den Ausfall der primären virtuellen Maschine hervor, um sicherzustellen, dass sie durch die sekundäre virtuelle Maschine ersetzt wird. Außerdem wird eine neue sekundäre virtuelle Maschine gestartet und die primäre virtuelle Maschine wird wieder in den Status „Geschützt“ versetzt.

Testen des Neustarts der sekundären virtuellen Maschine im vSphere Client

Sie können den Ausfall einer sekundären virtuellen Maschine herbeiführen, um den Fehlertoleranzschutz für eine ausgewählte primäre virtuelle Maschine zu testen.

Diese Option ist nicht verfügbar, wenn die virtuelle Maschine ausgeschaltet ist.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie im vSphere-Client die Ansicht „**Hosts & Cluster**“.
- 2 Klicken Sie mit der rechten Maustaste auf die fehlertolerante virtuelle Maschine und wählen Sie **Fehlertoleranz > Neustart sekundärer VM testen**.

Diese Aufgabe führt zum Beenden der sekundären virtuellen Maschine, die den Fehlertoleranzschutz für die ausgewählte primäre virtuelle Maschine bereitstellt. Anschließend wird eine neue sekundäre virtuelle Maschine gestartet und die primäre virtuelle Maschine wird wieder in den Status „Geschützt“ versetzt.

Anzeigen von Daten über fehlertolerante virtuelle Maschinen im vSphere-Client

Sie können fehlertolerante virtuelle Maschinen mithilfe des vSphere-Clients in der Bestandsliste von vCenter Server anzeigen.

HINWEIS Sie können die Fault Tolerance von der sekundären virtuellen Maschine aus nicht deaktivieren.

Die Registerkarte **Übersicht** für die primäre virtuelle Maschine enthält den Abschnitt (bzw. den Bereich) „vSphere Fault Tolerance“ mit Informationen über die virtuelle Maschine.

Fault Tolerance-Status

Zeigt den Fault Tolerance-Status der virtuellen Maschine an.

- Geschützt. Die primäre und die sekundäre virtuelle Maschine sind eingeschaltet und werden ordnungsgemäß ausgeführt.
- Nicht geschützt. Die sekundäre VM wird nicht ausgeführt. Mögliche Ursachen hierfür sind in der Tabelle aufgeführt.

Tabelle 27-1. Ursachen für den Status „Nicht geschützt“ der primären virtuellen Maschine

Ursache für den Status „Nicht geschützt“	Beschreibung
Starten	Die Fault Tolerance ist dabei, die sekundäre virtuelle Maschine zu starten. Diese Meldung wird nur für kurze Zeit angezeigt.
Sekundäre VM erforderlich	Die primäre virtuelle Maschine wird ohne eine sekundäre virtuelle Maschine ausgeführt und ist somit aktuell nicht geschützt. Dieses Problem tritt auf, wenn im Cluster kein kompatibler Host für die sekundäre virtuelle Maschine verfügbar ist. Beheben Sie dies, indem Sie einen kompatiblen Host bereitstellen. Falls ein kompatibler Host im Cluster online ist, sind möglicherweise weitere Nachforschungen erforderlich. Unter bestimmten Umständen kann dieses Problem durch das Deaktivieren und erneute Aktivieren der Fault Tolerance behoben werden.

Tabelle 27-1. Ursachen für den Status „Nicht geschützt“ der primären virtuellen Maschine (Fortsetzung)

Ursache für den Status „Nicht geschützt“	Beschreibung
Deaktiviert	Fault Tolerance ist aktuell deaktiviert (es wird keine sekundäre virtuelle Maschine ausgeführt). Dies tritt ein, wenn die Fault Tolerance durch den Benutzer deaktiviert wird oder wenn vCenter Server die Fault Tolerance deaktiviert, nachdem die sekundäre virtuelle Maschine nicht eingeschaltet werden konnte.
VM wird nicht ausgeführt	Die Fault Tolerance ist aktiviert, aber die virtuelle Maschine ist ausgeschaltet. Schalten Sie die virtuelle Maschine ein, um den Status „Geschützt“ zu erhalten.

Sekundärer Speicherort	Zeigt den ESXi-Host an, auf dem die sekundäre virtuelle Maschine gehostet wird.
Gesamtmenge an sekundärer CPU	Die CPU-Nutzung der sekundären virtuellen Maschine in MHz.
Gesamtmenge an sekundärem Arbeitsspeicher	Die Arbeitsspeichernutzung der sekundären virtuellen Maschine in MB.
vLockstep-Intervall	Das Zeitintervall (in Sekunden), das die sekundäre virtuelle Maschine benötigt, um den aktuellen Ausführungsstatus der primären virtuellen Maschine wieder herzustellen. In der Regel beträgt dieses Intervall weniger als eine halbe Sekunde. Unabhängig von dem Wert für das vLockstep-Intervall geht während eines Failovers kein Status verloren.
Protokollbandbreite	Zeigt die Menge an Netzwerkkapazität an, die für das Senden von Protokollinformationen über vSphere Fault Tolerance vom Host, auf dem die primäre virtuelle Maschine läuft, an den Host, auf dem die sekundäre virtuelle Maschine läuft, benötigt wird.

Für jeden Host, der so konfiguriert ist, dass er Fault Tolerance unterstützt, können Sie Informationen zu dessen fehlertoleranten virtuellen Maschinen anzeigen, indem Sie im vSphere-Client auf die Registerkarte **Zusammenfassung** des Hosts zugreifen. Der Abschnitt **Fault Tolerance** dieses Bildschirms zeigt die Gesamtzahl primärer und sekundärer virtueller Maschinen an, die sich auf dem Host befinden, sowie die Anzahl der eingeschalteten virtuellen Maschinen. Falls der Host ESX/ESXi 4.1 oder höher ist, zeigt dieser Abschnitt auch die Version von Fault Tolerance an, die auf dem Host ausgeführt wird. Anderenfalls wird die Build-Nummer des Hosts aufgelistet. Damit zwei Hosts kompatibel sind, müssen ihre FT-Versionsnummern oder die Build-Nummern der Hosts übereinstimmen.

Best Practices für Fault Tolerance

Um optimale Fault Tolerance-Ergebnisse erzielen zu können, sollten Sie bestimmte empfohlene Vorgehensweisen einhalten.

Mit den folgenden Empfehlungen für die Host- und Netzwerkkonfiguration lassen sich die Stabilität und Leistung Ihres Clusters verbessern.

Hostkonfiguration

Hosts, auf denen die primären und sekundären virtuellen Maschinen ausgeführt werden, sollten mit annähernd denselben Prozessorfrequenzen arbeiten, anderenfalls könnte es sein, dass die sekundären virtuellen Maschinen häufiger neu gestartet werden. Plattform-Energieverwaltungsfunktionen, die sich nicht abhängig von der Arbeitslast anpassen (z. B. die Energiebeschränkung und erzwungene Niedrigfrequenzmodi zum Einsparen von Energie), können große Abweichungen der Prozessorfrequenzen verursachen. Falls sekundäre virtuelle Maschinen regelmäßig neu gestartet werden, deaktivieren Sie alle Energieverwaltungsmodi auf den Hosts, die fehlertolerante virtuelle Maschinen ausführen, oder stellen Sie sicher, dass alle Hosts im selben Energieverwaltungsmodus laufen.

Hostnetzwerkkonfiguration

Anhand der folgenden Richtlinien können Sie das Netzwerk Ihres Hosts konfigurieren, um Fault Tolerance mit verschiedenen Kombinationen von Datenverkehrstypen (z. B. NFS) und mehreren physischen Netzwerkkarten zu unterstützen.

- Verteilen Sie jede Netzwerkkartengruppe über zwei physische Switches, um die L2-Domänenkontinuität für jedes VLAN zwischen den zwei physischen Switches zu gewährleisten.
- Verwenden Sie deterministische Gruppierungsrichtlinien, um sicherzugehen, dass bestimmte Datenverkehrstypen eine Affinität mit einer bestimmten Netzwerkkarte (Aktiv/Standby) bzw. mit mehreren Netzwerkkarten (z. B. ID des virtuellen Quell-Ports) haben.
- Paaren Sie Datenverkehrstypen dort, wo Aktiv/Standby-Richtlinien verwendet werden, um in einer Failoversituation die Auswirkungen zu minimieren, wenn beide Datenverkehrstypen eine vNIC teilen.
- Konfigurieren Sie dort, wo Aktiv/Standby-Richtlinien verwendet werden, alle aktiven Adapter eines bestimmten Datenverkehrstyps (z. B. Fault Tolerance-Protokollierung) für denselben physischen Switch. Dies minimiert die Anzahl der Netzwerk-Hops und reduziert die Chancen, dass die Switch-zu-Switch-Links überbucht werden.

HINWEIS Der Datenverkehr für die Fault Toleranceprotokollierung zwischen den primären und sekundären virtuellen Maschinen erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr kann vertrauliche Daten enthalten, wie z. B. Kennwörter im Klartext. Um zu verhindern, dass solche Daten preisgegeben werden, stellen Sie sicher, dass dieses Netzwerk gesichert ist, insbesondere gegen sogenannte „Man-in-the-middle“-Angriffe. Verwenden Sie z. B. ein privates Netzwerk für den Datenverkehr für die Fault Toleranceprotokollierung.

Homogene Cluster

vSphere Fault Tolerance kann in Clustern mit uneinheitlichen Hosts arbeiten, am besten funktioniert sie jedoch in Clustern mit kompatiblen Knoten. Wenn Sie Ihren Cluster erstellen, sollten alle Hosts über folgende Konfiguration verfügen:

- Gemeinsamen Zugriff auf Datenspeicher, die von den virtuellen Maschinen verwendet werden.
- Dieselbe Netzwerkkonfiguration für virtuelle Maschinen.
- Die gleichen BIOS-Einstellungen (Energieverwaltung und Hyper-Threading) für alle Hosts.

Führen Sie **Übereinstimmung prüfen** aus, um Inkompatibilitäten zu identifizieren und zu beheben.

Leistung

Verwenden Sie zur Erhöhung der für den Protokollierungsdatenverkehr zwischen primären und sekundären virtuellen Maschinen verfügbaren Bandbreite eine 10 Gbit-Netzwerkkarte und aktivieren Sie die Verwendung von Jumbo-Frames.

Speichern von ISOs auf gemeinsam genutztem Speicher für einen unterbrechungsfreien Zugriff

Speichern Sie ISOs, auf die durch virtuelle Maschinen mit aktivierter Fault Tolerance zugegriffen wird, auf gemeinsam genutztem Speicher, auf den beide Instanzen der fehlertoleranten virtuellen Maschine zugreifen können. Wenn Sie diese Konfiguration verwenden, setzt die CD-ROM in der virtuellen Maschine auch bei einem Failover den normalen Betrieb fort.

Für virtuelle Maschinen mit aktivierter Fault Tolerance können Sie ISO-Images verwenden, auf die nur die primäre virtuelle Maschine zugreifen kann. In diesem Fall kann die primäre virtuelle Maschine auf den ISO zugreifen, bei einem Failover meldet die CD-ROM jedoch Fehler, als ob kein Medium vorhanden wäre. Diese Situation kann akzeptabel sein, wenn die CD-ROM für einen vorübergehenden, unkritischen Vorgang, z. B. einen Patch, verwendet wird.

Vermeiden von Netzwerkpartitionen

Eine Netzwerkpartition tritt ein, wenn bei einem vSphere HA-Cluster ein Fehler des Verwaltungsnetzwerks auftritt, der zur Folge hat, dass einige der Hosts von vCenter Server sowie voneinander isoliert werden. In der Dokumentation zur *vSphere-Verfügbarkeit* finden Sie weitere Details. Wenn eine Partition eintritt, wird der Schutz durch Fault Tolerance möglicherweise herabgestuft.

In einem partitionierten vSphere HA-Cluster, bei dem Fault Tolerance verwendet wird, kann es vorkommen, dass die primäre virtuelle Maschine (oder ihre sekundäre virtuelle Maschine) in einer Partition landet, die von einem Master-Host verwaltet wird, der für die virtuelle Maschine nicht verantwortlich ist. Wenn ein Failover benötigt wird, wird eine sekundäre virtuelle Maschine nur dann neu gestartet, wenn sich die primäre virtuelle Maschine in einer Partition befunden hat, die von dem Master-Host verwaltet wird, der für die virtuelle Maschine verantwortlich ist.

Um die Chancen zu verringern, dass bei Ihrem Verwaltungsnetzwerk ein Fehler auftritt, der zu einer Netzwerkpartition führt, befolgen Sie die Empfehlungen in der Dokumentation zur *vSphere-Verfügbarkeit*.

Anzeigen der Fault Tolerance-Fehler im vSphere-Client

Wenn Fehler im Bezug auf Ihre Implementierung von Fault Tolerance von vCenter Server generiert werden, wird der Bildschirm „Fehlerdetails“ angezeigt.

Dieser Bildschirm listet Fehler im Bezug auf Fault Tolerance auf und zeigt für jeden Fehler den Fehlertyp (Rot ist ein Fehler, Gelb ist eine Warnung), den Namen der virtuellen Maschine oder des Hosts und eine kurze Beschreibung an.

Sie können diesen Bildschirm auch für eine bestimmte fehlgeschlagene Fault Tolerance-Aufgabe aufrufen. Wählen Sie dazu entweder in dem Fenster „Kürzlich bearbeitete Aufgaben“ oder in der Registerkarte **Aufgaben & Ereignisse** die Aufgabe für das Element aus, bei dem der Fehler aufgetreten ist, und klicken Sie auf den Link **Details anzeigen**, der in der Spalte „Details“ angezeigt wird.

Überwachen eines einzelnen Hosts mit dem vSphere Client

28

Wenn Sie mithilfe des vSphere-Clients eine Verbindung mit einem einzelnen Host herstellen, können Sie den Systemstatus des Hosts überwachen und Ereignisse, Systemprotokolle und Leistungsdiagramme anzeigen.

Dieses Kapitel behandelt die folgenden Themen:

- „Diagramme anzeigen“, auf Seite 455
- „Arbeiten mit erweiterten und benutzerdefinierten Diagrammen“, auf Seite 456
- „Überwachen des Serversystemstatus“, auf Seite 459
- „Überwachen von Ereignissen, Alarmen und automatisierten Aktionen“, auf Seite 461
- „Anzeigen von Lösungen“, auf Seite 476
- „Konfigurieren von SNMP-Einstellungen für vCenter Server“, auf Seite 477
- „Systemprotokolldateien“, auf Seite 478

Diagramme anzeigen

Sie können eine direkte Verbindung mit ESX/ESXi-Hosts herstellen und Informationen zur Ressourcennutzung im Liniendiagrammformat anzeigen.

Voraussetzungen

Stellen Sie über den vSphere-Client eine Verbindung zu einem ESX/ESXi-Host her.

Vorgehensweise

- 1 Wählen Sie den Host in der Bestandsliste aus.
- 2 Klicken Sie auf die Registerkarte **Leistung**.
- 3 Wählen Sie einen Ressourcentyp aus dem Dropdown-Menü **Wechseln zu** aus.
- 4 (Optional) Klicken Sie auf **Diagrammoptionen**, um Leistungsdiagramme zu ändern.

Arbeiten mit erweiterten und benutzerdefinierten Diagrammen

Verwenden Sie erweiterte Diagramme oder erstellen Sie Ihre eigenen Diagramme, um mehr Leistungsdaten anzuzeigen. Erweiterte Diagramme können nützlich sein, wenn Sie ein Problem zwar erkennen, aber mehr statistische Daten benötigen, um die Ursache des Problems ausfindig zu machen.

Zu den erweiterten Diagrammen gehören die folgenden Funktionen:

- Weitere Informationen. Beim Bewegen der Maus über einen Datenpunkt in einem Diagramm werden Details zu diesem Datenpunkt angezeigt.
- Anpassbare Diagramme. Ändern der Diagrammeinstellungen. Speichern der benutzerdefinierten Einstellungen, um eigene Diagramme zu erstellen.
- Exportieren in ein Spreadsheet.
- Speichern in eine Image-Datei oder in ein Spreadsheet.

Festlegen der erweiterten Leistungsdiagramme als Standard

Sie können den vSphere-Client so konfigurieren, dass beim Öffnen der Registerkarte **Leistung** standardmäßig die erweiterten Leistungsdiagramme angezeigt werden. In der Standardeinstellung werden die Überblicksleistungsdiagramme angezeigt.

Voraussetzungen

Stellen Sie sicher, dass Sie über eine Verbindung mit einem vCenter Server-System verfügen, indem Sie den vSphere-Client verwenden.

Vorgehensweise

- 1 Wählen Sie **Bearbeiten > Clienteeinstellungen**.
- 2 Klicken Sie im Abschnitt **Registerkarten** des Dialogfelds „Clienteeinstellungen“ auf **Erweiterte Leistungsdiagramme als Standard**.
- 3 Klicken Sie auf **OK**.

Ändern der Leistungsdiagrammeinstellungen

Sie können ein Leistungsdiagramm anpassen, indem Sie die zu überwachenden Objekte, die einzuschließenden Leistungsindikatoren, den Zeitraum und den Diagrammtyp festlegen. Sie können vorkonfigurierte Diagrammansichten anpassen und neue Diagrammansichten erstellen.

Voraussetzungen

Stellen Sie über den vSphere Client eine Verbindung mit dem Host her.

Vorgehensweise

- 1 Wählen Sie ein Bestandslistenobjekt aus und klicken Sie auf die Registerkarte **Leistung**.
- 2 Klicken Sie auf **Diagrammoptionen**.
- 3 Wählen Sie eine Metrikgruppe für das Diagramm.

- 4 Wählen Sie einen Zeitraum für die Metrikgruppe aus.

Wenn Sie **Benutzerdefiniert** auswählen, führen Sie eine der folgenden Aktionen aus.

- Wählen Sie **Letzte** und legen Sie für den Überwachungszeitraum des Objekts die Anzahl an Stunden, Tagen, Wochen oder Monaten fest.
- Wählen Sie **Von** und wählen Sie das Start- und das Enddatum aus.

Sie können auch die Optionen für den Zeitraum anpassen, indem Sie das Erfassungsintervall einstellen.

- 5 Wählen Sie einen Diagrammtyp aus.

Beachten Sie Folgendes, wenn Sie die Option für gestapelte Diagramme auswählen.

- In der Liste der Metriken kann nur ein Element ausgewählt werden.
- Gestapelte Diagramme für jede einzelne virtuelle Maschine stehen nur für Hosts zur Verfügung.
- Klicken Sie auf den beschreibenden Namen eines Indikators, um Informationen zu seiner Funktion und darüber zu erhalten, ob die ausgewählte Metrik für Diagramme einzelner virtueller Maschinen gestapelt werden kann.

- 6 Wählen Sie unter Objekte die im Diagramm anzuzeigenden Bestandslistenobjekte aus.

Die Objekte können ebenfalls über die Schaltflächen **Alle** oder **Keine** angegeben werden.

- 7 Wählen Sie unter Leistungsindikatoren die im Diagramm anzuzeigenden Datenindikatoren aus.

Sie können Leistungsindikatoren auch mithilfe der Schaltflächen **Alle** oder **Keine** angeben.

Klicken Sie auf den Namen eines Indikators, um im Fenster „Indikatorbeschreibung“ Informationen zu dem Indikator anzuzeigen.

- 8 Klicken Sie auf **Akzeptieren**.

Änderungen an den Diagrammeinstellungen sind sofort wirksam, nachdem sie übernommen wurden.

- 9 Klicken Sie auf **OK**.

Erstellen eines benutzerdefinierten erweiterten Diagramms

Sie können Ihre eigenen Diagramme erstellen, indem Sie benutzerdefinierte Diagrammeinstellungen speichern. Neue Diagramme werden dem Menü **Wechseln zu** hinzugefügt und sind dort nur dann sichtbar, wenn Diagramme für das ausgewählte Objekt angezeigt werden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Passen Sie die Diagrammeinstellungen an, wie unter „[Ändern der Leistungsdiagrammeinstellungen](#)“, auf Seite 456 beschrieben.
- 2 Klicken Sie auf **Diagrammeinstellungen speichern**.
- 3 Geben Sie einen Namen für Ihre Einstellungen ein.
- 4 Klicken Sie auf **OK**.

Die Diagrammeinstellungen werden gespeichert und dem Menü **Wechseln zu** wird ein Eintrag für Ihr Diagramm hinzugefügt.

Löschen einer benutzerdefinierten Ansicht erweiterter Diagramme

Sie können die benutzerdefinierten Ansichten von erweiterten Diagrammen vom vSphere-Client aus löschen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie ein beliebiges Objekt im Datacenter aus, um die Registerkarte **Leistung** zu aktivieren.
- 2 Klicken Sie auf die Registerkarte **Leistung** und anschließend auf **Erweitert**.
- 3 Klicken Sie auf **Diagrammoptionen**.
- 4 Klicken Sie auf **Diagrammeinstellungen verwalten**.
- 5 Wählen Sie ein Diagramm aus und klicken Sie auf **Löschen**.
Das Diagramm wird gelöscht und aus dem Menü **Wechseln zu** entfernt.
- 6 Klicken Sie auf **OK**.

Speichern von Diagrammdaten in eine Datei

Sie können Daten aus den erweiterten Leistungsdiagrammen in verschiedenen Grafikformaten oder im Microsoft Excel-Format in einer Datei speichern.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie auf der Registerkarte **Leistung** auf **Erweitert**.
- 2 Klicken Sie auf **Speichern**.
- 3 Navigieren Sie im Dialogfeld „Leistungsdiagramm speichern“ zu dem Speicherort, an dem die Datei gespeichert werden soll.
- 4 Geben Sie einen Namen für die Datei ein.
- 5 Wählen Sie einen Dateityp.
- 6 Klicken Sie auf **Speichern**.

Die Datei wird im von Ihnen angegebenen Format am von Ihnen angegebenen Speicherort gespeichert.

Exportieren von Leistungsdaten in ein Spreadsheet

Sie können Leistungsdaten aus den erweiterten Diagrammen in eine Microsoft Office Excel-Datei exportieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie das Objekt aus der Bestandsliste aus.

2 Wählen Sie **Datei > Bericht > Leistung**.

Wenn Leistungsdaten für das ausgewählte Bestandslistenobjekt nicht verfügbar sind, ist die Option „Leistungsdaten exportieren“ nicht verfügbar.

3 Geben Sie einen Dateinamen und einen Speicherort ein.

4 Wählen Sie den Datums- und Zeitbereich für das Diagramm aus.

5 Wählen Sie unter **Diagrammoptionen** den Diagrammtyp aus.

6 Wählen Sie die Metrikgruppen aus, die im Diagramm angezeigt werden sollen.

Sie können die Objekte auch angeben, indem Sie **Alle** oder **Kein** auswählen.

7 (Optional) Klicken Sie zum Anpassen der Optionen auf **Erweitert**, wählen Sie die Objekte und Leistungsindikatoren aus, die in das Diagramm einbezogen werden sollen, und klicken Sie auf **OK**.

8 Geben Sie die Größe des Diagramms in der exportierten Datei an.

9 Klicken Sie auf **OK**, um die Daten zu exportieren.

Überwachen des Serversystemstatus

Sie können den vSphere Web Client verwenden, um den Zustand von Host-Hardwarekomponenten wie CPU-Prozessoren, Arbeitsspeicher, Lüftern und anderen Komponenten zu überwachen.

Das Tool zum Überwachen des Hoststatus ermöglicht Ihnen, den Status verschiedener Hosthardwarekomponenten zu überwachen, z. B.:

- CPU-Prozessoren
- Arbeitsspeicher
- Lüfter
- Temperatur
- Spannung
- Betrieb
- Netzwerk
- Akku
- Speicher
- Kabel/Interconnect
- Softwarekomponenten
- Watchdog
- PCI-Geräte
- Andere

Das Tool zum Überwachen des Hoststatus stellt Daten dar, die über SMASH-Profilen (Systems Management Architecture for Server Hardware) gesammelt werden. Die angezeigten Informationen richten sich nach den verfügbaren Sensoren in Ihrer Serverhardware. SMASH ist eine Industriestandard-Spezifikation, die Protokolle zum Verwalten einer Vielzahl an Systemen im Datencenter zur Verfügung stellt. Weitere Informationen finden Sie unter <http://www.dmtf.org/standards/smash>.

Sie können den Systemzustand eines Hosts überwachen, indem Sie den vSphere Client entweder direkt mit einem Host oder den vSphere Web Client mit einem vCenter Server-System verbinden. Sie können auch Alarme festlegen, die ausgelöst werden, wenn sich der Systemstatus des Hosts ändert.

HINWEIS Die Interpretation von Hardwareüberwachungsdaten hängt vom jeweiligen Hardwareanbieter ab. Ihr Hardwareanbieter kann Ihnen dabei helfen, dass Sie die Ergebnisse der Überwachung der Hosthardwarerekomponenten verstehen.

Überwachen des Systemstatus bei einer Direktverbindung mit dem Host

Wenn Sie den vSphere-Client direkt mit einem Host verbinden, können Sie den Systemstatus auf der Registerkarte **Konfiguration** des Hosts ansehen.

Voraussetzungen

Erforderliche Berechtigung: **Host-.Konfiguration.Erweiterte Konfiguration**

Vorgehensweise

- 1 Melden Sie sich unter Verwendung des vSphere-Clients beim Host an und zeigen Sie die Bestandsliste an.
- 2 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Systemstatus**.

Bei ordnungsgemäßer Funktionsweise einer Komponente ist die Statusanzeige grün. Die Farbe der Statusanzeige ändert sich in gelb oder rot, wenn eine Systemkomponente einen Leistungsschwellenwert überschreitet oder nicht ordnungsgemäß funktioniert. Im Allgemeinen weist die gelbe Anzeige auf einen Leistungsabfall hin. Die rote Anzeige signalisiert, dass eine Komponente nicht mehr ausgeführt wird oder den höchsten Schwellenwert überschritten hat. Wenn der Status leer ist, bedeutet dies, dass der Statusüberwachungsdienst den Status der Komponente nicht ermitteln kann.

In der Spalte **Lesen** werden die aktuellen Werte für die Sensoren angezeigt. Für die Lüfter werden in der Spalte z. B. Umdrehungen pro Minute (RPM) und für die Temperatur Werte in Grad Celsius aufgelistet

Zurücksetzen der Hardware Sensoren bei einer Direktverbindung mit dem Host

Einige Hosthardwaresensoren zeigen Daten an, die über die Zeit akkumuliert werden. Sie können diese Sensoren zurücksetzen, um die gesammelten Daten zu löschen und mit der Erfassung neuer Daten zu beginnen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich beim ESXi-Host an.

Wenn Sie die Sensordaten zur Fehlerbehebung oder anderen Zwecken aufbewahren möchten, erstellen Sie einen Screenshot, exportieren Sie die Daten oder laden Sie ein Support-Paket herunter, bevor Sie die Sensoren zurücksetzen.

Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Konfiguration** und anschließend auf **Systemstatus**.
- 2 Klicken Sie auf **Sensoren zurücksetzen**.

Zurücksetzen der Systemstatussensoren bei einer Verbindung mit vCenter Server

Einige Hosthardwaresensoren zeigen Daten an, die über die Zeit akkumuliert werden. Sie können diese Sensoren zurücksetzen, um die gesammelten Daten zu löschen und mit der Erfassung neuer Daten zu beginnen.

Wenn Sie die Sensordaten zur Fehlerbehebung oder anderen Zwecken aufbewahren möchten, erstellen Sie einen Screenshot, exportieren Sie die Daten oder laden Sie ein Support-Paket herunter, bevor Sie die Sensoren zurücksetzen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Stellen Sie sicher, dass das vCenter-Hardwarestatus-Plug-In aktiviert ist.

Vorgehensweise

- 1 Wählen Sie einen Host im Objektnavigator oder der Bestandslistenstruktur aus.
- 2 Klicken Sie auf **Sensoren zurücksetzen**.

Überwachen von Ereignissen, Alarmen und automatisierten Aktionen

vSphere enthält ein vom Benutzer konfigurierbares Subsystem für Ereignisse und Alarme. Dieses Subsystem überwacht alle vSphere-Ereignisse und speichert die Daten in Protokolldateien und der vCenter Server-Datenbank. Mithilfe dieses Subsystems können Sie außerdem die Bedingungen angeben, zu denen die Alarme ausgelöst werden. Alarme können bei geänderten Systembedingungen dafür sorgen, dass sich der Status von milden Warnmeldungen bis hin zu ernsteren Alarmen ändert, und automatische Alarmaktionen auslösen. Diese Funktionalität ist nützlich, wenn Sie darüber informiert werden oder Sofortmassnahmen ergreifen möchten, wenn bei einem bestimmten Bestandslistenobjekt oder einer Gruppe von Objekten bestimmte Ereignisse auftreten oder Bedingungen sich ändern.

Ereignisse

Ereignisse sind Aufzeichnungen von Benutzeraktionen oder Systemaktionen, die auf Objekten in vCenter Server oder auf einem Host ausgeführt werden. Zu den Aktionen, die möglicherweise als Ereignisse aufgezeichnet werden, gehören z. B. Folgende:

- Ein Lizenzschlüssel läuft ab
- Eine virtuelle Maschine wird eingeschaltet
- Ein Benutzer meldet sich bei einer virtuellen Maschine an
- Eine Verbindung zum Host wird unterbrochen

Die Ereignisdaten enthalten Details zum Ereignis, wie z. B. der Name des Benutzers, der es generiert hat, der Zeitpunkt, zu dem es aufgetreten ist, und den Typ des Ereignisses. Es gibt drei Ereignistypen:

- Informationen
- Warnung
- Fehler

Im vSphere-Client werden Ereignisdaten auf der Registerkarte **Aufgaben und Ereignisse** des ausgewählten Bestandslistenobjekts angezeigt. Siehe „[Anzeigen von Ereignissen](#)“, auf Seite 463.

Alarme

Alarme sind Benachrichtigungen, die als Reaktion auf ein Ereignis, eine Menge von Bedingungen oder den Status eines Bestandslistenobjekts aktiviert werden. Eine Alarmdefinition besteht aus den folgenden Elementen:

- Name und Beschreibung - Bietet eine identifizierende Bezeichnung und eine Beschreibung.
- Alarmtyp - Definiert den Typ des Objekts, der überwacht wird.
- Auslöser - Definiert das Ereignis, die Bedingung oder den Status, der den Alarm auslöst, und definiert den Schweregrad der Benachrichtigung.
- Toleranzschwellenwerte (Berichte) - Bietet zusätzliche Einschränkungen für die Schwellenwerte für Bedingungs- und Statusauslöser, die überschritten werden müssen, um den Alarm auszulösen.
- Aktionen - Definiert Vorgänge, die als Reaktion auf ausgelöste Alarme auftreten. VMware stellt Sätze von vordefinierten bestandslistenobjektspezifischen Aktionen zur Verfügung.

Alarme haben die folgenden Schweregradstufen:

- Normal – Grün
- Warnung – Gelb
- Alarm – Rot

Alarmdefinitionen werden mit dem aus der Bestandsliste ausgewählten Objekt verknüpft. Ein Alarm überwacht den Typ der Bestandslistenobjekte, die in ihrer Definition angegeben sind.

Sie möchten beispielsweise die CPU-Nutzung aller virtuellen Maschinen in einem bestimmten Host-Cluster überwachen. Sie können den Cluster aus der Bestandsliste auswählen und ihm eine VM-Alarm hinzufügen. Wenn aktiviert, überwacht der Alarm alle im Cluster ausgeführten virtuellen Maschinen und wird ausgelöst, wenn eine der Maschinen die im Alarm definierten Kriterien erfüllt. Wenn Sie nur eine bestimmte virtuelle Maschine im Cluster überwachen möchten, wählen Sie die virtuelle Maschine aus der Bestandsliste aus und fügen Sie ihr einen Alarm hinzu. Eine einfache Möglichkeit, dieselben Alarme für eine Gruppe von Objekten anzuwenden, besteht darin, die Objekte in einem Ordner zu platzieren und den Alarm für den Ordner zu definieren.

HINWEIS Sie können Alarme nur von dem Objekt aus, in dem der Alarm definiert ist, aktivieren, deaktivieren und anpassen. Wenn Sie beispielsweise einen Alarm in einem Cluster definiert haben, um virtuelle Maschinen zu überwachen, können Sie diesen Alarm nur über den Cluster aktivieren, deaktivieren oder anpassen. Sie können keine Änderungen am Alarm einer einzelnen virtuellen Maschine vornehmen.

Alarmaktionen

Alarmaktionen sind Vorgänge, die als Reaktion auf den Auslöser auftreten. Beispielsweise können Sie festlegen, dass eine E-Mail-Benachrichtigung an einen oder mehrere Administratoren gesendet werden soll, wenn ein Alarm ausgelöst wird.

HINWEIS Für Standardalarme sind keine Aktionen vorkonfiguriert. Sie müssen manuell festlegen, welche Aktionen durchgeführt werden sollen, wenn das Ereignis, die Bedingung oder der Status auftreten, die den Alarm auslösen.

Anzeigen von Ereignissen

Sie können alle vSphere-Ereignisse oder die einem einzelnen Objekt zugewiesenen Ereignisse anzeigen. Die Ereignisliste für ein ausgewähltes Bestandslistenobjekt umfasst Ereignisse für untergeordnete Objekte.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Nur Lesen**

Vorgehensweise

- ◆ Wählen Sie zum Anzeigen einer Liste von Ereignissen, die mit einem ausgewählten Bestandslistenobjekt und seinen untergeordneten Objekten verknüpft sind, die Registerkarte **Aufgaben und Ereignisse** aus und klicken Sie auf **Ereignisse**.
 - a Wählen Sie ein Ereignis aus, um die Ereignisdetails anzuzeigen.
 - b Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.
 - c Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen von Systemprotokollen

Zu den Informationen in den Systemprotokolleinträgen gehören der Name der Person, die das Ereignis generiert hat, der Zeitpunkt, zu dem das Ereignis erstellt wurde, und der Ereignistyp.

Voraussetzungen

Stellen Sie über den vSphere-Client eine Verbindung zu einem ESX/ESXi-Host her.

Erforderliche Berechtigung: **Global. Diagnose**.

Vorgehensweise

- 1 Wählen Sie zum Anzeigen der Systemprotokolleinträge **Home > Verwaltung > Systemprotokolle**.
- 2 Wählen Sie das Protokoll im Dropdown-Menü aus.
- 3 (Optional) Klicken Sie auf **Alle anzeigen** oder **Nächste # Zeilen anzeigen**, um zusätzliche Protokolleinträge anzuzeigen.
- 4 (Optional) Filtern Sie die Protokolleinträge.
 - a Wählen Sie **Ansicht > Filtern** aus.
 - b Geben Sie die Filterkriterien in das Feld „Filter“ ein.

Exportieren von Ereignisdaten

Sie können alle oder einen Teil der Ereignisse exportieren, die in der vCenter Server-Datenbank gespeichert sind.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Nur Lesen**

Vorgehensweise

- 1 Wählen Sie **Datei > Exportieren > Ereignisse exportieren**.

- 2 (Nur verknüpfter Modus) Wählen Sie in der **vCenter Server**-Liste den Server aus, auf dem die Ereignisse aufgetreten sind.
- 3 Geben Sie Ereignis-, Zeit- und Limit-Attribute für die Ereignisse an, die Sie exportieren möchten.
- 4 Geben Sie einen Dateinamen und einen Speicherort an.
- 5 Klicken Sie auf **OK**.

vCenter Server erstellt die Datei am angegebenen Speicherort. Die Datei enthält **Typ**, **Uhrzeit** und **Beschreibung** der Ereignisse.

Anzeigen von ausgelösten Alarmen und Alarmdefinitionen

Ausgelöste Alarme sind an mehreren Stellen des vSphere-Clients und des vSphere Web Client sichtbar.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- Klicken Sie zum Anzeigen aller ausgelösten Alarme in der Statusleiste auf **Alarme**.
- Wählen Sie zum Anzeigen von Alarmen, die auf einem ausgewählten Bestandslistenobjekt ausgelöst wurden, auf der Registerkarte **Alarme** die Option > **Ausgelöste Alarme**.
- Wählen Sie zum Anzeigen einer Liste von Alarmen, die mit dem ausgewählten Bestandslistenobjekt verknüpft sind, auf der Registerkarte **Alarme** die Option > **Definitionen**. In der Spalte **Definiert in** wird das Objekt angezeigt, für das der Alarm gesetzt wurde..

Einrichten eines Alarms

Sie können Bestandslistenobjekte überwachen, indem Sie Alarme für sie einrichten. Wählen Sie zum Einrichten eines Alarms den Typ des zu überwachenden Bestandslistenobjekts aus, legen Sie fest, wann und für wie lange der Alarm ausgelöst wird, und definieren Sie die Aktionen, die ausgeführt werden, wenn der Alarm ausgelöst wird. Alarme werden im Dialogfeld „Alarmeinstellungen“ definiert.

Voraussetzungen

Stellen Sie sicher, dass Sie über eine Verbindung mit einem vCenter Server-System verfügen, indem Sie den vSphere-Client verwenden.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

- [Anzeigen und Bearbeiten der Alarmeinstellungen](#) auf Seite 465
Alarme werden im Dialogfeld „Alarmeinstellungen“ erstellt und geändert. Sie können von jedem Objekt aus Alarmeinstellungen anzeigen, allerdings können Sie die Einstellungen nur über das Objekt ändern, auf dem der Alarm definiert ist.
- [Angaben von Alarmname, -definition und -typ](#) auf Seite 466
Zu den allgemeinen Einstellungen gehören Alarmname, Beschreibung und Typ. Zudem können Sie auf der Registerkarte „Allgemein“ den Alarm aktivieren und deaktivieren. Wählen Sie beim Angeben des Alarmtyps den Typ des Bestandslistenobjekts und den Aktivitätstyp (Ereignisse oder Bedingungen und Statuszustände) aus, den Sie überwachen möchten. Die Optionen auf der Registerkarte „Auslöser“ ändern sich je nach dem zu überwachenden Aktivitätentyp, den Sie auswählen.

- [Angeben, wie der Alarm ausgelöst wird \(Bedingungs- oder statusbasiert\)](#) auf Seite 466

Auf der Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“ können Sie die Ereignisse, die Statuszustände und die Bedingungen angeben, die den Alarm auslösen. Die Optionen, die Sie auf der Registerkarte „Allgemein“ des Dialogfelds „Alarmeinstellungen“ auswählen, bestimmen die Optionen, die auf Registerkarte „Auslöser“ zur Verfügung stehen. Eine Alarmdefinition muss mindestens einen Auslöser enthalten, damit Sie gespeichert werden kann.

- [Angeben, wie der Alarm ausgelöst wird \(ereignisbasiert\)](#) auf Seite 467

Auf der Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“ können Sie die Ereignisse, die Statuszustände und die Bedingungen angeben, die den Alarm auslösen. Die Optionen, die Sie auf der Registerkarte „Allgemein“ des Dialogfelds „Alarmeinstellungen“ auswählen, bestimmen die Optionen, die auf Registerkarte „Auslöser“ zur Verfügung stehen. Eine Alarmdefinition muss mindestens einen Auslöser enthalten, damit Sie gespeichert werden kann.

- [Angeben der Alarmtoleranz und Häufigkeit](#) auf Seite 468

Sie können die Berichterstellungsfunktionen zum Anwenden eines Toleranzbereichs für die Alarmauslöser verwenden. Dies kann hilfreich sein, um vorübergehende Probleme von schwerwiegenden, chronischen Problemen zu unterscheiden. Mithilfe der Berichtseinstellungen können Sie einen Wert angeben, um den eine Bedingung oder Zustand den Auslöserwert überschreiten muss, damit der Alarm ausgelöst wird.

- [Die im Auslösungsfall auszuführenden Aktionen angeben](#) auf Seite 468

Sie können die Aktionen angeben, die das System bei Auslösung eines Alarms oder bei einer Statusänderung durchführt. Sie können Alarme und Alarmaktionen unabhängig voneinander aktivieren und deaktivieren.

- [Aktivieren und Deaktivieren von Alarmaktionen](#) auf Seite 474

Sie können Alarmaktionen für jedes Bestandslistenobjekt deaktivieren. Alarmaktionen werden nicht wie Alarme deaktiviert, noch ist es dasselbe wie das Bestätigen von Alarmen. Wenn Alarmaktionen deaktiviert werden, kann der Alarm zwar nach wie vor ausgelöst werden, aber seine zugewiesenen Aktionen werden nicht ausgeführt. Sie werden möglicherweise Alarmaktionen deaktivieren, wenn Sie beispielsweise vorhaben, einen Host in den Wartungsmodus zu versetzen. Wenn Sie Alarmaktionen auf einem ausgewählten Bestandslistenobjekt deaktivieren, werden alle Aktionen für alle Alarme auf diesem Objekt deaktiviert. Es ist nicht möglich, eine Teilmenge der Alarmaktionen zu deaktivieren. Alarmaktionen gelten weiterhin für die untergeordneten Objekte.

Anzeigen und Bearbeiten der Alarmeinstellungen

Alarme werden im Dialogfeld „Alarmeinstellungen“ erstellt und geändert. Sie können von jedem Objekt aus Alarmeinstellungen anzeigen, allerdings können Sie die Einstellungen nur über das Objekt ändern, auf dem der Alarm definiert ist.

Voraussetzungen

Stellen Sie sicher, dass Sie über eine Verbindung mit einem vCenter Server-System verfügen, indem Sie den vSphere-Client verwenden.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- ◆ Öffnen Sie zum Anzeigen oder Ändern der Alarmeinstellungen das Dialogfeld „Alarmeinstellungen“:

Option	Beschreibung
Erstellen eines neuen Alarms	Wählen Sie ein Bestandslistenobjekt und anschließend Datei > Neu > Alarm aus.
Alarm zum Objekt hinzufügen	Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt und wählen Sie Alarm > Alarm hinzufügen .
Anzeigen von Alarmdefinitionen	Wählen Sie die Registerkarte Alarme aus, klicken Sie auf die Unterregisterkarte Definitionen des Bestandslistenelements mit dem gewünschten Alarm und doppelklicken Sie auf einen Alarm in der Liste.

Angeben von Alarmname, -definition und -typ

Zu den allgemeinen Einstellungen gehören Alarmname, Beschreibung und Typ. Zudem können Sie auf der Registerkarte „Allgemein“ den Alarm aktivieren und deaktivieren. Wählen Sie beim Angeben des Alarmtyps den Typ des Bestandslistenobjekts und den Aktivitätstyp (Ereignisse oder Bedingungen und Statuszustände) aus, den Sie überwachen möchten. Die Optionen auf der Registerkarte „Auslöser“ ändern sich je nach dem zu überwachenden Aktivitätstyp, den Sie auswählen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt und wählen Sie **Alarme > Alarm hinzufügen**.
- 2 Geben Sie einen Namen und eine Beschreibung ein.
- 3 Wählen Sie den Typ des Bestandslistenobjekts aus, den dieser Alarm überwachen soll.
- 4 Wählen Sie den Aktivitätstyp aus, den dieser Alarm überwachen soll.
Die Optionen auf der Registerkarte **Auslöser** ändern sich je nach dem Aktivitätstyp, den Sie auswählen.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu beenden, oder wählen Sie eine andere Registerkarte aus, um weitere Änderungen am Alarm vorzunehmen.

Weiter

HINWEIS Ein Alarm, für den keine Auslöser definiert wurden, kann nicht gespeichert werden.

Angeben, wie der Alarm ausgelöst wird (Bedingungs- oder statusbasiert)

Auf der Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“ können Sie die Ereignisse, die Statuszustände und die Bedingungen angeben, die den Alarm auslösen. Die Optionen, die Sie auf der Registerkarte „Allgemein“ des Dialogfelds „Alarmeinstellungen“ auswählen, bestimmen die Optionen, die auf der Registerkarte „Auslöser“ zur Verfügung stehen. Eine Alarmdefinition muss mindestens einen Auslöser enthalten, damit Sie gespeichert werden kann.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Öffnen Sie die Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“. Siehe „[Angeben von Alarmname, -definition und -typ](#)“, auf Seite 466.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Wählen Sie den Auslöser aus, den Sie ändern möchten, oder klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen.
- 2 Klicken Sie auf die Spalte **Auslösertyp** und wählen Sie eine Option aus dem Dropdown-Menü aus.
- 3 Klicken Sie auf die Spalte **Bedingung** und wählen Sie eine Option aus dem Dropdown-Menü aus.
- 4 Klicken Sie auf die Spalte **Warnung** und wählen Sie eine Option aus dem Dropdown-Menü aus, um den Schwellenwert für das Auslösen einer Warnung festzulegen.
- 5 (Optional) Klicken Sie auf die Spalte **Bedingungslänge** und wählen Sie eine Option aus dem Dropdown-Menü aus.
- 6 Klicken Sie auf die Spalte **Alarm** und wählen Sie eine Option aus dem Dropdown-Menü aus, um den Schwellenwert für das Auslösen einer Warnung festzulegen.
- 7 (Optional) Klicken Sie auf die Spalte **Bedingungslänge** und wählen Sie eine Option aus dem Dropdown-Menü aus.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, fügen Sie optional weitere Auslöser hinzu, oder konfigurieren Sie eine oder mehrere der folgenden Optionen für diesen Alarm:

- Schwellenwerte für Alarmwiederholungen
- Häufigkeit der Alarmwiederholungen
- Alarmaktionen
- Häufigkeit der Alarmaktion

Angeben, wie der Alarm ausgelöst wird (ereignisbasiert)

Auf der Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“ können Sie die Ereignisse, die Statuszustände und die Bedingungen angeben, die den Alarm auslösen. Die Optionen, die Sie auf der Registerkarte „Allgemein“ des Dialogfelds „Alarmeinstellungen“ auswählen, bestimmen die Optionen, die auf Registerkarte „Auslöser“ zur Verfügung stehen. Eine Alarmdefinition muss mindestens einen Auslöser enthalten, damit Sie gespeichert werden kann.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Öffnen Sie die Registerkarte „Auslöser“ des Dialogfelds „Alarmeinstellungen“.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Wählen Sie den Auslöser aus, den Sie ändern möchten, oder klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen.
- 2 Klicken Sie auf die Spalte **Ereignis** und wählen Sie eine Option aus dem Dropdown-Menü aus.
- 3 Klicken Sie auf die Spalte **Status** und wählen Sie eine Option aus dem Dropdown-Menü aus.

- 4 (Optional) Klicken Sie auf **Erweitert** in der Spalte **Bedingungen**, um zusätzliche Bedingungen zu konfigurieren, die erfüllt werden müssen, damit der Alarm ausgelöst wird.
 - a Klicken Sie auf **Hinzufügen**, um ein Argument hinzuzufügen.
 - b Klicken Sie auf die Spalte **Argument** und wählen Sie eine Option aus dem Dropdown-Menü aus.
 - c Klicken Sie auf die Spalte **Operator** und wählen Sie eine Option aus dem Dropdown-Menü aus.
 - d Klicken Sie auf die Spalte **Wert** und geben Sie einen Wert in das Textfeld ein.
 - e Fügen Sie mehr Argumente hinzu oder klicken Sie auf **OK**, um das Dialogfeld zu beenden und zum Dialogfeld „Alarmeinstellungen“ zurückzukehren.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, oder fügen Sie optional weitere Auslöser hinzu bzw. konfigurieren Sie weitere Alarmaktionen.

Angeben der Alarmtoleranz und Häufigkeit

Sie können die Berichterstellungsfunktionen zum Anwenden eines Toleranzbereichs für die Alarmauslöser verwenden. Dies kann hilfreich sein, um vorübergehende Probleme von schwerwiegenden, chronischen Problemen zu unterscheiden. Mithilfe der Berichtseinstellungen können Sie einen Wert angeben, um den eine Bedingung oder Zustand den Auslöserwert überschreiten muss, damit der Alarm ausgelöst wird.

Zu den Berichtseinstellungen gehören der Bereich und die Häufigkeit. Der Bereich ist der Schwellenwert, um den die überwachte Bedingung oder der überwachte Status die angegebene Auslösergrenze überschreiten muss, damit der Alarm ausgelöst wird. Die Häufigkeit stellt die Dauer zwischen jedem Neuauslösen dar, solange die Bedingung oder der Status besteht. Die Registerkarte **Berichte** ist für Alarme mit ereignis-basierenden Auslösern deaktiviert.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Öffnen Sie die Registerkarte „Berichte“ des Dialogfelds „Alarmeinstellungen“.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 (Optional) Geben Sie an, um wie weit die Bedingungen die Auslösergrenzen über- bzw. unterschreiten müssen, damit der Alarm erneut ausgelöst wird.
- 2 (Optional) Wählen Sie eine **Häufigkeit**.

Die Häufigkeit legt den Zeitraum fest, während dessen ein ausgelöster Alarm nicht erneut gemeldet wird. Nach Ablauf des Zeitraums wird der Alarm erneut gemeldet, wenn die Bedingung oder der Status noch wahr ist.

Weiter

Geben Sie optional Alarmaktionen an oder klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu beenden.

Die im Auslösungsfall auszuführenden Aktionen angeben

Sie können die Aktionen angeben, die das System bei Auslösung eines Alarms oder bei einer Statusänderung durchführt. Sie können Alarme und Alarmaktionen unabhängig voneinander aktivieren und deaktivieren.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Öffnen Sie die Registerkarte „Aktionen“ des Dialogfelds „Alarmeinstellungen“.

Stellen Sie sicher, dass vCenter Server ordnungsgemäß für die Verwendung von SNMP-E-Mail- oder Trap-Benachrichtigungen als Alarmaktion konfiguriert ist.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

■ [Senden einer E-Mail als Alarmaktion](#) auf Seite 470

Der im Lieferumfang von vCenter Server enthaltene SMTP-Agent kann zum Senden von E-Mail-Benachrichtigungen verwendet werden, wenn Alarme ausgelöst werden.

■ [Senden von SNMP-Traps als Alarmaktion](#) auf Seite 471

Der im Lieferumfang von vCenter Server enthaltene SNMP-Agent kann zum Senden von Traps verwendet werden, wenn Alarme auf einem vCenter Server ausgelöst werden. Die vorgegebenen Hardwarestatusalarme senden standardmäßig SNMP-Traps.

■ [Ausführen eines Skripts oder eines Befehls als Alarmaktion](#) auf Seite 472

Sie können einen Alarm so konfigurieren, dass ein Skript oder ein Befehl ausgeführt wird, wenn der Alarm ausgelöst wird.

Vorgehensweise

- 1 Wählen Sie die Aktion aus, die Sie ändern möchten, oder klicken Sie auf **Hinzufügen**, um eine Aktion hinzuzufügen.
- 2 Klicken Sie auf die Spalte **Aktion** und wählen Sie eine Option aus dem Dropdown-Menü aus.
- 3 Klicken Sie in die Spalte **Konfiguration** und geben Sie Konfigurationsinformationen für diejenigen Aktionen ein, für die zusätzliche Informationen benötigt werden:

Option	Aktion
E-Mail-Benachrichtigung senden	Geben Sie E-Mail-Adressen ein, wobei Sie diese durch ein Komma trennen, und drücken Sie die Eingabetaste .
Migrieren einer VM	Führen Sie die Schritte des Assistenten für das Migrieren einer virtuellen Maschine aus.
Befehl ausführen	<p>Führen Sie eine der folgenden Aktionen aus und drücken Sie die Eingabetaste:</p> <ul style="list-style-type: none"> ■ Wenn der Befehl eine .exe-Datei ist, geben Sie den vollständigen Pfadnamen des Befehls ein und setzen Sie die Parameter. Geben Sie beispielsweise Folgendes ein, um den Befehl cmd.exe im Verzeichnis C:\tools mit den Parametern alarmName und targetName auszuführen: c:\tools\cmd.exe alarmName targetName ■ Wenn der Befehl eine .bat-Datei ist, geben Sie den vollständigen Pfadnamen des Befehls als Argument für den Befehl c:\windows\system32\cmd.exe ein. Fügen Sie ggf. Parameter hinzu. Geben Sie beispielsweise Folgendes ein, um den Befehl cmd.bat im Verzeichnis C:\tools mit den Parametern alarmName und targetName auszuführen: c:\windows\system32\cmd.exe /c c:\tools\cmd.bat alarmName targetName <p>Für .bat-Dateien müssen der Befehl und seine Parameter als Zeichenfolge angegeben werden.</p>

- 4 (Optional) Geben Sie in jeder Spalte für die Alarmstatusänderung an, ob der Alarm ausgelöst werden soll, wenn sich der Alarmstatus ändert.

Manche Aktionen unterstützen das Neuauslösen beim Ändern des Alarmstatus nicht.

- 5 Geben Sie für Wiederholungsaktionen im Feld **Wiederholen nach** das Zeitintervall für die Wiederholung ein.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, oder navigieren Sie zu einer anderen Registerkarte, um weitere Änderungen vorzunehmen.

Senden einer E-Mail als Alarmaktion

Der im Lieferumfang von vCenter Server enthaltene SMTP-Agent kann zum Senden von E-Mail-Benachrichtigungen verwendet werden, wenn Alarime ausgelöst werden.

Voraussetzungen

Stellen Sie sicher, dass der SMTP-Agent von vCenter Server ordnungsgemäß für das Versenden von E-Mail-Benachrichtigungen konfiguriert ist.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Klicken Sie auf der Registerkarte „Aktionen“ des Dialogfelds „Alarmeinstellungen“ auf „Hinzufügen“, um eine Aktion hinzuzufügen.
- 2 Wählen Sie in der Spalte **Aktionen** die Option **E-Mail-Benachrichtigung senden** aus dem Dropdown-Menü aus.
- 3 Geben Sie in der Spalte **Konfiguration** die Adressen der Empfänger ein. Verwenden Sie Kommas zum Trennen mehrerer Adressen.
- 4 (Optional) Konfigurieren Sie Alarmübergänge und die Häufigkeit. Weitere Informationen hierzu finden Sie unter „[Die im Auslösungsfall auszuführenden Aktionen angeben](#)“, auf Seite 468.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, oder navigieren Sie zu einer anderen Registerkarte, um weitere Änderungen vorzunehmen.

vCenter Server-E-Mail-Agent-Benachrichtigungen

In den folgenden Tabellen werden die Informationen beschrieben, die in alarm- und ereignisbasierenden E-Mail-Benachrichtigungen enthalten sind. In der ersten Tabelle werden die Informationen beschrieben, die in allen E-Mail-Benachrichtigungen enthalten sind. Die zweite Tabelle enthält zusätzliche Informationen, die in ereignisbasierenden Benachrichtigungen enthalten sind.

Tabelle 28-1. Allgemeine Details zu SNMP-E-Mail-Benachrichtigungen

E-Mail-Eintrag	Beschreibung
Ziel	Objekt, für das der Alarm ausgelöst wurde.
Alter Status	Vorheriger Alarmstatus. Gilt nur für Statusauslöser.
Neuer Status	Aktueller Alarmstatus. Gilt nur für Statusauslöser.
Metrischer Wert	Schwellenwert zum Auslösen des Alarms. Gilt nur für metrische Bedingungsauflöser.
Alarmdefinition	Alarmdefinition in vCenter Server, einschließlich des Alarmnamens und des Status.
Beschreibung	Lokalisierte Zeichenfolge, die eine Zusammenfassung des Alarms enthält. Beispiel: Alarm Neuer_Alarm auf Host1.vmware.com geändert von Grau in Rot.

Tabelle 28-2. Zusätzliche Details zur Benachrichtigung für von Ereignissen ausgelöste Alarime

Detail	Beschreibung
Ereignisdetails	Name des VMODL-Ereignistyps.
Übersicht	Alarmzusammenfassung, einschließlich des Ereignistyps, Alarmnamens und Zielobjekts.

Tabelle 28-2. Zusätzliche Details zur Benachrichtigung für von Ereignissen ausgelöste Alarmen (Fortsetzung)

Detail	Beschreibung
Datum	Uhrzeit und Datum der Auslösung des Alarms.
Benutzername	Person, die die Aktion initiiert hat, aufgrund der das Ereignis erstellt wurde. Ereignisse, die durch eine interne Systemaktivität verursacht wurden, haben keinen Wert für Benutzernamen.
Host	Host, auf dem der Alarm ausgelöst wurde.
Ressourcenpool	Ressourcenpool, in dem der Alarm ausgelöst wurde.
Datencenter	Datencenter, in dem der Alarm ausgelöst wurde.
Argumente	Mit dem Alarm übergebene Argumente und deren Werte.

Senden von SNMP-Traps als Alarmaktion

Der im Lieferumfang von vCenter Server enthaltene SNMP-Agent kann zum Senden von Traps verwendet werden, wenn Alarme auf einem vCenter Server ausgelöst werden. Die vorgegebenen Hardwarestatusalarms senden standardmäßig SNMP-Traps.

Voraussetzungen

Stellen Sie sicher, dass die vCenter Server- und ESXi-SNMP-Agenten ordnungsgemäß konfiguriert sind.

Stellen Sie sicher, dass die SNMP-Trap-Empfängeragenten ordnungsgemäß konfiguriert sind.

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Klicken Sie auf der Registerkarte „Aktionen“ im Dialogfeld „Alarmeinstellungen“ auf **Hinzufügen**.
- 2 Wählen Sie in der Spalte **Aktionen** die Option **Trap-Benachrichtigung senden** aus dem Dropdown-Menü aus.
- 3 (Optional) Konfigurieren Sie Alarmübergänge und die Häufigkeit.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, oder navigieren Sie zu einer anderen Registerkarte, um weitere Änderungen vorzunehmen.

SNMP-Trap-Benachrichtigungen

In der folgenden Tabelle werden die Informationen beschrieben, die in den vCenter Server- und ESXi-Trap-Benachrichtigungen enthalten sind.

Tabelle 28-3. SNMP-Trap-Benachrichtigung - Details

Trap-Eintrag	Beschreibung
Typ	Der Status, den vCenter Server für den Alarm überwacht. Überwacht werden können die Nutzung des Hostprozessors (oder der CPU), die Nutzung des Hostspeichers, der Hoststatus, die Nutzung des Prozessors (oder der CPU) der virtuellen Maschine, die Nutzung des Speichers der virtuellen Maschine, der Status der virtuellen Maschine und das Taktsignal der virtuellen Maschine.
Name	Der Name des Hosts oder der virtuellen Maschine, der bzw. die den Alarm auslöst.
Alter Status	Der Alarmstatus, bevor der Alarm ausgelöst wurde.
Neuer Status	Der Alarmstatus, wenn der Alarm ausgelöst wird.
Objektwert	Der Objektwert, wenn der Alarm ausgelöst wird.

Ausführen eines Skripts oder eines Befehls als Alarmaktion

Sie können einen Alarm so konfigurieren, dass ein Skript oder ein Befehl ausgeführt wird, wenn der Alarm ausgelöst wird.

Verwenden Sie die Alarmumgebungsvariablen, um komplexe Skripts zu definieren und sie mehreren Alarmen oder Bestandslistenobjekten zuzuweisen. Sie können z. B. ein Skript schreiben, anhand dem die folgenden Trouble-Ticket-Informationen in ein externes System eingetragen werden, wenn ein Alarm ausgelöst wird:

- Alarmname
- Objekt, für das der Alarm ausgelöst wurde
- Ereignis, das den Alarm ausgelöst hat
- Werte für die Alarmauslösung

Verwenden Sie beim Schreiben des Skripts die folgenden Umgebungsvariablen:

- VMWARE_ALARM_NAME
- VMWARE_ALARM_TARGET_NAME
- VMWARE_ALARM_EVENTDESCRIPTION
- VMWARE_ALARM_ALARMVALUE

Sie können das Skript jedem Alarm für ein Objekt zuweisen, ohne das Skript ändern zu müssen.

Voraussetzungen

Erforderliche Berechtigung: **Alarme.Alarm erstellen** oder **Alarme.Alarm ändern**

Vorgehensweise

- 1 Klicken Sie auf der Registerkarte „Aktionen“ des Dialogfelds „Alarmeinstellungen“ auf **Hinzufügen**, um eine Aktion hinzuzufügen.
- 2 Wählen Sie in der Spalte **Aktionen** die Option **Befehl ausführen** aus dem Dropdown-Menü aus.
- 3 Geben Sie in der Spalte **Konfiguration** die Skript- bzw. Befehlsinformationen ein:

Für diesen Typ des Befehls...	Geben Sie Folgendes ein...
EXE - ausführbare Dateien	Vollständiger Pfadname des Befehls. Geben Sie beispielsweise Folgendes ein, um den Befehl <code>cmd.exe</code> im Verzeichnis <code>C:\tools</code> auszuführen: <code>c:\tools\cmd.exe</code>
BAT - Stapeldatei	Vollständiger Pfadname des Befehls als Argument für den Befehl <code>c:\windows\system32\cmd.exe</code> . Geben Sie beispielsweise Folgendes ein, um den Befehl <code>cmd.bat</code> im Verzeichnis <code>C:\tools</code> auszuführen: <code>c:\windows\system32\cmd.exe /c c:\tools\cmd.bat</code> HINWEIS Der Befehl und seine Parameter müssen als eine Zeichenfolge angegeben werden.

Wenn Ihr Skript nicht die Alarmumgebungsvariablen verwendet, fügen Sie alle erforderlichen Parameter im Konfigurationsfeld hinzu. Beispiel:

```
c:\tools\cmd.exe AlarmName targetName
c:\windows\system32\cmd.exe /c c:\tools\cmd.bat alarmName targetName
```

- 4 (Optional) Konfigurieren Sie Alarmübergänge und die Häufigkeit. Siehe [„Die im Auslösungsfall auszuführenden Aktionen angeben“](#), auf Seite 468.

Weiter

Klicken Sie auf **OK**, um die Alarmdefinition zu speichern und das Dialogfeld zu beenden, oder navigieren Sie zu einer anderen Registerkarte, um weitere Änderungen vorzunehmen.

Alarmumgebungsvariablen für Skripts

Um die Skriptkonfiguration für Alarmaktionen zu vereinfachen, bietet VMware Umgebungsvariablen für VMware-Alarme. Mit den Variablen können Sie komplexere Skripts definieren und sie mehreren Alarmen oder Bestandslistenobjekten zuweisen, damit die Alarmaktion beim Auslösen des Alarms ausgeführt wird.

Tabelle 28-4. Alarmumgebungsvariablen

Variablenname	Variablenbeschreibung	Unterstützter Alarmtyp
VMWARE_ALARM_NAME	Der Name des ausgelösten Alarms.	Bedingung, Status, Ereignis
VMWARE_ALARM_ID	Die MOID des ausgelösten Alarms.	Bedingung, Status, Ereignis
VMWARE_ALARM_TARGET_NAME	Der Name des Elements, für das der Alarm ausgelöst wird.	Bedingung, Status, Ereignis
VMWARE_ALARM_TARGET_ID	Die MOID des Elements, für das der Alarm ausgelöst wird.	Bedingung, Status, Ereignis
VMWARE_ALARM_OLDSTATUS	Der alte Status des Alarms.	Bedingung, Status, Ereignis
VMWARE_ALARM_NEWSTATUS	Der neue Status des Alarms.	Bedingung, Status, Ereignis
VMWARE_ALARM_TRIGGERINGSUMMARY	Eine mehrzeilige Zusammenfassung des Alarms.	Bedingung, Status, Ereignis
VMWARE_ALARM_DECLARINGSUMMARY	Eine einzeilige Deklaration des Alarmausdrucks.	Bedingung, Status, Ereignis
VMWARE_ALARM_ALARMVALUE	Der Wert, der den Alarm auslöst hat.	Bedingung, Status
VMWARE_ALARM_EVENTDESCRIPTION	Eine Beschreibung für das Alarmstatus-Änderungsereignis.	Bedingung, Status
VMWARE_ALARM_EVENTDESCRIPTION	Eine Beschreibung des Ereignisses, das den Alarm ausgelöst hat.	Ereignis
VMWARE_ALARM_EVENT_USERNAME	Der Benutzername, der dem Ereignis zugewiesen ist.	Ereignis
VMWARE_ALARM_EVENT_DATACENTER	Der Name des Datacenters, in dem das Ereignis aufgetreten ist.	Ereignis
VMWARE_ALARM_EVENT_COMPUTERESOURCE	Der Name des Clusters oder Ressourcenpools, in dem das Ereignis aufgetreten ist.	Ereignis
VMWARE_ALARM_EVENT_HOST	Der Name des Hosts, auf dem das Ereignis aufgetreten ist.	Ereignis
VMWARE_ALARM_EVENT_VM	Der Name der virtuellen Maschine, auf der das Ereignis aufgetreten ist.	Ereignis
VMWARE_ALARM_EVENT_NETWORK	Der Name des Netzwerks, in dem das Ereignis aufgetreten ist.	Ereignis

Tabelle 28-4. Alarmumgebungsvariablen (Fortsetzung)

Variablenname	Variablenbeschreibung	Unterstützter Alarmtyp
VMWARE_ALARM_EVENT_DATASTORE	Der Name des Datenspeichers, auf dem das Ereignis aufgetreten ist.	Ereignis
VMWARE_ALARM_EVENT_DVS	Der Name des vSphere Distributed Switch, auf dem das Ereignis aufgetreten ist.	Ereignis

Befehlszeilenparameter für Alarme

VMware bietet Befehlszeilenparameter, die die Standard-Alarmumgebungsvariablen ersetzen. Sie können diese Parameter verwenden, wenn Sie ein Skript als Alarmaktion für eine Bedingung, einen Status oder einen Ereignisalarm ausführen.

Mit den Befehlszeilenparametern können Sie Alarminformationen weiterleiten, ohne ein Alarmskript ändern zu müssen. Sie können diese Parameter z. B. einsetzen, wenn Sie ein externes Programm verwenden, für das Sie über keine Quelldateien verfügen. Sie übergeben die erforderlichen Daten, indem Sie die Ersetzungsparameter verwenden, die Vorrang haben vor den Umgebungsvariablen. Die Parameter können Sie über das Dialogfeld **Konfiguration** im Alarmdefinitionsassistenten oder von der Befehlszeile aus übergeben.

Tabelle 28-5. Befehlszeilenparameter für Alarmaktionsskripts

Variable	Beschreibung
{eventDescription}	Der Text des alarmStatusChange-Ereignisses. Die Variable {eventDescription} wird nur für Bedingungs- und Statusalarme unterstützt.
{targetName}	Der Name des Elements, für das der Alarm ausgelöst wird.
{alarmName}	Der Name des Alarms, der ausgelöst wird.
{triggeringSummary}	Eine Zusammenfassung der Werte für den Alarmauslöser.
{declaringSummary}	Eine Zusammenfassung der Werte für die Alarmdeklaration.
{oldStatus}	Der Alarmstatus, bevor der Alarm ausgelöst wird.
{newStatus}	Der Alarmstatus, nachdem der Alarm ausgelöst wurde.
{target}	Das Bestandslistenobjekt, für das der Alarm festgelegt ist.

Aktivieren und Deaktivieren von Alarmaktionen

Sie können Alarmaktionen für jedes Bestandslistenobjekt deaktivieren. Alarmaktionen werden nicht wie Alarme deaktiviert, noch ist es dasselbe wie das Bestätigen von Alarmen. Wenn Alarmaktionen deaktiviert werden, kann der Alarm zwar nach wie vor ausgelöst werden, aber seine zugewiesenen Aktionen werden nicht ausgeführt. Sie werden möglicherweise Alarmaktionen deaktivieren, wenn Sie beispielsweise vorhaben, einen Host in den Wartungsmodus zu versetzen. Wenn Sie Alarmaktionen auf einem ausgewählten Bestandslistenobjekt deaktivieren, werden alle Aktionen für alle Alarme auf diesem Objekt deaktiviert. Es ist nicht möglich, eine Teilmenge der Alarmaktionen zu deaktivieren. Alarmaktionen gelten weiterhin für die untergeordneten Objekte.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Alarm.Alarmaktion deaktivieren**

Vorgehensweise

- Klicken Sie zum Deaktivieren von Alarmaktionen mit der rechten Maustaste auf das Bestandslistenobjekt und wählen Sie **Alarm > Alarmaktionen deaktivieren**.

- Klicken Sie zum Aktivieren von Alarmaktionen mit der rechten Maustaste auf das Bestandslistenobjekt und wählen Sie **Alarm > Alarmaktionen aktivieren**.

Bestätigen von ausgelösten Alarmen

Wenn ein Alarm bestätigt wird, werden seine Alarmaktionen eingestellt. Alarme werden weder gelöscht noch zurückgesetzt, wenn sie bestätigt werden.

Durch das Bestätigen eines Alarms teilen Sie anderen Benutzern mit, dass Sie das Problem übernehmen. Als Beispiel dient ein Host, auf dem ein Alarm zum Überwachen der CPU-Nutzung eingerichtet ist. Wird er ausgelöst, wird eine E-Mail an den Administrator gesendet. Die CPU-Nutzung steigt rasant an und löst somit den Alarm aus. Eine E-Mail wird daraufhin an den Administrator des Hosts gesendet. Der Administrator bestätigt den ausgelösten Alarm, um anderen Administratoren mitzuteilen, dass er an dem Problem arbeitet, und um zu verhindern, dass der Alarm weitere E-Mails sendet. Der Alarm ist aber nach wie vor im System sichtbar.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Alarm.Alarm bestätigen**

Vorgehensweise

- 1 Navigieren Sie zum Bestandslistenbereich.
- 2 Falls der Statusbereich nicht verfügbar ist, wählen Sie **Ansicht > Statusleiste**, um den Statusbereich anzuzeigen.
- 3 Klicken Sie in der Statusleiste auf **Alarme**, um das Fenster „Ausgelöste Alarme“ anzuzeigen.
- 4 Klicken Sie mit der rechten Maustaste auf den Alarm und wählen Sie **Alarm bestätigen**.

Wenn Sie mehrere Alarme gleichzeitig bestätigen möchten, halten Sie die Umschalttaste gedrückt, klicken Sie auf die einzelnen Alarme, um sie auszuwählen, klicken Sie mit der rechten Maustaste auf die ausgewählten Objekte und wählen Sie **Alarm bestätigen**.

Zurücksetzen ausgelöster Ereignisalarme

Ein durch ein Ereignis ausgelöster Alarm wird möglicherweise nicht in den normalen Status zurückgesetzt, wenn vCenter Server das Ereignis, das die normale Bedingung identifiziert, nicht abrufen. Setzen Sie in solchen Fällen den Alarm manuell zurück, um ihn in den normalen Status zurückzusetzen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Erforderliche Berechtigung: **Alarm.Alarmstatus festlegen**

Vorgehensweise

- 1 Suchen Sie den ausgelösten Alarm für das Objekt im Fenster Ausgelöste Alarme oder auf der Registerkarte **Alarme**.
- 2 Klicken Sie mit der rechten Maustaste auf den Alarm und wählen Sie **Alarm auf Grün zurücksetzen**.

Identifizieren deaktivierter Alarmaktionen

Falls Probleme mit Alarmaktionen für ein bestimmtes Bestandslistenobjekt auftreten, stellen Sie sicher, dass Alarmaktionen für das Objekt aktiviert sind.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie je nach dem Gültigkeitsbereich der Objekte, die Sie untersuchen möchten, ein übergeordnetes Objekt aus.
 - vCenter Server
 - Datacenter
 - Cluster
 - Host
 - Virtueller Switch
 - Datenspeicher-Cluster
- 2 Wählen Sie die Registerkarte, die den untergeordneten Objekten entspricht, die Sie untersuchen möchten.

Wenn beispielsweise das ausgewählte Bestandslistenobjekt ein Datacenter ist, wählen Sie die Registerkarte „Hosts“.
- 3 Navigieren Sie zur Spalte **Alarmaktionen**.

Möglicherweise müssen Sie horizontal blättern, um die Spalte in den sichtbaren Bereich zu holen.

Der Wert in der Spalte **Alarmaktionen** gibt an, ob Alarmaktionen für die aufgeführten Objekte aktiviert oder deaktiviert sind.

Anzeigen von Lösungen

Sie können Lösungen, die in einer vCenter Server-Instanz installiert wurden, mit vCenter Solutions Manager bereitstellen, überwachen und mit ihnen arbeiten. Der Solutions Manager zeigt Informationen über den Status einer Lösung an.

Sie können von der Startseite des vSphere-Client aus zum Solutions Manager navigieren. In der Solutions Manager-Ansicht werden Informationen über die Lösung angezeigt.

- Lösungsname
- Lösungsstatus
- vService-Anbieter

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Client auf das Solutions Manager-Symbol.
- 2 Navigieren Sie durch die Registerkarten des Solutions Managers.
 - Registerkarte **Übersicht**. Listet die Anzahl der installierten Lösungen und eine kurze Statusübersicht für jede Lösung auf.

- Registerkarte **Lösungen**. Listet alle verwalteten Lösungen auf.
 - Registerkarte **Status**. Gibt den Systemzustand der vCenter-Dienste an. Zudem werden für jeden Dienst die Alarme oder Warnungen angezeigt.
- 3 Klicken Sie in der Solutions Manager-Bestandsliste auf eine der Lösungen.
- Registerkarte **Übersicht**. Listet Informationen zur Lösung auf, einschließlich eines Links zum Produkt und den Anbieter-Websites, eines Links zum Starten der Management-UI in einem separaten Fenster sowie eines Links zur virtuellen Maschine bzw. zur vApp, die diese Lösung ausführt.
- Durch die Auswahl des Anbieter-Website-Links gelangen Sie zur Seite „Übersicht“ der virtuellen Maschine oder vApp. Ein Link unter „Verwaltet von“ führt Sie zur Lösung zurück.
- Registerkarte **Virtuelle Maschinen**. Listet alle virtuelle Maschinen auf, die zur Lösung gehören
 - Registerkarte **vService-Anbieter**.
 - Registerkarte **Management** oder eine andere Registerkarte, die die Lösung angegeben hat.

Konfigurieren von SNMP-Einstellungen für vCenter Server

Sie müssen SNMP-Einstellungen konfigurieren, um SNMP mit vCenter Server zu verwenden.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Zum Abschließen der folgenden Aufgabe muss der vSphere-Client mit vCenter Server verbunden sein. Außerdem benötigen Sie den DNS-Namen und die IP-Adresse des SNMP-Empfängers, die Portnummer des Empfängers und den Community-Bezeichner.

Vorgehensweise

- 1 Wählen Sie **Verwaltung > vCenter Server-Einstellungen**.
- 2 Wenn vCenter Server Teil einer Gruppe im verknüpften Modus ist, wählen Sie unter **Aktueller vCenter Server** den entsprechenden Server aus.
- 3 Klicken Sie in der Navigationsleiste auf **SNMP (SNMP)**.
- 4 Geben Sie die folgenden Informationen für den **primären Empfänger** der SNMP-Traps ein.

Option	Beschreibung
Empfängerinternetadresse	Der DNS-Name oder die IP-Adresse des SNMP-Empfängers.
Empfängerport	Die Portnummer des Empfängers, an die der SNMP-Agent Traps sendet. Wenn der Portwert nicht angegeben wird, verwendet vCenter Server den Standardport 162 .
Community	Der Community-Bezeichner.

- 5 (Optional) Verwenden Sie die Optionen **Empfänger 2 aktivieren**, **Empfänger 3 aktivieren** und **Empfänger 4 aktivieren**, um weitere Empfänger zu aktivieren.
- 6 Klicken Sie auf **OK**.

Das vCenter Server-System ist jetzt bereit, Traps an das von Ihnen angegebene Verwaltungssystem zu senden.

Weiter

Konfigurieren Sie Ihre SNMP-Verwaltungssoftware zum Empfangen und Interpretieren von Daten aus dem SNMP-Agenten von vCenter Server. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Überwachung und -Leistung*.

Systemprotokolldateien

Zusätzlich zu Listen von Ereignissen und Alarmen generieren vSphere-Komponenten auch verschiedene Protokolle.

Diese Protokolle enthalten zusätzliche Informationen zu Aktivitäten in der vSphere-Umgebung.

Anzeigen von Systemprotokolleinträgen

Sie können von vSphere-Komponenten generierte Systemprotokolle anzeigen.

Vorgehensweise

- 1 Klicken Sie auf der Startseite eines vSphere Clients, der mit einem vCenter Server-System oder einem ESX/ESXi-Host verbunden ist, auf **Systemprotokolle**.
- 2 Wählen Sie aus dem Dropdown-Menü das gewünschte Protokoll und den gewünschten Eintrag aus.
- 3 Wählen Sie **Anzeigen > Filtern**, um die Filteroptionen anzusehen.
- 4 Geben Sie Text in das Datenfeld ein.
- 5 Klicken Sie auf **Löschen**, um das Datenfeld zu leeren.

Anzeigen von Systemprotokollen auf einem ESXi -Host

Sie können die Schnittstelle der direkten Konsole zum Anzeigen der Systemprotokolldateien auf einem ESXi-Host verwenden. Diese Protokolle enthalten detaillierte Informationen zu Ereignissen des Systembetriebs.

Vorgehensweise

- 1 Wählen Sie in der direkten Konsole **Systemprotokolle anzeigen (View System Logs)**.
- 2 Drücken Sie zum Anzeigen eines bestimmten Protokolls die entsprechende Taste.
vCenter Server-Agent-Protokolle (vpxa) werden angezeigt, wenn der Host von vCenter Server verwaltet wird.
- 3 Drücken Sie die Eingabe- oder Leertaste, um die Meldungen zu durchlaufen.
- 4 (Optional) Führen Sie eine Suche mithilfe eines regulären Ausdrucks durch.
 - a Drücken Sie die Schrägstrichtaste (/).
 - b Geben Sie den zu suchenden Text ein.
 - c Drücken Sie die Eingabetaste.
Der gefundene Text wird auf dem Bildschirm hervorgehoben.
- 5 Drücken Sie „q“, um zur direkten Konsole zurückzukehren.

Externe Systemprotokolle

Der technische Support von VMware kann für die Behebung von Problemen mit dem Produkt eine Reihe von Dateien anfordern. Im vorliegenden Abschnitt werden die Typen und Speicherorte der Protokolldateien für die verschiedenen ESXi-Komponentensysteme beschrieben.

HINWEIS Auf Windows-Systemen werden verschiedene Protokolldateien im Verzeichnis mit den lokalen Einstellungen gespeichert, das sich in folgendem Pfad befindet: C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\. Dieser Ordner wird standardmäßig ausgeblendet.

ESXi -Systemprotokolle

Sie benötigen möglicherweise die Systemprotokolldateien des ESXi, um technische Probleme zu beheben.

Die ESXi-Systemprotokolle befinden sich im Verzeichnis `/var/run/log`.

Systemprotokolle des vSphere Clients

Sie benötigen möglicherweise die Systemprotokolldateien des vSphere Clients, um technische Probleme zu beheben.

In [Tabelle 28-6](#) werden die Protokolldateien aufgeführt, die mit der vSphere Client-Maschine in Zusammenhang stehen.

Tabelle 28-6. Systemprotokolle des vSphere Clients

Komponente	Speicherort
Installationsprotokoll des vSphere Clients	Temp-Verzeichnis auf der vSphere Client-Maschine. Beispiel für Version vor Windows 2008: C:\Dokumente und Einstellungen\Local Settings\Temp\vminst.log oder vim-vic-msi.log Beispiel für Windows 2008 und Windows 7: C:\Benutzer\user_name\AppData\Local\Temp\vminst.log oder vim-vic-msi.log
Dienstprotokoll des vSphere Clients	\vpx -Verzeichnis im Verzeichnis der Anwendungsdaten auf der vSphere Client-Maschine. Beispiel für Version vor Windows 2008: C:\Dokumente und Einstellungen\user_name\Local Settings\Application Data\VMware\vpx\viclient-x.log Beispiel für Windows 2008 und Windows 7: C:\Benutzer\user_name\Local Settings\AppData\Local\VMware\vpx\viclient-x.log x(=0, 1, ... 9)

Systemprotokolle exportieren

Wenn der vSphere Client mit vCenter Server verbunden ist, können Sie Hosts auswählen, von denen Systemprotokolle heruntergeladen werden sollen.

Der vSphere Client muss mit dem vCenter Server-System verbunden sein, um Diagnosedaten für ESX/ESXi-Hosts und vCenter Server zu speichern. Wenn Sie direkt mit einem ESX/ESXi-Host verbunden sind, können Sie Diagnosedaten nur für diesen bestimmten ESX/ESXi-Host speichern.

Erforderliche Berechtigungen:

- Zum Anzeigen von Diagnosedaten: **Schreibgeschützte Benutzer**
- Zum Verwalten von Diagnosedaten: **Global.Lizenzen**

Vorgehensweise

- 1 Wählen Sie **Datei > Exportieren > Systemprotokolle exportieren**.
- 2 Wenn Sie mit vCenter Server verbunden sind, wählen Sie das Objekt aus, dessen Daten Sie exportieren möchten.

Durch die Auswahl eines Objekts werden auch alle ihm untergeordneten Objekte ausgewählt.

- 3 Wenn Sie mit vCenter Server verbunden sind, wählen Sie **Informationen zu vCenter Server und vSphere Client einbeziehen** aus, um vCenter Server- und vSphere Clientprotokolle sowie Hostprotokolle herunterzuladen.

- 4 Klicken Sie auf **Durchsuchen** und geben Sie den Speicherort für die Protokolldateien an.

Der Host oder das vCenter Server-System generiert .zip-Archive, die die Protokolldateien enthalten. Das Fenster **Kürzlich bearbeitete Aufgaben** zeigt die Aufgabe „Diagnosepaket generieren“ in Bearbeitung an.

Das Dialogfeld zum Herunterladen der Protokollpakete wird nach Abschluss der Aufgabe zum Generieren des Diagnosepakets angezeigt. Im Dialogfeld wird der Downloadstatus jedes einzelnen Pakets angezeigt.

Verschiedene Netzwerkfehler können dazu führen, dass ein Download fehlschlägt. Nach der Auswahl eines Downloads im oberen Teil des Dialogfelds wird ggf. die Fehlermeldung für den Vorgang im unteren Teil des Dialogfelds unterhalb vom Namen und Speicherort der Protokollpaketdatei angezeigt.

- 5 Falls beim Herunterladen ein Fehler auftritt, klicken Sie auf **Wiederholen**, um die generierten Pakete erneut herunterzuladen.

Diagnosepakete, die Protokolldateien für die angegebenen Objekte enthalten, werden an den angegebenen Speicherort heruntergeladen.

Konfiguration von Syslog auf ESXi -Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Diensts verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Client aus.
- 2 Klicken Sie auf die Registerkarte **Konfiguration**.
- 3 Klicken Sie im Bereich „Software“ auf **Erweiterte Einstellungen**.
- 4 Wählen Sie in der Strukturansicht **Syslog**.
- 5 Klicken Sie zum Einrichten der globalen Protokollierung auf **Global** und nehmen Sie die entsprechenden Änderungen in den rechten Feldern vor.

Option	Beschreibung
Syslog.global.defaultRotate	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis <code>/scratch</code> auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format <code>[Datenspeichername] Pfad_zur_Datei</code> aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <code>[storage1] /systemlogs</code> dem Pfad <code>/vmfs/volumes/storage1/systemlogs</code> zuzuordnen.

Option	Beschreibung
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von Syslog.global.LogDir angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. <code>ssl://Hostname1:514</code> . UDP (Standard), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

- 6 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll.
 - a Klicken Sie auf **loggers**.
 - b Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten, und geben Sie die gewünschte Anzahl der Rotationen und die gewünschte Protokollgröße ein.
- 7 Klicken Sie auf **OK**.

Änderungen an der syslog-Option werden sofort wirksam.

Sammeln von Protokolldateien

Der technische Support von VMware kann eine Reihe von Dateien anfordern, um Sie bei der Beseitigung von technischen Problemen zu unterstützen. In den folgenden Abschnitten werden Skriptprozesse zum Generieren und Sammeln einiger dieser Dateien beschrieben.

Einstellen der ausführlichen Protokollierung

Sie können die Ausführlichkeit von Protokolldateien bestimmen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- 1 Wählen Sie **Verwaltung > vCenter Server-Einstellungen**.
- 2 Wählen Sie **Protokollierungsoptionen**.
- 3 Wählen Sie im Popup-Menü die Option **Ausführlich**.
- 4 Klicken Sie auf **OK**.

Erfassen von vSphere -Protokolldateien

Sie können vSphere-Protokolldateien in einem einzelnen Speicherort erfassen.

Voraussetzungen

Starten Sie den vSphere Client und melden Sie sich bei einem vCenter Server-System an.

Vorgehensweise

- ◆ Zeigen Sie mithilfe einer der folgenden Methoden die Protokolldatei an.

Aufgabe	Aktion
Zeigen Sie die Datei viclient-*.log an	Wechseln Sie in das Verzeichnis %temp%.
Laden Sie das Protokollpaket von dem vSphere-Client herunter, der mit einem vCenter Server-System verbunden ist.	Wählen Sie Administration > Systemprotokolle exportieren aus, um das Protokollpaket herunterzuladen. Das Protokollpaket wird als .zip-Datei generiert. Standardmäßig werden die vpxd-Protokolle innerhalb des Pakets als .gz-Dateien komprimiert. Zum Dekomprimieren dieser Dateien müssen Sie gunzip verwenden.
Erstellen von vCenter Server-Protokollpaketen über ein vCenter Server-System	Wählen Sie Start > Programme > VMware > vCenter Server-Protokollpaket generieren aus. Mit dieser Funktion können Sie auch dann vCenter Server-Protokollpakete generieren, wenn Sie mit dem vSphere-Client keine Verbindung zu vCenter Server herstellen können. Das Protokollpaket wird als .zip-Datei generiert. Standardmäßig werden die vpxd-Protokolle innerhalb des Pakets als .gz-Dateien komprimiert. Zum Dekomprimieren dieser Dateien müssen Sie gunzip verwenden.

Erfassen von ESXi -Protokolldateien

Sie können alle relevanten Informationen über das ESXi-System und die Konfiguration sowie ESXi-Protokolldateien erfassen und verpacken. Anhand dieser Informationen können Probleme analysiert werden.

Vorgehensweise

- ◆ Führen Sie das folgende Skript in der ESXi-Shell aus: `/usr/bin/vm-support`
Die Ergebnisdatei weist das folgende Format auf: `esx-Datum-eindeutige-xnummer.tgz`

Deaktivieren der Komprimierung für vpxd-Protokolldateien

Standardmäßig werden vpxd-Protokolldateien von vCenter Server zusammengefasst und in .gz-Dateien komprimiert. Sie können diese Einstellung deaktivieren, sodass die vpxd-Protokolle nicht komprimiert werden.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client bei vCenter Server an.
- 2 Wählen Sie **Verwaltung > vCenter Server-Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Einstellungen**.
- 4 Geben Sie im Textfeld **Schlüssel** die Zeichenfolge `log.compressOnRoll` ein.
- 5 Geben Sie im Textfeld **Wert** die Zeichenfolge `false` ein.
- 6 Klicken Sie auf **Hinzufügen** und anschließend auf **OK**.

Index

Zahlen

3DNow!, EVC-Modi **144**

A

Abfragegrenze **31**

abhängige Hardware iSCSI

Konfigurations-Workflow **343**

und zugeordnete Netzwerkkarten **344**

Abhängige iSCSI, Netzwerk **347**

abmelden, vSphere Client **14**

Active Directory

Konfigurieren von Einstellungen **31**

Server **31**

Active Directory-Zeitüberschreitung **83**

Adapter

Ethernet, , *siehe* Netzwerkkarten

Siehe auch Speicher-Controller

Administrator, Rolle **78**

Affinitätsregeln

Erstellen **413, 414**

Intra-VM **425**

Storage DRS **424**

Agent-Manager **236**

AHCI SATA-Controller, , *siehe* Speicher-Controller

Aktive Adapter **261**

Aktive Sitzungen, Senden einer Nachricht **23**

Aktive Uplinks **296, 300**

aktivieren, Übereinstimmungsprüfungen für
Hostprofilrichtlinien **246**

aktualisieren

Distributed Switch **266**

Hardware der virtuellen Maschine **153**

VMware Tools **157**

vSphere Distributed Switch **266**

Aktualisierte Informationen **11**

Aktueller Multipathing-Status **375**

Akzeptanzebene des Host-Image-Profiles **27**

Alarmaktionen

Ausführen eines Skripts **468**

Beschrieben **461**

deaktivieren **474**

E-Mail-Benachrichtigungen **470**

Einrichten **468**

Trap-Benachrichtigungen **468**

Alarme

Aktionen deaktivieren **474**

allgemeine Einstellungen **466**

anzeigen **464**

Auf Bestandslistenobjekt festlegen **464**

Ausgelöst **464**

Ausgelöste Alarme bestätigen **475**

Ausgelöste Ereignisalarme zurücksetzen **475**

Auslöser **466**

Auslöstertoleranzgrenzwerte **468**

Bedingungs- oder statusbasiert **466**

Befehle **472**

Benachrichtigungs-E-Mails **468**

Berichteinstellungen **468**

Beschrieben **461**

Definitionen **464**

erstellen **464**

Häufigkeit **468**

Netzwerk **471**

Senden einer E-Mail als Alarmaktion **470**

Skripts **472, 473**

SMTP-Einstellungen **470**

SNMP-Traps **471**

Alarme erstellen **464**

Alarme, Auslöser **467**

Alarme, deaktivierte Aktionen **476**

Alarme, Einstellungen anzeigen **465**

Alarme, Umgebungsvariablen **472**

Alarmumgebungsvariablen **473, 474**

AMD Opteron-basierte Systeme **428**

AMD-Überschreibungsmaske **163**

Anbieter-Provider

aktualisieren **381**

anzeigen **380**

Aufheben der Registrierung **381**

registrieren **380**

Ändern von Clustereinstellungen **435**

anfängliche Platzierung **402**

anhalten

vApps **225**

virtuellen Maschinen **202**

Anmeldung, vSphere Client **14**

Anmerkungen **19**

Anpassung

Erstellen der Windows-Spezifikation **131**

- Erstellen von Linux-Spezifikationen **128**
 - Erstellen von Windows-Spezifikationen **129**
 - Exportieren von Spezifikationen **133**
 - Gastbetriebssystem, Anforderungen **121**
 - Importieren von Spezifikationen **134**
 - Kopieren von Spezifikationen **133**
 - Linux **121**
 - Spezifikationen ändern **133**
 - Windows **121**
 - Anpassungsspezifikationen **127**
 - Anteile, Storage I/O Control **393**
 - Anteile und Grenzwerte, Storage I/O Control **394**
 - Antwortdatei aktualisieren **252**
 - Anwenden von Netzwerkrichtlinien **291**
 - Anwendungsbeispiele, Fault Tolerance **441**
 - Arbeitsspeicher
 - Affinität **167**
 - Berechnen für Videoanzeigen **192**
 - Hinzufügen im laufenden Betrieb **167**
 - Statusüberwachung **459**
 - Verwalten von Zuteilungen **388**
 - virtuell **99**
 - Zuteilung **166**
 - Arbeitsspeicheraffinität, NUMA-Knoten **429**
 - Assistent zum Erstellen neuer virtueller Maschinen, Öffnen **94**
 - Attribute, benutzerdefiniert **20**
 - Aufgaben
 - abbrechen **57**
 - Alle Aufgaben anzeigen **55**
 - anzeigen **15, 55**
 - Auf Hosts und Datencentern filtern **56**
 - Aufbewahrungsrichtlinie konfigurieren **34**
 - Geplant **58**
 - Geplante Aufgaben anzeigen **56**
 - Geplante Aufgaben entfernen **61**
 - Grundlegende Informationen **55**
 - Klonen einer virtuellen Maschine **110**
 - Kürzlich bearbeitete Aufgaben anzeigen **56**
 - Mit Schlüsselwörtern filtern **57**
 - planen **59**
 - Regeln **62**
 - Richtlinien **62**
 - umplanen **60**
 - Ausführliche Protokollierung, konfigurieren **481**
 - Ausgelöste Alarmer, Bestätigen **475**
 - Auslagerung auf SSD **392**
 - Auslagerungsdatei, löschen **391**
 - Auslagerungsdateien **390**
 - Auslöser, Ereignisbasiert **467**
 - Ausschalten
 - vApps **224**
 - virtuellen Maschinen **202**
 - Außerkräftsetzungseinstellungen, Verteilte Portgruppen **47, 268**
 - Authentication Proxy **80, 82**
 - Authentifizierung
 - Benutzer **73**
 - ESXi **73**
 - ESXi-Benutzer **73**
 - Auto Deploy **251**
 - Automatische Hostregistrierung, deaktivieren **341**
 - Automatisierungsebene
 - Datenspeicher-Cluster **417**
 - Storage DRS **422**
 - virtuelle Maschinen **403**
- ## B
- Bandbreite
 - Durchschnitt **309, 311**
 - Spitze **309, 311**
 - Baseboard Management Controller (BMC) **409**
 - Beanspruchen von Pfaden **374**
 - Beanspruchungsregeln **374**
 - bearbeiten
 - Hostprofile **243**
 - Hostprofilrichtlinien **243**
 - vApp-Eigenschaften **226, 227**
 - Befehle, Alarmer **472**
 - Benachrichtigungen, , *siehe* Traps
 - Benachrichtigungs-E-Mails, Alarmer **468**
 - Benutzer
 - Ändern auf Hosts **74**
 - Anzeigen der Benutzerliste **75**
 - Authentifizierung **73**
 - Direktzugriff **73**
 - durchsuchen **83**
 - entfernen **77**
 - Entfernen von Hosts **75**
 - Exportieren einer Benutzerliste **75**
 - Hinzufügen zu ESXi **74**
 - Sicherheit **73**
 - benutzerdefinierte Attribute, hinzufügen **20**
 - Benutzerdefinierte Sysprep-Antwortdatei **131**
 - benutzerdefinierter Automatisierungsmodus, DRS **403**
 - Benutzerverwaltung, ESXi **73**
 - Berechtigungen
 - Administrator **76**
 - ändern **77**
 - Durchsuchen **17**
 - entfernen **77**
 - Root-Benutzer **76**

- Überblick **76**
- und Rechte **76**
- Validierung **77, 78**
- vpxuser **76**
- bereitstellen, OVF-Vorlagen **147**
- Bereitstellen, OVF-Vorlagen **147**
- Beschleunigung, deaktivieren **205**
- Best Practices, Fault Tolerance **451**
- Bestandsliste
 - Auswählen der Objekte **21**
 - durchsuchen **17**
 - Organisieren **37**
 - Topologiezuordnungen **89**
- Bestandsliste durchsuchen, Berechtigungen **17**
- Bestandslistenfenster **17**
- Bestandslistenobjekte, Alarm festlegen für **464**
- Betrieb, Statusüberwachung **459**
- Betriebszustände, Virtuelle Maschine **202**
- Bindung auf Host, Verteilte Portgruppen **47, 268**
- BIOS, Einstellungen **204**
- Blockierte Ports
 - Verteilte Portgruppen **315, 316**
 - Verteilte Ports **316**
- Burstgröße **309–312, 316**

C

- Cachespeicher für die Arbeitsspeicherkompri-
mierung
 - aktivieren **392**
 - deaktivieren **392**
 - Größe festlegen **393**
- CAM-Server **82**
- CDP **330, 332**
- CHAP
 - deaktivieren **358**
 - Für Erkennungsziele **357**
 - Für iSCSI-Initiatoren **356**
 - Für statische Ziele **357**
- CHAP-Authentifizierung **355**
- Cisco Discovery-Protokoll **44, 265, 330, 332**
- Cisco-Switches **330**
- Cluster
 - Auswählen **96**
 - Entfernen von Hosts **86**
 - Erstellen **40**
 - EVC **141, 142**
 - Verwalten von Profilen **249**
- Clusterbildung, Datenspeicher **415, 419**
- Clustereinstellungen
 - Affinitätsregeln **413, 414**
 - CPUID-Details **145**
 - Speicherort der VM-Auslagerungsdatei **391**
- Cold-Migration **135**
- Community-String **32**

- Computernamen, Generieren mit einem
Skript **122**
- Controller
 - Paravirtuelles SCSI **185**
 - SCSI **101**
 - SCSI-Typen **184**
 - Siehe auch* Speicher-Controller
- CPU
 - Statusüberwachung **459**
 - Verwalten von Zuteilungen **385**
 - virtuell **428**
- CPU-Affinität, NUMA-Knoten **428**
- CPU-Funktionen, virtuelle Maschinen **144**
- CPU-Kompatibilität, für vMotion **140**
- CPUID, Anzeigen von Details **145**
- CPUs
 - Anteile **161**
 - CPU/MMU-Virtualisierung aktivieren **164**
 - Definition **158**
 - erweiterte Einstellungen **162**
 - Gemeinsamer Kernzugriff mit Hyper-Threa-
ding **162**
 - Grenzwerte **161**
 - hinzufügen **99**
 - Hinzufügen im laufenden Betrieb **160**
 - Hotplug **159**
 - Identifikationsmaske **163**
 - Konfiguration **160**
 - Parameter **158**
 - Planen von Affinität **163**
 - Reservierung **161**
 - Sicherheit deaktivieren **163**

D

- Datenbank
 - Anzahl der Verbindungen konfigurieren **34**
 - Aufbewahrungsrichtlinie **34**
 - Begrenzen der Größe **34**
- Datencenter
 - Datencenterweite Netzwerke erstellen **43**
 - erstellen **38**
 - Topologiezuordnungen **89**
- Datencenter erstellen **38**
- Datencenterweite Netzwerke erstellen **43**
- Datenspeicher
 - Auswählen **97**
 - erstellen **41**
 - gruppieren **370**
 - Hinzufügen von Erweiterungen **368**
 - ISO-Datei **188**
 - Kapazität, erhöhen **368**
 - konfigurieren auf NFS-Volumes **362**
 - mounten **364**
 - NFS **361**

- Pfade **375**
 - Überprüfen von Eigenschaften **337**
 - umbenennen **369**
 - Verwalten von Duplizierten **363**
 - VMFS **101, 361**
 - Wartungsmodus **419**
 - Datenspeicher auswählen **97**
 - Datenspeicher-Cluster
 - Automatisierungsebene **417**
 - Datenspeicher entfernen **419**
 - Datenspeicher hinzufügen **419**
 - Erstellen **416, 417**
 - Grundlegende Informationen **415**
 - Wartungsmodus **419**
 - Datenspeicher-Taktsignale bei vSphere HA **439**
 - deaktivieren
 - Fault Tolerance **448**
 - Protokollierung für Gastbetriebssysteme **69**
 - Variable Informationsgröße **69**
 - Deaktivieren von Pfaden **376**
 - Debuggen und Statistiken **205**
 - DHCP-Einstellungen **231**
 - Diagnosedaten
 - Erstellen eines Berichts **479**
 - Export **478**
 - Exportieren **479**
 - Diagnosepakete, Generieren **479**
 - Diagnosepartition, konfigurieren **370**
 - Diagramme
 - anpassen **456**
 - Anpassen **456**
 - anzeigen **455**
 - Benutzerdefinierte zum Menü „Wechseln zu“ hinzufügen **457**
 - Daten exportieren **458**
 - Daten in eine Datei speichern **458**
 - Einstellungen **456**
 - erweitert **456**
 - Dienste, syslogd **26, 71, 480**
 - DirectPath I/O, vMotion **286**
 - DirectPath I/O Gen. 2 **286**
 - Direkte Konsole, Umleiten auf einen seriellen Port **25**
 - Direktzugriff **73**
 - Disk.EnableNaviReg **341**
 - Disk.MaxLUN **360**
 - Diskettenlaufwerke
 - hinzufügen **189**
 - konfigurieren **190**
 - Distributed Switch
 - aktualisieren **266**
 - Cisco Discovery-Protokoll **44, 265**
 - Einstellungen für die Ressourcenpools **279**
 - Hinzufügen **261**
 - Hinzufügen eines Hosts **45, 263**
 - Hosts **264**
 - IP-Adresse **44, 265**
 - Jumbo-Frames **283**
 - Kontaktinformationen des Administrators **44, 265**
 - Maximale Anzahl an Ports **44, 265**
 - Maximalwert für MTU **44, 265**
 - Neuer Ressourcenpool **280**
 - Schnittstellen **264**
 - virtuelle Maschinen **277**
 - Virtuelle Maschinen darauf oder davon migrieren **277**
 - Virtuelle Netzwerkadapter **273**
 - Virtueller Netzwerkadapter **274**
 - DNS **332**
 - DNS-Konfiguration
 - vApps **232**
 - vSphere Distributed Switch **275**
 - DNS-Suche **433**
 - DPM **402, 408, 409**
 - DRS
 - anfängliche Platzierung **402**
 - deaktivieren **404**
 - Erstellen von Regeln **413**
 - Lastenausgleich **402**
 - Manuell **402**
 - Migration **402**
 - Teilautomatisiert **402**
 - Vollautomatisiert **402**
 - DRS-Cluster
 - Erstellen **402**
 - Hinzufügen nicht verwalteter Hosts **405**
 - Hinzufügen verwalteter Hosts **405**
 - Verwalten von Ressourcen mit **401**
 - DRS-Gruppen
 - Host **412**
 - Virtuelle Maschine **413**
 - drucken, vSphere-Clientfenster **17**
 - Durchschnittliche Bandbreite **310–312, 316**
 - Durchschnittsbandbreite **309**
 - durchsuchen
 - Bestandslistenobjekte **18**
 - Einfache Suche **18**
 - Durchsuchen, erweitert **18**
 - DVD/CD-ROM, hinzufügen **186**
 - dynamische Erkennung, konfigurieren **354**
 - Dynamische Erkennungsadressen **353**
- ## E
- E-Mail, Inhalt der vCenter Server-Benachrichtigungen **470**
 - E-Mail-Absendereinstellungen, konfigurieren **31**

- E-Mail-Nachrichten **31**
 - EFI
 - Ändern der Startverzögerung **204**
 - Einstellungen **204**
 - Eigenschaften, Verteilte Ports **269**
 - Einfache Suche **18**
 - Einschalten
 - vApps **223**
 - virtuellen Maschinen **202**
 - Einschränken von Benutzern oder Gruppen **31**
 - Einstellungen, vCenter Server **25, 28**
 - Einstellungen für die Ressourcenpools
 - Distributed Switch **279**
 - vSphere Distributed Switch **281**
 - Einstellungen für die Ressourcenzuteilung, ändern **384**
 - Empfängerinternetadresse **32**
 - Empfehlungen, Speicher-DRS **421**
 - Energieverwaltung des Hosts, Benutzerdefinierte Richtlinie **387**
 - Energieverwaltungsrichtlinien, Einstellung **387**
 - Enhanced vMotion Compatibility, , *siehe* EVC
 - Enhanced vMotion Compatibility (EVC) **402**
 - entfernen, Plug-Ins **22**
 - Ereignisse
 - anzeigen **463**
 - Aufbewahrungsrichtlinie konfigurieren **34**
 - Exportieren **463**
 - Ereignisse, Beschreibung **461**
 - Erfassungsintervalle **29**
 - Erkennung
 - Adresse **353**
 - Dynamisch **354**
 - statisch **355**
 - erneut prüfen
 - Datenspeicher **360**
 - Speicheradapter **360**
 - Speichergeräte **360**
 - erstellen
 - Datenspeicher **41**
 - Hostprofile **241**
 - vApps **222**
 - virtuellen Maschinen **93**
 - Erstellen
 - Cluster **40**
 - Hostprofile **241**
 - Ressourcenpools **41**
 - Erstellen eines vSphere HA-Clusters **434**
 - Erstellen von hostweiten Netzwerken **42**
 - erweiterte Attribute
 - Hosts **430**
 - Storage I/O Control **396**
 - virtuelle Maschinen **431**
 - Erweiterte Diagramme, Als Standard festlegen **456**
 - erweiterte Einstellungen
 - vCenter Server **35**
 - Disk.EnableNaviReg **341**
 - Disk.MaxLUN **360**
 - Erweiterte Suche **18**
 - Erweiterungen
 - Fehlerbehebung **22**
 - Hinzufügen zu Datenspeicher **368**
 - Vergrößern **368**
 - EST **322**
 - ESX Agent Manager **236**
 - ESXi
 - Authentifizierung **73**
 - Benutzer **73**
 - herunterfahren **35**
 - Hinzufügen von Benutzern **74**
 - Neustarten **35**
 - syslog-Dienst **26, 71, 480**
 - ESXi Shell
 - aktivieren **65**
 - Aktivieren mit dem vSphere Client **65**
 - konfigurieren **65**
 - Zeitüberschreitung für den Leerlauf festlegen **65**
 - Zeitüberschreitung für die Verfügbarkeit festlegen **65**
 - Zeitüberschreitungen **66**
 - EVC
 - Aktivieren auf einem Cluster **142**
 - CPUID-Details **145**
 - Erstellen eines Clusters **141**
 - konfigurieren **143**
 - Unterstützung für virtuelle ESXi-Hosts **140**
 - EVC-Modi
 - ohne 3DNow! **144**
 - virtuelle Maschinen **144**
 - Exportieren
 - Diagnosedaten **479**
 - Hostbenutzer **75**
 - Hostprofile **242**
 - Listen **17**
 - OVF-Vorlagen **147, 149**
 - virtuelle Maschinen **149**
 - Exportieren von Lizenzdaten **54**
 - Extensible Firmware Interface, , *siehe* EFI
 - External Switch Tagging **322**
- ## F
- Failback **296, 298, 300, 316**
 - Failover **291, 293, 374**
 - Failover testen, Fault Tolerance **449**

- Failover-Hosts angeben **437**
 - Failover-Reihenfolge, Verteilte Portgruppen **298, 316**
 - Failover-Richtlinien
 - Portgruppe **296**
 - Standard-Switches **294**
 - Verteilte Portgruppen **298, 316**
 - Verteilte Ports **300**
 - Fault Tolerance
 - aktivieren **443**
 - Anwendungsbeispiele **441**
 - Best Practices **451**
 - Checkliste **442**
 - deaktivieren **448**
 - Deaktivieren **447**
 - Failover testen **449**
 - Fehler **453**
 - Fehlermeldungen **441**
 - Gesamtmenge an sekundärem Arbeitsspeicher **450**
 - Gesamtmenge an sekundärer CPU **450**
 - Netzwerkkonfiguration **444, 445**
 - Neustart sekundärer VM testen **449**
 - Optionen **447**
 - Protokollbandbreite **450**
 - Protokollierung **275, 444, 445**
 - Sekundäre VM migrieren **448**
 - Sekundärer Speicherort **450**
 - Überprüfung der Richtlinieneinhaltung **446**
 - version **442**
 - vLockstep-Intervall **450**
 - Voraussetzungen **442**
 - vSphere-Konfiguration **442**
 - Fehler, Fault Tolerance **453**
 - Fehlerbehebung
 - Debuggen und Statistiken **205**
 - Erweiterungen **22**
 - Installation von Software in der virtuellen Maschine **205**
 - Plug-Ins **22**
 - Protokolldateien **478, 481**
 - Fehlermeldungen
 - Fault Tolerance **441**
 - vSphere HA **433**
 - Fehlertoleranz bei Bedarf **441**
 - Fehlertoleranzstatus
 - Deaktiviert **450**
 - Sekundäre VM erforderlich **450**
 - Starten **450**
 - VM wird nicht ausgeführt **450**
 - Fenster **17**
 - Festplatten
 - Anteile **181**
 - Format **379**
 - Grenzwerte **181**
 - Modi **179**
 - Schnell **112**
 - Thick **112**
 - Thin- und Thick-Format **113**
 - unabhängig **213**
 - Vergrößern **379**
 - Fibre-Channel-NPIV-Einstellungen **176**
 - filtern, Listen **16**
 - Firewall, Konfigurieren der Kommunikation **35**
 - Firewalleinstellungen **64**
 - Firewalls
 - Zugriff für Dienste **63**
 - Zugriff für Verwaltungs-Agenten **63**
 - Flash-Lesecache **177**
 - Format des Portnamens, Verteilte Portgruppen **47, 268**
 - Fortsetzen
 - vApps **225**
 - virtuellen Maschinen **202**
- ## G
- Gastanpassung
 - Anforderungen **121, 127**
 - Entfernen von Spezifikationen **133**
 - Erstellen von Linux-Spezifikationen **128**
 - Erstellen von Windows-Spezifikationen **129, 131**
 - Exportieren von Spezifikationen **133**
 - Importieren von Spezifikationen **134**
 - Kopieren von Spezifikationen **133**
 - Linux-Anpassung beim Klonen oder Bereitstellen **126**
 - Skripts **122**
 - Spezifikationen ändern **133**
 - Windows-Anpassung beim Klonen oder Bereitstellen **123**
 - Gastbetriebssystem, Netzwerkkarte entfernen **273**
 - Gastbetriebssysteme
 - Aktivieren von Kopier- und Einfügevorgängen **68**
 - ändern **156**
 - Anpassungsanforderungen **121**
 - Auswählen **98**
 - Begrenzen der variablen Informationsgröße **69**
 - Deaktivieren der Protokollierung **69**
 - Gefälschte Übertragungen **305, 307, 308, 316**
 - gemeinsam nutzen, Festplatten **104**
 - Gemeinsamer Kernzugriff mit Hyper-Threading **162**

- Geplante Aufgaben
 - abbrechen **57**
 - Abbrechen **61**
 - entfernen **61**
 - Erstellen **59**
 - Grundlegende Informationen **58**
 - Klonen einer virtuellen Maschine **110**
 - Prozessregeln **62**
 - Regeln **62**
- Gerätetrennung, Verhindern **70**
- Grafikkarten
 - Anzahl der Anzeigen auswählen **192**
 - konfigurieren **192**
- Gruppen
 - DRS-Host **412**
 - durchsuchen **83**
 - Virtuelle DRS-Maschine **413**
- Gruppierungsrichtlinien
 - Portgruppe **296**
 - Verteilte Portgruppen **298, 316**
 - Verteilte Ports **300**

H

- Hardware, Virtuelle Maschine **151**
- Hardware der virtuellen Maschine
 - aktualisieren **153**
 - Ermitteln der Version **154**
 - Virtuelle Festplatten **178**
- Hardware-iSCSI-Initiatoren
 - anzeigen **342**
 - Einrichten von Erkennungsadressen **353**
 - Installieren **342**
 - konfigurieren **341**
- Hardwarebeschleunigung
 - aktivieren **377**
 - Grundlegende Informationen **377**
- Hardwaregeräte, SCSI-Controller **183**
- Hardwarestatus, Sensoren zurücksetzen **460, 461**
- Hardwarevirtualisierung (HV) **442**
- herunterfahren, Einstellungen für virtuelle Maschinen **202**
- Herunterfahren, Einstellungen für virtuelle Maschinen **207**
- herunterladen, Diagnosepakete **479**
- hierarchisch gleichwertig **397**
- hinzufügen
 - Lizenzschlüssel **52, 53**
 - NFS-Speicher **362**
 - Paravirtueller SCSI-Controller **185**
 - SCSI-Controller **183**
 - SCSI-Geräte **190**
 - USB-Controller **195**
 - USB-Geräte zu Clientcomputern **199**

- Hinzufügen
 - Verteilte Portgruppen **46, 267**
 - vSphere Distributed Switch **261**
- Hinzufügen eines VMkernel-Netzwerkadapters **258**
- Hinzufügen im laufenden Betrieb aktivieren **159, 167**
- Hinzufügen von Hosts **39**
- Host
 - Referenz **248**
 - wechseln in den Wartungsmodus **407**
- Host in den Testmodus versetzen **50**
- Host-Cache-Konfiguration **392**
- Host-DRS-Gruppen **412**
- Host-Netzwerk, anzeigen **256**
- Hosteinschränkungen, vSphere Client **25**
- Hostisolierungsreaktion **438**
- Hostkonfiguration, erweiterte Einstellungen **341**
- Hostname, konfigurieren **81**
- Hostprofil
 - Elemente anhängen **246**
 - SR-IOV **287, 288**
- Hostprofil importieren **242**
- Hostprofile
 - Aktualisieren vom Referenzhost **249**
 - Aus Hostprofilansicht erstellen **241**
 - Elemente über den Host anhängen **247**
 - Elemente über die Ansicht „Hostprofile“ anhängen **246**
 - erstellen **241**
 - Exportieren **242**
 - Profile bearbeiten **243**
 - Profile importieren **242**
 - Profile übernehmen **247, 248**
 - Profile verwalten **246**
 - Richtlinie bearbeiten **243**
 - Übereinstimmung prüfen **250**
 - Übereinstimmungsprüfungen für Richtlinien aktivieren **246**
 - Verwendungsmodell **239**
 - Vom Host erstellen **241**
 - zugreifen **240**
- Hostprofile, Antwortdatei importieren **252**
- Hostprofile, Profile klonen **243**
- Hostregistrierung, deaktivieren **341**
- Hosts
 - benutzerdefinierte Attribute **19**
 - Clusterbildung **96**
 - Entfernen aus Cluster **86**
 - Entfernen aus einem DRS-Cluster **408**
 - Entfernen aus vCenter Server **87**
 - erweiterte Attribute **430**
 - ESXi **35**

- geeignet für Migration **163**
- Hardwareüberwachung **459**
- hinzufügen **39**
- Hinzufügen von ESXi-Benutzern **74**
- Hinzufügen zu DRS-Clustern **405**
- Hinzufügen zu einem vSphere Distributed Switch **45, 263**
- konfigurieren **25**
- Mit vCenter Server verbinden **85**
- neu verbinden **86**
- Speicherort der VM-Auslagerungsdatei **390**
- Systemzustand **460**
- Trennen der Verbindung **85**
- Verbinden von virtuellen Maschinen zu **96**
- verwalten **85**
- Von vCenter Server trennen **85**
- Hoststatus, Sensoren zurücksetzen **460, 461**
- Hostüberwachung, aktivieren **436**
- Hyper-Threading
 - aktivieren **385**
 - deaktivieren **385**
 - Serverkonfiguration für **386**
- Hyper-Threading-Modi **386**

I

- iLO, konfigurieren **409**
- Image-Dateien, ISO **187, 188**
- Informationsfenster **17**
- Installieren, Plug-Ins **21**
- Intelligent Platform Management Interface (IPMI), konfigurieren **409**
- Inter-VM-Anti-Affinitätsregeln, Erstellen **425**
- Internet Protocol Version 6 **321**
- Intra-VM-Anti-Affinitätsregeln **425**
- IOMMU **286**
- IP-Adresse
 - bearbeiten **275**
 - vCenter Server **30**
- IP-Adressen
 - Generieren mit einem Skript **122**
 - Zulässige hinzufügen **64**
- IP-Adressenkonfiguration **231**
- IP-Pools **231**
- IP-Speicherportgruppen, Erstellen **258, 273**
- IPv4 **433**
- IPv6 **321, 433, 444**
- iSCSI-Initiatoren
 - CHAP konfigurieren **356**
 - Einrichten von CHAP-Parametern **355**
 - Hardware **341**
 - Konfigurieren erweiterter Parameter **359**
- iSCSI-Netzwerk
 - Adapter binden **352**

- Ändern der Richtlinie **351**
- Erstellen einer VMkernel-Schnittstelle **349**
- iSCSI-SAN **442**
- ISO-Imagedateien **187, 188**
- ISO-Images **451**
- Isolierungsreaktion, Host **438**

J

- Jumbo-Frames
 - aktivieren **283**
 - Aktivieren für abhängige Hardware-iSCSI **353**
 - Aktivieren für Software-iSCSI **353**
 - Verwenden mit iSCSI **352**
 - virtuelle Maschinen **282, 283**

K

- Kabel/Interconnect, Statusüberwachung **459**
- Kein Zugriff, Rolle **78**
- Klone **107**
- klonen
 - vApps **224**
 - virtuelle Maschinen **108, 112**
 - Vorlagen **111, 113**
- Knoten des virtuellen Geräts **191**
- konfigurieren
 - dynamische Erkennung **354**
 - Hosts **25**
 - statische Erkennung **355**
- Konsolen, virtuelle Maschinen **16**
- Kontaktinformationen des Administrators **44, 265**
- Konvertieren, Virtuelle Maschinen in Vorlagen **111**
- Kopieren und Einfügen, Deaktiviert für Gastbetriebssysteme **68**

L

- Lange Vorgänge **32**
- Lastausgleich, Verteilte Portgruppen **298, 316**
- Lastausgleich, Richtlinien, Standard-Switches **294**
- Lastenausgleich, Datenspeicher **415**
- Laufzeiteinstellungen, konfigurieren **30**
- Leistung, Erweiterte Diagramme **456**
- Leistungsdiagramme
 - Anpassen **456**
 - Daten exportieren **458**
 - Daten in eine Datei speichern **458**
 - Erweiterte Diagramme
 - Grundlegende Informationen **456**
 - Löschen von Ansichten **458**
- Link Layer Discovery Protocol (LLDP) **330–332**
- Linux
 - Anforderungen für die Anpassung **121**

- Anpassen beim Klonen oder Bereitstellen **126**
- Anpassen von Gastbetriebssystemen **121**
- Listen
 - Exportieren **17**
 - filtern **16**
- Listen durchsuchen, Anpassen für große Domänen **83**
- Live-Port verschieben, Verteilte Portgruppen **47, 268**
- Lizenzbericht, Daten exportieren **54**
- Lizenzen
 - anzeigen **51**
 - zuweisen **50**
- Lizenzierung
 - Lizenzschlüssel hinzufügen **52, 53**
 - Prozessorbasiert **52**
 - zuweisen **52**
- Lizenzierungseinschränkungen, vSphere Client **49**
- Lizenzschlüssel **49, 51**
- Lizenzverwaltung **49, 51**
- LLDP, aktivieren **331**
- Logische Prozessoren **385**
- Lokale Auslagerung auf einem Host
 - DRS-Cluster **389**
 - Eigenständiger Host **389**
- löschen, Vorlagen **118**
- Löschen von Ressourcenpools, vSphere Distributed Switch **282**
- Lösungen anzeigen **236, 476**
- Lüfter, überwachen **459**
- LUNs, Ändern der Anzahl an LUNs, nach denen gesucht wird **360**

M

- MAC-Adressänderungen **305, 307, 316**
- MAC-Adresse
 - Bereichsbasierte Zuteilung **333**
 - Generierung **333**
 - Konfiguration **334**
 - konfigurieren **333**
 - Präfixbasierte Zuteilung **333**
 - statisch **334**
 - Zuteilungsparameter anpassen **333**
- MAC-Adressen, zuweisen **169**
- manuelle DRS **402**
- Maskenwerte **163**
- Maximale Anzahl an Ports **44, 265**
- Maximalwert für MTU **44, 265**
- Mehrere Monitore, auswählen **192**
- Mehrfachpfad-Plug-Ins, Beanspruchen von Pfaden **374**
- Migration, Grundlegende Informationen **135**
- migrieren
 - Angehaltene virtuelle Maschinen **138**

- Ausgeschaltete virtuelle Maschinen **138**
- Eingeschaltete virtuelle Maschinen **136**
- Mit vMotion **136**
- virtuelle Maschinen **135**
- Von virtuellen Maschinen mit Storage vMotion **137**
- von VM-Festplatten **137**

MTU **282, 283**

Multipathing-Status **375**

N

Name-IP-Generator **122**

NetFlow

- aktivieren **314–316**
- Collector-Einstellungen **329**
- deaktivieren **314–316**
- konfigurieren **329**
- Verteilte Portgruppen **314, 316**
- Verteilte Ports **315**

Network I/O Control **313**

Netzwerk

- erweitert **321**
- Sicherheitsrichtlinien **308**
- SNMP-Traps **471**

Netzwerk-Failover-Ermittlung **296, 300**

Netzwerkadapter

- anzeigen **256, 266**
- Distributed Switch **273**
- Siehe auch* NICs

Netzwerke

- DHCP-Einstellungen **231**
- IP-Adressenkonfiguration **231**
- Proxy-Server-Einstellungen **232**
- Ressourceneinstellungen **279–282**
- Ressourcenpools **279**
- Statusüberwachung **459**
- verbinden **100**

Netzwerkeinschränkungen, vSphere Client **255**

Netzwerkkarten

- Entfernen von aktiver virtueller Maschine **273**
- Entfernen von einem vSphere Distributed Switch **272, 273**
- Gastbetriebssystem **273**
- Hinzufügen zu einem vSphere Distributed Switch **272**
- konfigurieren **169**
- Spanning Tree-Protokoll **100**
- Zuordnen zu VMkernel **350**
- Zuweisen von MAC-Adressen **169**

Netzwerkkonfiguration, Fault Tolerance **444, 445**

Netzwerkpartition **451**

- Netzwerkressourcenpools
 - Verteilte Portgruppen **313, 316**
 - Verteilte Ports **314**
- Netzwerkrichtlinien
 - Distributed Switch **291**
 - Standard-Switch **291**
- Netzwerkverbindungen, erstellen **349**
- Netzwerkverbindungseinstellungen **233**
- Neuer Ressourcenpool, Distributed Switch **280**
- Neusignierung **363**
- Neustart sekundärer VM testen, Fault Tolerance **449**
- Neustarteinstellungen, Für virtuelle Maschinen **202**
- Neuverbinden von Hosts **86**
- NFS-Speicher, hinzufügen **362**
- NIC-Gruppierung, Standard-Switches **294**
- NMP, Beanspruchen von Pfaden **374**
- Normale Vorgänge **32**
- NPIV
 - Ändern von WWNs **339**
 - Zuweisen von WWNs **338**
- NTP **81**
- NUMA
 - Arbeitsspeicheraffinität **430**
 - CPU-Affinität **428, 430**
 - virtuell **428**
- Nur lesen, Rolle **78**
- NX-Flag **163**
- O**
 - Objekte, auswählen **21**
 - Optionen für das Starten von Clients, Einstellung **64**
 - Optionen für das Starten von Diensten, Einstellung **64**
 - Optionen für virtuelle Maschinen, vSphere HA **438**
 - optische Laufwerke
 - Mit Hostgerät verbinden **187**
 - Verbindung zum Clientgerät **187**
 - OVA, auswählen, *Siehe auch* OVF
 - OVF
 - Exportieren von Vorlagen **147, 149**
 - Speicherort der Dateien **149**
 - Umgebungseigenschaften definieren **230**
 - Vorlagen bereitstellen **147**
- P**
 - Parallele Schnittstellen
 - ändern **176**
 - hinzufügen **175**
 - Parameter der Konfigurationsdatei, bearbeiten **156**
 - Paravirtueller SCSI-Controller **185**
 - Passthrough-Gerät, Hinzufügen zu einer virtuellen Maschine **285**
 - PCI **284**
 - PCI-Geräte, Snapshotunterstützung **191**
 - PCIe-Geräte **286**
 - Pfad-Failover **374**
 - Pfade, deaktivieren **376**
 - Pfadrichtlinien, Ändern des Standardeinstellungen **376**
 - Pfadverwaltung **374**
 - Physische Netzwerkadapter
 - entfernen **272**
 - Hinzufügen zu einem vSphere Distributed Switch **272**
 - verwalten **272**
 - Physische Prozessoren **385**
 - physischer Kompatibilitätsmodus **104**
 - Planen eines vSphere HA-Clusters **433**
 - Planen von Affinität **163**
 - Plug-Ins
 - aktivieren **21**
 - deaktivieren **21**
 - entfernen **22**
 - Fehlerbehebung **22**
 - herunterladen **21**
 - Installieren **21**
 - Installierte anzeigen **21**
 - verwalten **21**
 - Portblockierung **291**
 - Portgruppen
 - Failback **296**
 - Failover-Reihenfolge **296**
 - Lastausgleich **296**
 - Netzwerk-Failover-Ermittlung **296**
 - Schicht 2-Sicherheit **306**
 - Switches benachrichtigen **296**
 - Traffic-Shaping **311**
 - Portgruppen mit früher Bindung **46, 268**
 - Portgruppen mit später Bindung **46, 268**
 - Portkonfiguration **260**
 - Portrichtlinien, Verteilte Portgruppen **315, 316**
 - Portspiegelung
 - erstellen **325**
 - Funktionskompatibilität **323**
 - LRO **323**
 - Name **326, 328**
 - Paketlänge **326**
 - Quellen **326–328**
 - Sitzungstypen **323**
 - Status **327, 328**
 - TSO **323**
 - Überprüfen der Einstellungen **327**

- Versionskompatibilität **323**
- VLAN **326–328**
- vMotion **323**
- Ziele **326, 327, 329**
- Privates VLAN
 - entfernen **271**
 - Erstellen **270**
 - Primär **271**
 - Sekundär **271**
- Profile, verwalten **249**
- Promiscuous-Modus **305, 307, 308, 316**
- Protokolldateien
 - Deaktivieren der Komprimierung **482**
 - ESXi **482**
 - Export **478**
 - extern **478**
 - Sammeln **481, 482**
- Protokolle
 - ESXi **479**
 - Sammeln **481**
 - vSphere Client **479**
- Protokolle, System, *Siehe auch* Fehlerbehebung
- Protokollierung
 - aktivieren **204**
 - Deaktivieren für Gastbetriebssysteme **69**
- Protokollierungsdetails, Festlegen der Protokollierungsebene **33**
- Protokollierungsoptionen, konfigurieren **33**
- Proxy-Server-Einstellungen, Netzwerke **232**
- Prozessorbasierte Lizenzierung **52**
- Prozessoren
 - Statusüberwachung **459**
 - Siehe auch* CPUs
- Prüfen, Anzahl ändern **360**
- PVLAN **303**
- PVSCSI, *Siehe auch* Paravirtueller SCSI-Controller

Q

- QOS-Richtlinien, Verteilte Portgruppen **302, 316**

R

- Raw-Gerätezuordnung **372**
- RDM **442**
- RDMs, Pfadverwaltung **373**
- Rechte und Berechtigungen **76**
- Referenzhost **248**
- Registerkarten, Erste Schritte **15**
- Registerkarten „Erste Schritte“
 - deaktivieren **15**
 - wiederherstellen **15**
- Ressourcenpool, Verteilte Portgruppen **280**
- Ressourcenpools
 - auswählen **97**

- Bearbeiten von Attributen **399**
- entfernen **401**
- Entfernen virtueller Maschinen **401**
- Erstellen **41, 398**
- hierarchisch gleichwertig **397**
- Hinzufügen virtueller Maschinen **400**
- löschen **401**
- Netzwerke **279**
- Root-Ressourcenpool **397**
- übergeordnetes Element **397**
- übertragen **405**
- Ressourcenverwaltung
 - anpassen **430**
 - Hosts **383**
- Ressourcenzuordnungen
 - anzeigen **90**
 - drucken **90**
 - Exportieren **90**
 - Festlegen der maximalen Anzahl an Zuordnungs-Objekten **90**
- Richtlinien, CPU-Energieverwaltung **387**
- Rollen
 - Administrator **78**
 - bearbeiten **79**
 - entfernen **77, 80**
 - erstellen **78**
 - Kein Zugriff **78**
 - klonen **79**
 - Kopieren **79**
 - Nur Lesen **78**
 - Sicherheit **78**
 - Standard **78**
 - umbenennen **79**
 - und Berechtigungen **78**
- Root-Anmeldung, Berechtigungen **76**
- Root-Ressourcenpool **397**
- Routing **332**

S

- SAN LUN **104**
- SAN-LUNs **177, 179**
- SATA-Controller
 - Knotenzuweisung **182**
 - maximale Anzahl **182**
 - Standardverhalten **182**
 - Siehe auch* Speicher-Controller
- Schicht 2-Sicherheit **305**
- Schicht 2-Sicherheitsrichtlinie **305**
- Schnell bereitgestellte Festplatten **112, 113**
- Schnittstellen
 - parallel **171**
 - Parallele Schnittstellen hinzufügen **175**
 - Parallelen Port ändern **176**

- Seriell **171**
 - Seriellen Port ändern **174**
 - vSphere Distributed Switch **43, 264**
- Schwellenwert, Storage I/O Control **396**
- Scratch-Partition aktivieren **26**
- SCSI
 - Ändern des Controller-Typs **184**
 - Controller auswählen **101**
 - Controller hinzufügen **183**
 - gemeinsame Busverwendung **184**
 - Geräte ändern **191**
 - Geräte hinzufügen **190**
 - Paravirtuelle Controller **185**
 - Unterstützte Controllertypen **184**
 - VMware Paravirtuell **101**
- SCSI-Controller
 - hinzufügen **182**
 - maximale Anzahl **182**
 - Standardzuweisungen für virtuelle Festplatten **182**
 - Typen **182**
 - und Knoten des virtuellen Geräts **182**
- Sekundäre VM migrieren, Fault Tolerance **448**
- Sensoren zurücksetzen, Hoststatus **460, 461**
- Serielle Schnittstellen
 - ändern **174**
 - Bedingungen für Netzwerkverbindungen **172**
 - Bedingungen für physische Verbindungen **171**
 - Firewall-Regelsatz hinzufügen **172**
 - hinzufügen **172**
 - Verbindungstypen **171**
- Serieller Port, Umleiten der direkten Konsole mithilfe des vSphere Clients **25**
- Serverkonfiguration für Hyper-Threading **386**
- Sicherheit, Berechtigungen **76**
- Sicherheit von Hosts, Verkleinern von virtuellen Festplatten **68**
- Sicherheitsrichtlinie
 - Richtlinienausnahmen **305**
 - Verteilte Portgruppen **307, 316**
 - Virtuelle Switches **305**
- Sicherheitsrichtlinien, Verteilte Ports **308**
- Signalprüfung, Standard-Switches **294**
- Single Root I/O Virtualization (SR-IOV) **286, 287**
- Sitzungen
 - anzeigen **22**
 - vSphere Client, beenden **23**
- Skripts, Alarme **472, 473**
- SMASH **459**
- SMTP
 - Benachrichtigung **31**
 - konfigurieren **470**
 - Server **31**
- Snapshots
 - Aktivitäten der virtuellen Maschine **212**
 - Arbeitsspeicher **212**
 - Ausschließen virtueller Festplatten **213**
 - Dateien virtueller Maschinen stilllegen **212**
 - Delta-Festplatten **210**
 - erstellen **212, 213**
 - Grundlegende Informationen **210**
 - Hierarchie **210**
 - Konsolidieren **218**
 - löschen **217, 218**
 - Option „Alle löschen“ **217**
 - Option „Löschen“ **217**
 - stilllegen **213**
 - übergeordnetes Element **210**
 - untergeordnetes Element **210**
 - Verhalten **210**
 - virtuelle Maschinen mit dynamischen Festplatten **213**
 - Wechseln (Befehl) **216**
 - wiederherstellen **215, 216**
 - Wiederherstellen des übergeordneten **216**
- SNMP
 - Community-String **32**
 - Einstellungen **32**
 - Empfängerinternetadresse **32**
 - konfigurieren **477**
 - Traps **32**
- SNMP-Traps **471**
- Software-FCoE
 - und VMkernel **339**
 - Adapter aktivieren **340**
- Software-iSCSI, Netzwerk **347**
- Software-iSCSI-Adapter
 - deaktivieren **346**
 - konfigurieren **345**
- Software-iSCSI-Initiatoren, aktivieren **345**
- Software-iSCSI-Initiatoren, Einrichten von Erkennungsadressen **353**
- Sonstige Richtlinien, Verteilte Portgruppen **315, 316**
- Speicher
 - Bereitgestellt **378**
 - iSCSI **442**
 - NAS **442**
 - NFS **442**
 - Nicht freigegeben **378**
 - Speichereinschränkungen, vSphere Client **336**
 - Statusüberwachung **459**
 - Verwendet von virtuellen Maschinen **378**
 - vSphere Client, Speichereinschränkungen **336**
- Speicher-APIs, Storage Awareness **380**

- Speicher-Controller
 - AHCI SATA **182**
 - BusLogic Parallel **182**
 - Einschränkungen **182**
 - Einschränkungen in Bezug auf VMware Paravirtual SCSI **185**
 - IDE **182**
 - Kompatibilität **182**
 - LSI Logic SAS **182**
 - maximale Anzahl **182**
 - SCSI **182**
 - Und Snapshots **182**
 - VMware Paravirtual SCSI **182, 185**
- Speicher-DRS
 - Empfehlungen **421**
 - Wartungsmodus **419**
- Speicheradapter
 - anzeigen **337**
 - erneut prüfen **360**
 - Grundlegende Informationen **342**
- Speicherfilter, deaktivieren **371**
- Speichergerät, umbenennen **359**
- Speichergeräte
 - Anzeigen für einen Adapter **337**
 - Anzeigen für einen Host **336**
 - erneut prüfen **360**
 - Pfade **375**
 - verwalten **359**
- Speichern, Geräteknoten, Verwendung nicht standardmäßiger Geräteknoten **102**
- Speicherort der Auslagerungsdatei **168, 391**
- Speicherort der VM-Auslagerungsdatei **391**
- Sperrmodus
 - aktivieren **67**
 - vSphere Client **67**
- Spitzenbandbreite **309–312, 316**
- SR-IOV
 - aktivieren **287, 288**
 - Hostprofil **287, 288**
- SSL-Zertifikat **86**
- Standard-Gateway, bearbeiten **275**
- Standard-Switch **257**
- Standard-Switches
 - Burstgröße **310**
 - Durchschnittliche Bandbreite **310**
 - Failover **294**
 - Gefälschte Übertragungen **305**
 - Lastausgleich, Richtlinien **294**
 - MAC-Adressänderungen **305**
 - NIC-Gruppierung **294**
 - Portkonfiguration **260**
 - Promiscuous-Modus **305**
 - Sicherheitsrichtlinie **305**
- Signalprüfung **294**
- Spitzenbandbreite **310**
- Traffic-Shaping-Richtlinien **310**
- Verbindungsstatus **294**
- Standby-Adapter **261**
- Standby-Einstellungen, Für virtuelle Maschinen **202**
- Standby-Modus **402, 408, 409**
- Standby-Uplinks **296, 300**
- Start des Diensts
 - Ändern der Richtlinie **64**
 - Festlegen der Optionen **64**
- Starteinstellungen der VM **207**
- Starten, vSphere Client **14**
- Starten und Herunterfahren von virtuellen Maschinen **434**
- Startoptionen
 - BIOS-Einstellungen ändern **204**
 - Verzögerung ändern **204**
- statische Erkennung, konfigurieren **355**
- Statische Erkennungsadressen **353**
- Statistik, Erfassungsintervalle **29**
- Status, Verteilte Ports **269**
- Statusleiste **15**
- Storage DRS
 - Affinitätsregeln **424**
 - aktivieren **416**
 - Anti-Affinitätsregeln **425**
 - Automatisierungsebene **422**
 - deaktivieren **416**
 - Empfehlungen **421**
 - geplante Aufgabe **422**
 - Grundlegende Informationen **416**
 - Statistik **427**
- Storage I/O Control
 - aktivieren **396**
 - Anforderungen **393**
 - Anteile und Grenzwerte **393–395**
 - Einschränkungen **393**
 - Schwellenwert **396**
 - überwachen **394**
- Storage vMotion **135**
- Subnetzmaske, bearbeiten **275**
- Support-Informationen **49**
- Switches benachrichtigen **296, 298, 300, 316**
- syslog **26, 71, 480**
- Sysprep-Antwortdatei
 - Benutzerdefiniert **131**
 - sysprep.inf **131**
 - sysprep.xml **131**
- Systemprotokolle
 - ESXi **479**

- herunterladen **479**
- konfigurieren **481**
- Systems Management Architecture for Server Hardware, , *siehe* SMASH
- Systemzustand, überwachen **460**

T

- Teilautomatisiertes DRS **402**
- Temperatur, überwachen **459**
- Thick-Provisioned Festplatten **112, 113**
- Thin Provisioning **102, 377**
- Thin-Festplatten, Erstellen **378**
- Traffic-Shaping
 - Portgruppen **311**
 - Verteilte Portgruppen **311, 316**
- Traffic-Shaping bei ausgehendem Datenverkehr **312**
- Traffic-Shaping bei eingehendem Datenverkehr **312**
- Traffic-Shaping-Richtlinien
 - Uplink-Ports **312**
 - Verteilte Ports **312**
- Trap-Benachrichtigungen, Alarmer **468**
- Traps, SNMP **471**
- TSO **282**

U

- Übergeordneter Ressourcenpool **397**
- Überprüfung der Richtlinieneinhaltung
 - Fault Tolerance **446**
 - Hostprofile **246**
- übertragen, Ressourcenpool **405**
- überwachen
 - Storage I/O Control **394**
 - vSphere Client **455**
- Überwachung virtueller Maschinen **438**
- umbenennen, Vorlagen **117**
- Umgebungsvariablen, Alarmer **472, 473**
- Unabhängige Festplatte **213**
- Unabhängige Hardware-iSCSI-Adapter
 - IP-Adresse ändern **342**
 - Namen ändern **342**
- Uplink-Adapter
 - Duplex **260**
 - entfernen **272**
 - Geschwindigkeit **260**
 - hinzufügen **261**
 - Hinzufügen zu einem vSphere Distributed Switch **272**
 - verwalten **272**
- Uplink-Portgruppen, VLAN-Richtlinien **303**
- Uplink-Ports
 - Traffic-Shaping-Richtlinien **312**
 - VLAN-Richtlinien **303, 304**

- Uplink-Zuweisungen **266**
- USB-Controller
 - Entfernen aus der virtuellen Maschine **196**
 - Hinzufügen zu einer virtuellen Maschine **195**
- USB-Geräte
 - Entfernen der virtuellen Maschine **198**
 - Hinzufügen zu Clientcomputern **199**
 - Hostgerät zur virtuellen Maschine hinzufügen **197**
 - Remoteclientgerät von VM entfernen **201**
 - Unterstützte Geräte für den Mac OS X-Gast **198**
 - Verhalten mit Hot-Add-Vorgängen **198**
 - Vom Clientcomputer der VM im vSphere-Client hinzufügen **200**
- USB-Passthrough
 - Arbitrator für **194**
 - Controller für **194, 198**
 - Geräte, *Siehe auch* USB-Geräte
 - Konfigurieren von einem Clientcomputer auf eine VM **198**
 - Konfigurieren von einem Host auf eine virtuelle Maschine **194**
 - Vermeiden von Datenverlust **198**

V

- Validierung
 - aktivieren **31**
 - von Benutzern oder Gruppen **31**
 - Zeitraum **31**
- vApps
 - anhalten **225**
 - Anmerkungen bearbeiten **233**
 - Auffüllen **225**
 - Auswahl des Proxy-Servers **232**
 - Auswählen von Netzwerkverknüpfungen **233**
 - Benutzerdefinierte Eigenschaften bearbeiten **230**
 - DHCP auswählen **231**
 - Eigenschaften bearbeiten **226, 227**
 - Einstellungen für das Ausschalten **224**
 - Einstellungen für das Einschalten **223**
 - erstellen **222**
 - Erstellen von Objekten **225**
 - Erweiterte Eigenschaften **229**
 - Erweiterte IP-Zuteilungseigenschaften bearbeiten **230**
 - fortsetzen **225**
 - Hinzufügen von Objekten **226**
 - IP-Pools **231**
 - klonen **224**
 - Konfigurieren der IP-Adresse **231**
 - Konfigurieren von DNS **232**
 - Konfigurieren von Netzwerken **227**

- Optionen zum Herunterfahren **226**
- OVF-Umgebungseigenschaften definieren **230**
- Ressourcen bearbeiten **227**
- Startoptionen **226**
- verwalten **221**
- Variable Informationsgröße für Gastbetriebssystem
 - Begrenzen **69**
 - deaktivieren **69**
- vCenter Converter-Client-Plug-In **147**
- vCenter Server
 - aktive Sitzungen, Anzeige **22**
 - benutzerdefinierte Attribute **19**
 - Datenbankverbindungen **34**
 - erweiterte Einstellungen **35**
 - ID **30**
 - IP-Adresse **30**
 - Kommunikation über eine Firewall **35**
 - konfigurieren **28**
 - Konfigurieren von SNMP **477**
 - Lizenz **28**
 - Lizenz zuweisen **28**
 - Lizenzierung **28**
 - Name **30**
 - SNMP **470**
- vCenter Server-E-Mail-Agent **470**
- vCenter Server-Einschränkungen, vSphere Client **28**
- Verbindungsstatus, Standard-Switches **294**
- version, Virtuelle Maschine **97**
- Verteilte Portgruppen
 - Anzahl der Ports **46, 268**
 - Außerkräftsetzungseinstellungen **47, 268**
 - Beschreibung **46, 268**
 - Bindung auf Host **47, 268**
 - Blockierte Ports **315, 316**
 - Burstgröße **311, 316**
 - Durchschnittliche Bandbreite **311, 316**
 - Failover-Reihenfolge **298, 316**
 - Failover-Richtlinien **298, 316**
 - Format des Portnamens **47, 268**
 - Gefälschte Übertragungen **307, 316**
 - Gruppierungsrichtlinien **298, 316**
 - Hinzufügen **46, 267**
 - Lastausgleich **298, 316**
 - Live-Port verschieben **47, 268**
 - MAC-Adressänderungen **307, 316**
 - Name **46, 268**
 - NetFlow **314, 316**
 - Network I/O Control **313, 316**
 - Netzwerkressourcenpools **313, 316**
 - Portgruppentyp **46, 268**
 - Portrichtlinien **315, 316**
 - Promiscuous-Modus **307, 316**
 - PVLAN **302, 316**
 - QOS-Richtlinien **302, 316**
 - Ressourcenpool **280**
 - Sicherheitsrichtlinie **307, 316**
 - Sonstige Richtlinien **315, 316**
 - Spitzenbandbreite **311, 316**
 - Switches benachrichtigen **298, 316**
 - Traffic-Shaping **311, 316**
 - virtuelle Maschinen **278**
 - VLAN-Richtlinie **302, 316**
 - VLAN-Trunking **302, 316**
 - Zurücksetzen bei Verbindungstrennung konfigurieren **47, 268**
- Verteilte Ports
 - Blockieren **315**
 - Blockierte Ports **316**
 - Eigenschaften **269**
 - Failback **300**
 - Failover-Reihenfolge **300**
 - Gruppierungs- und Failover-Richtlinien **300**
 - Lastausgleich **300**
 - NetFlow **315**
 - Network I/O Control **314**
 - Netzwerk-Failover-Ermittlung **300**
 - Netzwerkressourcenpools **314**
 - Portrichtlinien **316**
 - Status **269**
 - Switches benachrichtigen **300**
 - Traffic-Shaping-Richtlinien **312**
 - überwachen **269**
 - VLAN-Richtlinien **303**
- verwalten, virtuellen Maschinen **207**
- Verwalten **335**
- Verwaltung von Netzwerkressourcen **279**
- Verwaltungsnetzwerk **433**
- Verwaltungsschnittstelle, Absichern **63**
- Verwaltungszugriff, Firewalls **63**
- Verzeichnisdienst
 - Active Directory **81**
 - Konfigurieren eines Hosts **81**
- Verzeichnisserver, anzeigen **82**
- VGT **322**
- Virtual Guest Tagging **322**
- Virtual Serial Port Concentrator **171, 172**
- Virtual SMP **99**
- Virtual Switch Tagging **322**
- Virtuelle CPUs, Anzahl ändern **428**
- Virtuelle Festplatten
 - Anforderungen für die Anpassung des Gastbetriebssystems **121**

- Clusterfunktionen **102**
- Erstellen **102**
- Flaches Format **102**
- gemeinsam nutzen **104**
- Konfiguration **178**
- konfigurieren **177**
- Modi **102**
- Schnell-Format **102**
- sparse **177**
- Thin Provisioning **177**
- Typen **102**
- Verkleinern **68**
- Verwendung des nicht standardmäßigen Gerä-
teknostens **102, 104**
- virtuelle Geräte, USB-Controller hinzufügen **195**
- virtuelle Hardware
 - Arbeitsspeicher **99**
 - CPU-Hyper-Threading **162**
 - CPU/MMU-Aktivierung **164**
 - CPUs **99**
 - Erweiterte CPU-Einstellungen **162, 163**
 - Festplatten **102**
 - Grafikkarten **192**
 - Hinzufügen im laufenden Betrieb aktivie-
ren **159**
 - Hinzufügen virtueller CPUs im laufenden Be-
trieb **160**
 - Hinzufügen von Host-USB-Geräten zur virtuel-
len Maschine **197**
 - Hinzufügen von USB-Geräten **200**
 - Netzwerkkarten **100**
 - Parallele Schnittstellen **175, 176**
 - SCSI-Controller **101**
 - SCSI-Geräte **190, 191**
 - Serielle Schnittstellen **172**
- Virtuelle Maschine, Arbeitsspeicher **166**
- virtuelle Maschine, Konsole **208**
- Virtuelle Maschine, Netzwerke **257**
- virtuelle Maschinen
 - Aktivieren der Protokollierung **204**
 - Arbeitsspeicher **165**
 - Auf einen oder von einem vSphere Distributed
Switch migrieren **277**
 - Aus Vorlage bereitstellen **114**
 - Auslagerungsdatei **168**
 - Auswahl der Konfigurationsoption für das Er-
stellen **95**
 - Auswählen des Gastbetriebssystems **98**
 - Begrenzen der variablen Informationsgrö-
ße **69**
 - benennen **96**
 - benutzerdefinierte Attribute **19**
 - Beschleunigung **205**
 - CPU-Konfiguration **160**
 - CPU-Ressourcen **158**
 - Deaktivieren der Protokollierung **69**
 - Debuggen **205**
 - Diskettenlaufwerke **189, 190**
 - DRS-Automatisierungsebene **403**
 - Energieverwaltungseinstellungen **201**
 - entfernen **209**
 - Entfernen aus einem DRS-Cluster **406**
 - Entfernen aus Ressourcenpools **401**
 - erstellen **94, 95**
 - erweiterte Attribute **431**
 - EVC-Modi **144**
 - Exportieren **149**
 - Festplatten **179**
 - Gastbetriebssystem **156**
 - geplante Aufgabe zum Klonen **110**
 - Hardware **151**
 - Hardwareversion **154**
 - Hardwareversionen **153**
 - hinzufügen **209**
 - Hinzufügen im laufenden Betrieb aktivie-
ren **167**
 - Hinzufügen zu DRS-Clustern **406**
 - Hinzufügen zu Ressourcenpools **400**
 - klonen **108**
 - konfigurieren **151**
 - Konsole anzeigen **16**
 - Konvertieren in Vorlagen **111**
 - Konvertieren von Vorlagen **119**
 - Kopieren und Einfügen deaktivieren **68**
 - Migration **135**
 - migrieren **135, 137, 138**
 - Migrieren auf einen oder von einem Distribu-
ted Switch **277**
 - Mit RDMs **372**
 - Netzwerk **277, 278**
 - Netzwerkadapter **170**
 - Netzwerkkarte **170**
 - Neustartpriorität **438**
 - Öffnen einer Konsole **208**
 - optische Laufwerke **186**
 - Ressourcen **151**
 - Snapshots **210**
 - Speicherort der Auslagerungsdatei **390, 391**
 - Speicherort der Konfigurationsdatei **155**
 - Upgrade der Hardwareversion **153**
 - Verhindern der Gerätetrengung **70**
 - Versionen **97**
 - Virtual SMP **99**
 - Vorlagen konvertieren **111**

- Wiederherstellen eines Hosts **209**
- Zuweisen von WWNs **338**
- Zuweisen zu einem bestimmten Prozessor **386**
- Siehe auch* virtuelle Hardware
- Virtuelle Maschinen
 - abschließen **106**
 - Konfigurieren von Geräten **186**
 - Netzwerkconfiguration **169**
- Virtuelle Netzwerkadapter, entfernen **276**
- virtuelle NUMA **428**
- Virtuelle Prozessoren, , *siehe* CPUs
- virtuellen Maschinen
 - Betriebszustände **202**
 - Entfernen vom Datenspeicher **209**
 - Entfernen von einem Host **209**
 - erstellen **93**
 - Herunterfahren, Einstellungen **207**
 - Namen ändern **155**
 - Starteinstellungen **207**
 - verwalten **207**
 - Siehe auch* Vorlagen, Klone
- Virtueller Adapter **275**
- virtueller Arbeitsspeicher
 - konfigurieren **165**
 - Zuteilung **165**
- virtueller Kompatibilitätsmodus **104**
- Virtuelles LAN **322**
- VLAN
 - Portspiegelung **326–328**
 - Privat **270**
- VLAN-ID
 - Primär **270**
 - Sekundär **270**
- VLAN-Richtlinie, Verteilte Portgruppen **302, 316**
- VLAN-Richtlinien
 - Uplink-Portgruppen **303**
 - Uplink-Ports **303, 304**
 - Verteilte Ports **303**
- VLAN-Trunking, Verteilte Portgruppen **302, 316**
- VLAN-Typ **303**
- VM Component Protection **433**
- VM-Affinität **411, 413, 414**
- VM-Anti-Affinität **411, 413, 414**
- VM-Außerkräftsetzungen **439**
- VM-DRS-Gruppen **413**
- VM-Einschränkungen, vSphere Client **152**
- VM-Hardwareversion **153**
- VM-Host-Affinitätsregel **411–414**
- VM-VM-Affinitätsregel **411, 413**
- VMCP **433**
- VMDK **442**
- VMFS, Neusignierung **363**
- VMFS-Datenspeicher
 - aktualisieren **366**
 - Ändern von Signaturen **364**
 - erneut prüfen **360**
 - Erstellen auf Fibre-Channel-Speicher **361**
 - Erstellen auf iSCSI-Speicher **361**
 - erstellen auf SCSI-Festplatte **361**
 - Erstellen auf Speichergerät **361**
 - Hinzufügen von Erweiterungen **368**
 - Kapazität, erhöhen **368**
 - löschen **370**
- VMFS-Neusignierung **363**
- VMFS-Volume **177**
- VMFS2-Datenspeicher, aktualisieren **366**
- VMFS3, aktualisieren **367**
- VMkernel
 - Gateway **259, 276**
 - Jumbo-Frames **283**
 - Präfix **259, 276**
 - Routing **259, 276**
- VMkernel-Netzwerkadapter
 - bearbeiten **275**
 - Fehlertoleranzprotokollierung **275**
 - hinzufügen **258, 273**
 - vMotion aktivieren **275**
- VMkernel-Schnittstellen **350**
- vMotion
 - 3DNow! **144**
 - Aktivieren auf einem virtuellen Netzwerkadapter **275**
 - CD-ROM, Migrationseinschränkungen **187**
 - DirectPath I/O **286**
 - Kompatibilität **163, 284**
 - Kompatibilitätsprüfungen **140**
 - Migrieren von virtuellen Maschinen **136**
 - Portspiegelung **323**
- VMotion-Schnittstellen, Erstellen **258, 273**
- VMware Paravirtual SCSI-Controller **185**
- VMware Tools
 - aktualisieren **157**
 - Anforderung für Anpassung **121**
- VMware-Kompatibilitätshandbuch, Zugriff **121**
- Vmxnet (erweitert) **282, 283**
- Vollautomatisiertes DRS **402**
- Voraussetzungen, Fault Tolerance **442**
- Vorlagen
 - Ändern des Namens **117**
 - Aufheben der Registrierung **117**
 - Aus der Bestandsliste entfernen **118**
 - Bereitstellen von virtuellen Maschinen **114**
 - erstellen **111**
 - Erstellen **112**
 - klonen **112, 113**

- Konvertieren in virtuelle Maschinen **119**
 - Konvertieren virtueller Maschinen in **111**
 - löschen **118**
 - Löschen **117**
 - OVF **149**
 - umbenennen **117**
 - Wiederherstellen eines Hosts **209**
 - Wiederherstellen in Bestandsliste **118**
 - vpdx, Protokolldateien **482**
 - vService, Abhängigkeit hinzufügen **193, 228**
 - vService, Bearbeiten einer vService-Abhängigkeit **193, 228**
 - vServices überwachen **237**
 - vServices-Abhängigkeit entfernen **194, 229**
 - vServices, Konfiguration **192**
 - vSPC **171, 172**
 - vSphere Authentication Proxy **80, 82**
 - vSphere Client
 - abmelden **14**
 - Anmeldung **14**
 - beenden **14**
 - Drucken von Daten **17**
 - Informationen **13**
 - Lizenzierungseinschränkungen **49**
 - Protokolle **479**
 - Sitzungen **23**
 - Starten **14**
 - vSphere Client, Hosteinschränkungen **25**
 - vSphere Client, Netzwerke **255**
 - vSphere Client, Netzwerkeinschränkungen **255**
 - vSphere Client, vCenter Server-Einschränkungen **28**
 - vSphere Client, VM-Einschränkungen **152**
 - vSphere Distributed Switch
 - aktualisieren **266**
 - bearbeiten **275**
 - CDP **330**
 - Cisco Discovery-Protokoll **44, 265, 330**
 - Einstellungen für die Ressourcenpools **281**
 - Hinzufügen **261**
 - Hinzufügen eines Hosts **45, 263**
 - Hinzufügen eines VMkernel-Netzwerkadapters **273**
 - Hosts **264**
 - Hosts verwalten **263**
 - IP-Adresse **44, 265**
 - Jumbo-Frames **283**
 - Kontaktinformationen des Administrators **44, 265**
 - LLDP **331**
 - Löschen von Ressourcenpools **282**
 - Maximale Anzahl an Ports **44, 265**
 - Maximalwert für MTU **44, 265**
 - Network I/O Control **279**
 - Portspiegelung **322**
 - Schnittstellen **264**
 - Schutz vor der Imitation von MAC-Adressen **305**
 - Schutz vor Prüfung des Datenverkehrs **305**
 - Sicherheitsrichtlinie **305**
 - Spiegeln **322**
 - virtuelle Maschinen **277**
 - Virtuelle Maschinen darauf oder davon migrieren **277**
 - Virtuelle Netzwerkadapter **273**
 - Virtueller Netzwerkadapter **274**
 - Siehe auch* Distributed Switch Network I/O Control
 - vSphere DRS, Erstellen von Regeln **414**
 - vSphere HA
 - Checkliste **433**
 - Clustereinstellungen **434**
 - Fehlermeldungen **433**
 - Konfigurieren von Clustereinstellungen **436**
 - Optionen für virtuelle Maschinen **438**
 - Überwachung virtueller Maschinen **438**
 - vSphere HA-Cluster
 - erstellen **435**
 - Erstellen **434, 446**
 - planen **433**
 - vSphere HA-Zugangssteuerung, Richtlinie **437**
 - vSphere Standard-Switch
 - anzeigen **256**
 - Gruppierungs- und Failover-Richtlinien **296**
 - Portkonfiguration **260**
 - Schutz vor der Imitation von MAC-Adressen **305**
 - Schutz vor Prüfung des Datenverkehrs **305**
 - Sicherheitsrichtlinie **305**
 - vSphere-Administration mit vSphere Client **9**
 - vSphere-CLI **26**
 - vSphere-Client
 - Fenster **17**
 - Kommunikation über eine Firewall **35**
 - Sitzungen **22**
 - VST **322**
- ## W
- Wake-On-LAN (WOL), testen **410**
 - Wake-Protokolle **409**
 - Wartungsmodus
 - Affinitätsregeln ignorieren **420**
 - Datenspeicher **419, 420**
 - Hosts **407**
 - Hosts, Wechseln in den Wartungsmodus **407**
 - Watchdog, Statusüberwachung **459**

wechseln in den Wartungsmodus, Host **407**
 Windows
 Anforderungen für die Anpassung **121**
 Anpassen beim Klonen oder Bereitstellen **123**
 Anpassen von Gastbetriebssystemen **121**
 World Wide Names, , *siehe* WWNs
 WWNNs **338**
 WWNs
 ändern **339**
 Zuweisen zu virtuellen Maschinen **338**
 WWPNS **338**

Z

Zeitüberschreitung
 ESXi Shell **66**
 Intervall **32**
 Zeitüberschreitung bei Sitzung im Leerlauf **66**
 Zeitüberschreitungs-
 einstellungen, konfigurieren **32**
 Zeitüberschreitungsintervall, Einstellung **31**
 Zeitzonen **60**
 Zugangssteuerung
 konfigurieren **436**
 Richtlinie **436**
 zulässige IP-Adressen, Firewall **64**
 Zuordnungen **89**
 Zuordnungen für Raw-Geräte **102, 104, 177, 179**
 Zurücksetzen bei Verbindungstrennung konfigurieren, Verteilte Portgruppen **47, 268**
 Zurücksetzen virtueller Maschinen **202**
 Zuteilen von bereichsbasierten MAC-Adressen **333**
 Zuteilen von präfixbasierten MAC-Adressen **333**
 Zuteilungsparameter der MAC-Adresse anpassen **333**
 Zuweisen von Lizenzschlüsseln **50, 52**

