Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client

Update 3
Geändert am 29. Juli 2022
VMware vSphere 7.0
VMware ESXi 7.0
VMware Host Client 1.37.0

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

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

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

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

Inhalt

Informationen zur Verwaltung eines einzelnen Hosts von vSphere - VMware Host Client

Verwaltung eines einzelnen Hosts von vSphere - VMware Host Client bietet Informationen zur Verwaltungen einzelner Hosts mit dem VMware Host Client.

Der VMware Host Client kann zur Notfallverwaltung verwendet werden, wenn vCenter Server nicht verfügbar ist. Sie können mit dem VMware Host Client normale und erweiterte administrative sowie einfache Fehlerbehebungsaufgaben durchführen.

Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Zur Förderung dieses Grundsatzes bei unseren Kunden, Partnern und der internen Community haben wir diesen Leitfaden aktualisiert, indem wir Vorkommen nicht neutraler Sprache entfernt haben.

Zielgruppe

Diese Informationen sind für alle Benutzer hilfreich, die einzelne ESXi-Hosts mit dem VMware Host Client verwalten möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

Aktualisierte Informationen

Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Revision	Beschreibung
21. OKT. 2022	Geringfügige Aktualisierungen für Konfigurieren von Zeroing für den Userworld-Arbeitsspeicher.
19. OKT. 2022	Geringfügige Aktualisierungen für Aktivieren oder Deaktivieren von virtualisierungsbasierter Sicherheit für eine vorhandene VM im VMware Host Client.
13. OKT. 2022	Die Leerzeichen in den Codeausschnitten von Verbindungsherstellung vom VMware Host Client zu einem ESXi-Host nach dem Upgrade auf eine neuere Version von ESXi ist nicht möglich wurden entfernt.
29. JULI. 2022	■ Die Kennwortanforderungen für ESXi in Konfigurieren der Kennwort- und Kontosperrrichtlinie im VMware Host Client wurden aktualisiert. ■ Schritt 3 des Verfahrens in Konfigurieren der Zeitüberschreitung für SOAP-Sitzungen im VMware Host Client wurde aktualisiert.
26. Mai 2022	Die Informationen im Abschnitt Ändern der Autostart-Konfiguration im VMware Host Client wurden aktualisiert.
16. Mai 2022	Zum Abschnitt Generieren eines Support-Pakets im VMware Host Client wurde ein Screenshot hinzugefügt.
12. APR 2022	Zum Abschnitt Verwenden der Spaltenkonfiguration von Controllern für virtuelle Maschinen im VMware Host Client wurde ein Screenshot hinzugefügt, der die Spaltenkonfiguration anzeigt.

Revision	Beschreibung
28. OKT. 2021	■ Alle Themen, die Informationen zum Erstellen einer virtuellen Maschine enthalten, wurden in Erstellen einer virtuellen Maschine im VMware Host Client konsolidiert. ■ Alle Themen, die Informationen zum Bereitstellen einer virtuellen Maschine aus einer OVF- oder OVA-Datei enthalten, wurden in Bereitstellung einer virtuellen Maschine aus einer OVF- oder OVA-Datei im VMware Host Client konsolidiert. ■ Alle Themen, die Informationen zum Registrieren einer vorhandenen virtuellen Maschine enthalten, wurden in Registrieren einer vorhandenen virtuellen Maschine im VMware Host Client konsolidiert. ■ Geringfügiges Update für Hinzufügen eines ESXi-Benutzers im VMware Host Client. ■ Geringfügiges Update für Bearbeiten der Uhrzeitkonfiguration eines ESXi-Hosts im VMware Host Client. ■ Verbindungsherstellung vom VMware Host Client zu einem ESXi-Host nach dem Upgrade auf eine neuere Version von ESXi ist nicht möglich Wurde aktualisiert und die alten Versionsinformationen wurden entfernt. ■ Die Tabelle „Maximaler Arbeitsspeicher der virtuellen Maschine“ in Ändern der Arbeitsspeicherkonfiguration wurde aktualisiert. ■ Geringfügiges Update für Ändern der Anzahl virtueller CPUs im VMware Host Client. ■ Die Diagramme in Einrichten eines Netzwerks für iSCSI und iSER und Best Practices für die Konfiguration des Netzwerks mit Software-iSCSI wurden aktualisiert.
05. OKT. 2021	Erstversion.

VMware Host Client – Übersicht

1

Der VMware Host Client ist ein auf HTML5 basierender Client, mit dem eine Verbindung zu einzelnen ESXi-Hosts hergestellt wird und diese verwaltet werden.

Sie können mit VMware Host Client normale und erweiterte administrative sowie einfache Fehlerbehebungsaufgaben auf dem ESXi-Zielhost durchführen. Des Weiteren können Sie VMware Host Client zur Notfallverwaltung verwenden, wenn vCenter Server vorübergehend nicht verfügbar ist.

Es ist wichtig zu wissen, dass VMware Host Client und vSphere Client nicht identisch sind. Mit dem vSphere Client stellen Sie eine Verbindung zu vCenter Server her und verwalten mehre ESXi-Hosts, während Sie mit dem VMware Host Client lediglich einen einzigen ESXi-Host verwalten.

Zu den Funktionen des VMware Host Client zählen unter anderem die folgenden Vorgänge:

- Einfache Virtualisierungsvorgänge wie Bereitstellen und Konfigurieren von virtuellen Maschinen von unterschiedlicher Komplexität
- Erstellen und Verwalten von Netzwerken und Datenspeichern
- Fortgeschrittenes Optimieren von Optionen auf Hostebene zur Leistungssteigerung

Dieses Kapitel enthält die folgenden Themen:

Systemanforderungen für VMware Host Client

Stellen Sie sicher, dass Ihr Browser VMware Host Client unterstützt.

Die folgenden Gastbetriebssysteme und Webbrowserversionen werden für VMware Host Client unterstützt.

Unterstützte Browser	Mac OS	Windows 32-Bit und 64-Bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+

Unterstützte Browser	Mac OS	Windows 32-Bit und 64-Bit	Linux
Microsoft Edge	90+	90+	Nicht verfügbar
Safari	9.0+	Nicht verfügbar	Nicht verfügbar

Verwenden der VMware Host Client

Die eingebettete VMware Host Client-Instanz ist ein HTML5-basierter Client, der nur zur Verwaltung einzelner ESXi-Hosts verwendet wird. Wenn vCenter Server vorübergehend nicht verfügbar ist, können Sie VMware Host Client zur Notfallverwaltung verwenden.

Starten und Anmelden des VMware Host Client

Sie können mit dem VMware Host Client einzelne ESXi-Hosts verwalten und verschiedene administrative und Fehlerbehebungsaufgaben an den virtuellen Maschinen durchführen.

Hinweis Der VMware Host Client kann nur von Administratoren verwendet werden.

Verfahren

1. Geben Sie in einem Browser den Namen oder die IP-Adresse des Zielhosts im Format **`http://`*`Hostname`*`/ui`** bzw. **`http://`*`Host-IP-Adresse`*`/ui`** ein.

   Ein Anmeldebildschirm wird angezeigt.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Klicken Sie zum Fortfahren auf **Anmelden**.
4. Lesen Sie die Seite mit dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware und entscheiden Sie, ob Sie dem Programm beitreten möchten.

   Informationen über das Programm und darüber, wie Sie es jederzeit konfigurieren können, finden Sie unter Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit.
5. Klicken Sie auf **OK**.

Ergebnisse

Sie sind nun beim ESXi-Zielhost angemeldet.

Abmelden vom VMware Host Client

Wenn Sie den ESXi-Zielhost nicht mehr anzeigen oder verwalten müssen, melden Sie sich beim VMware Host Client ab.

Hinweis Durch das Schließen einer VMware Host Client-Sitzung wird der Host nicht beendet.

Verfahren

- Klicken Sie zum Abmelden vom ESXi-Host, auf den Benutzernamen oben im VMware Host Client-Fenster und wählen Sie im Dropdwn-Menü **Abmelden**.

  Sie sind nun vom VMware Host Client abgemeldet. Auf dem ESXi-Zielhost werden alle normalen Aktivitäten weiterhin durchgeführt.

Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit

Sie können am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, um VMware anonymes Feedback oder Informationen zur Verbesserung der Qualität, Zuverlässigkeit und Funktionalität von VMware-Produkten und -Diensten zur Verfügung zu stellen.

VMware-Programm zur Verbesserung der Benutzerfreundlichkeit

VMware Tools ist Teil des Programms zur Verbesserung der Benutzerfreundlichkeit von VMware.

Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html eingesehen werden.

Abmeldung und erneute Anmeldung beim Programm zur Verbesserung der Benutzerfreundlichkeit im VMware Host Client

Sie können sich jederzeit beim Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) abmelden oder erneut anmelden.

Verfahren

1. Um sich bei CEIP abzumelden bzw. erneut anzumelden, klicken Sie auf den Benutzernamen im oberen Seitenbereich von VMware Host Client.
2. Zeigen Sie auf **Client-Einstellungen**> **Nutzungsstatistiken senden**, um sich bei CEIP abzumelden bzw. erneut anzumelden.

Host-Verwaltung mit dem VMware Host Client

2

Mit dem VMware Host Client können Sie einzelne ESXi-Hosts verwalten, während vCenter Server-Upgrades stattfinden oder wenn vCenter Server nicht mehr reagiert oder nicht mehr verfügbar ist.

Der VMware Host Client verfügt über eine Reihe wichtiger Fehlerbehebungsfunktionen, mit denen Sie Aufgaben auf dem ESXi-Host durchführen können, auf dem Sie angemeldet sind, wenn vCenter Server nicht verfügbar ist. Zu diesen Funktionen gehören u. a. die Konfiguration erweiterter Hosteinstellungen, Lizenzierung, Verwaltung von Zertifikaten, Verwendung der ESXi Shell, Aktivierung des Sperrmodus uvm.

Dieses Kapitel enthält die folgenden Themen:

Verwalten von Systemeinstellungen im VMware Host Client

Sie können mit dem VMware Host Client erweiterte Hosteinstellungen verwalten, dem Host Lizenzen zuweisen oder von ihm entfernen, Start- und Stopprichtlinien für Hostdienste konfigurieren und die Datum-und Uhrzeit-Konfiguration des Hosts verwalten.

Verwalten von erweiterten Einstellungen im VMware Host Client

Sie können die Einstellungen eines Hosts mit dem VMware Host Client ändern.

Vorsicht Das Ändern der erweiterten Optionen wird nicht unterstützt, es sei denn, der technische Support von VMware oder ein KB-Artikel weisen Sie an, dies zu tun. In allen anderen Fällen wird das Ändern dieser Optionen als nicht unterstützt betrachtet. In den meisten Fällen werden mit den Standardeinstellungen bereits beste Ergebnisse erzielt.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **System**.
2. Klicken Sie auf **Erweiterte Einstellungen**.
3. Klicken Sie mit der rechten Maustaste auf das jeweilige Element in der Liste und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird angezeigt.
4. Bearbeiten Sie den Wert und klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.
5. (Optional) Klicken Sie mit der rechten Maustaste auf das jeweilige Element in der Liste und wählen Sie **Auf Standardeinstellungen zurücksetzen**, um die ursprünglichen Einstellungen des Elements wiederherzustellen.

Erstellen einer ersten Begrüßungsnachricht für die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) und den VMware Host Client

Mithilfe des VMware Host Client können Sie eine Begrüßungsnachricht erstellen, die auf dem ersten Bildschirm der DCUI (Direct Console User Interface) und im Anmeldefenster des VMware Host Client angezeigt wird. Sie können auch eine Begrüßungsnachricht erstellen, die gegebenenfalls nach der Anmeldung eines Benutzers beim VMware Host Client angezeigt wird.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.

Option	Aktion
Erstellen Sie eine Begrüßungsnachricht, die vor der Anmeldung bei der DCUI und dem VMware Host Client angezeigt wird	a Geben Sie **`Annotations.WelcomeMessage`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Annotations.WelcomeMessage` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. Das Dialogfeld **Option bearbeiten** wird geöffnet. c Geben Sie die Begrüßungsnachricht im Textfeld **Neuer Wert** ein. Zum Festlegen der Standardmeldung lassen Sie das Textfeld **Neuer Wert** leer.
Erstellen Sie eine Begrüßungsnachricht, die nach der Anmeldung beim VMware Host Client angezeigt wird.	a Geben Sie **`UserVars.HostClientWelcomeMessage`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `UserVars.HostClientWelcomeMessage` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. Das Dialogfeld **Option bearbeiten** wird geöffnet. c Geben Sie die Begrüßungsnachricht im Textfeld **Neuer Wert** ein. Zum Festlegen der Standardmeldung lassen Sie das Textfeld **Neuer Wert** leer.
Aktivieren oder deaktivieren Sie die Anzeige der Begrüßungsnachricht, nachdem Sie sich beim VMware Host Client angemeldet haben.	a Geben Sie **`UserVars.HostClientEnableMOTDNotification`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `UserVars.HostClientEnableMOTDNotification` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. Das Dialogfeld **Option bearbeiten** wird geöffnet. c Geben Sie im Textfeld **Neuer Wert** den neuen Wert ein. Mit dem Wert null (0) wird die Anzeige der Begrüßungsnachricht deaktiviert. Mit dem Wert eins (1) wird die Anzeige der Begrüßungsnachricht aktiviert.

2 Klicken Sie auf **Speichern**.

3 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Konfigurieren der Zeitüberschreitung für die Sitzung der VMware Host Client-Benutzeroberfläche

In VMware Host Client läuft die Sitzung der Benutzeroberfläche automatisch nach 15 Minuten ab. Anschließend müssen Sie sich erneut beim VMware Host Client anmelden.

Sie können den standardmäßigen Zeitüberschreitungswert für Inaktivität erhöhen, indem Sie einen erweiterten Konfigurationsparameter ändern. Die Standardeinstellung beträgt 900 Sekunden.

Verfahren

- Konfigurieren Sie die Zeitüberschreitung für die Sitzung der Benutzeroberfläche.

Option	Aktion
In den erweiterten VMware Host Client-Einstellungen	a Klicken Sie auf **Verwalten** in der VMware Host Client-Bestandsliste und anschließend auf **Erweiterte Einstellungen** b Geben Sie **`UserVars.HostClientSessionTimeout`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. c Klicken Sie mit der rechten Maustaste auf `UserVars.HostClientSessionTimeout` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. Das Dialogfeld **Option bearbeiten** wird geöffnet. d Geben Sie im Textfeld **Neuer Wert** die Zeitüberschreitungseinstellung in Sekunden ein. **Hinweis** Mit dem Wert NULL (0) wird die Zeitüberschreitung deaktiviert. e Klicken Sie auf **Speichern**. f (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.
Im Dropdown-Menü „Benutzereinstellungen“	a Klicken Sie im oberen Bereich des Fensters VMware Host Client auf den Benutzernamen und wählen Sie **Einstellungen > Timeout der Anwendung > aus.** b Zur Angabe der Zeitüberschreitung bei Inaktivität wählen Sie die Uhrzeit aus. c Zum Deaktivieren der Zeitüberschreitung bei Inaktivität wählen Sie `Off` aus.

Konfigurieren der Zeitüberschreitung für SOAP-Sitzungen im VMware Host Client

In VMware Host Client können Sie die Zeitüberschreitung für die SOAP-Sitzung konfigurieren.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.
2. Geben Sie **`Config.HostAgent.vmacore.soap.sessionTimeout`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**.
3. Klicken Sie mit der rechten Maustaste auf `Config.HostAgent.vmacore.soap.sessionTimeout` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.

4 Geben Sie im Textfeld **Neuer Wert** die Zeitüberschreitungseinstellung in Sekunden ein.

   Mit dem Wert „0“ wird die Zeitüberschreitung deaktiviert.

5 Klicken Sie auf **Speichern**.

6 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Konfigurieren der Kennwort- und Kontosperrrichtlinie im VMware Host Client

Für ESXi-Hosts müssen Sie ein Kennwort mit vordefinierten Anforderungen verwenden. Mithilfe der erweiterten Option `Security.PasswordQualityControl` können Sie die erforderliche Kennwortlänge und Zeichenklassenanforderungen ändern oder Passphrasen zulassen. Sie können auch die Anzahl der Kennwörter festlegen, die für jeden Benutzer gespeichert werden soll. Verwenden Sie dazu die erweiterte Option `Security.PasswordHistory`. Mit der erweiterten Option `Security.PasswordMaxDays` können Sie die maximale Anzahl an Tagen zwischen Kennwortänderungen festlegen.

Hinweis Führen Sie nach Änderungen an den Einstellungen für das Standardkennwort immer zusätzliche Tests durch.

Wenn Sie sich mit falschen Anmeldedaten anmelden, wird über die Kontosperrrichtlinie festgelegt, wann und wie lange Ihr Konto im System gesperrt wird.

ESXi-Kennwörter

ESXi erzwingt Kennwortanforderungen für den Zugriff.

- Wenn Sie ein Kennwort erstellen, müssen darin standardmäßig Zeichen aus drei der vier folgenden Zeichenklassen enthalten sein: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen, wie z. B. Unter- oder Schrägstriche.
- Das Kennwort muss standardmäßig aus mindestens 7 und maximal 40 Zeichen bestehen.
- Kennwörter dürfen kein Wort aus einem Wörterbuch und keinen Teil eines Worts aus einem Wörterbuch enthalten.
- Kennwörter dürfen den Benutzernamen oder Teile des Benutzernamens nicht enthalten.

Hinweis Wenn ein Kennwort mit einem Großbuchstaben beginnt, wird dieser bei der Berechnung der verwendeten Zeichenklassen nicht berücksichtigt. Endet ein Kennwort mit einer Ziffer, wird diese bei der Berechnung der verwendeten Zeichenklassen ebenfalls nicht berücksichtigt.

Beispiel für ESXi-Kennwörter

Die folgenden Beispielkennwörter veranschaulichen potenzielle Kennwörter, wenn die Option wie folgt festgelegt ist:

```
retry=3 min=disabled,disabled,disabled,7,7
```

Mit dieser Einstellung wird ein Benutzer bis zu drei Mal (retry=3) zur Eingabe eines neuen Kennworts aufgefordert, wenn ein Kennwort nicht ausreichend stark ist oder das Kennwort zweimal nicht korrekt eingegeben wurde. Kennwörter mit einer oder zwei Zeichenklassen und Kennwortsätzen sind nicht zulässig, da die ersten drei Elemente deaktiviert sind. Kennwörter mit drei oder vier Zeichenklassen erfordern sieben Zeichen.

Die folgenden Kennwortkandidaten erfüllen die Kennwortanforderungen:

- xQaTEhb!: Enthält acht Zeichen aus drei Zeichenklassen.
- xQaT3#A: Enthält sieben Zeichen aus vier Zeichenklassen.

Die folgenden Kennwortkandidaten erfüllen nicht die Kennwortanforderungen:

- Xqat3hi: Beginnt mit einem Großbuchstaben, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.
- xQaTEh2: Endet mit einer Ziffer, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.

Kennwortqualitätskontrolle

Sie können die Qualität von Kennwörtern mithilfe der erweiterten Option `Security.PasswordQualityControl` steuern.

`Security.PasswordQualityControl` besteht aus mehreren Einstellungen mit folgendem Muster:

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

Einstellungen für die Kennwortqualitätskontrolle	Beschreibung	Standard
`retry=N`	Die Häufigkeit, mit der der Benutzer ein neues Kennwort angeben muss, wenn das Kennwort falsch oder nicht ausreichend stark ist.	`retry=3`
`min=N0,N1,N2,N3,N4`	Zeichenklasse und geforderte Mindestlänge der Passphrase. ■ `N0` ist die Mindestlänge von Kennwörtern aus einer einzelnen Zeichenklasse. ■ `N1` ist die Mindestlänge von Kennwörtern aus zwei Zeichenklassen. ■ `N2` ist die Mindestlänge für eine Passphrase. ■ `N3` ist die Mindestlänge für drei Zeichenklassen. ■ `N4` ist die Mindestlänge für vier Zeichenklassen. Sie können `disabled` verwenden, um ein Kennwort mit der angegebenen Anzahl an Zeichenklassen nicht zuzulassen.	`min=disabled,disabled,disabled,7,7`
`max=N`	Die maximal zulässige Kennwortlänge.	`max=40`
`passphrase=N`	Die Anzahl der Wörter, die für eine Passphrase erforderlich sind. Um sicherzustellen, dass die `passphrase` erkannt wird, legen Sie `N2` in der Einstellung `min` nicht auf `disabled` fest.	`passphrase=3`
`similar=permit|deny`	Gibt an, ob ein Kennwort dem alten Kennwort ähneln darf. Stellen Sie zur Verwendung dieser Einstellung sicher, dass Sie die Option `Security.PasswordHistory` auf einen Wert ungleich null festlegen.	`similar=deny`

ESXi-Passphrase

Anstelle eines Kennworts können Sie eine Passphrase verwenden. Passphrasen sind standardmäßig deaktiviert. Sie können die Standardeinstellung mithilfe der erweiterten Option `Security.PasswordQualityControl` ändern.

Beispielsweise können Sie diese Option wie folgt ändern.

```
retry=3 min=disabled,disabled,16,7,7
```

In diesem Beispiel sind Passphrasen mit mindestens 16 Zeichen zulässig. Die Passphrase muss aus mindestens 3 Wörtern bestehen, die durch Leerzeichen getrennt sind.

Beispiel für Kennwortverlauf und Rotationsrichtlinie

Um einen Verlauf von 5 Kennwörtern zu speichern, legen Sie die Option `Security.PasswordHistory` auf 5 fest.

Um eine 90-tägige Richtlinie für die Kennwortrotation zu erzwingen, legen Sie die Option `Security.PasswordMaxDays` auf 90 fest.

ESXi-Kontosperrrichtlinie

Benutzer werden nach einer vorher festgelegten Anzahl von aufeinanderfolgenden Fehlversuchen gesperrt. Standardmäßig werden Benutzer nach fünf aufeinanderfolgenden Fehlerversuchen innerhalb von drei Minuten gesperrt. Ein gesperrtes Konto wird automatisch nach 15 Minuten wieder entsperrt. Sie können die maximal zulässige Anzahl an Fehlversuchen und den Zeitraum, in dem das Benutzerkonto gesperrt wird, mithilfe der erweiterten Optionen `Security.AccountLockFailures` und `Security.AccountUnlockTime` ändern.

Führen Sie die folgenden Schritte aus, um die Administratorkennwörter und das Kontosperrungsverhalten zu konfigurieren.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.

Option	Aktion
Konfigurieren Sie die erforderliche Kennwortlänge und die geforderte Zeichenklasse oder lassen Sie Passphrasen zu.	a Geben Sie **`Security.PasswordQualityControl`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Security.PasswordQualityControl` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.
Konfigurieren der Anzahl der für jeden Benutzer zu speichernden Kennwörter	a Geben Sie **`Security.PasswordHistory`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Security.PasswordHistory` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. **Hinweis** Mit dem Wert „0“ wird der Kennwortverlauf deaktiviert.
Konfigurieren der maximalen Anzahl an Tagen zwischen Kennwortänderungen	a Geben Sie **`Security.PasswordMaxDays`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Security.PasswordMaxDays` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

Option	Aktion
Konfigurieren der Anzahl der fehlgeschlagenen Anmeldeversuche, die bis zur Sperrung zulässig sind	a Geben Sie **`Security.AccountLockFailures`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Security.AccountLockFailures` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus. **Hinweis** Mit dem Wert „0“ wird das Sperren von Konten deaktiviert.
Konfigurieren Sie den Zeitraum, während dem das Konto des Benutzers gesperrt ist	a Geben Sie **`Security.AccountUnlockTime`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**. b Klicken Sie mit der rechten Maustaste auf `Security.AccountUnlockTime` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

Das Dialogfeld **Option bearbeiten** wird geöffnet.

2 Geben Sie im Textfeld **Neuer Wert** die neue Einstellung ein.

3 Klicken Sie auf **Speichern**.

4 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Konfigurieren von Syslog im VMware Host Client

Zum Konfigurieren des Syslog-Diensts können Sie den VMware Host Client verwenden.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.

2 Geben Sie im Textfeld **Suchen** den Namen der zu ändernden Einstellung ein und klicken Sie auf das Symbol **Suchen**.

Option	Beschreibung
Syslog.global.LogHost	Remotehost, an den Syslog-Meldungen weitergeleitet werden, und der Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einschließen, wie z. B. `protocol://hostName1:port`, wobei udp, tcp oder ssl als `protocol` fungieren kann. Sie können nur Port 514 für UDP verwenden. Das SSL-Protokoll verwendet TLS 1.2. Beispiel: `ssl://hostName1:1514`. Bei dem Wert `port` kann es sich um eine beliebige Dezimalzahl zwischen 1 und 65535 handeln. Es gibt zwar keinen festen Grenzwert für die Anzahl der Remotehosts, die Syslog-Meldungen empfangen; es wird jedoch empfohlen, die Anzahl der Remotehosts auf fünf oder weniger zu begrenzen.
Syslog.global.logCheckSSLCerts	Erzwingen Sie die Überprüfung der SSL-Zertifikate, wenn Sie sich bei einem Remotehost anmelden.
Syslog.global.defaultRotate	Maximale Anzahl der beizubehaltenden Archive. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.

Option	Beschreibung
Syslog.global.defaultSize	Standardgröße des Protokolls in KB, 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 `/scratch` auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Geben Sie das Verzeichnis im Format [*Datenspeichername*] *Pfad_zur_Datei* an, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad `[storage1] /systemlogs` dem Pfad `/vmfs/volumes/storage1/systemlogs` 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.

3 Klicken Sie mit der rechten Maustaste auf den Namen der Einstellung und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.

4 Klicken Sie zur Prüfung der SSL-Zertifikate bei der Anmeldung bei einem Remotehost auf **True** unter **Neuer Wert**.

5 Klicken Sie auf **Speichern**.

6 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Konfigurieren erweiterter Optionen für TLS-/SSL-Schlüssel

Sie können die Sicherheitsprotokolle und kryptografischen Algorithmen konfigurieren, die zum Verschlüsseln der Kommunikation mit dem ESXi-Host verwendet werden.

Der TLS-Schlüssel (Transport Layer Security) sichert die Kommunikation mit dem Host mithilfe des TLS-Protokolls. Beim ersten Start generiert der ESXi-Host den TLS-Schlüssel als 2048-Bit-RSA-Schlüssel. Aktuell wird die automatische Erzeugung von ECDSA-Schlüsseln für TLS von ESXi nicht implementiert. Der private TLS-Schlüssel ist nicht für die Verwendung durch den Administrator vorgesehen.

Der SSH-Schlüssel sichert die Kommunikation mit dem ESXi-Host unter Verwendung des SSH-Protokolls. Beim ersten Start erzeugt das System den SSH-Schlüssel als 2048-Bit-RSA-Schlüssel. Der SSH-Server ist standardmäßig deaktiviert. Der SSH-Zugriff ist in erster Linie zur Fehlerbehebung gedacht. Der SSH-Schlüssel ist nicht für die Verwendung durch den Administrator vorgesehen. Für die Anmeldung über SSH sind Administratorrechte erforderlich, die gleichbedeutend mit allen Hostberechtigungen sind. Informationen zum Aktivieren von SSH-Zugriff finden Sie unter Aktivieren von Secure Shell (SSH) im VMware Host Client.

Sie können die folgenden Schlüsseleinstellungen für die Sicherheit des ESXi-Hosts konfigurieren.

Schlüssel	Standard	Beschreibung
UserVars.ESXiVPsAllowedCiphers	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	Die standardmäßige Schlüsselsteuerzeichenfolge.
UserVars.ESXiVPsDisabledProtocols	sslv3,tlsv1,tlsv1.1	Aktiviert standardmäßig TLS-Protokolle der Versionen v1.0, v1.1 und v1.2. SSL v3.0 ist deaktiviert. Wenn Sie kein Protokoll angeben, werden alle Protokolle aktiviert.
Config.HostAgent.ssl.keyStore.allowAny	False	Sie können dem Truststore der ESXi-Zertifizierungsstelle jedes Zertifikat hinzufügen.
Config.HostAgent.ssl.keyStore.allowSelfSigned	False	Sie können selbstsignierte Zertifikate ohne Zertifizierungsstelle zum Truststore der ESXi-Zertifizierungsstelle hinzufügen, d. h. Zertifikate, für die das CA-Bit nicht festgelegt ist.
Config.HostAgent.ssl.keyStore.discardLeaf	True	Verwirft untergeordnete Zertifikate, die dem Truststore der ESXi-Zertifizierungsstelle hinzugefügt wurden.

So konfigurieren Sie die Einstellungen für ESXi-Sicherheitsschlüssel:

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.
2. Geben Sie den Sicherheitsschlüssel im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**.
3. Klicken Sie mit der rechten Maustaste auf den Sicherheitsschlüssel und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.
4. Geben Sie im Feld **Neuer Wert** den neuen Wert ein und klicken Sie auf **Speichern**.
5. (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Konfigurieren von Zeroing für den Userworld-Arbeitsspeicher

Mit VMware Host Client können Sie über die erweiterte Option `Mem.MemEagerZero` festlegen, wie Seiten für virtuelle Maschinen und Benutzerspeicheranwendungen gelöscht und mit Nullbyte aufgefüllt werden.

Um alle Seiten nach Zuteilung zu virtuellen Maschinen und Benutzerspeicheranwendungen zu löschen und mit Nullbyte aufzufüllen, legen Sie `Mem.MemEagerZero` auf eins (1) fest. Wenn der Arbeitsspeicher nicht wiederverwendet wird, verhindert diese Einstellung, dass die Informationen einer virtuellen Maschine oder User Space-Anwendung anderen Clients zugänglich gemacht werden, während der vorherige Inhalt im Arbeitsspeicher beibehalten wird.

Wenn Sie `Mem.MemEagerZero` auf 1 festlegen, werden die Seiten gelöscht und mit Nullbyte aufgefüllt, sobald eine Benutzerbereichsanwendung beendet wird. Unter folgenden Bedingungen werden bei virtuellen Maschinen solche Seiten gelöscht und mit Nullbyte aufgefüllt:

- Die virtuelle Maschine ist nun ausgeschaltet.
- Die Seiten der virtuellen Maschine werden migriert.
- Der ESXi-Host fordert VM-Arbeitsspeicher zurück.

Hinweis Für virtuelle Maschinen können Sie dieses Verhalten festlegen, indem Sie die erweiterte Option `sched.mem.eagerZero` auf **`TRUE`** setzen.

Informationen zum Festlegen der erweiterten Optionen für virtuelle Maschinen finden Sie in der Dokumentation zur *vSphere-Ressourcenverwaltung*.

Führen Sie die folgenden Schritte aus, um Zeroing (löschen und mit Nullbyte auffüllen) für den Userworld-Arbeitsspeicher zu konfigurieren.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.
2. Geben Sie **`Mem.MemEagerZero`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**.
3. Klicken Sie mit der rechten Maustaste auf `Mem.MemEagerZero` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.
4. Geben Sie im Textfeld **Neuer Wert** den neuen Wert ein.

   Der Standardwert lautet null (0).
5. Klicken Sie auf **Speichern**.
6. (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Ändern der Autostart-Konfiguration im VMware Host Client

Konfigurieren Sie Autostart-Optionen, die der ESXi-Host beim Start und Beenden anwenden soll.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **System**.

2 Klicken Sie auf **Autostart**.

3 Klicken Sie auf **Einstellungen bearbeiten**.

4 Wählen Sie **Ja**, um das Ändern der Autostart-Konfiguration zu aktivieren.

Option	Beschreibung
Startverzögerung	Nachdem Sie den ESXi-Host gestartet haben, beginnt er mit dem Einschalten der virtuellen Maschinen, für die der automatische Start konfiguriert ist. Nachdem der ESXi-Host die erste virtuelle Maschine eingeschaltet hat, wartet der Host die angegebene Verzögerungszeit ab und schaltet dann die nächste virtuelle Maschine ein.
Stoppverzögerung	Die Verzögerung beim Herunterfahren ist die maximale Zeit, für die der ESXi-Host auf den Abschluss eines Befehls zum Herunterfahren wartet. Virtuelle Maschinen werden in umgekehrter Reihenfolge der Startreihenfolge heruntergefahren. Nachdem der ESXi-Host die erste virtuelle Maschine innerhalb des von Ihnen festgelegten Zeitraums heruntergefahren hat, fährt der Host die nächste virtuelle Maschine herunter. Wenn eine virtuelle Maschine nicht innerhalb der angegebenen Verzögerungszeit heruntergefahren wird, führt der Host einen Ausschaltbefehl aus und beginnt dann mit dem Herunterfahren der nächsten virtuellen Maschine. Der ESXi-Host wird erst heruntergefahren, nachdem alle virtuellen Maschinen herunterfahren wurden.
Aktion stoppen	Wählen Sie die entsprechende Aktion beim Herunterfahren für die virtuellen Maschinen auf dem Host aus, wenn der Host heruntergefahren wird. ■ **Systemstandard** ■ **Ausschalten** ■ **Anhalten** ■ **Herunterfahren**
Auf Taktsignal warten	Wählen Sie **Ja** aus, um die Option **Auf Taktsignal warten** zu aktivieren. Sie können diese Option verwenden, wenn auf dem Gastbetriebssystem der virtuellen Maschine VMware Tools installiert ist. Nachdem der ESXi-Host die erste virtuelle Maschine eingeschaltet hat, schaltet der Host sofort die nächste virtuelle Maschine ein. Die Startreihenfolge, in der virtuelle Maschinen eingeschaltet werden, wird fortgesetzt, nachdem die virtuelle Maschine das erste Taktsignal empfangen hat.

Wenn Sie eine Verzögerungsoption auf `-1` festlegen, verwendet das System die Standardoption.

5 Klicken Sie auf **Speichern**.

Bearbeiten der Uhrzeitkonfiguration eines ESXi-Hosts im VMware Host Client

Mit dem VMware Host Client können Sie die Uhrzeiteinstellungen eines Hosts manuell konfigurieren oder die Uhrzeit und das Datum des Hosts mit einem NTP- oder PTP-Server synchronisieren. NTP bietet eine Zeitgenauigkeit im Millisekundenbereich und PTP eine Zeitgenauigkeit im Mikrosekundenbereich.

Der NTP-Dienst auf dem Host fragt in regelmäßigen Abständen die Uhrzeit und das Datum vom NTP-Server ab. Sie können mithilfe der Schaltflächen **Starten**, **Beenden** oder **Neustarten** den Status des NTP-Diensts auf dem Host jederzeit unabhängig von der ausgewählten Startrichtlinie für den NTP-Dienst ändern.

PTP stellt eine präzise Uhrzeitsynchronisierung für die virtuellen Maschinen innerhalb eines Netzwerks bereit. Sie können den PTP-Dienst auf dem Host mithilfe der Schaltflächen **Starten**, **Beenden** oder **Neu starten** jederzeit ändern. Durch das Starten oder Beenden des PTP-Diensts wird PTP automatisch aktiviert oder deaktiviert. Um die Änderung bei der manuellen Aktivierung oder Deaktivierung von PTP anzuwenden, starten oder beenden Sie den PTP-Dienst.

Weitere Informationen zu Diensten finden Sie unter Verwalten von Diensten im VMware Host Client.

Hinweis Die NTP- und PTP-Dienste können nicht gleichzeitig ausgeführt werden.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten**.

2 Klicken Sie auf der Registerkarte **System** auf **Uhrzeit und Datum**.

3 Legen Sie Uhrzeit und Datum für den Host fest.

Option	Aktion
Datum und Uhrzeit auf diesem Host manuell konfigurieren	a Klicken Sie auf **NTP-Einstellungen bearbeiten**. Das Dialogfeld **NTP-Einstellungen bearbeiten** wird angezeigt. b Legen Sie Uhrzeit und Datum für den Host manuell fest. c Klicken Sie auf **Speichern**.
NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)	a Klicken Sie auf **NTP-Einstellungen bearbeiten**. Das Dialogfeld **NTP-Einstellungen bearbeiten** wird angezeigt. b Wählen Sie das Optionsfeld **NTP (Network Time Protocol) verwenden** aus. c Geben Sie in das Textfeld **NTP-Server** die IP-Adressen oder Hostnamen der NTP-Server ein, die Sie verwenden möchten. d Wählen Sie im Dropdown-Menü **Startrichtlinie für NTP-Dienst** eine Option zum Starten und Beenden des NTP-Diensts auf dem Host aus. ■ **Mit Port-Verwendung starten und beenden**: Startet oder beendet den NTP-Dienst, wenn der NTP-Client-Port im Sicherheitsprofil des Hosts für den Zugriff aktiviert oder deaktiviert wird. ■ **Mit dem Host starten und beenden**: Startet und beendet den NTP-Dienst, wenn der Host eingeschaltet oder heruntergefahren wird. ■ **Manuell starten und beenden** Aktiviert das manuelle Starten und Beenden des NTP-Diensts. Mit der Richtlinie **Manuell starten und beenden** ändert sich der Status des NTP-Diensts nur dann, wenn Sie die Steuerelemente auf der Benutzeroberfläche verwenden. e Klicken Sie auf **Speichern**.
PTP (Precision Time Protocol) verwenden (PTP-Client aktivieren)	a Klicken Sie auf **PTP-Einstellungen bearbeiten**. b Aktivieren Sie das Kontrollkästchen **Aktivieren**. c Wählen Sie im Dropdown-Menü **Netzwerkschnittstelle** eine Netzwerkschnittstelle aus. IPv4 und Subnetzmaske werden angezeigt. d Klicken Sie auf **Speichern**.

Verwalten von Hardware für einen ESXi-Host mit dem VMware Host Client

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie PCI-Geräte verwalten und Einstellungen zur Energieverwaltung vornehmen.

Host-Energieverwaltungsrichtlinien

Sie können in ESXi zahlreiche Energieverwaltungsfunktionen anwenden, die die Host-Hardware zur Einstellung des Gleichgewichts zwischen Leistung und Energie bereitstellt. Sie können steuern, wie ESXi diese Funktionen nutzt, indem Sie eine Energieverwaltungsrichtlinie auswählen.

Die Auswahl einer Richtlinie für hohen Energieverbrauch bietet mehr absolute Leistung, jedoch eine niedrigere Effizienz und Leistung pro Watt. Richtlinien für wenig Energieverbrauch bieten weniger absolute Leistung, aber eine höher Effizienz.

Sie können mit dem VMware Host Client eine Richtlinie für den Host auswählen, den Sie verwalten. Wenn Sie keine Richtlinie auswählen, verwendet ESXi standardmäßig die Richtlinie „Ausgeglichen“.

Tabelle 2-1. CPU-Energieverwaltungsrichtlinien

Energieverwaltungsrichtlinie	Beschreibung
Hochleistung	Keine Energieverwaltungsfunktionen verwenden
Ausgeglichen (Standard)	Energieverbrauch mit minimalen Leistungseinbußen reduzieren
Geringer Energieverbrauch	Energieverbrauch auf Gefahr einer geringeren Leistung reduzieren
Benutzerdefiniert	Benutzerdefinierte Energieverwaltungsrichtlinie Ermöglicht weiterreichende Konfigurationen

Wenn eine CPU mit einer niedrigeren Frequenz läuft, kann sie auch mit einer niedrigeren Spannung laufen und somit Energie sparen. Diese Art der Energieverwaltung wird typischerweise DVFS (Dynamic Voltage and Frequency Scaling) genannt. ESXi versucht, die CPU-Frequenzen so anzupassen, dass die Leistung der virtuellen Maschinen nicht beeinträchtigt wird.

Wenn eine CPU im Leerlauf ist, kann ESXi so genannte Deep-Halt-Zustände (auch „C-Status“ genannt) anwenden. Je niedriger der „C-Status“, desto weniger Betriebsleistung wird von der CPU verwendet, aber die CPU benötigt mehr Zeit, bis sie wieder läuft. Wenn sich eine CPU im Leerlauf befindet, wendet ESXi einen Algorithmus an, um die Dauer vorherzusagen, während derer sie sich im Leerlauf befinden wird, und wählt einen entsprechenden „C-Status“ aus, in den die CPU versetzt werden soll. In Energieverwaltungsrichtlinien, die keine niedrigen „C-Status“ nutzen, verwendet ESXi nur den flachsten Haltzustand (C1) für CPUs im Leerlauf.

Ändern der Energieverwaltungsrichtlinien im VMware Host Client

Ändern Sie die Energieverwaltungsrichtlinien des Hosts, den Sie verwalten, um dessen Energieverbrauch zu steuern.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Hardware**.
2. Klicken Sie auf **Energieverwaltung** und anschließend auf **Richtlinie ändern**.

   Die verfügbaren Energieverwaltungsrichtlinien werden angezeigt.
3. Klicken Sie auf das Optionsfeld neben der Richtlinie, die angewendet werden soll.
4. Klicken Sie auf **OK**.

Ändern der Hardwarebezeichnung im VMware Host Client

Im VMware Host Client können Sie die Hardwarebezeichnung aller verfügbaren PCI-Passthrough-Geräte auf einer virtuellen Maschine ändern. Mit Hardwarebezeichnungen können Sie die Platzierung virtueller Maschinen auf bestimmte Hardwareinstanzen beschränken. Sie können alle verfügbaren Geräte mit derselben Hardwarebezeichnung oder einer leeren Hardwarebezeichnung zu einer virtuellen Maschine hinzufügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten**.
2. Klicken Sie auf der Registerkarte **Hardware** auf **PCI-Geräte**.
3. Wählen Sie ein verfügbares Gerät aus der Liste aus und klicken Sie auf **Hardwarebezeichnung**.

   Die Option „Passthrough umschalten“ muss für das ausgewählte Gerät aktiv sein.

   Das Dialogfeld **Hardwarebezeichnung bearbeiten** wird angezeigt.
4. Bearbeiten Sie die Hardwarebezeichnung und klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

Ergebnisse

Die neue Hardwarebezeichnung wird in der Spalte „Hardwarebezeichnung“ angezeigt.

Lizenzierung für ESXi-Hosts

ESXi-Hosts werden mit vSphere-Lizenzen lizenziert. Jede vSphere-Lizenz besitzt eine bestimmte Kapazität, die Sie zur Lizenzierung mehrerer physischer CPUs auf ESXi-Hosts verwenden können.

Ab vSphere 7.0 deckt eine CPU-Lizenz eine CPU mit bis zu 32 Kernen ab. Wenn die CPU über mehr als 32 Kerne verfügt, benötigen Sie zusätzliche CPU-Lizenzen.

Anzahl der CPUs	Kerne pro CPU	Anzahl der CPU-Lizenzen
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

Wenn Sie einem Host eine vSphere Lizenz zuweisen, wird die Menge der verbrauchten Kapazität durch die Anzahl der physischen CPUs auf dem Host und die Anzahl der Kerne in jeder physischen CPU bestimmt. vSphere Desktop ist für die Verwendung in VDI-Umgebungen bestimmt und wird pro virtueller Maschine lizenziert.

Für die Lizenzierung eines ESXi-Hosts müssen Sie eine vSphere-Lizenz zuweisen, die die folgenden Voraussetzungen erfüllt:

- Die Lizenz benötigt eine Kapazität, die für die Lizenzierung aller physischen CPUs auf dem Host ausreichend ist.
- Die Lizenz muss alle vom Host verwendeten Funktionen unterstützen. Wenn beispielsweise dem Host ein vSphere Distributed Switch zugeordnet ist, muss die zugewiesene Lizenz die vSphere Distributed Switch-Funktion unterstützen.

Wenn Sie versuchen, eine Lizenz mit unzureichender Kapazität oder ohne Unterstützung der vom Host verwendeten Funktionen zuzuweisen, schlägt die Lizenzzuweisung fehl.

Wenn Sie das Lizenzierungsmodell mit bis zu 32 Kernen verwenden, können Sie eine vSphere-Lizenz für 10 CPUs mit 32 Kernen einer der folgenden Kombinationen von Hosts zuweisen:

- Fünf Hosts mit je 2 CPUs mit 32 Kernen pro CPU
- Fünf Hosts mit je 1 CPU mit 64 Kernen pro CPU
- Zwei Hosts mit je 2 CPUs mit 48 Kernen pro CPU und zwei Hosts mit je 1 CPU mit 20 Kernen pro CPU

CPUs mit 2 oder 4 Kernen, z. B. Intel-CPUs, die 2 oder 4 unabhängige CPUs auf einem einzigen Chip kombinieren, gelten als eine CPU.

Testmodus

Nach der Installation von ESXi wird das Programm für bis zu 60 aufeinander folgende Tage im Testmodus ausgeführt. Mit einer Testmoduslizenz sind alle Funktionen der höchsten vSphere-Produktedition verfügbar.

Nachdem Sie einem ESXi-Host eine Lizenz zugewiesen haben, können Sie den Host jederzeit vor Ablauf des Testzeitraums auf den Testmodus zurücksetzen, um die gesamten verfügbaren Funktionen für den verbleibenden Testzeitraum zu untersuchen.

Wenn Sie beispielsweise einen ESXi-Host 20 Tage lang im Testmodus verwenden, ihm dann eine vSphere Standard-Lizenz zuweisen und den Host nach 5 Tagen wieder in den Testmodus zurücksetzen, können Sie während der verbleibenden Testperiode von 35 Tagen sämtliche auf dem Host verfügbaren Funktionen erkunden.

Ablauf der Lizenzierungs- und Testphase

Für ESXi-Hosts führt der Ablauf des Lizenzierungs- oder Testzeitraums dazu, dass die Verbindung mit vCenter Server getrennt wird. Alle eingeschalteten virtuellen Maschinen werden weiterhin ausgeführt, virtuelle Maschinen können jedoch nach dem Ausschalten nicht mehr eingeschaltet werden. Sie können die aktuelle Konfiguration der bereits verwendeten Funktionen ändern. Sie können die Funktionen, die vor dem Ablauf der Lizenz ungenutzt blieben, nicht verwenden.

Hinweis Wenn Lizenzen ablaufen, wird 90 Tage vor dem Ablauf der jeweiligen Lizenz eine Benachrichtigung angezeigt.

Lizenzierung von ESXi-Hosts nach dem Upgrade

Wenn Sie einen ESXi-Host auf eine Version aktualisieren, die mit derselben Nummer beginnt, brauchen Sie die vorhandene Lizenz nicht durch eine neue zu ersetzen. Wenn Sie beispielsweise einen Host von ESXi 5.1 auf 5.5 upgraden, können Sie die gleiche Lizenz auf dem Host beibehalten.

Wenn Sie einen ESXi-Host auf eine Hauptversion aktualisieren, die mit einer anderen Nummer beginnt, wird die Testphase neu gestartet, und Sie müssen eine neue Lizenz zuweisen. Wenn Sie beispielsweise ein Upgrade eines ESXi-Hosts von Version 5.x auf 6.x durchführen, müssen Sie den Host mit einer vSphere 6-Lizenz lizenzieren.

vSphere Desktop

vSphere Desktop ist für VDI-Umgebungen wie Horizon View vorgesehen. Die Lizenznutzung für vSphere Desktop entspricht der Gesamtzahl der eingeschalteten virtuellen Desktop-Maschinen, die auf den Hosts ausgeführt werden und einer vSphere Desktop-Lizenz zugewiesen sind.

Anzeigen von Lizenzierungsinformationen über die VMware Host Client-Umgebung

Sie können die verfügbaren Lizenzen im VMware Host Client und deren Ablaufdatum, Lizenzschlüssel sowie verschiedene Funktionen anzeigen. Daneben können Sie die verfügbaren Produkte und Assets anzeigen.

Verfahren

- Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Lizenzierung**.

  Sie können den Lizenzschlüssel, das Ablaufdatum und alle verfügbaren Funktionen und Assets anzeigen.

Zuweisen eines Lizenzschlüssels zu einem ESXi-Host im VMware Host Client

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

Voraussetzungen

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

Hinweis Falls Sie vCenter Server zur Verwaltung Ihres ESXi-Hosts verwenden, können Sie Ihre Lizenzen nur über den vSphere Client ändern.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Lizenzierung**.

2 Klicken Sie auf **Lizenz zuweisen**, geben Sie einen Lizenzschlüssel im Format ***xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*** ein und klicken Sie auf **Lizenz überprüfen**.

3 Klicken Sie auf **Lizenz zuweisen**, um Ihre Änderungen zu speichern.

Entfernen einer Lizenz von einem ESXi-Host im VMware Host Client

Damit die Lizenzierungsmodelle der mit vSphere verwendeten Produkte weiterhin eingehalten werden, müssen Sie alle nicht zugewiesenen Lizenzen aus der Bestandsliste entfernen. Wenn Sie Lizenzen in Customer Connect geteilt, kombiniert oder aktualisiert haben, müssen Sie die alten Lizenzen entfernen.

Beispiel: Sie haben in Customer Connect ein Upgrade für eine vSphere-Lizenz von 6.5 auf 6.7 durchgeführt. Sie weisen die Lizenz den ESXi 6.7-Hosts zu. Nach der Zuweisung der neuen vSphere 6.7-Lizenzen müssen Sie die alte vSphere 6.5-Lizenz aus der Bestandsliste entfernen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Lizenzierung**.

2 Klicken Sie auf **Lizenz entfernen** und anschließend auf **OK**.

Verwalten von Diensten im VMware Host Client

Sie können im VMware Host Client auf dem Host, auf welchem Sie angemeldet sind, ausgeführte Dienste starten, beenden und neu starten sowie die Host-Dienstrichtlinien konfigurieren. Sie können Dienste bei einer Konfigurationsänderung des Hosts oder im Falle von vermuteten Funktions- oder Leistungsproblemen neu starten.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Dienste**.

2 Wählen Sie aus der Liste **Dienste** einen Dienst aus.

3 Wählen Sie im Dropdown-Menü **Aktionen** einen Vorgang aus.

- **Neu starten**
- **Starten**
- **Beenden**

4 (Optional) Wählen Sie im Dropdown-Menü **Aktionen** die Option **Richtlinien** aus und wählen Sie aus dem Menü eine Option für den Dienst aus.

- **Mit Firewall-Ports starten und beenden**
- **Mit dem Host starten und beenden**
- **Manuell starten und beenden**

Verwalten von Sicherheit und Benutzern auf einem ESXi-Host mit dem VMware Host Client

Die ESXi-Hypervisorarchitektur verfügt über viele integrierte Sicherheitsfunktionen, die Sie zur Verbesserung der Sicherheit konfigurieren können. Mit dem VMware Host Client können Sie Funktionen wie Active Directory konfigurieren und Zertifikate verwalten.

Verwalten der Host-Authentifizierung mit dem VMware Host Client

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie überprüfen, ob Active Directory und Smartcard-Authentifizierung aktiviert sind. Des Weiteren können Sie den Host mit einer Verzeichnisdienst-Domäne verknüpfen.

Verbinden eines ESXi-Hosts mit einer Verzeichnisdienst-Domäne mit dem VMware Host Client

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 finden Sie unter *vSphere-Sicherheit*.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Authentifizierung** und anschließend auf **Domäne beitreten**.
3. Geben Sie einen Domänennamen ein.

   Verwenden Sie das Fomular **`name.tld`** oder **`name.tld/container/path`**.
4. Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisdienst-Benutzerkontos ein, das über die Berechtigung verfügt, den Host mit der Domäne zu verbinden, und klicken Sie auf **Domäne beitreten**.
5. (Optional) Wenn Sie einen Authentifizierungs-Proxy verwenden möchten, geben Sie die IP-Adresse des Proxy-Servers ein und klicken Sie auf **Domäne beitreten**.

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.

Verwenden des vSphere Authentication Proxy

Statt Hosts explizit zur Active Directory-Domäne hinzuzufügen, können Sie mithilfe von vSphere Authentication Proxy ESXi-Hosts zu einer Active Directory-Domäne hinzufügen.

Sie müssen den Host nur so einrichten, dass er den Domänennamen des Active Directory-Servers und die IP-Adresse von vSphere Authentication Proxy kennt. Wenn vSphere Authentication Proxy aktiviert ist, werden Hosts, die mit Auto Deploy bereitgestellt werden, automatisch zur Active Directory-Domäne hinzugefügt. Sie können vSphere Authentication Proxy auch mit Hosts verwenden, die nicht mithilfe von Auto Deploy bereitgestellt werden.

In der Dokumentation *vSphere-Sicherheit* wird beschrieben, wie Sie vSphere Authentication Proxy aktivieren und welche vCenter Server-Ports für vSphere Authentication Proxy erforderlich sind.

Auto Deploy

Wenn Sie Hosts mithilfe von Auto Deploy bereitstellen, können Sie einen Referenzhost einrichten, der auf Authentication Proxy verweist. Sie richten dann eine Regel ein, die das Profil des Referenzhosts auf jeden mithilfe von Auto Deploy bereitgestellten ESXi-Host anwendet. vSphere Authentication Proxy speichert in der Zugriffssteuerungsliste (Access Control List, ACL) die IP-Adressen aller Hosts, die Auto Deploy mithilfe von PXE bereitstellt. Wenn der Host gestartet wird, kontaktiert er vSphere Authentication Proxy, und vSphere Authentication Proxy sorgt dafür, dass diese Hosts, die bereits in der ACL aufgeführt werden, der Active Directory-Domäne beitreten.

Auch dann, wenn Sie vSphere Authentication Proxy in einer Umgebung verwenden, die von VMCA bereitgestellten Zertifikate oder Zertifikate von Drittanbietern verwendet, funktioniert der Prozess nahtlos, wenn Sie die Anweisungen für die Verwendung von benutzerdefinierten Zertifikaten mit Auto Deploy befolgen.

Andere ESXi-Hosts

Sie können andere Hosts für die Verwendung von vSphere Authentication Proxy einrichten, wenn Sie möchten, dass der Host der Domäne ohne Verwendung der Active Directory-Anmeldedaten beitreten kann. Dies bedeutet, dass Sie keine Active Directory-Anmeldeinformationen an den Host übertragen und sie nicht im Hostprofil speichern müssen.

In diesem Fall fügen Sie die IP-Adresse des Hosts zur ACL von vSphere Authentication Proxy hinzu und vSphere Authentication Proxy autorisiert den Host standardmäßig anhand

dessen IP-Adresse. Sie können die Clientauthentifizierung so konfigurieren, dass vSphere Authentication Proxy das Zertifikat des Hosts überprüft.

Hinweis Sie können vSphere Authentication Proxy nicht in einer Umgebung verwenden, die nur IPv6 unterstützt.

Verwalten von Hostzertifikaten mit dem VMware Host Client

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie die Zertifikatdetails des Hosts wie Aussteller, Gültigkeitszeitraum usw. anzeigen und neue Zertifikate importieren.

Anzeigen von Zertifikatdetails zu einem ESXi-Host im VMware Host Client

Sie können die Zertifikatsinformationen für das Debuggen verwenden.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Zertifikate**.

   Folgende Zertifikatdetails können angezeigt werden:

Feld	Beschreibung
Aussteller	Der Aussteller des Zertifikats.
Nicht gültig nach	Das Datum, an dem das Zertifikat abläuft.
Nicht gültig vor	Das Datum, an dem das Zertifikat generiert wurde.
Betreff	Der während der Zertifikatgenerierung verwendete Betreff.

Importieren von neuen Zertifikaten zu einem ESXi-Host im VMware Host Client

Wenn Sie mit dem VMware Host Client bei einem ESXi-Host angemeldet sind, können Sie ein Zertifikat von einer vertrauenswürdigen Zertifzierungsstelle importieren.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Zertifikate** und anschließend auf **Neues Zertifikat importieren**.

3 Generieren einer Zertifikatssignieranforderung:

Option	Beschreibung
Generieren einer FQDN-Signieranforderung	■ Klicken Sie auf **FQDN-Signierungsanforderung generieren**, auf die Schaltfläche **In Zwischenablage kopieren** und dann auf **Schließen**. ■ Um das signierte Zertifikat zu generieren, leiten Sie die Zertifikatsignieranforderung an die Zertifizierungsstelle weiter. ■ Fügen Sie im Textfeld **Zertifikat** das generierte signierte Zertifikat im PEM-Format ein und klicken Sie auf **Importieren**.
Generieren einer IP-Signieranforderung	■ Klicken Sie auf **IP-Signierungsanforderung generieren**, auf die Schaltfläche **In Zwischenablage kopieren** und dann auf **Schließen**. ■ Um das signierte Zertifikat zu generieren, leiten Sie die Zertifikatsignieranforderung an die Zertifizierungsstelle weiter. ■ Fügen Sie im Textfeld **Zertifikat** das generierte signierte Zertifikat im PEM-Format ein und klicken Sie auf **Importieren**.

Sie müssen das Zertifikat nicht sofort importieren. Starten Sie den Host zwischen dem Generieren der Zertifikatsignieranforderung und dem Import des Zertifikats nicht neu. Auf diese Weise stellen Sie sicher, dass Sie das signierte Zertifikat verwenden können.

Die Zertifikatssignieranforderung wird anschließend an die Zertifzierungsstelle weitergeleitet, die das offizielle Zertifikat generiert.

Eine FQDN-Anforderung enthält den vollqualifizierten Namen des Hosts im entsprechenden allgemeinen Namensfeld des Zertifikats. Die IP-Signierungsanforderung enthält die aktuelle IP-Adresse des Hosts im allgemeinen Namensfeld.

Verwalten von Benutzern mit dem VMware Host Client

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

Über Benutzer und Rollen wird gesteuert, welche Benutzer Zugriff auf die Komponenten des ESXi-Hosts haben und welche Aktionen jeder Benutzer ausführen kann.

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

- Die Benutzer, die Sie erstellen, wenn Sie eine direkte Verbindung mit einem ESXi-Host herstellen, 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 mithilfe des vSphere Client erstellen. Sie müssen sich direkt beim Host mit dem VMware Host Client 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 im VMware Host Client

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

Voraussetzungen

Informationen zu Kennwortanforderungen finden Sie unter Konfigurieren der Kennwort- und Kontosperrrichtlinie im VMware Host Client oder in der Dokumentation zu *vSphere-Sicherheit*.

Verfahren

1 Melden Sie sich mit dem VMware Host Client bei ESXi an.

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

2 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.

3 Klicken Sie auf **Benutzer**.

4 Klicken Sie auf **Benutzer hinzufügen**.

5 Geben Sie 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.

   - Der Benutzername darf keine Leerzeichen enthalten.
   - Der Benutzername darf keine Nicht-ASCII-Zeichen enthalten.
   - 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`. Wenn das Kennwort nicht richtlinienkonform ist, werden die Kennwortanforderungen in einer Fehlermeldung angegeben.

6 Klicken Sie auf **Hinzufügen**.

Aktualisieren eines ESXi-Benutzers im VMware Host Client

Sie können die Beschreibung und das Kennwort für einen ESXi-Benutzer im VMware Host Client ändern.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.

2 Klicken Sie auf **Benutzer**.

3 Wählen Sie einen Benutzer in der Liste aus und klicken Sie auf **Benutzer bearbeiten**.

4 Aktualisieren Sie die Benutzerdetails und klicken Sie auf **Speichern**.

Entfernen eines lokalen ESXi-Benutzers von einem Host im VMware Host Client

Sie können einen lokalen ESXi-Benutzer vom 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.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.

2 Klicken Sie auf **Benutzer**.

3 Wählen Sie den Benutzer, den Sie entfernen möchten, in der Liste aus, klicken Sie auf **Benutzer entfernen** und klicken Sie dann auf **Ja**.

   Entfernen Sie den Root-Benutzer in keinem Fall.

Verwalten von ESXi-Rollen im VMware Host Client

ESXi gewährt nur denjenigen Benutzern Zugriff auf Objekte, denen Berechtigungen für das jeweilige Objekt zugewiesen wurden. Wenn Sie eine Benutzerberechtigung für das Objekt zuweisen, kombinieren Sie hierzu den Benutzer mit einer Rolle. Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten. Weitere Informationen zu Berechtigungen finden Sie in der Dokumentation *vSphere-Sicherheit*.

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 erstellen, übernehmen keine Rechte von den Standardrollen.

Benutzerdefinierte Rollen können Sie mit den Rollenbearbeitungsfunktionen in VMware Host Client erstellen und an Ihre Benutzeranforderungen anpassen. Zudem kann auf die Rollen, die Sie direkt auf einem Host erstellen, in vCenter Server nicht zugegriffen werden. Sie können diese Rollen nur verwenden, wenn Sie sich über den VMware Host Client direkt beim Host anmelden.

Hinweis Wenn Sie eine benutzerdefinierte Rolle hinzufügen und dieser Rolle keine Rechte zuweisen, wird die Rolle als schreibgeschützte Rolle mit den vom System definierten Rechten **System.Anonymous**, **System.View** und **System.Read** erstellt.

Wenn Sie einen ESXi-Host 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 VMware Host Client verwenden, um über eine direkte Verbindung mit dem ESXi-Host Hostrollen zu erstellen und Berechtigungen festzulegen.

Hinzufügen einer Rolle im VMware Host Client

Sie können 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“.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Rollen**.
3. Klicken Sie auf **Rolle hinzufügen**.
4. Geben Sie einen Namen für die neue Rolle ein.
5. Wählen Sie in der Liste Rechte aus, die der neuen Rolle zugeordnet werden sollen, und klicken Sie dann auf **Hinzufügen**.

Aktualisieren einer Rolle im VMware Host Client

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“.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Rollen**.
3. Wählen Sie eine Rolle in der Liste aus und klicken Sie auf **Rolle bearbeiten**.
4. Aktualisieren Sie die Rollendetails und klicken Sie auf **Speichern**.

Entfernen einer Rolle im VMware Host Client

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“.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Rollen**.
3. Wählen Sie den Namen der Rolle, die Sie entfernen möchten, in der Liste aus.
4. Klicken Sie auf **Rolle entfernen**, wählen Sie **Nur entfernen, wenn nicht verwendet** aus und klicken Sie auf **Ja**.

Verwalten von Hosts in vCenter Server

Um alle Hosts in Ihrer virtuellen Umgebung von einem Standort aus zu überwachen und die Hostkonfiguration zu vereinfachen, verbinden Sie die Hosts mit einem vCenter Server-System.

Informationen zur Konfigurationsverwaltung von ESXi-Hosts finden Sie in der *vSphere-Netzwerk*-Dokumentation, in der *vSphere-Speicher*-Dokumentation und in der *vSphere-Sicherheit*-Dokumentation.

Aktualisieren der VMware Host Client-Umgebung auf die neueste Version

Um in Erfahrung zu bringen, ob Sie die neueste Version des VMware Host Client verwenden, überprüfen Sie die in Ihrer Umgebung installierten VIBs und untersuchen Sie deren Versionsinformationen. Zur Aktualisierung Ihrer VMware Host Client-Umgebung können Sie eine URL oder einen Datenspeicherpfad zu einem vSphere-Installationspaket (vSphere Installation Bundle, VIB) oder zur Datei `metadata.zip` in ein ESXi-Offline-Paket eingeben.

Bei Eingabe einer VIB-Datei wird ein in Ihrer VMware Host Client-Umgebung vorhandenes VIB auf das neue VIB aktualisiert.

Wenn Sie ein Offline-Paket bereitstellen, aktualisieren Sie den gesamten ESXi-Host auf die von der Datei `metadata.zip` im Paket beschriebene Version. Stellen Sie sicher, dass das gesamte Offline-Paket über die URL verfügbar ist oder in den Datenspeicher hochgeladen wird.

Verfahren

- Führen Sie die folgenden Aufgaben aus, um Ihre Umgebung auf die neueste Version zu aktualisieren:

Aufgabe	Schritte
Laden Sie ein VIB in einen Datenspeicher hoch.	a Klicken Sie in der VMware Host Client-Umgebung auf **Speicher**. b Wählen Sie einen Datenspeicher aus der Liste aus und klicken Sie auf **Datenspeicherbrowser**. c Um das VIB zu speichern, wählen Sie ein Verzeichnis aus und klicken Sie auf **Hochladen**. d Navigieren Sie zu der Datei und doppelklicken Sie darauf.
Laden Sie ein Offline-Paket in einen Datenspeicher hoch.	a Laden Sie das ESXi-Offline-Paket herunter. b Laden Sie das ESXi-Offline-Paket auf den ESXi-Host hoch. Sie können das Offline-Paket entweder mit dem **Datenspeicherbrowser** oder mithilfe von SCP oder WinSCP hochladen. c Extrahieren Sie den Inhalt des Offline-Pakets auf den ESXi-Host. Melden Sie sich z. B. mithilfe von SSH beim Host an. d Navigieren Sie zu dem Verzeichnis, in das Sie das Offline-Paket hochgeladen haben. e Extrahieren Sie den Inhalt, indem Sie den Befehl `unzip` ausführen.
Aktualisieren Sie Ihre Umgebung.	a Klicken Sie im VMware Host Client auf **Verwalten** und anschließend auf **Pakete**. b Klicken Sie auf **Update installieren** und geben Sie die URL oder den Datenspeicherpfad zu einem VIB oder zu einer Datei `metadata.zip` in einem Offline-Paket ein. c Klicken Sie auf **Aktualisieren**. **Vorsicht** Wenn Sie einen von vSphere Lifecycle Manager verwalteten ESXi-Host aktualisieren, ist der Host danach möglicherweise nicht mehr konform. d Klicken Sie auf **Aktualisieren**, um sicherzustellen, dass das Update erfolgreich ist.

Verbindungsherstellung vom VMware Host Client zu einem ESXi-Host nach dem Upgrade auf eine neuere Version von ESXi ist nicht möglich

Nach dem Upgrade des Hosts von ESXi auf eine neuere Version wird in der Browserkonsole unter Umständen eine Fehlermeldung angezeigt, wenn Sie auf Ihren ESXi-Host mithilfe des VMware Host Client zugreifen. Die Verbindung schlägt möglicherweise fehl.

Problem

Nach dem Upgrade des ESXi-Hosts auf eine neuere Version schlagen Versuche, zu **`https://host-fqdn/ui`** oder **`https://1.2.3.4/ui`** zu navigieren, fehl. Es wird möglicherweise der folgende Fehler angezeigt:

```
503 Service Unavailable (Failed to connect to endpoint:
[N7Vmacore4Http16LocalServiceSpecE:0xffa014e8] _serverNamespace = /ui _isRedirect = false
_port = 8308)
```

Ursache

Eine Änderung zu `/etc/vmware/rhttpproxy/endpoints.conf` verbleibt nach einem Upgrade und sorgt dafür, dass der `/ui`-Endpoint den VMware Host Client überschreibt.

Wenn das `/ticket` in der Datei `endpoint.conf` auf dem ESXi-Host 6.0 oder höher fehlt, zeigt die im Browser integrierte Konsole für die virtuelle Maschine folgende Fehlermeldung an: `Verbindungsaufbau fehlgeschlagen`. Die VMware Remote Console funktioniert weiterhin.

Lösung

1. Melden Sie sich beim ESXi-Host entweder unter Verwendung von SSH oder ESXi-Shell an.

   Wenn Sie SSH verwenden, müssen Sie SSH möglicherweise zuerst aktivieren. Sie können SSH unter Verwendung von DCUI aktivieren.

2. Sichern Sie die Datei `endpoints.conf`.

   ```
   cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
   ```

3. Öffnen Sie die Datei `/etc/vmware/rhttpproxy/endpoints.conf` in einem Editor und entfernen Sie die folgende Zeile.

   ```
   /ui local 8308 redirect  allow
   ```

4. Starten Sie den **rhttpproxy**-Konfigurationsverwaltungsserver neu.

   ```
   /etc/init.d/rhttpproxy restart
   ```

5. Greifen Sie unter Verwendung des in der sicheren URL angegebenen vollständigen Namen des Hosts auf VMware Host Client zu, verwenden Sie dabei **`https://host-fqdn/ui`** oder eine gültige numerische IP-Adresse **`https://1.2.3.4/ui`**.

Wechseln zum vSphere Client

Für den Zugriff auf den vollständigen Funktionsumfang und erweiterte administrative und Fehlerbehebungsaufgaben auf dem ESXi-Host verbinden Sie den ESXi-Host mit vCenter Server.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **Mit vCenter Server verwalten** aus dem Dropdown-Menü aus.

   Die vCenter Server-Anmeldeseite wird in einem neuen Fenster geöffnet.

2 Geben Sie Ihre Anmeldedaten ein und klicken Sie auf **Anmelden**.

Trennen eines ESXi-Hosts von vCenter Server mit dem VMware Host Client

Wenn Sie die erweiterten Funktionen zur Host-Verwaltung von vCenter Server nicht mehr verwenden möchten oder vCenter Server ausgefallen ist und Sie Notfallmaßnahmen am Host ergreifen müssen, können Sie den ESXi-Host von vCenter Server trennen.

Das Trennen eines ESXi-Hosts kann einige Minuten dauern.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **Von vCenter Server trennen** aus dem Popup-Menü aus.

   Hinweis Durch Trennen eines Hosts wird vCenter Server mitgeteilt, dass dieser Host nicht reagiert.

2 Klicken Sie auf **Von vCenter Server trennen**.

Neustarten oder Herunterfahren eines ESXi-Hosts im VMware Host Client

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

Voraussetzungen

Um einen Host herunterfahren oder neu starten zu können, benötigen Sie die folgenden Berechtigungen.

- **Host.Konfiguration.Wartung**
- **Global.Ereignis protokollieren**

Führen Sie vor dem Neustart oder Herunterfahren eines Hosts immer die folgenden Aufgaben durch:

- Schalten Sie alle virtuellen Maschinen auf dem Host aus.
- Versetzen Sie den Host in den Wartungsmodus.

Verfahren

1 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Host herunterfahren** oder **Host neu starten**.

Hinweis Wenn sich der Host nicht im Wartungsmodus befindet, werden die virtuellen Maschinen, die sicher auf diesem Host ausgeführt werden, durch Herunterfahren oder Neustart nicht angehalten, und nicht gespeicherte Daten können verloren gehen. Wenn der Host Teil eines vSAN-Clusters ist, können Sie möglicherweise nicht mehr auf die vSAN-Daten auf dem Host zugreifen.

2 Klicken Sie auf **Herunterfahren** oder **Neustart**, um den Vorgang abzuschließen.

Verwenden der ESXi Shell

Die ESXi Shell ist auf ESXi-Hosts standardmäßig deaktiviert. Sie können bei Bedarf lokalen Zugriff und Remotezugriff auf die Shell aktivieren.

Um das Risiko eines nicht autorisierten Zugriffs zu reduzieren, aktivieren Sie die ESXi Shell nur zur Fehlerbehebung.

Die ESXi Shell ist unabhängig vom Sperrmodus. Selbst wenn der Host im Sperrmodus ausgeführt wird, können Sie sich weiterhin bei der ESXi Shell anmelden, soweit sie aktiviert ist.

Weitere Informationen hierzu finden Sie unter *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.

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 die ESXi Shell ausführen.

Hinweis Aktivieren Sie die ESXi Shell nur, wenn dies wirklich erforderlich ist.

Aktivieren von Secure Shell (SSH) im VMware Host Client

Aktivieren Sie Secure Shell (SSH), um mittels SSH remote auf die ESXi Shell zuzugreifen.

Verfahren

1 Klicken Sie zum Aktivieren und Deaktivieren von Secure Shell (SSH) in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host**.

2 Wählen Sie **Dienste** aus dem Dropdown-Menü aus und wählen Sie anschließend **Secure Shell (SSH)**.

3 Wählen Sie eine durchzuführende Aufgabe aus.

- Wenn Secure Shell (SSH) aktiviert ist, können Sie sie durch Klicken auf **Deaktivieren** deaktivieren.
- Wenn Secure Shell (SSH) deaktiviert ist, können Sie sie durch Klicken auf **Aktivieren** aktivieren.

Aktivieren der ESXi-Konsolen-Shell im VMware Host Client

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 VMware Host Client oder durch die Aktivierung der ESXi Shell auf den Host zugreifen.

Verfahren

1 Klicken Sie zum Aktivieren und Deaktivieren der Konsolen-Shell in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host**.

2 Wählen Sie **Dienste** aus dem Dropdown-Menü aus und wählen Sie anschließend **Konsolen-Shell**.

3 Wählen Sie eine durchzuführende Aufgabe aus.

- Wenn die Konsolen-Shell aktiviert ist, können Sie sie durch Klicken auf **Deaktivieren** deaktivieren.
- Wenn die Konsolen-Shell deaktiviert ist, können Sie sie durch Klicken auf **Aktivieren** aktivieren.

Erstellen einer Zeitüberschreitung für die Verfügbarkeit der ESXi Shell im VMware Host Client

Die ESXi Shell ist standardmäßig aktiviert. Zur Erhöhung der Sicherheit beim Aktivieren der Shell können Sie einen Zeitüberschreitungswert für die Verfügbarkeit der ESXi Shell festlegen.

Mit dem Zeitüberschreitungswert für die Verfügbarkeit wird festgelegt, wie lange sowohl lokale als auch Remote-Shell-Anmeldungen zulässig sind, bevor die Möglichkeit zur Anmeldung über die Shell deaktiviert wird. Bei Ablauf der Zeitüberschreitung für die Verfügbarkeit bleiben alle vorhandenen Shell-Sitzungen bestehen, neue Shell-Sitzungen sind jedoch nicht zulässig.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.

2 Geben Sie **`UserVars.ESXiShellTimeOut`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**.

3 Klicken Sie mit der rechten Maustaste auf `UserVars.ESXiShellTimeOut` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.

4 Geben Sie im Textfeld **Neuer Wert** die Zeitüberschreitungseinstellung ein.

   Mit dem Wert NULL (0) wird die Zeitüberschreitung deaktiviert.

5 Klicken Sie auf **Speichern**.

   Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Zeitüberschreitung wirksam wird.

6 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Erstellen einer Zeitüberschreitung für ESXi Shell-Leerlaufsitzungen im VMware Host Client

Wenn Sie die ESXi Shell auf einem Host aktivieren, sich aber nicht von der Sitzung abmelden, wird die Leerlaufsitzung auf unbestimmte Zeit ausgeführt. Die offene Verbindung erhöht die Möglichkeit für einen privilegierten Zugriff auf den ESXi-Host. Verhindern Sie dies, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis Sie bei einer interaktiven Leerlaufsitzung abgemeldet werden.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.

2 Geben Sie **`UserVars.ESXiShellInteractiveTimeOut`** im Textfeld **Suchen** ein und klicken Sie auf das Symbol **Suchen**.

3 Klicken Sie mit der rechten Maustaste auf `UserVars.ESXiShellInteractiveTimeOut` und wählen Sie **Option bearbeiten** im Dropdown-Menü aus.

   Das Dialogfeld **Option bearbeiten** wird geöffnet.

4 Geben Sie im Textfeld **Neuer Wert** die Zeitüberschreitungseinstellung ein.

   Mit dem Wert NULL (0) wird die Zeitüberschreitung deaktiviert.

5 Klicken Sie auf **Speichern**.

   Die Zeitüberschreitung wird nur für neu angemeldete Sitzungen wirksam.

6 (Optional) Um die Schlüsseleinstellung auf den Standardwert zurückzusetzen, klicken Sie mit der rechten Maustaste auf den entsprechenden Schlüssel in der Liste und wählen Sie **Auf Standardeinstellung zurücksetzen** aus.

Ergebnisse

Wenn die Sitzung sich im Leerlauf befindet, werden die Benutzer nach Ablauf der Zeitüberschreitungszeitspanne abgemeldet.

Versetzen eines Hosts in den Wartungsmodus im VMware Host Client

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.

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 oder sich bereits darin befindet, keine virtuellen Maschinen ausschalten oder eine Migration virtueller Maschinen auf diesen Host durchführen.

Um einen Host in den Wartungsmodus zu versetzen, müssen alle darauf ausgeführte virtuelle Maschinen ausgeschaltet oder auf einen anderen Host migriert werden. Wenn Sie versuchen, einen Host, auf dem virtuelle Maschinen ausgeführt werden, in den Wartungsmodus zu versetzen, muss DRS diese virtuellen Maschinen ausschalten oder migrieren, damit die Aufgabe abgeschlossen werden kann. Wenn es vor dem Ausschalten oder Migrieren der virtuellen Maschinen zu einem Timeout kommt, wird eine Fehlermeldung angezeigt.

Wenn alle virtuellen Maschinen auf dem Host inaktiv sind, ändert sich das Hostsymbol in **Wartungsphase** und der neue Betriebszustand wird im Fenster „Übersicht“ des Hosts angezeigt. Während sich der Host im Wartungsmodus befindet, können virtuelle Maschinen weder bereitgestellt noch eingeschaltet werden.

Voraussetzungen

Bevor Sie einen Host in den Wartungsmodus versetzen, schalten Sie alle darauf ausgeführten virtuelle Maschinen aus oder migrieren Sie sie manuell oder automatisch mittels DRS auf einen anderen Host.

Verfahren

- Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **In den Wartungsmodus wechseln**.

Ergebnisse

Der Host befindet sich im Wartungsmodus, bis Sie **Wartungsmodus beenden** auswählen.

Verwalten von Berechtigungen im VMware Host Client

Für ESXi werden Berechtigungen als Zugriffsrollen definiert, die aus den Rollen bestehen, die einem Benutzer für verschiedene Objekte (beispielsweise eine virtuelle Maschine oder einen

ESXi-Host) zugewiesen wurden. 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 sie mit dem VMware Host Client ausführen können.

Wenn eine direkte Verbindung mit einem Host mit dem VMware Host Client hergestellt wird, besitzen die Benutzerkonten „root“ und „vpxuser“ dieselben Zugriffsrechte für alle Objekte wie jeder Benutzer mit der Rolle „Administrator“.

Alle anderen Benutzer verfügen anfangs über keinerlei Berechtigungen für Objekte. Das bedeutet, die Benutzer können Objekte nicht anzeigen und keine Aufgaben für sie durchführen. Ein Benutzer mit Administratorrechten muss diesen Benutzern Rechte zuweisen, damit sie Aufgaben durchführen können.

Viele Aufgaben erfordern Berechtigungen für mehr als ein Objekt. Anhand der folgenden Regeln können Sie bestimmen, welche Rollen Benutzern für bestimmte Aufgaben zugewiesen werden müssen:

- Jede Aufgabe, die Festplattenspeicher 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.
- Jeder Host und Cluster hat seinen eigenen impliziten Ressourcenpool, der alle Ressourcen des Hosts oder Clusters enthält. Das direkte Bereitstellen einer virtuellen Maschine auf einem 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.

Zuweisen von Berechtigungen zu einem Benutzer für einen ESXi-Host im VMware Host Client

Um bestimmte Aktivitäten auf einem ESXi-Host ausführen zu können, benötigt ein Benutzer Berechtigungen, die einer konkreten Rolle zugeordnet sind. Im VMware Host Client können Sie Benutzern Rollen zuweisen und ihnen die Berechtigungen erteilen, die zur Durchführung von verschiedenen Aufgaben auf dem Host erforderlich sind.

Verfahren

1. Klicken Sie mit der rechten Maustaste auf den **Host** in der VMware Host Client-Bestandsliste und klicken Sie dann auf **Berechtigungen**.
2. Klicken Sie auf **Benutzer hinzufügen**.
3. Klicken Sie auf den Pfeil neben dem Textfeld **Benutzer auswählen** und wählen Sie den Benutzer aus, dem Sie eine Rolle zuweisen möchten.
4. Klicken Sie auf den Pfeil neben dem Textfeld **Rolle auswählen** und wählen Sie eine Rolle in der Liste aus.
5. (Optional) Wählen Sie **An alle untergeordneten Objekte weitergeben** oder **Als Gruppe hinzufügen** aus.

   Wenn Sie eine Berechtigung auf vCenter Server-Ebene festlegen und an die untergeordneten Objekte weitergeben, gilt die Berechtigung für Datencenter, Ordner, Cluster, Hosts, virtuelle Maschinen und weitere Objekte in der vCenter Server-Instanz.
6. Klicken Sie auf **Hinzufügen** und dann auf **Schließen**.

Entfernen von Berechtigungen für einen Benutzer im VMware Host Client

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.

Verfahren

1. Klicken Sie mit der rechten Maustaste auf den **Host** in der VMware Host Client-Bestandsliste und klicken Sie dann auf **Berechtigungen**.
2. Wählen Sie einen Benutzer in der Liste aus und klicken Sie auf **Benutzer entfernen**.
3. Klicken Sie auf **Schließen**.

Zuweisen von Benutzerberechtigungen für eine virtuelle Maschine im VMware Host Client

Weisen Sie einem Benutzer eine Rolle zu, um ihm die Berechtigung zu erteilen, bestimmte Aufgaben auf einer virtuellen Maschine durchzuführen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Berechtigungen** aus.
3. Klicken Sie auf **Benutzer hinzufügen**.
4. Klicken Sie auf den Pfeil neben dem Textfeld **Benutzer auswählen** und wählen Sie den Benutzer aus, dem Sie eine Rolle zuweisen möchten.
5. Klicken Sie auf den Pfeil neben dem Textfeld **Rolle auswählen** und wählen Sie eine Rolle in der Liste aus.
6. (Optional) Wählen Sie **An alle untergeordneten Objekte weitergeben** aus.

   Wenn Sie eine Berechtigung auf vCenter Server-Ebene festlegen und an die untergeordneten Objekte weitergeben, gilt die Berechtigung für Datencenter, Ordner, Cluster, Hosts, virtuelle Maschinen und ähnliche Objekte in der vCenter Server-Instanz.
7. Klicken Sie auf **Hinzufügen** und dann auf **Schließen**.

Entfernen von Berechtigungen für eine virtuelle Maschine im VMware Host Client

Damit ein Benutzer Aufgaben für eine bestimmte virtuelle Maschine nicht mehr ausführen kann, entfernen Sie die Berechtigungen des Benutzers für diese virtuelle Maschine.

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.

Verfahren

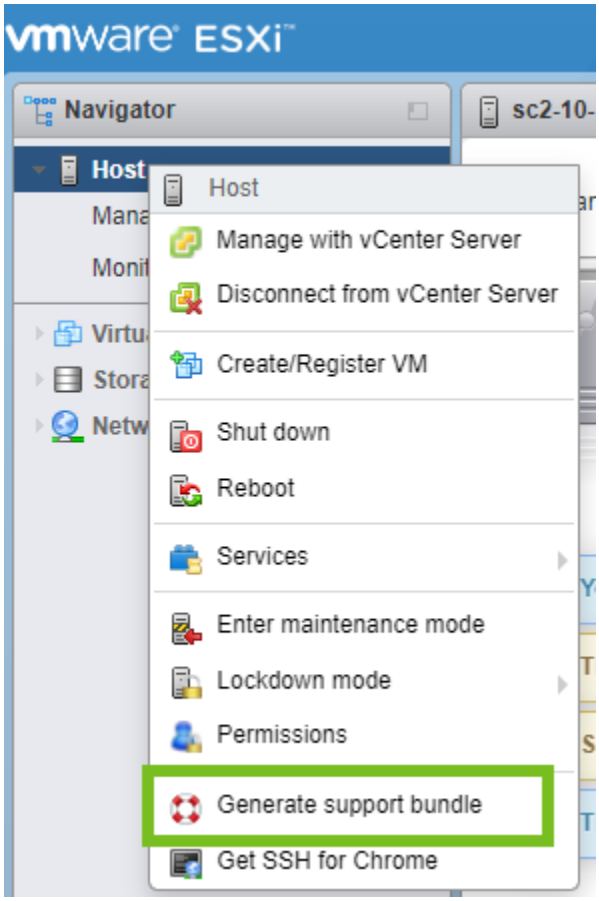
1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Berechtigungen** aus.
3. Wählen Sie einen Benutzer in der Liste aus und klicken Sie auf **Benutzer entfernen**.
4. Klicken Sie auf **Schließen**.

Generieren eines Support-Pakets im VMware Host Client

Sie können ein Support-Paket für den ESXi-Host erstellen, bei dem Sie angemeldet sind. Das Support-Paket enthält die Protokolldateien und Systeminformationen, die Sie zum Diagnostizieren und Lösen von Problemen verwenden können.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **Support-Paket generieren** aus dem Dropdown-Menü aus.



Nachdem das Support-Paket erstellt wurde, wird ein Dialogfeld mit einem Link angezeigt, unter dem Sie das Paket herunterladen können.

2 (Optional) Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen**, klicken Sie auf **Aufgaben** und wählen Sie ein Protokollpaket aus der Liste aus.

Sie können den Link zum Protokollpaket unter der Tabelle anzeigen.

Sperrmodus

Um die Sicherheit von ESXi-Hosts zu verbessern, können Sie diese in den Sperrmodus versetzen. Im Sperrmodus müssen alle Hostvorgänge standardmäßig über vCenter Server durchgeführt werden.

Normaler Sperrmodus und strenger Sperrmodus

Mit vSphere 6.0 und höher können Sie den normalen oder den strengen Sperrmodus wählen.

Normaler Sperrmodus

Im normalen Sperrmodus bleibt der DCUI-Dienst aktiv. Wenn die Verbindung mit dem vCenter Server-System unterbrochen wird und über den vSphere Client kein Zugriff mehr besteht, können sich die berechtigten Konten bei der Schnittstelle der direkten Konsole (DCUI) des ESXi-Hosts anmelden und den Sperrmodus verlassen. Nur die folgenden Konten haben Zugriff auf die Benutzerschnittstelle der direkten Konsole:

- Konten in der Liste der aus dem Sperrmodus ausgenommenen Benutzer mit Administratorrechten für den Host. Die Liste der ausgenommenen Benutzer ist für Dienstkonten gedacht, mit denen spezielle Aufgaben ausgeführt werden. Wenn Sie dieser Liste ESXi-Administratoren hinzufügen, widerspricht dies dem Zweck des Sperrmodus.
- In der erweiterten Option DCUI.Access für den Host definierte Benutzer. Diese Option dient für den Notfallzugriff auf die Schnittstelle der direkten Konsole für den Fall, dass die Verbindung mit vCenter Server unterbrochen wird. Diese Benutzer benötigen keine Administratorrechte auf dem Host.

Strenger Sperrmodus

Im strengen Sperrmodus wird der DCUI-Dienst beendet. Wenn die Verbindung mit vCenter Server unterbrochen wird und der vSphere Client nicht mehr verfügbar ist, steht auch der ESXi-Host nicht mehr zur Verfügung – es sei denn, die ESXi Shell und die SSH-Dienste sind aktiviert und ausgenommene Benutzer wurden definiert. Wenn Sie die Verbindung mit dem vCenter Server-System nicht mehr herstellen können, müssen Sie den Host neu installieren.

Sperrmodus und ESXi Shell bzw. SSH-Dienste

Im strengen Sperrmodus wird der DCUI-Dienst angehalten. ESXi Shell und SSH-Dienste sind jedoch vom Sperrmodus nicht betroffen. Damit der Sperrmodus eine wirksame Schutzmaßnahme darstellen kann, müssen auch die ESXi Shell und die SSH-Dienste deaktiviert sein. Diese Dienste sind standardmäßig deaktiviert.

Bei einem Host im Sperrmodus können Benutzer in der Liste der ausgenommenen Benutzer über die ESXi Shell und SSH auf den Host zugreifen, wenn sie die Administratorrolle auf dem Host besitzen. Das ist sogar im strengen Sperrmodus möglich. Daher ist die sicherste Option, den ESXi Shell- und den SSH-Dienst deaktiviert zu lassen.

Hinweis Die Liste der ausgenommenen Benutzer ist für Dienstkonten gedacht, mit denen sehr spezielle Aufgaben ausgeführt werden, und nicht für Administratoren. Wenn Sie der Liste „Ausnahme für Benutzer“ Administratoren hinzufügen, widerspricht dies dem Zweck des Sperrmodus.

Versetzen eines ESXi-Hosts in den normalen Sperrmodus mit dem VMware Host Client

Sie können einen Host mit dem VMware Host Client in den strengen Sperrmodus versetzen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host**, wählen Sie **Sperrmodus** aus dem Dropdown-Menü aus und wählen Sie anschließend **In den normalen Sperrmodus wechseln**.

   Es wird eine Warnmeldung angezeigt.

2 Klicken Sie auf **In den normalen Sperrmodus wechseln**.

Versetzen eines ESXi-Hosts in den strengen Sperrmodus mit dem VMware Host Client

Sie können einen Host mit dem VMware Host Client in den strengen Sperrmodus versetzen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host**, wählen Sie **Sperrmodus** aus dem Dropdown-Menü aus und wählen Sie anschließend **In den strengen Sperrmodus wechseln**.

   Es wird eine Warnmeldung angezeigt.

2 Klicken Sie auf **In den strengen Sperrmodus wechseln**.

Beenden des Sperrmodus mit dem VMware Host Client

Wenn Sie den normalen oder strengen Sperrmodus auf einem ESXi-Host aktiviert haben, können Sie ihn mit dem VMware Host Client beenden.

Verfahren

- Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host**, wählen Sie **Sperrmodus** aus dem Dropdown-Menü aus und wählen Sie anschließend **Sperre beenden**.

Angeben der Benutzerausnahmen für den Sperrmodus im VMware Host Client

In vSphere 6.0 und höher können Sie Benutzer über den VMware Host Client zur Liste „Ausnahme für Benutzer“ hinzufügen. Diese Benutzer verlieren ihre Berechtigungen nicht, wenn der Host in den Sperrmodus wechselt. Sie können Dienstkonten wie beispielsweise einen Backup-Agenten zur Liste „Ausnahme für Benutzer“ hinzufügen.

Ausgenommene Benutzer sind lokale Hostbenutzer oder Active Directory-Benutzer mit lokal für den ESXi-Host definierten Rechten. Sie sind keine Mitglieder einer Active Directory-Gruppe und keine vCenter Server-Benutzer. Diese Benutzer dürfen Vorgänge auf dem Host in Abhängigkeit von ihren Rechten durchführen. Dies bedeutet, dass beispielsweise ein Benutzer mit der Berechtigung „Nur Lesen“ den Sperrmodus auf einem Host nicht deaktivieren kann.

Hinweis Die Liste „Ausnahme für Benutzer“ ist für Dienstkonten gedacht, mit denen sehr spezielle Aufgaben ausgeführt werden, und nicht für Administratoren. Wenn Sie der Liste „Ausnahme für Benutzer“ Administratoren hinzufügen, widerspricht dies dem Zweck des Sperrmodus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Sicherheit und Benutzer**.
2. Klicken Sie auf **Sperrmodus**.
3. Klicken Sie auf **Benutzerausnahme hinzufügen**, geben Sie den Namen des Benutzers ein und klicken Sie auf **Ausnahme hinzufügen**.
4. (Optional) Wählen Sie in der Liste „Ausnahme für Benutzer“ einen Namen aus, klicken Sie auf **Benutzerausnahme entfernen** und klicken Sie auf **Bestätigen**.

Verwalten von CPU-Ressourcen mit dem VMware Host Client

Wenn Sie mit dem VMware Host Client eine Verbindung zu einem ESXi-Host herstellen, erhalten Sie Zugriff auf eine begrenzte Anzahl an Ressourcenverwaltungseinstellungen.

Anzeigen von Prozessorinformationen mit dem VMware Host Client

Im VMware Host Client können Sie auf Informationen zur aktuellen CPU-Konfiguration des ESXi-Hosts zugreifen, auf dem Sie angemeldet sind.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Host**.
2. Erweitern Sie **Hardware** und anschließend **CPU**.

   Sie können nun die Informationen über die Anzahl und den Typ der physischen Prozessoren sowie die Anzahl der logischen Prozessoren anzeigen.

Zuweisen einer virtuellen Maschine zu einem bestimmten Prozessor im VMware Host Client

Durch Verwendung der CPU-Affinität können Sie eine virtuelle Maschine einem bestimmten Prozessor zuweisen. Auf diese Weise können Sie eine virtuelle Maschine in Multiprozessor-Systemen einem bestimmten verfügbaren Prozessor zuweisen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
2. Erweitern Sie unter **Virtuelle HardwareCPU**.
3. Wählen Sie unter **Planen von Affinität** eine physische Prozessoraffinität für die virtuelle Maschine aus.

   Kennzeichnen Sie Bereiche mit einem Bindestrich und trennen Sie Werte durch Kommas.

   Beispiel: `0, 2, 4–7` steht für die Prozessoren 0, 2, 4, 5, 6 und 7.
4. Klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

Überwachen eines ESXi-Hosts im VMware Host Client

Wenn Sie mit dem VMware Host Client eine Verbindung zu einem Host herstellen, können Sie den Systemstatus des Hosts überwachen und Leistungsdiagramme, Ereignisse, Aufgaben, Systemprotokolle und Benachrichtigungen anzeigen.

Anzeigen von Diagrammen im VMware Host Client

Wenn Sie beim VMware Host Client angemeldet sind, können Sie auf dem ESXi-Host, den Sie verwalten, Informationen zur Ressourcennutzung in Form eines Liniendiagramms anzeigen.

Damit nicht zu viel Arbeitsspeicher verbraucht wird, enthält der VMware Host Client nur Statistiken zur vergangenen Stunde.

Verfahren

1. Klicken Sie im VMware Host Client auf **Überwachen** und anschließend auf **Leistung**.
2. (Optional) Wählen Sie zur Anzeige der Host-Auslastung in der vergangenen Stunde eine Option aus dem Dropdown-Menü aus.
   - Zur Anzeige der CPU-Auslastung des Hosts in der vergangenen Stunde in Prozent wählen Sie **CPU**.
   - Zur Anzeige der Arbeitsspeichernutzung des Hosts in der vergangenen Stunde wählen Sie **Arbeitsspeicher**.
   - Zur Anzeige der Netzwerknutzung des Hosts in der vergangenen Stunde wählen Sie **Netzwerk**.
   - Zur Anzeige der Festplattennutzung des Hosts in der vergangenen Stunde wählen Sie **Festplatte**.

Überwachen des Systemzustands der Hardware im VMware Host Client

Wenn Sie beim VMware Host Client angemeldet sind, können Sie den Systemzustand der ESXi-Hosthardware überwachen.

Hinweis Der Systemzustand der Hardware ist nur verfügbar, wenn die zugrunde liegende Software dies unterstützt.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen** und anschließend auf **Hardware**.
2. Wählen Sie den Typ der anzuzeigenden Informationen aus.
3. (Optional) Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.
4. (Optional) Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen von Ereignissen im VMware Host Client

Ereignisse sind Aufzeichnungen von Benutzeraktionen oder Systemaktionen, die auf einem ESXi-Host durchgeführt werden. Wenn Sie beim VMware Host Client angemeldet sind, können Sie alle Ereignisse auf dem Host, den Sie verwalten, anzeigen.

Voraussetzungen

Erforderliche Berechtigung: **Nur-Lesen**.

Verfahren

- Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen** und anschließend auf **Ereignisse**.
  a. (Optional) Wählen Sie ein Ereignis aus, um die Ereignisdetails anzuzeigen.
  b. (Optional) Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.
  c. (Optional) Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen von Aufgaben im VMware Host Client

Wenn Sie beim VMware Host Client angemeldet sind, können Sie mit dem ESXi-Host verbunden Aufgaben anzeigen. Sie können Informationen zu Initiator, Status, Ergebnissen, Beschreibungen usw. von Aufgaben anzeigen.

Verfahren

- Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen** und anschließend auf **Aufgaben**.
  a (Optional) Wählen Sie eine Aufgabe aus, zu der Details angezeigt werden sollen.
  b (Optional) Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.
  c (Optional) Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen von Systemprotokollen im VMware Host Client

Wenn Sie mit dem VMware Host Client bei einem ESXi-Host angemeldet sind, können Sie Protokolleinträge anzeigen und Informationen über die Art des Ereignisses sowie darüber erhalten, wer ein Ereignis generiert hat und wann das Ereignis erstellt wurde.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen** und anschließend auf **Protokolle**.

   Die Liste der Protokolle wird angezeigt.
2. (Optional) Klicken Sie auf ein Protokoll, um Details dazu anzuzeigen.
3. (Optional) Klicken Sie mit der rechten Maustaste auf ein Protokoll und wählen Sie eine der folgenden Optionen aus:
   - **In neuem Fenster öffnen**
   - **Support-Paket erstellen**

Anzeigen von Benachrichtigungen im VMware Host Client

Wenn Sie beim VMware Host Client angemeldet sind, können Sie Host-Benachrichtigungen und Empfehlungen zu Aufgaben anzeigen, die Sie durchführen sollten.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Überwachen** und anschließend auf **Benachrichtigungen**.
2. Wählen Sie eine Benachrichtigung aus der Liste aus, um die empfohlene Aktion anzuzeigen.

   Unter der Benachrichtigungsliste wird eine Meldung mit einer empfohlenen Aktion und einer Beschreibung angezeigt.

Verwalten von virtuellen Maschinen mit dem VMware Host Client

3

Virtuelle Maschinen können wie physische Computer konfiguriert werden und führen auch dieselben Aufgaben durch. Darüber hinaus unterstützen virtuelle Maschinen, die von physischen Computern nicht unterstützt werden.

Sie können mit dem VMware Host Client virtuelle Maschinen erstellen, registrieren und verwalten und tägliche administrative und Fehlerbehebungsaufgaben durchführen.

Dieses Kapitel enthält die folgenden Themen:

Erstellen einer virtuellen Maschine im VMware Host Client

Virtuelle Maschinen sind die Schlüsselkomponenten in einer virtuellen Infrastruktur. Sie können zur Hostbestandsliste 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.

Voraussetzungen

Vergewissern Sie sich, dass Sie über die Rechte **VirtualMachine.Inventory.Create** verfügen.

Je nach den Eigenschaften der virtuellen Maschine, die Sie erstellen möchten, benötigen Sie möglicherweise die folgenden zusätzlichen Berechtigungen:

- **VirtualMachine.Config.AddExistingDisk**, wenn ein virtuelles Festplattengerät eingeschlossen werden soll, das sich auf eine bestehende virtuelle Festplattendatei (nicht RDM) bezieht.
- **VirtualMachine.Config.AddNewDisk**, wenn ein virtuelles Festplattengerät eingeschlossen werden soll, das eine neue virtuelle Festplattendatei (nicht RDM) erstellt.
- **VirtualMachine.Config.RawDevice**, wenn ein Raw-Gerätezuordnungs (RDM)- oder SCSI-Passthrough-Gerät eingeschlossen werden soll.
- **VirtualMachine.Config.HostUSBDevice**, wenn ein VirtualUSB-Gerät eingeschlossen werden soll, das von einem USB-Hostgerät unterstützt wird.
- **VirtualMachine.Config.AdvancedConfig**, wenn Werte in `ConfigSpec.extraConfig` festgelegt werden sollen.
- **VirtualMachine.Config.SwapPlacement**, wenn swapPlacement festgelegt werden soll.
- **Datastore.AllocateSpace** ist in allen Datenspeichern erforderlich, in denen die virtuelle Maschine und deren virtuelle Festplatten erstellt werden.
- **Network.Assign** ist in dem Netzwerk erforderlich, das der neu erstellten virtuellen Maschine zugewiesen wird.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **VM erstellen/registrieren**.

   Der Assistent zum **Erstellen neuer virtueller Maschinen** wird angezeigt.
2. Wählen Sie **Eine neue virtuelle Maschine erstellen** und klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **Namen und Gastbetriebssystem auswählen** einen eindeutigen Namen für die virtuelle Maschine ein und konfigurieren Sie das Gastbetriebssystem.
   a. Geben Sie in das Textfeld **Name** einen neuen Namen für die virtuelle Maschine ein.
   b. Wählen Sie im Dropdown-Menü **Kompatibilität** die Kompatibilität der virtuellen Maschine aus.
   c. Wählen Sie im Dropdown-Menü **Gastbetriebssystemfamilie** das Gastbetriebssystem aus.

d Wählen Sie im Dropdown-Menü **Version des Gastbetriebssystems** die Version des Gastbetriebssystems aus.

e Wenn Sie VBS auf der virtuellen Maschine aktivieren möchten, aktivieren Sie das Kontrollkästchen **Auf Windows-Virtualisierung basierte Sicherheit aktivieren** und klicken Sie auf **Weiter**.

Hinweis Die Option **Auf Windows-Virtualisierung basierte Sicherheit aktivieren** wird nur unter den neuesten Windows-Betriebssystemversionen, z. B. Windows 10 und Windows Server 2016, und wenn die Kompatibilität der virtuellen Maschine ESXi 6.7 und höher entspricht, angezeigt.

Daraufhin werden „Hardwarevirtualisierung“, „IOMMU“, „EFI“ und „Sicherer Start“ für das Gastbetriebssystem verfügbar. Sie müssen im Gastbetriebssystem dieser virtuellen Maschine auch **Auf Virtualisierung basierende Sicherheit** aktivieren.

4 Klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite **Speicher auswählen** den Speichertyp für die virtuelle Maschine und einen Datenspeicher aus, in dem die Dateien der virtuellen Maschine gespeichert werden sollen.

a Um alle Festplatten und Konfigurationsdateien der virtuellen Maschine in einem Standarddatenspeicher abzulegen, klicken Sie auf die Schaltfläche **Standard**.

b Um die Festplatten der virtuellen Maschine im lokal auf dem Host vorhandenen PMem-Datenspeicher zu speichern, klicken Sie auf die Schaltfläche **Persistenter Arbeitsspeicher**.

c Wählen Sie einen Datenspeicher in der Liste aus und klicken Sie auf **Weiter**.

Hinweis Sie können die Konfigurationsdateien nicht in einem PMem-Datenspeicher speichern. Bei Verwendung von PMem müssen Sie einen regulären Datenspeicher für die Konfigurationsdateien der virtuellen Maschine auswählen.

6 Konfigurieren Sie auf der Seite **Einstellungen anpassen** die Hardware der virtuellen Maschine und die dazugehörigen Optionen und klicken Sie auf **Weiter**.

Weitere Informationen zu Optionen von virtuellen Maschinen und zur Konfiguration von virtuellen Festplatten, einschließlich der Anweisungen zum Hinzufügen verschiedener Geräte, finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

a Klicken Sie auf der Seite **Einstellungen anpassen** auf **Virtuelle Hardware** und fügen Sie ein neues virtuelles Hardwaregerät hinzu.

- Klicken Sie auf das Symbol **Festplatte hinzufügen**, um eine neue virtuelle Festplatte hinzuzufügen.

  Hinweis Sie können der virtuellen Maschine eine Standardfestplatte oder eine persistente Arbeitsspeicherfestplatte hinzufügen. Die persistente Arbeitsspeicherfestplatte wird im lokal auf dem Host vorhandenen PMem-Datenspeicher gespeichert.

- Klicken Sie auf das Symbol **Netzwerkadapter hinzufügen**, um der virtuellen Maschine eine Netzwerkkarte (NIC) hinzuzufügen.
- Klicken Sie auf das Symbol **Anderes Gerät hinzufügen**, um einen anderen Gerätetyp auszuwählen, der der virtuellen Maschine hinzugefügt werden soll.

  Hinweis Verwendet die virtuelle Maschine PMem-Speicher, nutzen die Festplatten, die in einem PMem-Datenspeicher gespeichert sind, und die NVDIMM-Geräte, die Sie der virtuellen Maschine hinzufügen, die gleichen PMem-Ressourcen. Daher müssen Sie die Größe der neu hinzugefügten Geräte entsprechend der dem Host zur Verfügung stehenden PMem-Menge anpassen. Sollte ein Teil der Konfiguration Ihre Aufmerksamkeit erfordern, macht der Assistent Sie darauf aufmerksam.

b (Optional) Um Geräteeinstellungen anzuzeigen und zu konfigurieren, erweitern Sie ein beliebiges Gerät.

Option	Beschreibung
CPU	Die CPU oder 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. Die Anzahl der virtuellen CPUs, die einer virtuellen Maschine zur Verfügung stehen, hängen von der Anzahl der lizenzierten CPUs auf dem Host und der Anzahl der vom Gastbetriebssystem unterstützten CPUs ab. Um die VMware-Funktion für virtuelle CPUs mit mehreren Kernen nutzen zu können, müssen die Anforderungen der Endbenutzer-Lizenzvereinbarung des Gastbetriebssystems erfüllt sein.
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. Über die Arbeitsspeicher-Ressourceneinstellung einer virtuellen Maschine wird festgelegt, welcher

Option	Beschreibung
	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.
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.
SCSI-Controller	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. 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.
SATA-Controller	Wenn eine virtuelle Maschine mehrere Festplatten oder CD/DVD-ROM-Laufwerke besitzt, können Sie bis zu drei zusätzliche SATA-Controller hinzufügen, denen die Geräte zugewiesen werden sollen. Wenn Sie die Geräte auf mehrere Controller verteilen, können Sie die Leistung verbessern und eine Überlastung durch einen zu hohen Datenverkehr vermeiden. Sie können auch weitere Controller hinzufügen, wenn Sie die Begrenzung von 30 Geräten für einen einzelnen Controller überschreiten. Sie können virtuelle Maschinen von SATA-Controllern starten und sie für virtuelle Festplatten mit hoher Kapazität verwenden.
Netzwerkadapter	Wenn Sie eine virtuelle Maschine konfigurieren, können Sie Netzwerkadapter hinzufügen und den Adaptertyp festlegen. Welche Typen von Netzwerkadaptern verfügbar sind, ist von den folgenden Faktoren abhängig: ■ Die Kompatibilität der virtuellen Maschine, die vom Host abhängig ist, der sie erstellt oder zuletzt aktualisiert hat. ■ Ob die Kompatibilität der virtuellen Maschine für den aktuellen Host auf die neueste Version aktualisiert wurde. ■ Das Gastbetriebssystem.
CD/DVD-Laufwerk	Sie können DVD- oder CD-Geräte so konfigurieren, dass sie mit Clientgeräten, Hostgeräten oder Datenspeicher-ISO-Dateien verbunden werden können.
Grafikkarte	Sie können die Standardeinstellungen auswählen oder benutzerdefinierte Einstellungen angeben. Sie können die Anzahl der Anzeigen und den gesamten Videospeicher angeben und die 3D-Unterstützung für Gastbetriebssysteme aktivieren, auf denen VMware 3D unterstützt.
PCI-Gerät	Sie können PCI-Geräte auf einem ESXi-Host konfigurieren, um sie für Passthrough verfügbar zu machen. Sie können auch die Hardwarebezeichnungen ändern, um die Platzierung der virtuellen Maschine auf bestimmte Hardwareinstanzen einzuschränken.

Option	Beschreibung
Dynamisches PCI-Gerät	PCI-Passthrough-Geräte werden automatisch nach Hersteller und Modellname gruppiert. Sie können die gewünschten Geräte nach Hersteller und Modellname konfigurieren, anstatt ein physisches PCI-Gerät über die Hardwareadresse auszuwählen. Sie können alle verfügbaren Geräte mit derselben Hardwarebezeichnung oder einer leeren Hardwarebezeichnung zu einer virtuellen Maschine hinzufügen. Wenn Sie eine virtuelle Maschine einschalten, werden bestimmte physische PCI-Passthrough-Geräte mit passenden Hersteller- und Modellnamen an die virtuelle Maschine angehängt.
Sicherheitsgeräte	Sie können vSGX (Virtual Intel® Software Guard Extensions) für virtuelle Maschinen konfigurieren und zusätzliche Sicherheit für Ihre Arbeitslasten bereitstellen. Sie können vSGX aktivieren oder deaktivieren, wenn Sie eine virtuelle Maschine bereitstellen oder eine vorhandene virtuelle Maschine bearbeiten.

c (Optional) Um ein Gerät zu entfernen, klicken Sie auf das Löschsymbol (⊗) neben dem Gerät.

Diese Option erscheint nur für virtuelle Hardware, die Sie sicher entfernen können.

d (Optional) Klicken Sie zum Anpassen von Optionen für virtuelle Maschinen auf die Schaltfläche **VM-Optionen**.

7 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Details und klicken Sie auf **Beenden**.

Bereitstellen einer virtuellen Maschine aus einer OVF- oder OVA-Datei im VMware Host Client

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie virtuelle Maschinen aus OVF- und VMDK-Dateien sowie aus OVA-Dateien bereitstellen.

Verfahren

1 OVF- und OVA-Beschränkungen für den VMware Host Client

Sie können virtuelle Maschinen mithilfe von OVF- und VMDK-Dateien oder OVA-Dateien im VMware Host Client erstellen. Für die Bereitstellungsmethode gelten jedoch einige Einschränkungen.

2 Bereitstellung einer virtuellen Maschine aus einer OVF- oder OVA-Datei im VMware Host Client

Mit dem Assistenzen zum **Erstellen neuer virtueller Maschinen** können Sie virtuelle Maschinen aus OVF- und VMDK-Dateien oder OVA-Dateien bereitstellen.

OVF- und OVA-Beschränkungen für den VMware Host Client

Sie können virtuelle Maschinen mithilfe von OVF- und VMDK-Dateien oder OVA-Dateien im VMware Host Client erstellen. Für die Bereitstellungsmethode gelten jedoch einige Einschränkungen.

Einschränkungen für OVA

Sie können OVA-Dateien mit einem Webbrowser oder einem Client hochladen. Aufgrund der beträchtlichen Anforderungen an Arbeitsspeicher kann es vorkommen, dass der Webbrowser nicht mehr reagiert oder das System instabil wird. Die Größe der OVA-Datei, die hochgeladen werden kann, hängt vom verfügbaren Arbeitsspeicher im System ab. VMware-Tests haben gezeigt, dass mit Google Chrome OVA-Dateien von einer Größe von ca. 1 GB hochgeladen werden können. Mit Mozilla Firefox können größere OVA-Dateien extrahiert werden, es kann jedoch vorkommen, dass er nicht mehr reagiert.

Zur Bereitstellung einer großen OVA-Datei wird empfohlen, die OVA zuerst durch Ausführen des Befehls tar `-xvf <file.ova>` auf dem System zu extrahieren. Anschließend können Sie dem Bereitstellungsassistenten die OVF- und VMDK-Dateien separat zuführen.

Einschränkungen für OVF

Die Größe von OVF-Dateien, die mit einem Webbrowser hochgeladen werden können, ist ebenfalls begrenzt. Für unterschiedliche Browser gelten unterschiedliche Grenzen für Dateigrößen. Für Mozilla Firefox gilt ein Grenzwert von 4 GB. Mit Google Chrome können größere Dateien hochgeladen werden; es bestehen keine bekannten Einschränkungen.

Bereitstellung einer virtuellen Maschine aus einer OVF- oder OVA-Datei im VMware Host Client

Mit dem Assistenzen zum **Erstellen neuer virtueller Maschinen** können Sie virtuelle Maschinen aus OVF- und VMDK-Dateien oder OVA-Dateien bereitstellen.

Die OVA-Bereitstellung ist aufgrund von Webbrowser-Beschränkungen auf Dateien unter einer Größe von 1 GB beschränkt. Um eine OVA-Datei von mehr als 1 GB bereitzustellen, extrahieren Sie die OVA-Datei mithilfe von tar. Stellen Sie die OVF- und die VMDK-Dateien dann separat zur Verfügung.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **VM erstellen/registrieren**.

   Der Assistent zum **Erstellen neuer virtueller Maschinen** wird angezeigt.

2. Wählen Sie auf der Seite **Erstellungstyp auswählen** die Option **Eine virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen** aus und klicken Sie auf **Weiter**.

3. Geben Sie auf der Seite **OVF- und VMDK-Dateien auswählen** einen eindeutigen Namen für die virtuelle Maschine ein.

   Hinweis Der Name der virtuellen Maschine kann bis zu 80 Zeichen lang sein.

4. Um eine OVF- und eine VMDK-Datei oder eine OVA-Datei für die Bereitstellung auszuwählen, klicken Sie auf den blauen Bereich.

   Der lokale Systemspeicher wird geöffnet.

5 Wählen Sie die Datei, von der aus die virtuelle Maschine bereitgestellt werden soll, aus und klicken Sie auf **Öffnen**.

   Die von Ihnen ausgewählte Datei wird im blauen Bereich angezeigt.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite **Speicher auswählen** den Speichertyp für die virtuelle Maschine aus.

   a Um alle Festplatten und Konfigurationsdateien der virtuellen Maschine in einem Standarddatenspeicher abzulegen, klicken Sie auf die Schaltfläche **Standard**.

   b Um die Festplatten der virtuellen Maschine im lokal auf dem Host vorhandenen PMem-Datenspeicher zu speichern, klicken Sie auf die Schaltfläche **Persistenter Arbeitsspeicher**.

   c Wählen Sie einen Datenspeicher in der Liste aus und klicken Sie auf **Weiter**.

   Wichtig Die Konfigurationsdateien können nicht in einem PMem-Datenspeicher gespeichert werden. Bei Verwendung von PMem müssen Sie einen regulären Datenspeicher für die Konfigurationsdateien der virtuellen Maschine auswählen.

8 Wählen Sie auf der Seite **Bereitstellungsoptionen** die Netzwerkzuordnungen und die Festplattenbereitstellung aus und geben Sie an, ob die virtuelle Maschine nach der Bereitstellung eingeschaltet werden soll.

9 Klicken Sie auf **Weiter**.

10 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Details und klicken Sie auf **Beenden**.

Ergebnisse

Die virtuelle Maschine wird in der VMware Host Client-Bestandsliste unter **Virtuelle Maschinen**angezeigt.

Registrieren einer vorhandenen virtuellen Maschine im VMware Host Client

Wenn Sie die Registrierung einer virtuellen Maschine bei einem Host aufheben, die virtuelle Maschine jedoch nicht aus dem Datenspeicher löschen, können Sie die virtuelle Maschine mithilfe des VMware Host Client erneut registrieren. Das erneute Registrieren einer virtuellen Maschine führt dazu, dass sie in der Bestandsliste angezeigt wird.

Verwenden Sie den Datenspeicherbrowser, um entweder einen Datenspeicher, ein Verzeichnis oder eine `.vmx`-Datei zum Hinzufügen zur Liste der von Ihnen zu registrierenden virtuellen Maschinen auszuwählen. Wenn Sie einen Datenspeicher oder ein Verzeichnis auswählen, wird nach allen `.vmx`-Dateien an diesem Speicherort gesucht. Sie können den Vorgang zum Durchsuchen mehr als einmal durchführen, um der Liste virtuelle Maschinen hinzuzufügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **VM erstellen/registrieren**.

   Der Assistent zum Erstellen einer **neuen virtuellen Maschine** wird angezeigt.

2. Wählen Sie auf der Seite **Erstellungstyp auswählen** die Option **Eine vorhandene virtuelle Maschine registrieren** aus und klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **VMs für die Registrierung auswählen** auf **Mindestens eine virtuelle Maschine, einen Datenspeicher oder ein Verzeichnis auswählen**, suchen Sie die zu registrierende virtuelle Maschine und klicken Sie auf **Auswählen**.
4. Um eine virtuelle Maschine aus der Liste zu entfernen, wählen Sie den Namen der Datei aus und klicken Sie auf **Auswahl entfernen**.
5. Um Ihre Auswahl aufzuheben und von vorn zu beginnen, klicken Sie auf **Alle entfernen**.
6. Klicken Sie auf **Weiter**.
7. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Details und klicken Sie auf **Beenden**.

Arbeiten mit Konsolen im VMware Host Client

Sie können im VMware Host Client über eine Browserkonsole oder VMware Remote Console (VMRC) auf eine virtuelle Maschine zugreifen und verschiedene Aufgaben daran durchführen.

Arbeiten mit der Browserkonsole

Hinweis Die Browserkonsole wird auf ESXi-Versionen, die älter sind als 6.0, nicht unterstützt. Für den Zugriff auf die Browserkonsole müssen Sie VMRC verwenden.

Über eine Browserkonsole erhalten Sie Zugriff auf das Gastbetriebssystem, ohne dass Sie zusätzliche Software installieren müssen. Weitere Konsolenfunktionen wie das Anhängen lokaler Hardware erhalten Sie, wenn Sie VMware Remote Console installieren.

Hinweis Browserkonsolen unterstützen derzeit nur amerikanische, japanische und deutsche Tastaturlayouts. Vor dem Öffnen der Konsole müssen Sie das gewünschte Tastaturlayout wählen.

Arbeiten mit VMware Remote Console

VMware Remote Console bietet Zugriff auf virtuelle Maschinen auf Remote-Hosts und führt Konsolen- und Gerätevorgänge für *VMware vSphere* durch, wie z. B. das Konfigurieren von Betriebssystemeinstellungen und Überwachen der VM-Konsole. Sie können zahlreiche Aufgaben an der virtuellen Maschine durchführen, z. B. Neu starten und Herunterfahren des Gastbetriebssystems, Fortsetzen und Anhalten der virtuellen Maschine, Konfigurieren von Updates zu VMware Tools, Konfigurieren und Verwalten der virtuellen Maschine und

verschiedener Geräte uvm. Mit VMRC können außerdem VM-Einstellungen geändert werden, wie z. B. RAM, CPU-Kerne und Festplatten. VMware Workstation™, VMware Fusion™ oder VMware Player™ fungieren als VMRC-Clients, daher brauchen Sie VMRC nicht herunterzuladen und zu installieren, wenn eines der drei Systeme auf Ihrem System installiert ist.

Den vollen Umfang an Konsolenfunktionen erhalten Sie, wenn Sie VMRC herunterladen und installieren.

Installieren der VMware Remote Console-Anwendung im VMware Host Client

Die VMware Remote Console (VMRC) ist eine eigenständige Konsolenanwendung, mit der Sie eine Verbindung zu Clientgeräten herstellen und VM-Konsolen auf Remote-Hosts starten können.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

Die Liste der auf dem Host verfügbaren virtuellen Maschinen wird angezeigt.

2 Wählen Sie eine virtuelle Maschine aus der Liste aus.

3 Klicken Sie auf das Symbolleistensymbol **Konsole** und wählen Sie die Option **VMRC herunterladen** aus.

Starten der Remote Console zu einer virtuellen Maschine im VMware Host Client

Mithilfe der VMware Remote Console können Sie auf virtuelle Maschinen im VMware Host Client zugreifen. Sie können eine oder mehrere Konsolen für den gleichzeitigen Zugriff auf verschiedene virtuelle Remotemaschinen starten.

Voraussetzungen

Stellen Sie sicher, dass die VMware Remote Console auf Ihrem lokalen System installiert ist.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen** und wählen Sie eine virtuelle Maschine aus der Liste aus.

2 Klicken Sie auf **Konsole** und wählen Sie **Remotekonsole starten** aus dem Dropdown-Menü aus.

Die VMware Remote Console wird als eigenständige Anwendung für die ausgewählte virtuelle Maschine geöffnet.

Öffnen einer Konsole der virtuellen Maschine im VMware Host Client

Mit dem VMware Host 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.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Wählen Sie eine eingeschaltete virtuelle Maschine aus der Liste aus.

3 Klicken Sie auf das Symbolleistensymbol **Konsole** und legen Sie fest, ob die Konsole in einem Popup-Fenster, in einem neuen Fenster oder auf einer neuen Registerkarte geöffnet wird.

Verwalten eines Gastbetriebssystems im VMware Host Client

Sie können mit dem VMware Host Client das Gastbetriebssystem der virtuellen Maschine verwalten. Sie können VMware Tools installieren und aktualisieren und das konfigurierte Gastbetriebssystem herunterfahren, neu starten und ändern.

Herunterfahren oder Neustarten eines Gastbetriebssystems mit dem VMware Host Client

Installieren Sie VMware Tools auf einer virtuellen Maschine, um das Gastbetriebssystem darauf herunterzufahren und neu zu starten.

Verfahren

- Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen** und wählen Sie eine virtuelle Maschine und die entsprechende Aufgabe aus.
  - Klicken Sie zum Herunterfahren einer virtuellen Maschine mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Gastbetriebssystem > Herunterfahren** aus.
  - Klicken Sie zum Neustarten einer virtuellen Maschine mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Gastbetriebssystem > Neustarten** aus.

Ändern des Gastbetriebssystemtyps im VMware Host 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, wendet vCenter Server die Standardwerte für die Konfiguration auf Grundlage des Gasttyps an. Das Ändern der Einstellungen des Gastbetriebssystems wirkt sich auf die verfügbaren Bereiche und Empfehlungen zu den Einstellungen der virtuellen Maschine aus.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

2 Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Allgemeine Optionen**.

3 Wählen Sie einen Typ und eine Version für das Gastbetriebssystem aus.

   Wenn Sie eine Windows-Betriebssystemversion auswählen, die VBS unterstützt, und die virtuelle Maschine mit ESXi 6.7 und höher kompatibel ist, wird auf der Registerkarte **VM-Optionen** die VBS-Zeile angezeigt.

4 (Optional) Klicken Sie auf **Virtualisierungsbasierte Sicherheit aktivieren**, um VBS zu aktivieren.

   Wichtig Wenn VBS aktiviert ist, müssen Sie die virtuelle Maschine mithilfe von EFI starten. Mit einer anderen Firmware lässt sich das Gastbetriebssystem unter Umständen nicht mehr starten.

5 Klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

Ergebnisse

Die Konfigurationsparameter der virtuellen Maschine für das Gastbetriebssystem werden geändert. Sie können das Gastbetriebssystem nun installieren.

Einführung in VMware Tools

Bei VMware Tools handelt es sich um mehrere Dienste und Module, über die zahlreiche Funktionen in VMware-Produkten für bessere Verwaltungsmöglichkeiten sowie für reibungslose Benutzerinteraktionen mit Gastbetriebssystemen aktiviert werden.

VMware Tools bietet die folgenden Möglichkeiten:

- leitet Meldungen vom Host- an das Gastbetriebssystem weiter
- passt Gastbetriebssysteme als Teil von vCenter Server und weiteren VMware-Produkten an
- führt einen Skriptsatz aus, der Sie dabei unterstützt, Vorgänge des Gastbetriebssystems zu automatisieren Die Skripts werden ausgeführt, wenn sich der Betriebsstatus der virtuellen Maschine ändert.
- Synchronisiert die Uhrzeit des Gastbetriebssystems mit der Uhrzeit des Hostbetriebssystems

Die Lebenszyklusverwaltung von VMware Tools bietet einen vereinfachten und skalierbaren Ansatz für das Installieren und Aktualisieren von VMware Tools. Es umfasst eine Reihe an Funktionsverbesserungen, treiberbezogenen Verbesserungen sowie Unterstützung für neue Gastbetriebssysteme.

Sie müssen die aktuelle Version von VMware Tools ausführen oder open-vm-tools verwenden, die im Rahmen der Linux-Betriebssystembereitstellung erhältlich sind. Obwohl ein Gastbetriebssystem ohne VMware Tools ausgeführt werden kann, sollten Sie in Ihrem Gastbetriebssystem immer die aktuelle Version von VMware Tools ausführen, um die neuesten Funktionen und Aktualisierungen nutzen zu können.

Sie können Ihre virtuellen Maschinen so konfigurieren, dass bei jedem Einschalten automatisch geprüft wird, ob Upgrades für VMware Tools vorhanden sind, und diese ggf. angewendet werden.

Informationen zum Aktivieren von automatischen Aktualisierungen von VMware Tools auf Ihren virtuellen Maschinen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.

VMware Tools installieren

Obwohl Sie Gastbetriebssysteme ohne VMware Tools verwenden können, sind viele VMware-Funktionen erst verfügbar, nachdem Sie VMware Tools installiert haben. VMware Tools verbessert die Leistung des Gastbetriebssystems Ihrer virtuellen Maschinen.

Das Installieren von VMware Tools ist Teil des Vorgangs zur Erstellung von neuen virtuellen Maschinen. Es ist wichtig, VMware Tools zu aktualisieren, sobald Aktualisierungen verfügbar sind. Informationen zum Erstellen virtueller Maschinen finden Sie im *VMware Tools-Benutzerhandbuch*.

Die Installation der VMware Tools erfolgt über ISO-Imagedateien. Eine ISO-Imagedatei sieht wie eine CD-ROM Ihres Gastbetriebssystems aus. Jeder Gastbetriebssystemtyp, einschließlich Windows, Linux, Solaris, FreeBSD und NetWare, hat eine ISO-Imagedatei. Wenn Sie VMware Tools installieren oder ein Upgrade durchführen, stellt das erste virtuelle CD-ROM-Laufwerk der virtuellen Maschine vorübergehend eine Verbindung zur ISO-Datei von VMware Tools Ihres Gastbetriebssystems her.

Informationen zur Installation oder zum Upgrade von VMware Tools auf virtuellen Windows-Maschinen, virtuellen Linux-Maschinen, virtuellen Mac OS X-Maschinen, virtuellen Solaris-Maschinen, virtuellen NetWare-Maschinen oder virtuellen FreeBSD-Maschinen finden Sie im *VMware Tools-Benutzerhandbuch*.

Installieren von VMware Tools aus dem VMware Host Client

Die VMware Tools bestehen aus einer Reihe von Dienstprogrammen, die Sie im Betriebssystem einer virtuellen Maschine installieren. VMware Tools verbessert die Leistung und die Verwaltung der virtuellen Maschine.

Sie können VMware Tools in einer oder mehr virtuellen Maschinen mithilfe des VMware Host Client installieren.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Wählen Sie eine virtuelle Maschine aus der Liste aus.

   Die virtuelle Maschine muss eingeschaltet sein, um VMware Tools zu installieren.

3 Klicken Sie auf **Aktionen**, wählen Sie im Dropdown-Menü **Gastbetriebssystem** aus und wählen Sie anschließend **VMware Tools installieren**.

Upgrade der VMware Tools

Sie können ein Upgrade von VMware Tools manuell durchführen oder virtuelle Maschinen so konfigurieren, dass sie Überprüfungen auf neuere Versionen von VMware Tools durchführen und diese installieren.

Das Gastbetriebssystem sucht nach der VMware Tools-Version, wenn Sie eine virtuelle Maschine einschalten. In der Statusleiste der virtuellen Maschine wird eine Meldung angezeigt, wenn eine neue Version verfügbar ist.

Wenn die installierte Version von VMware Tools bei virtuellen vSphere-Maschinen veraltet ist, wird in der Statusleiste die folgende Meldung angezeigt:

```
„Eine neuere Version von VMware Tools ist für diese virtuelle Maschine verfügbar."
```

In virtuellen Windows-Maschinen können Sie VMware Tools so einstellen, dass Sie über die Verfügbarkeit eines Upgrades benachrichtigt werden. Wenn diese Benachrichtigungsoption aktiviert ist, enthält das VMware Tools-Symbol in der Windows-Taskleiste ein gelbes „Vorsicht"-Symbol, wenn ein VMware Tools-Upgrade verfügbar ist.

Führen Sie bei der Installation eines VMware Tools-Upgrades dieselben Schritte aus wie bei der ersten Installation von VMware Tools. Ein Aktualisieren von VMware Tools bedeutet das Installieren einer neuen Version.

Für Windows- und Linux-Gastbetriebssysteme können Sie die virtuelle Maschine konfigurieren, um ein Aktualisieren von VMware Tools automatisch durchzuführen. Obwohl beim Einschalten der virtuellen Maschine eine Versionsprüfung durchgeführt wird, wird im Falle von Windows-Gastbetriebssystemen beim Ausschalten oder Neustarten der virtuellen Maschine ein automatisches Upgrade durchgeführt. In der Statusleiste wird die Meldung `VMware Tools-Dienst wird installiert...` angezeigt, wenn ein Upgrade-Vorgang läuft. Das Verfahren wird weiter unten erwähnt.

Hinweis Beim Upgrade von VMware Tools auf Windows-Gastbetriebssystemen wird der WDDM-Grafiktreiber automatisch installiert. Der WDDM-Grafiktreiber lässt zu, dass der in den Stromversorgungseinstellungen des Gastbetriebssystems verfügbare Energiesparmodus die Energiesparoptionen anpasst. Beispielsweise können Sie die Energiesparmoduseinstellung **Energiesparmodus ändern** verwenden, um Ihr Gastbetriebssystem so zu konfigurieren, dass es nach einer gewissen Zeit automatisch in den Energiesparmodus wechselt. Zudem können Sie mit dieser Einstellung verhindern, dass Ihr Gastbetriebssystem nach einiger gewissen Leerlaufzeit automatisch in den Energiesparmodus wechselt.

Für virtuelle vSphere-Maschinen können Sie die folgenden Prozesse verwenden, um ein Upgrade mehrerer virtueller Maschinen gleichzeitig durchzuführen.

- Melden Sie sich bei vCenter Server an, wählen Sie einen Host oder Cluster und geben Sie auf der Registerkarte **Virtuelle Maschinen** die virtuellen Maschinen an, auf denen ein VMware Tools-Upgrade durchgeführt werden soll.
- Verwenden Sie vSphere Lifecycle Manager, um ein koordiniertes Upgrade der virtuellen Maschinen auf Ordner- oder Datencenter-Ebene durchzuführen.

Einige Funktionen in einem bestimmten Release eines VMware-Produkts können von der Installation der Version oder vom Upgrade auf die Version von VMware Tools abhängen, die in diesem Release enthalten sind. Es ist nicht immer erforderlich, auf die neueste Version von VMware Tools zu aktualisieren. Neuere Versionen von VMware Tools sind mit mehreren Hostversionen kompatibel. Um unnötige Upgrades zu vermeiden, prüfen Sie, ob die zusätzlichen Funktionen in Ihrer Umgebung erforderlich sind.

Tabelle 3-1. Kompatibilitätsoptionen für virtuelle Maschinen

Kompatibilität	Beschreibung
ESXi 7.0 Update 3 und höher	Diese virtuelle Maschine (Hardwareversion 19) ist kompatibel mit ESXi 7.0 Update 3 und höher.
ESXi 7.0 Update 2 und höher	Diese virtuelle Maschine (Hardwareversion 19) ist kompatibel mit ESXi 7.0 Update 2 und höher.
ESXi 7.0 Update 1 und höher	Diese virtuelle Maschine (Hardwareversion 18) ist kompatibel mit ESXi 7.0 Update 1 und ESXi 7.0 Update 2.
ESXi 7.0 und höher	Diese virtuelle Maschine (Hardwareversion 17) ist kompatibel mit ESXi 7.0, ESXi 7.0 Update 1 und ESXi 7.0 Update 2.
ESXi 6.7 Update 2 und höher	Diese virtuelle Maschine (Hardwareversion 15) ist kompatibel mit ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 und ESXi 7.0 Update 2.
ESXi 6.7 und höher	Diese virtuelle Maschine (Hardwareversion 14) ist kompatibel mit ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 und ESXi 7.0 Update 2.
ESXi 6.5 und höher	Diese virtuelle Maschine (Hardwareversion 13) ist kompatibel mit ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 und ESXi 7.0 Update 2.
ESXi 6.0 und höher	Diese virtuelle Maschine (Hardwareversion 11) ist kompatibel mit ESXi 6.0, ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 und ESXi 7.0 Update 2.

Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility.

Aktualisieren von VMware Tools im VMware Host Client

Sie können ein Upgrade von VMware Tools in einer virtuellen Maschine mithilfe von VMware Host Client vornehmen.

Voraussetzungen

Schalten Sie die virtuelle Maschine ein.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Wählen Sie eine virtuelle Maschine aus der Liste aus.
3. Klicken Sie auf **Aktionen**, wählen Sie **Gastbetriebssystem** im Dropdown-Menü aus und wählen Sie anschließend **VMware Tools aktualisieren**.

Konfigurieren einer virtuellen Maschine im VMware Host Client

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-Quellen, Arbeitsspeicher und Festplatten.

Überprüfen der Hardwareversion einer virtuellen Maschine im VMware Host Client

Die Hardwareversion einer virtuellen Maschine finden Sie auf deren Übersichtsseite.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Wählen Sie eine virtuelle Maschine aus der Liste aus.

   Die Hardwarversion wird unter dem Namen der virtuellen Maschine angezeigt.

Ändern des Namens einer virtuellen Maschine im VMware Host Client

Nach der Erstellung einer virtuellen Maschine können Sie deren Namen 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

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Klicken Sie auf **VM-Optionen**.
4. Geben Sie einen neuen Namen für die virtuelle Maschine in das Textfeld **VM-Name** ein.
5. Klicken Sie auf **Speichern**.

Anzeigen des Speicherorts der Konfigurationsdatei der virtuellen Maschine im VMware Host Client

Sie können den Speicherort der Konfigurations- und Arbeitsdateien einer virtuellen Maschine mit dem VMware Host Client anzeigen.

Diese Informationen sind nützlich, wenn Sie Sicherungssysteme konfigurieren.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Allgemeine Optionen**.
4. Notieren Sie sich den Speicherort der Konfigurations- und Arbeitsdateien.
5. Klicken Sie auf **Abbrechen**, um Bildschirm zu schließen.

Konfigurieren der Betriebszustände der virtuellen Maschine im VMware Host Client

Die Änderung der Betriebszustände der virtuellen Maschinen ist sinnvoll, wenn auf dem Host Wartungsarbeiten ausgeführt werden. Sie können die standardmäßigen Systemeinstellungen für die Steuerelemente für die Betriebszustände der virtuellen Maschine auf der Symbolleiste verwenden oder Sie können die Steuerelemente konfigurieren, um mit dem Gastbetriebssystem

zu interagieren. Legen Sie beispielsweise für das Steuerelement **Ausschalten** 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.

Sie können keine **Einschalten** ()-Aktion konfigurieren. Mit dieser Aktion wird eine virtuelle zuvor ausgeschaltete Maschine eingeschaltet, oder eine virtuelle Maschine wird gestartet und ein Skript wird ausgeführt, wenn die virtuelle Maschine angehalten wurde und VMware Tools installiert und verfügbar ist. Ist VMware Tools nicht installiert, wird die angehaltene virtuelle Maschine wieder gestartet und es wird kein Skript ausgeführt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Berechtigungen zum Ausführen der beabsichtigten Ein-/Ausschaltvorgänge auf der virtuellen Maschine verfügen.
- Installieren Sie VMWare Tools in der virtuellen Maschine, damit Sie optionale Energiefunktionen festlegen können.
- Schalten Sie die virtuelle Maschine aus, bevor Sie die VMware Tools-Optionen bearbeiten.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Erweitern Sie auf der Registerkarte **VM-Optionen** die Option **VMware Tools**.
4. Wählen Sie im Dropdown-Menü eine Option für die Steuerung **Ausschalten** () der virtuellen Maschine aus.

Option	Beschreibung
Ausschalten	Stoppt die virtuelle Maschine sofort. Eine Ausschaltaktion fährt das Gastbetriebssystem herunter oder schaltet die virtuelle Maschine aus. Eine Meldung weist darauf hin, dass das Gastbetriebssystem möglicherweise nicht ordnungsgemäß heruntergefahren wird. Verwenden Sie diese Ausschaltoption nur bei Bedarf.
Gast herunterfahren	Verwendet VMware Tools, um die virtuelle Maschine ordnungsgemäß herunterzufahren. Ein „weiches“ Ausschalten ist nur dann möglich, wenn die Tools auf dem Gastbetriebssystem installiert sind.
Systemstandard	Befolgt die Systemeinstellungen. Der aktuelle Wert der Systemeinstellungen wird in runden Klammern angezeigt.

5 Wählen Sie im Dropdown-Menü eine Option für die Steuerung **Anhalten** () aus.

Option	Beschreibung
Anhalten	Hält alle Aktivitäten der virtuellen Maschine an. Wenn VMware Tools installiert und verfügbar ist, führt eine Anhalteaktion ein Skript aus und hält die virtuelle Maschine an. Wenn VMware Tools nicht installiert ist, hält eine Anhalteaktion die virtuelle Maschine ohne Ausführen des Skriptes an.
Gast in Standbymodus versetzen	Versetzt das Gastbetriebssystem in den Standby-Modus. Durch diese Option werden alle Prozesse beendet, doch alle virtuellen Geräte bleiben mit der virtuellen Maschine verbunden.
Systemstandard	Befolgt die Systemeinstellungen. Der aktuelle Wert der Systemeinstellungen wird in runden Klammern angezeigt.

6 Wählen Sie im Dropdown-Menü eine Option für die Steuerung **Zurücksetzen** () aus.

Option	Beschreibung
Zurücksetzen	Das Gastbetriebssystem wird heruntergefahren und neu gestartet, ohne dass die virtuelle Maschine ausgeschaltet wird. Wenn VMWare Tools nicht installiert ist, setzt die Zurücksetzen-Aktion die virtuelle Maschine zurück.
Gast neu starten	Verwendet VMware Tools für einen ordnungsgemäßen Neustart. Ein „weiches“ Ausschalten ist nur dann möglich, wenn die Tools auf dem Gastbetriebssystem installiert sind.
Standard	Befolgt die Systemeinstellungen. Der aktuelle Wert der Systemeinstellungen wird in runden Klammern angezeigt.

7 Klicken Sie auf **Speichern**.

Bearbeiten der Parameter der Konfigurationsdatei im VMware Host Client

Zum Beheben bestimmter Probleme mit Ihrem System werden Sie in der VMware-Dokumentation oder von einem Mitarbeiter des technischen Supports von VMware möglicherweise angewiesen, Konfigurationsparameter der virtuellen Maschine zu ändern oder hinzuzufügen.

Wichtig Das Ändern oder Hinzufügen von Parametern in Fällen, in denen für ein System keine Probleme vorliegen, kann zu einer verringerten Systemleistung und Instabilität führen.

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 das vorhandene Paar beispielsweise Schlüsselwort/Wert lautet und Sie es in Schlüsselwort/Wert2 ändern, lautet das neue Schlüsselwort Wert2.

- 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.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Erweitern Sie auf der Registerkarte **VM-Optionen** die Option **Erweitert**.
4. Klicken Sie in der Zeile „Konfigurationsparameter“ auf **Konfiguration bearbeiten**.

   Das Dialogfeld **Konfigurationsparameter** wird geöffnet.
5. (Optional) Klicken Sie zum Hinzufügen eines Parameters auf **Parameter hinzufügen** und geben Sie einen Namen und einen Wert für den Parameter ein.
6. (Optional) Sie können einen Parameter ändern, indem Sie im Feld **Wert** einen neuen Wert für diesen Parameter eingeben.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld **Konfigurationsparameter** zu schließen.
8. Klicken Sie auf **Speichern**.

Konfigurieren von Autostart für eine virtuelle Maschine im VMware Host Client

Sie können Autostart-Optionen für eine virtuelle Maschine konfigurieren, mit denen veranlasst wird, dass sie vor oder nach anderen virtuellen Maschinen auf dem Host gestartet wird.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste.

3 Wählen Sie **Autostart** aus dem Popup-Menü aus und klicken Sie auf eine Autostart-Option für diese virtuelle Maschine.

Option	Beschreibung
Priorität erhöhen	Erhöht die Startpriorität dieser virtuellen Maschine, sodass sie vor anderen VMs gestartet wird.
Priorität senken	Senkt die Startpriorität dieser virtuellen Maschine, sodass sie nach anderen VMs gestartet wird.

Upgrade der Kompatibilität von virtuellen Maschinen mithilfe des VMware Host Client

Die Kompatibilität der virtuellen Maschine legt die virtuelle Hardware fest, die für die virtuelle Maschine verfügbar ist. Dies entspricht der physischen Hardware, die auf der Hostmaschine zur Verfügung steht. Sie können ein Upgrade der Kompatibilitätsebene vornehmen, um eine virtuelle Maschine mit der neuesten Version von ESXi kompatibel zu machen, die auf dem Host läuft.

Informationen über Versionen und Kompatibilität der Hardware für virtuelle Maschinen finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Voraussetzungen

- Erstellen Sie eine Sicherung oder einen Snapshot der virtuellen Maschinen. Weitere Informationen hierzu finden Sie unter Verwenden von Snapshots zum Verwalten virtueller Maschinen.
- Aktualisieren Sie VMware Tools. Falls Sie auf virtuellen Maschinen mit Microsoft Windows ein Upgrade der Kompatibilität vor einem Upgrade von VMware Tools durchführen, gehen auf der virtuellen Maschine möglicherweise die Netzwerkeinstellungen verloren.
- Stellen Sie sicher, dass dem ESXi-Host alle `.vmdk`-Dateien auf einem VMFS3-, VMFS5- oder NFS-Datenspeicher zur Verfügung stehen.
- Stellen Sie sicher, dass die virtuelle Maschine in VMFS3-, VMFS5- oder NFS-Datenspeichern gespeichert ist.
- Vergewissern Sie sich, dass die Kompatibilitätseinstellungen für die virtuellen Maschinen nicht der letzten unterstützten Version entsprechen.
- Ermitteln Sie die ESXi-Versionen für die virtuellen Maschinen, mit denen die Kompatibilität hergestellt werden soll. Weitere Informationen hierzu finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Upgrade der VM-Kompatibilität** im Popup-Menü aus.

3 Wählen Sie die neueste unterstützte Version aus und klicken Sie auf **Upgrade**.

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 dieser Begriffe kann Ihnen bei der Planung Ihrer Strategie für die CPU-Ressourcenzuweisung helfen.

CPU

Die CPU oder der Prozessor ist die Komponente eines Computersystems, die die für die Ausführung der Anwendung erforderlichen Aufgaben durchführt. Die CPU ist das primäre Element, das die Funktionen des Computers ausführt. CPUs enthalten Kerne.

CPU-Socket

Ein CPU-Socket ist ein physischer Connector auf der Hauptplatine eines Computers, der eine einzelne physische CPU akzeptiert. Einige Hauptplatinen weisen mehrere Sockets auf und können mehrere Prozessoren mit mehreren Kernen (Mehrkern-CPUs) verbinden.

Kern

Ein Kern umfasst eine Einheit, die einen L1-Cache und funktionale Einheiten enthält, die zur Ausführung von Anwendungen erforderlich sind. Kerne können Anwendungen oder Threads unabhängig ausführen. Es können sich ein oder mehrere Kerne auf einer einzelnen CPU befinden.

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 sich beispielsweise die Auslastung der Buchhaltung am Jahresende erhöht, können Sie die Reserve des Ressourcenpools „Buchhaltung“ erhöhen.

vSphere Virtual Symmetric Multiprocessing (Virtual SMP)

Virtual SMP oder vSphere Virtual Symmetric Multiprocessing ist eine Funktion, die es einer einzelnen virtuellen Maschine ermöglicht, mehrere Prozessoren aufzuweisen.

Einschränkungen für virtuelle CPUs

Die maximale Anzahl der virtuellen CPUs, die einer virtuellen Maschine zugewiesen werden können, beträgt 768. Die Anzahl der virtuellen CPUs richtet sich nach der Anzahl der logischen CPUs auf dem Host und dem Typ des Gastbetriebssystems, das auf der virtuellen Maschine installiert ist.

Beachten Sie die folgenden Einschränkungen:

- Eine virtuelle Maschine kann nicht mehr virtuelle CPUs aufweisen als die Anzahl an logischen Kernen auf dem Host. Die Anzahl der logischen Kerne entspricht der Anzahl an physischen Kernen, wenn das Hyper-Threading deaktiviert ist, oder der zweifachen Anzahl der Kerne, wenn das Hyper-Threading aktiviert ist.
- Bei einer ausgeführten virtuellen Maschine mit maximal 128 virtuellen CPUs können Sie die virtuellen CPUs nicht im laufenden Betrieb hinzufügen, um deren Anzahl zu erhöhen. Um die Anzahl der virtuellen CPUs über diesen Grenzwert hinaus zu ändern, müssen Sie zuerst die virtuelle Maschine ausschalten. Wenn eine ausgeführte virtuelle Maschine jedoch bereits mehr als 128 virtuelle CPUs aufweist, können Sie virtuelle CPUs im laufenden Betrieb hinzufügen und deren Anzahl auf bis zu 768 erhöhen.
- Die maximale Anzahl der virtuellen CPU-Sockets für eine virtuelle Maschine beträgt 128. Wenn Sie eine virtuelle Maschine mit mehr als 128 virtuellen CPUs konfigurieren möchten, müssen Sie virtuelle CPUs mit mehreren Kernen verwenden.
- Virtual SMP wird nicht von jedem Gastbetriebssystem unterstützt, und Gastbetriebssysteme, die diese Funktion unterstützen, unterstützen möglicherweise nur eine geringere Anzahl von Prozessoren als die auf dem Host verfügbare Anzahl. Informationen zur Unterstützung von Virtual SMP finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.
- Systeme mit einem Prozessor können die Leistung der virtuellen Maschine, je nach Arbeitslast, beeinträchtigen. Es wird empfohlen, die Arbeitslast zu testen, um zu ermitteln, ob Hyper-Threading auf den Hosts aktiviert oder deaktiviert werden soll.

Konfigurieren von virtuellen CPUs mit mehreren Kernen

Die Unterstützung virtueller CPUs mit mehreren Kernen von VMware ermöglicht Ihnen, in einer virtuellen Maschine die Anzahl der Kerne pro virtuellem Socket zu steuern. Mithilfe dieser Funktion können auch Betriebssysteme mit Socket-Beschränkungen mehrere Kerne der Host-CPU verwenden und die Leistung erhöhen.

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.

Der Einsatz virtueller CPUs mit mehreren Kernen kann dann sinnvoll sein, wenn Sie mit Betriebssystemen oder Anwendungen arbeiten, die nur eine begrenzte Anzahl von CPU-Sockets nutzen können.

Sie können eine mit ESXi 7.0 Update 1 und höher kompatible virtuelle Maschine so konfigurieren, dass sie maximal 768 virtuelle CPUs aufweist. Die Zahl der virtuellen CPUs auf einer virtuellen Maschine kann die Anzahl der tatsächlich auf dem Host vorhandenen logischen CPUs nicht übersteigen. Die Anzahl der logischen CPUs entspricht der Anzahl der physischen Prozessorkerne bzw. der doppelten Anzahl, wenn Hyper-Threading aktiviert ist. Wenn beispielsweise ein Host über 128 logische CPUs verfügt, können Sie die virtuelle Maschine für 128 virtuelle CPUs konfigurieren.

Sie konfigurieren, wie die virtuellen CPUs in Bezug auf die Kerne und die Kerne pro Sockel zugewiesen werden. Legen Sie die Anzahl der CPU-Kerne für die virtuelle Maschine fest und wählen Sie anschließend die Anzahl der Kerne pro Socket aus, je nachdem, ob Sie eine Single-Core-CPU, Dual-Core-CPU, Tri-Core-CPU usw. verwenden. Ihre Auswahl bestimmt die Anzahl der Sockets, über die die virtuelle Maschine verfügt.

Die maximale Anzahl der virtuellen CPU-Sockets für eine virtuelle Maschine beträgt 128. Wenn Sie eine virtuelle Maschine mit mehr als 128 virtuellen CPUs konfigurieren möchten, müssen Sie virtuelle CPUs mit mehreren Kernen verwenden.

Weitere Informationen zu CPUs mit mehreren Kernen finden Sie unter *Handbuch zur vSphere-Ressourcenverwaltung*.

Ändern der Anzahl virtueller CPUs im VMware Host Client

Eine mit ESXi 7.0 Update 1 und höher kompatible virtuelle Maschine kann bis zu 768 virtuelle CPUs aufweisen. Die Anzahl der virtuellen CPUs kann geändert werden, wenn die virtuelle Maschine abgeschaltet ist. Wenn das Hinzufügen virtueller CPUs im laufenden Betrieb aktiviert ist, können Sie die Anzahl der virtuellen CPUs auch während der Ausführung der virtuellen Maschine erhöhen.

Das Hinzufügen virtueller CPUs im laufenden Betrieb ist bei virtuellen Maschinen möglich, die über Mehrkern-CPU-Unterstützung verfügen und mit ESXi 5.0 und höher kompatibel sind. Wenn die virtuelle Maschine eingeschaltet und das Hinzufügen von CPUs im laufenden Betrieb aktiviert ist, können Sie virtuelle CPUs der laufenden virtuellen Maschine hinzufügen. Sie können nur ein Vielfaches der Anzahl der Kerne pro Socket hinzufügen.

Bei einer virtuellen Maschine mit maximal 128 virtuellen CPUs können Sie die virtuellen CPUs nicht im laufenden Betrieb hinzufügen, um deren Anzahl weiter zu erhöhen. Um die Anzahl der virtuellen CPUs über diesen Grenzwert hinaus zu ändern, müssen Sie zuerst die virtuelle Maschine ausschalten. Wenn eine virtuelle Maschine jedoch bereits mehr als 128 virtuelle CPUs aufweist, können Sie virtuelle CPUs im laufenden Betrieb hinzufügen und deren Anzahl auf bis zu 768 erhöhen.

Die maximale Anzahl der virtuellen CPU-Sockets für eine virtuelle Maschine beträgt 128. Wenn Sie eine virtuelle Maschine mit mehr als 128 virtuellen CPUs konfigurieren möchten, müssen Sie virtuelle CPUs mit mehreren Kernen verwenden.

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 virtuelle CPUs hinzufügen.
- Sollen im laufenden Betrieb CPUs mit mehreren Kernen hinzugefügt werden, vergewissern Sie sich, dass die virtuelle Maschine mit ESXi 5.0 und höher kompatibel ist.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.CPU-Anzahl ändern** verfügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Erweitern Sie „CPU“ in der Registerkarte **Virtuelle Hardware** und wählen Sie die Anzahl der Kerne aus dem Dropdown-Menü **CPU** aus.
4. Wählen Sie im Dropdown-Menü **Kerne pro Socket** die Anzahl der Kerne pro Socket aus.
5. Klicken Sie auf **Speichern**.

Zuteilen von CPU-Ressourcen im VMware Host Client

Um den Arbeitslastbedarf zu verwalten, können Sie die Anzahl der CPU-Ressourcen, die einer virtuellen 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 oder GHz angegeben.

Reservierung

Gibt die garantierte Mindestzuteilung für eine virtuelle Maschine an. Diese Reservierung wird in MHz oder GHz 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.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **CPU** und teilen Sie die CPU-Kapazität für die virtuelle Maschine zu.

Option	Beschreibung
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.
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.

4 Klicken Sie auf **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 Arbeitsspeicher-Ressourceneinstellung 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

Sie können die Menge des einer virtuellen Maschine zugeteilten Arbeitsspeichers neu konfigurieren, um die Leistung zu erhöhen.

Die minimale Arbeitsspeichergröße ist 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 für virtuelle Maschinen, die BIOS-Firmware verwenden, ist 24560 GB. Sie müssen die EFI-Firmware für virtuelle Maschinen mit einer Arbeitsspeichergröße von mehr als 6128 GB verwenden.

Die maximale Arbeitsspeichergröße einer virtuellen Maschine hängt vom physischen Arbeitsspeicher des ESXi-Hosts und den Kompatibilitätseinstellungen 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. Der Maximalwert für beste Leistung stellt den Schwellenwert dar, bei dessen Überschreitung der physische Arbeitsspeicher des ESXi-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.

Die Arbeitsspeichergröße muss ein Vielfaches von 4 MB sein.

Tabelle 3-2. Maximaler Arbeitsspeicher der virtuellen Maschine

Seit der Hostversion	Kompatibilität der virtuellen Maschine	Maximale Arbeitsspeichergröße
ESXi 7.0 Update 3	ESXi 7.0 Update 3 und höher	24560 GB
ESXi 7.0 Update 2	ESXi 7.0 Update 2 und höher	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 und höher	24560 GB
ESXi 7.0	ESXi 7.0 und höher	6128 GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 und höher	6128 GB
ESXi 6.7	ESXi 6.7 und höher	6128 GB
ESXi 6.5	ESXi 6.5 und höher	6128 GB
ESXi 6.0	ESXi 6.0 und höher	4080 GB

Die ESXi-Hostversion gibt den Zeitpunkt an, seit dem die höhere Arbeitsspeichergröße unterstützt wird. Beispielsweise ist die Arbeitsspeichergröße einer virtuellen Maschine, die mit ESXi 6.0 und höher kompatibel ist und auf ESXi 6.5 ausgeführt wird, auf 4080 GB beschränkt.

Voraussetzungen

Stellen Sie sicher, dass Sie die Berechtigung **Virtuelle Maschine.Konfiguration.Arbeitsspeicher ändern** auf der virtuellen Maschine besitzen.

Verfahren

1 Klicken Sie in der Bestandsliste mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.

2 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** den Bereich **Arbeitsspeicher** und ändern Sie die Arbeitsspeicherkonfiguration.

   a Geben Sie im Textfeld **Arbeitsspeicher** die Menge an RAM ein, die der virtuellen Maschine zugewiesen werden soll.

   b Wählen Sie aus, ob der Arbeitsspeicher in MB, GB oder TB angegeben wird.

3 Klicken Sie auf **OK**.

Zuteilen von Speicherressourcen zu einer virtuellen Maschine im VMware Host Client

Sie können die Anzahl der Arbeitsspeicherressourcen, die einer virtuellen Maschine zugeteilt wurden, unter Verwendung von Anteilen, Reservierungen und Grenzwerteinstellungen ändern. Der Host bestimmt die entsprechende Menge an physischem RAM, die den virtuellen Maschinen auf Grundlage dieser Einstellungen zugeteilt wird. Abhängig von der Belastung und dem Status können Sie einer virtuellen Maschine einen hohen oder einen niedrigen Anteilswert zuteilen.

Die folgenden benutzerdefinierten Einstellungen betreffen die Arbeitsspeicher-Ressourcenzuteilung einer virtuellen Maschine.

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. Wenn die Reservierung nicht eingehalten werden kann, wird die virtuelle Maschine nicht eingeschaltet.

Anteile

Jeder virtuellen Maschine werden Arbeitsspeicheranteile zugeteilt. Je mehr Anteile eine virtuelle Maschine hat, desto größer ist der Anteil an Hostarbeitsspeicher, der ihr zugeteilt wird. Anteile stellen eine relative Metrik zum Zuteilen von Arbeitsspeicherkapazität dar. Weitere Informationen zu Anteilswerten finden Sie im *Handbuch zur vSphere-Ressourcenverwaltung*.

Sie können einer virtuellen Maschine keine Reservierung zuweisen, die größer als der konfigurierte Arbeitsspeicher der virtuellen Maschine ist. Wenn Sie einer virtuellen Maschine eine große Reservierung zuweisen und die konfigurierte Arbeitsspeichergröße für diese virtuelle Maschine verringern, wird die Reservierung ebenfalls verringert, damit sie mit der neuen konfigurierten Arbeitsspeichergröße übereinstimmt.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Arbeitsspeicher** und teilen Sie die Arbeitsspeicherkapazität für die virtuelle Maschine zu.

Option	Beschreibung
Reservierung	Garantierte Arbeitsspeicherzuteilung für diese virtuelle Maschine.
Grenzwert	Obergrenze für die Arbeitsspeicherzuteilung für diese virtuelle Maschine. Wählen Sie **Unbegrenzt**, wenn Sie keine Obergrenze definieren möchten.
Anteile	Die Werte **Niedrig**, **Normal**, **Hoch** und **Benutzerdefiniert** werden mit der Summe aller Anteile aller virtuellen Maschinen auf dem Server verglichen.

4 Klicken Sie auf **Speichern**.

Ändern der Einstellungen zum Hinzufügen von Arbeitsspeicher im laufenden Betrieb im VMware Host Client

Mit dem Hinzufügen von Arbeitsspeicher im laufenden Betrieb können Sie Arbeitsspeicherressourcen für eine virtuelle Maschine hinzufügen, während diese eingeschaltet ist.

Das Hinzufügen von Arbeitsspeicher im laufenden Betrieb produziert zusätzlich Arbeitsspeicher-Overhead auf dem ESXi-Host für die virtuelle Maschine.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Stellen Sie sicher, dass die virtuelle Maschine über ein Gastbetriebssystem verfügt, das das Hinzufügen von Arbeitsspeicher im laufenden Betrieb unterstützt.
- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 4.x und höher kompatibel ist.
- Stellen Sie sicher, dass VMware Tools installiert ist.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Arbeitsspeicher** und aktivieren Sie **Arbeitsspeicher-Hotplug**.

4 Klicken Sie auf **Speichern**.

Hinzufügen eines NVDIMM-Geräts zu einer VM im VMware Host Client

Fügen Sie einer virtuellen Maschine ein virtuelles NVDIMM-Gerät hinzu, damit diese den nicht flüchtigen, oder persistenten, Arbeitsspeicher des Computers nutzen kann. Ein nicht flüchtiger Arbeitsspeicher (non-volatile memory, NVM) oder persistenter Arbeitsspeicher (PMem) verbindet die hohen Datenübertragungsraten eines flüchtigen Arbeitsspeichers mit der Persistenz und Stabilität eines herkömmlichen Speichers. Das virtuelle NVDIMM-Gerät ist ein virtuelles NVM-Gerät, das gespeicherte Daten über Neustarts oder Stromausfälle hinaus beibehalten kann.

Virtuelle Maschinen verbrauchen die PMem-Ressource des Hosts über ein virtuelles, nicht flüchtiges, duales Inline-Arbeitsspeichermodul (NVDIMM) oder über eine virtuelle, persistente Arbeitsspeicherfestplatte.

Weitere Informationen zu persistentem Arbeitsspeicher finden Sie unter Verwalten von persistentem Arbeitsspeicher.

Voraussetzungen

- Stellen Sie sicher, dass das Gastbetriebssystem der virtuellen Maschine PMem unterstützt.
- Stellen Sie sicher, dass die Version der virtuellen Hardware 14 oder höher ist.
- Stellen Sie sicher, dass Sie über das Recht **Datenspeicher.Speicher zuteilen** verfügen.
- Stellen Sie sicher, dass der Host oder Cluster, auf dem sich die virtuelle Maschine befindet, über vorhandene PMem-Ressourcen verfügt.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf **Anderes Gerät hinzufügen** und wählen Sie anschließend im Dropdown-Menü die Option **NVDIMM** aus.

   Das NVDIMM-Gerät wird in der Geräteliste der virtuellen Hardware angezeigt. Jede virtuelle Maschine kann über maximal 64 NVDIMM-Geräte verfügen.
4. Konfigurieren Sie das neu hinzugefügte NVDIMM-Gerät.
   a. Erweitern Sie in der Geräteliste der virtuellen Hardware den Eintrag **Neues NVDIMM**.
   b. Geben Sie die Größe des neuen NVDIMM-Geräts ein.

      Hinweis Sie können die Größe des NVDIMM-Geräts zu einem späteren Zeitpunkt ändern. Die virtuelle Maschine muss ausgeschaltet sein.

   c. Wählen Sie den Speicherort des NVDIMM-Controllers aus oder übernehmen Sie den Standard-Controller.
5. Klicken Sie auf **Speichern**, um den Assistenten zu schließen.

Netzwerkkonfiguration virtueller Maschinen

Die ESXi-Netzwerkfunktionen ermöglichen die Kommunikation zwischen virtuelle Maschinen auf demselben Host, zwischen virtuelle 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 wie 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.

Grundlegendes zu Netzwerkadaptern

Wenn Sie eine virtuelle Maschine konfigurieren, können Sie Netzwerkadapter hinzufügen und den Adaptertyp festlegen.

Typen von Netzwerkadaptern

Welche Typen von Netzwerkadaptern verfügbar sind, ist von den folgenden Faktoren abhängig:

- Die Kompatibilität der virtuellen Maschine, die vom Host abhängig ist, der sie erstellt oder zuletzt aktualisiert hat.
- Ob die Kompatibilität der virtuellen Maschine für den aktuellen Host auf die neueste Version aktualisiert wurde.
- Das Gastbetriebssystem.

Bei den unterstützten Netzwerkkarten wird zurzeit zwischen einer lokalen Umgebung und VMware Cloud on AWS unterschieden. Die folgenden Typen von Netzwerkkarten werden in einer lokalen Bereitstellung unterstützt:

E1000E

Emulierte Version der Intel 82574 Gigabit-Ethernetnetzwerkkarte. E1000E ist der Standardadapter für Windows 8 und Windows Server 2012.

E1000

Emulierte Version der Intel 82545EM-Gigabit-Ethernet-Netzwerkkarte mit den Treibern, die in den meisten neueren Gastbetriebssystemen, wie z. B. Windows XP und höher und den Linux-Versionen 2.4.19 und höher, zur Verfügung stehen.

Flexibel

Identifiziert sich beim Start einer virtuellen Maschine als Vlance-Adapter, initialisiert sich und arbeitet abhängig davon, von welchem Treiber er initialisiert wird, jedoch entweder als Vlance- oder als VMXNET-Adapter. Wenn VMware Tools installiert ist, ändert der VMXNET-Treiber den Vlance-Adapter in den leistungsfähigeren VMXNET-Adapter.

Vlance

Emulierte Version der AMD 79C970 PCnet32 LANCE-Netzwerkkarte, bei der es sich um eine ältere 10-MBit/s-Netzwerkkarte handelt, für die Treiber in älteren 32-Bit-Gastbetriebssystemen zur Verfügung stehen. Eine virtuelle Maschine, die mit diesem Netzwerkadapter konfiguriert ist, kann ihr Netzwerk unmittelbar verwenden.

VMXNET

Optimiert für den Einsatz in einer virtuellen Maschine. Besitzt keine physische Entsprechung. Da die Betriebssystem-Hersteller keine integrierten Treiber für diese Karte anbieten, müssen Sie VMware Tools installieren, damit ein Treiber für den VMXNET-Netzwerkadapter verfügbar ist.

VMXNET 2 (Erweitert)

Basiert auf dem VMXNET-Adapter, bietet jedoch Hochleistungsfunktionen, die in modernen Netzwerken häufig verwendet werden, wie z. B. Jumbo-Frames und Hardware-Offloads. VMXNET 2 (Erweitert) ist nur für einige Gastbetriebssysteme auf ESX/ESXi 3.5 und höher verfügbar.

VMXNET 3

Eine paravirtualisierte Netzwerkkarte, die auf Leistung ausgelegt ist. VMXNET 3 bietet alle bei VMXNET 2 verfügbaren Funktionen sowie mehrere neue Funktionen, wie z. B. Multiqueue-Unterstützung (unter Windows auch Skalierung der Empfangsseite genannt), IPv6-Offloads und MSI/MSI-X-Interrupt-Delivery. VMXNET 3 ist nicht mit VMXNET oder VMXNET 2 verwandt.

PVRDMA

Eine paravirtualisierte Netzwerkkarte, die RDMA (Remote Direct Memory Access, Remotezugriff auf den direkten Speicher) zwischen virtuellen Maschinen durch die OFED verbs-API unterstützt. Alle virtuellen Maschinen müssen über ein PVRDMA-Gerät verfügen und sollten mit einem Distributed Switch verbunden sein. PVRDMA unterstützt VMware vSphere vMotion und die Snapshot-Technologie. Es ist in virtuellen Maschinen mit Hardwareversion 13 und dem Gastbetriebssystem Linux-Kernel 4.6 und höher verfügbar.

Informationen zum Zuweisen eines PVRDMA-Netzwerkadapters zu einer virtuellen Maschine finden Sie in der *vSphere-Netzwerk*-Dokumentation.

SR-IOV-Passthrough

Darstellung einer virtuellen Funktion (VF) auf einer physischen Netzwerkkarte mit SR-IOV-Unterstützung. Die virtuelle Maschine und der physische Adapter tauschen Daten aus, ohne den VMkernel als Zwischenkomponente zu nutzen. Dieser Adaptertyp ist für virtuelle Maschinen geeignet, bei denen die Latenz zu Fehlern führen kann oder die mehr CPU-Ressourcen benötigen.

SR-IOV-Passthrough ist in ESXi 6.0 und höher für die Gastbetriebssysteme Red Hat Enterprise Linux 6 und höher und Windows Server 2008 R2 mit SP2 verfügbar.
Eine Betriebssystemversion enthält möglicherweise einen Standard-VF-Treiber für gewisse Netzwerkkarten. Sie müssen für andere Netzwerkkarten den Treiber von einem vom Netzwerkkarten- bzw. Hostanbieter angegebenen Speicherort herunterladen und ihn manuell installieren.

Informationen zum Zuweisen eines SR-IOV-Passthrough-Netzwerkadapters zu einer virtuellen Maschine finden Sie in der *vSphere-Netzwerk*-Dokumentation.

Weitere Aspekte zur Netzwerkadapterkompatibilität finden Sie im *VMware-Kompatibilitätshandbuch* auf http://www.vmware.com/resources/compatibility.

Legacy-Netzwerkadapter und Versionen virtueller ESXi-Hardware

Die Standard-Netzwerkadaptertypen für virtuelle Legacy-Maschinen richten sich nach den Adaptern, die für das Gastbetriebssystem verfügbar und damit kompatibel sind, sowie nach der Version der virtuellen Hardware, auf der die virtuelle Maschine erstellt wurde.

Wenn Sie kein Upgrade einer virtuellen Maschine zur Verwendung einer Version virtueller Hardware durchführen, bleiben die Adaptereinstellungen unverändert. Wenn Sie die virtuelle Maschine aktualisieren, um von der neueren virtuellen Hardware zu profitieren, werden die Standardadaptereinstellungen wahrscheinlich geändert, damit sie kompatibel mit dem Gastbetriebssystem und der aktualisierten Hosthardware sind.

Weitere Informationen zur Überprüfung der für Ihr unterstütztes Gastbetriebssystem verfügbaren Netzwerkadapter für eine bestimmte Version von vSphere ESXi finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.

Netzwerkadapter und virtuelle Legacy-Maschinen

Virtuelle Legacy-Maschinen sind virtuelle Maschinen, die vom verwendeten Produkt unterstützt werden, jedoch für das Produkt nicht aktuell sind. Die Standard-Netzwerkadaptertypen für virtuelle Legacy-Maschinen richten sich nach den Adaptern, die für das Gastbetriebssystem verfügbar und damit kompatibel sind, sowie nach der Version der virtuellen Hardware, auf der die virtuelle Maschine erstellt wurde.

Wenn Sie die virtuelle Maschine nicht aktualisieren, damit sie einem Upgrade auf eine neuere Version eines ESXi-Hosts entspricht, bleiben die Adaptereinstellungen unverändert. Wenn Sie die virtuelle Maschine aktualisieren, um von der neueren virtuellen Hardware zu profitieren, werden die Standardadaptereinstellungen wahrscheinlich geändert, damit sie kompatibel mit dem Gastbetriebssystem und der aktualisierten Hosthardware sind.

Weitere Informationen zur Überprüfung der für Ihr unterstütztes Gastbetriebssystem verfügbaren Netzwerkadapter für eine bestimmte Version von vSphere ESXi finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.

Ändern der Konfiguration des virtuellen Netzwerkadapters im VMware Host Client

Sie können die Einstellung zur Verbindung beim Einschalten, die MAC-Adresse und die Netzwerkverbindung des Netzwerkadapters einer virtuellen Maschine konfigurieren.

Voraussetzungen

Erforderliche Rechte:

- **Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern** zum Bearbeiten der MAC-Adresse und des Netzwerks.
- **Virtuelle Maschine.Interaktion.Geräteverbindung** zum Ändern von **Verbinden** und **Beim Einschalten verbinden**.
- **Netzwerk .Netzwerk zuweisen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Klicken Sie auf die Registerkarte **Virtuelle Hardware** und wählen Sie den entsprechenden Netzwerkadapter (Netzwerkkarte) aus der Hardwareliste aus.
4. (Optional) Wenn die virtuelle Netzwerkkarte (Network Interface Card, NIC) beim Einschalten der virtuellen Maschine verbunden werden soll, wählen Sie **Beim Einschalten verbinden** aus.
5. (Optional) Wählen Sie den Adaptertyp im Dropdown-Menü **Adaptertyp** aus.
6. 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.

7. Klicken Sie auf **Speichern**.

Hinzufügen eines Netzwerkadapters zu einer virtuellen Maschine im VMware Host Client

Wenn Sie einer virtuellen Maschine einen Netzwerkadapter (Netzwerkkarte) hinzufügen, müssen Sie den Adaptertyp und die Netzwerkverbindung auswählen und angeben, ob das Gerät beim Einschalten der virtuellen Maschine verbunden werden soll.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf **Netzwerkadapter hinzufügen**.

4 Wählen Sie im Bereich „Netzwerkverbindung“ ein Netzwerk mit einer bestimmten Bezeichnung oder ein Legacy-Netzwerk aus.

5 (Optional) Wenn die virtuelle Netzwerkkarte (Network Interface Card, NIC) beim Einschalten der virtuellen Maschine konfiguriert werden soll, wählen Sie **Beim Einschalten verbinden** aus.

6 Klicken Sie auf **Speichern**.

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 auf dem Gastbetriebssystem als einzelne Festplatte angezeigt. Die virtuelle Festplatte besteht aus einer oder mehreren Dateien auf dem 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 Option ist nützlich, wenn Sie in Ihren virtuellen Maschinen Anwendungen ausführen, die die physischen Merkmale des Speichergeräts erkennen müssen. Das Zuordnen einer SAN-LUN ermöglicht Ihnen auch die Verwendung vorhandener SAN-Befehle für die Speicherverwaltung der Festplatte.

Wenn Sie einem VMFS-Volume 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 haben nur die Möglichkeit, ihre Daten in einer virtuellen Festplattendatei zu 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.

Informationen zu Bereitstellungsrichtlinien für virtuelle Festplatten

Wenn Sie bestimmte Vorgänge für die Verwaltung virtueller Maschinen ausführen, können Sie eine Bereitstellungsrichtlinie für die virtuelle Festplattendatei angeben. Zu diesen Vorgängen zählen das Erstellen einer virtuellen Festplatte, das Klonen einer virtuellen Maschine in eine Vorlage oder das Migrieren einer virtuellen Maschine.

NFS-Datenspeicher mit Hardwarebeschleunigung und VMFS-Datenspeicher unterstützen die folgenden Festplattenbereitstellungsrichtlinien. Auf NFS-Datenspeichern, die die Hardwarebeschleunigung nicht unterstützen, steht nur das Thin-Format zur Verfügung.

Mithilfe von Storage vMotion oder Cross-Host Storage vMotion können Sie virtuelle Laufwerke von einem Format in ein anderes umwandeln.

Thick-Provision Lazy-Zeroed

Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird zugeteilt, wenn die Festplatte erstellt wird. Daten, die auf dem physischen Gerät verbleiben, werden beim Erstellvorgang nicht gelöscht, sondern zu einem späteren Zeitpunkt bei Bedarf beim ersten Schreiben von der virtuellen Maschine durch Nullbyte ersetzt. Virtuelle Maschinen lesen keine veralteten Daten vom physischen Gerät.

Thick-Provision Eager-Zeroed

Ein Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Thick-Provision Lazy-Zeroed-Format-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von virtuellen Festplatten in diesem Format kann länger dauern als das Anlegen anderer Festplattentypen. Das Vergrößern einer virtuellen Festplatte im Eager-Zeroed-Thick-Format führt dazu, dass die virtuelle Maschine für geraume Zeit einfriert.

Thin-bereitstellen

Verwenden Sie dieses Format, um Speicherplatz zu sparen. Für eine Festplatte mit diesem Format stellen Sie genauso viel Datenspeicherplatz bereit, wie die Festplatte ausgehend von dem Wert erfordern würde, den Sie für die Größe der virtuellen Festplatte eingeben. Die Festplatte besitzt jedoch zunächst nur eine geringe Größe und verwendet nur so viel Datenspeicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. Wenn die Festplatte später mehr Speicherplatz benötigt, kann sie auf ihre maximale Kapazität anwachsen und den gesamten für sie bereitgestellten Datenspeicherplatz in Anspruch nehmen.

Thin-Bereitstellung stellt die schnellste Methode zum Erstellen einer virtuellen Festplatte dar, da lediglich eine Festplatte nur mit den Header-Informationen erstellt wird. Speicherblöcke werden nicht zugewiesen oder auf Null gesetzt. Speicherblöcke werden bei ihrem ersten Zugriff zugewiesen oder auf Null gesetzt.

Hinweis Wenn eine virtuelle Festplatte Clusterlösungen wie z. B. Fault Tolerance unterstützt, verwenden Sie für die Festplatte nicht das Format „Thin“.

Ändern der Konfiguration der virtuellen Festplatte im VMware Host Client

Wenn kein Speicherplatz mehr zur Verfügung steht, können Sie die Größe der Festplatte erhöhen. Sie können den Knoten des virtuellen Geräts und den dauerhaften Modus der Konfiguration der virtuellen Festplatte für eine virtuelle Maschine ändern.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

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

- **Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern** auf der virtuellen Maschine
- **Virtuelle Maschine.Konfiguration.Virtuelle Festplatte erweitern** auf der virtuellen Maschine
- **Datenspeicher.Speicher zuteilen** im Datenspeicher.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option Festplatte, um die Festplattenoptionen anzuzeigen.
4. (Optional) Sie können die Größe der Festplatte ändern, indem Sie im Textfeld einen neuen Wert eingeben und im Dropdown-Menü die Einheiten auswählen.

5 (Optional) Um die Art und Weise zu ändern, wie sich Snapshots auf Festplatten auswirken, wählen Sie im Dropdown-Menü **Festplattenmodus** einen Festplattenmodus aus.

Option	Beschreibung
Abhängig	Abhängige Festplatten sind in Snapshots enthalten.
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 persistenten 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 der virtuellen Maschine gelöscht.

6 Klicken Sie auf **Speichern**.

Hinzufügen einer neuen Standardfestplatte zu einer virtuellen Maschine in VMware Host Client

Sie können einer vorhandenen virtuellen Maschine eine virtuelle Festplatte hinzufügen oder Sie können eine Festplatte hinzufügen, wenn Sie die Hardware der virtuellen Maschine während der Erstellung anpassen. Sie müssen beispielsweise weitere Festplattenspeicher für eine vorhandene virtuelle Maschine mit einer schweren Arbeitslast bereitstellen. Beim Erstellen der virtuellen Maschine können Sie beispielsweise eine Festplatte hinzufügen, die als Startlaufwerk vorkonfiguriert ist.

Voraussetzungen

- Vergewissern Sie sich, dass Sie mit den Konfigurationsoptionen und Einschränkungen beim Hinzufügen virtueller Festplatten vertraut sind. Weitere Informationen hierzu finden Sie unter Konfiguration der virtuellen Festplatte.
- Bevor Sie einer virtuellen Maschine Festplatten mit mehr als 2 TB hinzufügen, lesen Sie den Abschnitt *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Stellen Sie sicher, dass Sie das Recht **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen** für den Zielordner oder Zieldatenspeicher haben.

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 (Optional) Zum Löschen einer vorhandenen Festplatte führen Sie den Mauszeiger über die Festplatte und klicken auf das Symbol **Entfernen** (**X**).

   Die Festplatte wird aus der virtuellen Maschine entfernt. Wenn andere virtuelle Maschinen dieselbe Festplatte gemeinsam verwenden, werden die Festplattendateien nicht entfernt.

4 Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte hinzufügen** und anschließend im Dropdown-Menü die Option **Neue Standardfestplatte** aus.

   Die Festplatte wird in der Geräteliste der virtuellen Hardware angezeigt.

5 Erweitern Sie **Neue Festplatte**.

6 (Optional) Geben Sie einen Wert für die Festplattengröße ein und wählen Sie im Dropdown-Menü die Einheiten aus.

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

8 Wählen Sie das Format für die Festplatte der virtuellen Maschine aus.

Option	Beschreibung
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der Speicher, den die virtuelle Festplatte benötigt, wird während des Erstellens zugewiesen. Alle Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Erstellens, 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 Erstellens durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.
Thin-Bereitstellung	Verwendet das Format „Thin-bereitgestellt“. Eine Festplatte mit diesem Format verwendet zunächst genau die Menge an Datenspeicherplatz, die sie anfänglich benötigt. Wenn die Thin-bereitgestellte Festplatte später mehr Speicherplatz benötigt, kann sie auf die maximal zugeteilte Kapazität anwachsen.

9 Wählen Sie im Dropdown-Menü **Anteile** einen Wert für die Anteile aus, die der virtuellen Festplatte zugewiesen werden sollen.

   Der Anteilswert stellt die relative Metrik zur Steuerung der Festplattenbandbreite dar. Die Werte „Niedrig“, „Normal“, „Hoch“ und „Benutzerdefiniert“ werden mit der Summe aller Anteile aller virtuellen Maschinen auf dem Host verglichen.

10 Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie im Textfeld die Anzahl der Anteile ein.

11 Geben Sie im Feld **Grenzwert – IOPs** den oberen Grenzwert für Speicherressourcen an, die der virtuellen Maschine zugeteilt werden sollen, oder wählen Sie **Unbegrenzt**.

Dieser Wert ist der obere Grenzwert der E/A-Vorgänge pro Sekunde, die der virtuellen Festplatte zugeteilt wurden.

12 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: Es soll von einem LSI Logic-Controller gestartet und mit einer anderen virtuellen Maschine eine Datenplatte gemeinsam verwendet werden. Diese virtuelle Maschine verwendet einen BusLogic-Controller, bei dem die gemeinsame Bus-Nutzung aktiviert ist.

13 (Optional) Wählen Sie einen Festplattenmodus aus.

Option	Beschreibung
Abhängig	Abhängige Festplatten sind in Snapshots enthalten.
Unabhängig – Dauerhaft	Festplatten im dauerhaften Modus verhalten sich wie herkömmliche physische Computerfestplatten. Sämtliche Daten, die im persistenten 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. Die virtuelle Festplatte wird bei jedem Neustart der virtuellen Maschine in denselben Status zurückversetzt. Änderungen an der Festplatte werden in eine Redo-Protokolldatei geschrieben und daraus gelesen. Diese Datei wird beim Ausschalten oder Zurücksetzen gelöscht.

14 Klicken Sie auf **Speichern**.

Hinzufügen einer vorhandenen Festplatte zu einer virtuellen Maschine im VMware Host Client

Sie können einer virtuellen Maschine eine vorhandene virtuelle Festplatte hinzufügen, wenn Sie die Hardware der virtuellen Maschine während oder nach der Erstellung der virtuellen Maschine anpassen. Beispiel: Sie können eine vorhandene Festplatte hinzufügen, die als ein Startlaufwerk vorkonfiguriert ist.

Beim Erstellen einer virtuellen Maschine werden der virtuellen Maschine basierend auf dem von Ihnen ausgewählten Gastbetriebssystem standardmäßig eine Festplatte und ein SCSI- oder SATA-Controller hinzugefügt. Wenn diese Festplatte nicht Ihren Anforderungen entspricht, könnten Sie sie entfernen und am Ende des Erstellungsvorgangs eine vorhandene Festplatte hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass Sie mit Controllern und virtuellen Geräteknoten für verschiedene virtuelle Festplattenkonfigurationen vertraut sind.

- Stellen Sie sicher, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen** für den Zielordner oder Zieldatenspeicher verfügen.

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte hinzufügen** und wählen Sie anschließend **Vorhandene Festplatte** aus dem Dropdown-Menü aus.
4. (Optional) Zum Löschen einer vorhandenen Festplatte führen Sie den Mauszeiger über die Festplatte und klicken auf das Symbol **Entfernen** (**X**).

   Die Festplatte wird aus der virtuellen Maschine entfernt. Wenn andere virtuelle Maschinen dieselbe Festplatte gemeinsam verwenden, werden die Festplattendateien nicht entfernt.
5. Erweitern Sie in der Spalte „Datenspeicher“ einen Datenspeicher, wählen Sie einen Ordner für die virtuelle Maschine und dann die hinzuzufügende Festplatte aus.

   Die Festplattendatei wird in der Spalte „Inhalt“ angezeigt. Im Menü **Dateityp** werden die kompatiblen Dateitypen für die Festplatte angezeigt.
6. Klicken Sie auf **Auswählen** und anschließend auf **Speichern**, um die vorhandene Festplatte hinzuzufügen.

Hinzufügen einer persistenten Arbeitsspeicherfestplatte im Hostclient

Sie können einer vorhandenen virtuellen Maschine eine virtuelle Festplatte hinzufügen oder Sie können eine Festplatte hinzufügen, wenn Sie die Hardware der virtuellen Maschine während der Erstellung anpassen. Sie müssen beispielsweise weitere Festplattenspeicher für eine vorhandene virtuelle Maschine mit einer schweren Arbeitslast bereitstellen. Beim Erstellen der virtuellen Maschine können Sie beispielsweise eine Festplatte hinzufügen, die als Startlaufwerk vorkonfiguriert ist.

Beim Erstellen einer virtuellen Maschine werden der virtuellen Maschine basierend auf dem von Ihnen ausgewählten Gastbetriebssystem standardmäßig eine Festplatte und ein SCSI- oder SATA-Controller hinzugefügt. Wenn diese Festplatte nicht Ihren Anforderungen entspricht, könnten Sie sie entfernen und am Ende des Erstellungsvorgangs eine vorhandene Festplatte hinzufügen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie mit den Konfigurationsoptionen und Einschränkungen beim Hinzufügen virtueller Festplatten vertraut sind. Weitere Informationen hierzu finden Sie unter Konfiguration der virtuellen Festplatte.
- Bevor Sie einer virtuellen Maschine Festplatten mit mehr als 2 TB hinzufügen, lesen Sie den Abschnitt *vSphere-Administratorhandbuch für virtuelle Maschinen*.

- Stellen Sie sicher, dass Sie das Recht **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen** für den Zielordner oder Zieldatenspeicher haben.

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte hinzufügen** und anschließend im Dropdown-Menü die Option **Neue persistente Arbeitsspeicherfestplatte** aus.

   Die Festplatte wird in der Geräteliste der virtuellen Hardware angezeigt. Die Festplatte ist standardmäßig im lokal auf dem Host vorhandenen PMem-Datenspeicher gespeichert. Sie können diesen nicht ändern.

4 (Optional) Konfigurieren Sie die Einstellungen für die neue Festplatte und klicken Sie auf **Speichern**, um den Assistenten zu schließen.

   a Erweitern Sie **Neue Festplatte**.

   b Geben Sie einen Wert für die Festplattengröße ein und wählen Sie im Dropdown-Menü die Einheiten aus.

   Hinweis Alle persistenten Arbeitsspeicherfestplatten und NVDIMM-Module, die Sie der virtuellen Maschine hinzufügen, nutzen gemeinsam die gleichen PMem-Ressourcen. Daher müssen Sie die Größe der neu hinzugefügten persistenten Arbeitsspeichergeräte entsprechend der dem Host zur Verfügung stehenden PMem-Menge anpassen. Sollte ein Teil der Konfiguration Ihre Aufmerksamkeit erfordern, macht der Assistent Sie darauf aufmerksam.

   c Wählen Sie im Dropdown-Menü **Anteile** einen Wert für die Anteile aus, die der virtuellen Festplatte zugeteilt werden sollen.

   Der Anteilswert stellt die relative Metrik zur Steuerung der Festplattenbandbreite dar. Die Werte „Niedrig“, „Normal“, „Hoch“ und „Benutzerdefiniert“ werden mit der Summe aller Anteile aller virtuellen Maschinen auf dem Host verglichen.

d Wählen Sie im Dropdown-Menü **Controller-Ort** den Speicherort des von der neuen Festplatte verwendeten Controllers aus.

e Wählen Sie einen Festplattenmodus aus.

Option	Beschreibung
Abhängig	Abhängige Festplatten sind in Snapshots enthalten.
Unabhängig – Dauerhaft	Festplatten im dauerhaften Modus verhalten sich wie herkömmliche physische Computerfestplatten. Sämtliche Daten, die im persistenten 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. Die virtuelle Festplatte wird bei jedem Neustart der virtuellen Maschine in denselben Status zurückversetzt. Änderungen an der Festplatte werden in eine Redo-Protokolldatei geschrieben und daraus gelesen. Diese Datei wird beim Ausschalten oder Zurücksetzen gelöscht.

Verwenden von Festplattenfreigaben zur Priorisierung virtueller Maschinen im VMware Host 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 die Zugriffsebene festlegen, die virtuelle Maschinen auf Ressourcen haben. 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. Sie können keine Festplatten-E/A clusterübergreifend bündeln.

Der Freigabewert stellt die relative Metrik zur Steuerung der Festplattenbandbreite für alle virtuellen Maschinen dar.

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

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.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Festplatte, um die Festplattenoptionen anzuzeigen.

4 Wählen Sie im Dropdown-Menü **Anteile** einen Wert für die Anteile aus, die der virtuellen Maschine zugewiesen werden sollen.

5 Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie im Textfeld die Anzahl der Anteile ein.

6 Geben Sie im Feld **Grenzwert – IOPs** den oberen Grenzwert für die Speicherressourcen ein, die der virtuellen Maschine zugeteilt werden sollen, oder wählen Sie **Unbegrenzt**.

7 Klicken Sie auf **Speichern**.

Konfiguration von Controllern zu virtuellen Maschinen im VMware Host Client

Im VMware Host Client können Sie virtuellen Maschinen verschiedene Controller wie USB-, SCSI-, paravirtuelle SCSI- und SATA-Controller hinzufügen. Des Weiteren können Sie die Konfiguration der gemeinsamen Verwendung des SCSI-Busses und den SCSI-Controllertyp ändern.

Hinzufügen eines USB-Controllers zu einer virtuellen Maschine im VMware Host Client

Sie können virtuellen Maschinen USB-Controller hinzufügen, um USB-Passthrough von einem ESXi-Host oder von einem Clientcomputer an eine virtuelle Maschine zu unterstützen.

In vSphere Client können Sie einen xHCI-Controller und einen EHCI+UHCI-Controller hinzufügen. Von Hardwareversion 11 bis Hardwareversion 16 werden pro xHCI-Controller acht Root-Hubports unterstützt (vier logische USB 3.1-Ports und vier logische USB 2.0-Ports). Für Hardwareversion 17 werden pro xHCI-Controller acht Root-Hubports unterstützt (vier logische USB 3.1-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 3-3. USB-Controller-Unterstützung

Controller-Typ	Unterstützte USB-Geräteversion	Unterstützt für Passthrough vom ESXi-Host zu einer VM	Unterstützt für Passthrough vom Clientcomputer zu einer VM
EHCI+UHCI	2.0 und 1.1	Ja	Ja
xHCI	3.1, 2.0 und 1.1	Ja Nur USB 3.1-, USB 2.0- und USB 1.1-Geräte	Ja Gastbetriebssystem mit Windows 8 oder höher, Windows Server 2012 und höher oder Linux mit einem 2.6.35-Kernel oder höher.

Bei Mac OS X-Systemen ist der EHCI+UHCI-Controller, der für die Verwendung von USB-Maus und -Tastatur benötigt wird, standardmäßig aktiviert.

Für virtuelle Maschinen mit Windows-oder Linux-Gastbetriebssystemen können Sie einen oder zwei Controller unterschiedlicher Typen hinzufügen. 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 USB-Geräte an diese Controller anschließen, stehen sie der virtuellen Maschine nicht zur Verfügung.

Voraussetzungen

- Stellen Sie sicher, dass die ESXi-Hosts über USB-Controller-Hardware und -Module verfügen, die USB 3.1-, USB 2.0- und USB 1.1-Geräte unterstützen.
- Stellen Sie sicher, dass die Client-Computer über USB-Controller-Hardware und -Module verfügen, die USB 3.1-, 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**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und wählen Sie anschließend **USB-Controller** aus dem Dropdown-Menü aus.

   Der neue USB-Controller wird unten in der Geräteliste der virtuellen Hardware angezeigt.
4. Erweitern Sie **Neuer USB-Controller**, um den USB-Controllertyp zu ändern.

   Wenn Kompatibilitätsfehler angezeigt werden, beheben Sie diese, bevor Sie den Controller hinzufügen.
5. Klicken Sie auf **Speichern**.

Nächste Schritte

Fügen Sie ein oder mehrere USB-Geräte zur virtuellen Maschine hinzu.

Hinzufügen von SCSI-Controllern im VMware Host Client

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 ein neuer SCSI-Controller erstellt.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte hinzufügen** und wählen Sie anschließend **Neue Festplatte** aus dem Dropdown-Menü aus.
4. Erweitern Sie die Festplatte, sodass alle Optionen angezeigt werden.
5. Wählen Sie im Abschnitt **Speicherort des Controllers** eine nicht verwendete SCSI-Bus-Nummer im Dropdown-Menü 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.
6. Klicken Sie auf **Speichern**.

Ergebnisse

Die neue Festplatte und der neue SCSI-Controller werden gleichzeitig erstellt.

Ändern der Konfiguration der gemeinsamen Verwendung des SCSI-Busses im VMware Host 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 ändern, wenn diese sich auf einem ESXi-Host befindet.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie in der Registerkarte **Virtuelle Hardware** den SCSI-Controller, den Sie bearbeiten möchten.

4 Wählen Sie den Verwendungstyp in der Liste **Gemeinsame Verwendung des SCSI-Busses** 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.

5 Klicken Sie auf **Speichern**.

Ändern des SCSI-Controller-Typs im VMware Host Client

Sie können virtuelle Festplatten und RDMs an virtuelle Maschinen anhängen, indem Sie einen virtuellen SCSI-Controller auf den virtuellen Maschinen konfigurieren.

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 haben als Standard-Controller einen BusLogic-Adapter.

Wenn Sie eine virtuelle Maschine mit LSI Logic erstellen und eine virtuelle Festplatte hinzufügen, die BusLogic-Adapter verwendet, startet die virtuelle Maschine von der Festplatte mit den BusLogic-Adaptern. 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-Adaptern betrieben werden.

Vorsicht Wenn Sie den SCSI-Controller-Typ ändern, kann dies zu einem Startfehler in einer virtuellen Maschine führen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Klicken Sie auf die Registerkarte **Virtuelle Hardware** und erweitern Sie einen SCSI-Controller.

4 Wählen Sie im Dropdown-Menü einen SCSI-Controllertyp aus.

5 Klicken Sie auf **Speichern**.

Informationen 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.

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 im VMware Host Client

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.
- Machen Sie sich mit den Einschränkungen von VMware Paravirtual SCSI vertraut. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- 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 und anschließend VMware Tools installieren.

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und wählen Sie anschließend **SCSI-Controller** aus dem Dropdown-Menü aus.

   Die neuen SCSI-Controller werden in der Hardwareliste angezeigt.

4 Klicken Sie auf **Neuer SCSI-Controller** und wählen Sie **VMware Paravirtual** aus dem Dropdown-Menü aus.

5 Klicken Sie auf **Speichern**.

Hinzufügen eines SATA-Controllers zu einer virtuellen Maschine im VMware Host Client

Wenn eine virtuelle Maschine mehrere Festplatten oder CD/DVD-ROM-Laufwerke besitzt, können Sie bis zu drei zusätzliche SATA-Controller hinzufügen, denen die Geräte zugewiesen werden sollen. Wenn Sie die Geräte mehreren Controllern zuweisen, können Sie die Leistung verbessern und eine Überlastung durch einen zu hohen Datenverkehr vermeiden. Sie können auch weitere Controller hinzufügen, wenn Sie die Begrenzung von 30 Geräten für einen einzelnen Controller überschreiten.

Sie können virtuelle Maschinen von SATA-Controllern starten und sie für virtuelle Festplatten mit hoher Kapazität verwenden.

Nicht alle Gastbetriebssysteme unterstützen AHCI-SATA-Controller. Wenn Sie typischerweise virtuelle Maschinen mit Kompatibilität zu ESXi 5.5 und höher und Mac OS X-Gastbetriebssystemen erstellen, wird standardmäßig ein SATA-Controller für die virtuellen Festplatten und CD/DVD-ROM-Laufwerke hinzugefügt. Die meisten Gastbetriebssysteme, einschließlich Windows Vista und höher, haben einen Standard-SATA-Controller für CD/DVD-ROM-Laufwerke. Informationen zur Verifizierung finden Sie im *VMware-Kompatibilitätshandbuch* auf http://www.vmware.com/resources/compatibility.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 5.5 und höher kompatibel ist.
- Stellen Sie sicher, dass Sie mit dem Verhalten und den Einschränkungen von Speicher-Controllern vertraut sind. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.
- Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und wählen Sie anschließend **SATA-Controller** aus dem Dropdown-Menü aus.

   Der SATA-Controller wird in der Hardwareliste angezeigt.

4 Klicken Sie auf **Speichern**.

Hinzufügen eines NVMe-Controllers im VMware Host Client

Wenn eine virtuelle Maschine über mehrere Festplatten verfügt, können Sie bis zu vier virtuelle NVMe-Controller hinzufügen, denen die Festplatten zugewiesen werden können. Durch die Verwendung eines NVMe-Controllers wird der Software-Overhead für die E/A-Verarbeitung des Gastbetriebssystems im Vergleich zu AHCI SATA- oder SCSI-Controllern erheblich reduziert.

Die optimale Leistung von NVMe-Controllern wird mit virtuellen Festplatten in einem All-Flash-Festplatten-Array, einer lokalen NVMe-SSD und PMem-Speicher erzielt.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine über ein Gastbetriebssystem verfügt, das NVMe unterstützt.
- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 6.5 oder höher kompatibel ist.
- Stellen Sie sicher, dass Sie mit dem Verhalten und den Einschränkungen von Speicher-Controllern vertraut sind. Weitere Informationen finden Sie im *Administratorhandbuch für virtuelle Maschinen*.
- Stellen Sie sicher, dass Sie die Berechtigung **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen** auf der virtuellen Maschine besitzen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf das Symbol **Anderes Gerät hinzufügen** und wählen Sie anschließend im Dropdown-Menü die Option **NVMe-Controller** aus.

Ergebnisse

Der virtuellen Maschine wird ein neuer NVMe-Controller hinzugefügt.

Nächste Schritte

Sie können der virtuellen Maschine eine Festplatte hinzufügen und sie dem neuen NVMe-Controller zuordnen.

Andere VM-Gerätekonfiguration im VMware Host Client

Zusätzlich zum Konfigurieren der CPU und des Arbeitsspeichers virtueller Maschinen und zum Hinzufügen von Festplatten und virtueller Netzwerkadapter können Sie virtuelle Hardware wie DVD/CD-ROM-Laufwerke, Diskettenlaufwerke und SCSI-Geräte hinzufügen und konfigurieren. Sie können auch ein virtuelles Watchdog-Timer (VWDT)-Gerät, Präzisionsuhrgerät und PCI-Geräte hinzufügen.

Hinzufügen eines CD-/DVD-Laufwerks zu einer virtuellen Maschine im VMware Host 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 möchten, das von einem USB-CD-/DVD-Laufwerk auf dem Host gestützt wird, müssen Sie das Laufwerk als SCSI-Gerät hinzufügen. Das Hinzufügen oder Entfernen von SCSI-Geräten von einem ESXi-Host im laufenden Betrieb wird nicht unterstützt.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und wählen Sie anschließend **CD-/DVD-Laufwerk** aus dem Dropdown-Menü aus.
4. Erweitern Sie **CD-/DVD-Laufwerk** und wählen Sie eine Option.

Option	Beschreibung
Physisches Laufwerk verwenden	a Wählen Sie **Clientgerät** als Speicherort aus. b Wählen Sie im Dropdown-Menü **Gerätemodus** die Option **CD-ROM emulieren** oder **Passthrough-CD-ROM** aus.
ISO-Image verwenden	a Wählen Sie **Datenspeicher-ISO-Datei** als Speicherort aus. b 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 CD-ROM-Laufwerk beim Start der virtuellen Maschine nicht verbunden werden soll, deaktivieren Sie **Beim Einschalten verbinden**.
6. Wählen Sie den Knoten des virtuellen Geräts aus, den das Laufwerk in der virtuellen Maschine verwendet.
7. Klicken Sie auf **Speichern**.

Hinzufügen eines Diskettenlaufwerks zu einer virtuellen Maschine im VMware Host 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.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und wählen Sie anschließend im Dropdown-Menü die Option **Diskettenlaufwerk** aus.

   Das Diskettenlaufwerk wird in der Hardwareliste angezeigt.
4. Erweitern Sie **Diskettenlaufwerk** und wählen Sie den gewünschten Gerätetyp aus.

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, von dem aus Sie auf den VMware Host Client zugreifen.
Vorhandenes Disketten-Image verwenden	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.

5. (Optional) Wählen Sie **Beim Einschalten verbinden**, um das Gerät zu konfigurieren, zu dem bei Einschalten der virtuellen Maschine eine Verbindung hergestellt werden soll.
6. Klicken Sie auf **Speichern**.

Hinzufügen eines USB-Geräts zu einer virtuellen Maschine im VMware Host Client

Mithilfe des VMware Host Client können Sie einer virtuellen Maschine ein USB-Gerät hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass ein USB-Controller vorhanden ist. Weitere Informationen finden Sie unter Hinzufügen eines USB-Controllers zu einer virtuellen Maschine im VMware Host Client.
- Fügen Sie dem ESXi-Host, auf dem sich die virtuelle Maschine befindet, ein physisches USB-Gerät hinzu, indem Sie das USB-Gerät am Host anschließen.

Hinweis Wenn für den ESXi-Host keine USB-Geräte verfügbar sind, können Sie der virtuellen Maschine kein USB-Gerät hinzufügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine in der Liste und wählen Sie im Dropdown-Menü **Einstellungen bearbeiten** aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und anschließend im Dropdown-Menü die Option **USB-Gerät** aus.

   Das USB-Gerät wird in der Hardwareliste der verfügbaren Hardwaregeräte für die virtuelle Maschine angezeigt.
4. Wählen Sie im Dropdown-Menü **USB-Gerät** das USB-Gerät aus, das der virtuellen Maschine hinzugefügt werden soll.
5. Klicken Sie auf **Speichern**.

Hinzufügen eines Sound Controllers zu einer virtuellen Maschine im VMware Host Client

Mithilfe des VMware Host Client können Sie einer virtuellen Maschine einen Sound Controller hinzufügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und dann im Dropdown-Menü die Option **Sound Controller** aus.

   Der Sound Controller wird in der Liste der verfügbaren Hardwaregeräte für die virtuelle Maschine angezeigt.
4. Wählen Sie im Dropdown-Menü **Soundkarte** den Sound Controller aus, mit dem eine Verbindung zur virtuellen Maschine hergestellt werden soll.
5. Klicken Sie auf **Speichern**.

Konfiguration der parallelen und seriellen Schnittstellen im VMware Host Client

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 virtuelle 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.

Hinzufügen einer seriellen Schnittstelle zu einer virtuellen Maschine in VMware Host 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 Virtual Serial Port Concentrator (vSPC) URI einen seriellen Port über das Netzwerk anschließen.

Voraussetzungen

- Machen Sie sich mit den verschiedenen Medientypen, auf die der Port zugreifen kann, den vSPC-Verbindungen und anderen möglichen Bedingungen vertraut. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Fügen Sie zum Anschließen einer seriellen Schnittstelle über ein Netzwerk einen Firewall-Regelsatz hinzu. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erforderliche Berechtigung: **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen**

  Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und anschließend **Serieller Port**.

   Der serielle Port wird in der Hardwareliste angezeigt.

4 Erweitern Sie den seriellen Port in der Hardwareliste und wählen Sie den Medienporttyp aus, auf den zugegriffen werden soll.

Option	Beschreibung
Ausgabedatei verwenden	Navigieren Sie zum Speicherort der Datei auf dem Host, den Sie zum Speichern der Ausgabe des virtuellen seriellen Ports verwenden möchten.
Physischen seriellen Port verwenden	Wählen Sie im Dropdown-Menü eine Schnittstelle aus.
Named Pipe verwenden	a Geben Sie im 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.
Netzwerk verwenden	a Wählen Sie im Dropdown-Menü **Richtung** die Option **Server** oder **Client** aus. b Geben Sie die Port-URI ein. Der URI ist das Remoteende der seriellen Ports, zu der der serielle Port der virtuellen Maschine eine Verbindung herstellen soll. c 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) Deaktivieren Sie die Option **Beim Einschalten verbinden**, wenn das Gerät mit der parallelen Schnittstelle beim Einschalten der virtuellen Maschine nicht verbunden werden soll.

6 Klicken Sie auf **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 VMware Host Client

Über den parallelen Port können Sie Peripheriegeräte mit virtuellen Maschinen verbinden, z. B. Drucker oder Scanner. Sie senden die Ausgabe solcher Geräte an eine Datei auf dem Hostcomputer.

Hinweis Um einer virtuellen Maschine, die auf einem ESXi 4.1- oder früheren Host ausgeführt wird, einen parallelen Port hinzuzufügen, können Sie die Ausgabe auch an einen physischen parallelen Port auf dem Host senden. Diese Option ist mit ESXi 5.0 und höheren Hostversionen nicht verfügbar.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und anschließend **Paralleler Port**.

   Der parallele Port wird in der Hardwareliste angezeigt.
4. Erweitern Sie den parallelen Port und navigieren Sie im Feld „Verbindung“ zu einem Ordner, in dem die Datei erstellt werden soll.

   Der Dateipfad wird im Textfeld **Verbindung** angezeigt.
5. (Optional) Wählen Sie **Beim Einschalten verbinden**, um das Gerät zu konfigurieren, zu dem bei Einschalten der virtuellen Maschine eine Verbindung hergestellt werden soll.
6. Klicken Sie auf **Speichern**.

Verwenden eines virtuellen Watchdog-Timers

Sie können ein virtuelles Watchdog-Timer-Gerät (VWDT) hinzufügen, um bei der Systemleistung innerhalb einer virtuellen Maschine Eigenständigkeit sicherzustellen. Wenn das Gastbetriebssystem nicht mehr reagiert und aufgrund von Softwarefehlern nicht selbst eine Wiederherstellung durchführen kann, wartet der VWDT einen vordefinierten Zeitraum ab und startet dann das System neu.

Sie können den VWDT so aktivieren, dass er entweder vom Gastbetriebssystem oder von der BIOS- oder EFI-Firmware gestartet werden kann. Wenn Sie festlegen, dass der VWDT von der BIOS- oder EFI-Firmware gestartet wird, wird er vor dem Hochfahren des Gastbetriebssystems gestartet.

Der VWDT spielt eine wichtige Rolle bei gastbasierten Clusterlösungen, bei denen jede virtuelle Maschine im Cluster bei einem Ausfall eigenständig wiederhergestellt werden kann.

Hinzufügen eines virtuellen Watchdog Timer-Geräts zu einer virtuellen Maschine im VMware Host Client

Sie können einer virtuellen Maschine ein virtuelles Watchdog-Timer-Gerät hinzufügen, um zu verhindern, dass die virtuelle Maschine über einen längeren Zeitraum einen Ausfall des Gastbetriebssystems erleidet.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Vergewissern Sie sich, dass Sie über die Berechtigung**Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.
- Stellen Sie sicher, dass das Gastbetriebssystem der virtuellen Maschine das VWDT-Gerät unterstützt.
- Stellen Sie sicher, dass die Version der virtuellen Hardware 17 ist.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Anderes Gerät hinzufügen** und anschließend **Watchdog-Timer**.

   Das Watchdog-Timer-Gerät wird in der Hardwareliste angezeigt.
4. (Optional) Wählen Sie **Mit BIOS-/EFI-Start starten**, um den Watchdog-Timer durch das BIOS oder die EFI-Firmware zu starten.

   Wenn Sie diese Option auswählen, wird das VWDT-Gerät vor dem Gastbetriebssystem gestartet. Wenn der Start des Gastbetriebssystems zu lange dauert oder den Watchdog-Timer nicht unterstützt, wird die virtuelle Maschine möglicherweise ständig neu gestartet.
5. Klicken Sie auf **Speichern**.

Hinzufügen eines Präzisionsuhrgeräts zu einer virtuellen Maschine im VMware Host Client

Eine Präzisionsuhr ist ein virtuelles Gerät, das auf einer virtuellen Maschine ausgeführt wird und auf die Systemzeit eines Hosts zugreift. Durch das Hinzufügen einer Präzisionsuhr zu einer virtuellen Maschine stellen Sie die Uhrzeitsynchronisierung und eine hochpräzise Zeitstempelung sicher.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.

- Stellen Sie sicher, dass die Version der virtuellen Hardware 17 ist.
- Vergewissern Sie sich, dass Sie über die Berechtigung**Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern** auf der virtuellen Maschine verfügen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf **Anderes Gerät hinzufügen** und wählen Sie **Präzisionsuhr** aus.

   Das Präzisionsuhrgeräts wird in der Hardwareliste angezeigt.

4 (Optional) Wählen Sie das Uhrzeitsynchronisierungsprotokoll aus.

5 Klicken Sie auf **Speichern**.

Hinzufügen eines PCI-Geräts zu einer virtuellen Maschine im VMware Host Client

DirectPath I/O ermöglicht einem Gastbetriebssystem einer virtuellen Maschine den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind. Mithilfe dieser Technologie können Sie jede virtuelle Maschine mit bis zu sechzehn physischen PCI-Geräten verbinden. Sie können Dynamic DirectPath I/O verwenden, um einer virtuellen Maschine mehrere PCI-Passthrough-Geräte zuzuweisen. Ab vSphere 7.0 können Sie die PCI-Passthrough-Geräte nach Hersteller und Modellname identifizieren.

Hinweis Einige VM-Vorgänge sind nicht mehr verfügbar, wenn Sie ein PCI- oder PCIe-Passthrough-Gerät zur virtuellen Maschine hinzufügen.

Weitere Informationen zur Konfiguration der Hardwarebezeichnung finden Sie unter Ändern der Hardwarebezeichnung im VMware Host Client.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Vergewissern Sie sich, dass Sie über die Berechtigung**Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen** auf der virtuellen Maschine verfügen.
- Stellen Sie sicher, dass die PCI-Geräte mit dem Host verbunden und als „für Passthrough verfügbar“ gekennzeichnet sind.
- Wenn Sie einer virtuellen Maschine ein dynamisches PCI-Gerät hinzufügen möchten, stellen Sie sicher, dass es sich bei der Version der virtuellen Hardware um Version 17 handelt.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf **Anderes Gerät hinzufügen** und wählen Sie ein Gerät aus.

Option	Aktion
PCI-Gerät	a Klicken Sie auf **PCI-Gerät**. Ein neues Gerät wird in der Hardwareliste angezeigt. b Wählen Sie im Dropdown-Menü ein PCI-Gerät aus, das mit der virtuellen Maschine verbunden werden soll.
Dynamisches PCI-Gerät	a Klicken Sie auf **Dynamisches PCI-Gerät**. Ein neues Gerät wird in der Hardwareliste angezeigt. b Erweitern Sie **Neues PCI-Gerät** und wählen Sie im Dropdown-Menü die PCI-Passthrough-Geräte aus, die mit der virtuellen Maschine verbunden werden sollen. Sie können PCI-Passthrough-Geräte nach Hersteller, Modellname und Hardwarebezeichnung identifizieren. Hardwarebezeichnungen werden, sofern verfügbar, in Klammern angezeigt. **Hinweis** Wenn Sie einer virtuellen Maschine ein PCI-Gerät hinzufügen, wird die volle Speichergröße der virtuellen Maschine automatisch reserviert.

4 Klicken Sie auf **Speichern**.

Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen

Mithilfe von vSphere Client können Sie vSGX (Virtual Intel® Software Guard Extensions) für virtuelle Maschinen konfigurieren und zusätzliche Sicherheit für Ihre Arbeitslasten bereitstellen.

Einige moderne Intel-CPUs implementieren eine Sicherheitserweiterung namens Intel® Software Guard Extensions (Intel SGX). Intel SGX ist eine prozessorspezifische Technologie zur Definition privater Speicherbereiche, die als Enclaves bezeichnet werden. Intel SGX schützt die Inhalte einer Enclave vor Offenlegung und Änderung, sodass außerhalb der Enclave ausgeführter Code nicht auf die Inhalte zugreifen kann.

vSGX ermöglicht virtuellen Maschinen die Verwendung der Intel SGX-Technologie, sofern diese auf der Hardware verfügbar ist. Um vSGX zu verwenden, muss der ESXi-Host auf einer SGX-fähigen CPU installiert sein, und SGX muss im BIOS des ESXi-Hosts aktiviert sein. Sie können den vSphere Client verwenden, um SGX für eine virtuelle Maschine zu aktivieren.

Aktivieren von vSGX auf einer virtuellen Maschine im VMware Host Client

Um den Enclave-Inhalt vor Offenlegung und Änderungen zu schützen, können Sie vSGX auf einer virtuellen Maschine auf dem VMware Host Client aktivieren.

Einige Vorgänge und Funktionen sind nicht mit SGX kompatibel.

- Migration mit Storage vMotion
- Anhalten oder Fortsetzen der virtuellen Maschine
- Erstellen eines Snapshots der virtuellen Maschine
- Fault Tolerance
- Aktivieren von Gastintegrität (GI, Plattform für VMware AppDefense 1.0).

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Stellen Sie sicher, dass die virtuelle Maschine EFI-Firmware verwendet.
- Stellen Sie sicher, dass der ESXi-Host Version 7.0 oder höher aufweist.
- Stellen Sie sicher, dass es sich bei dem Gastbetriebssystem auf der virtuellen Maschine um Linux, Windows 10 (64 Bit) oder höher oder Windows Server 2016 (64 Bit) und höher handelt.
- Vergewissern Sie sich, dass Sie über die Berechtigung **Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern** auf der virtuellen Maschine verfügen.
- Stellen Sie sicher, dass der ESXi-Host auf einer SGX-fähigen CPU installiert ist und SGX im BIOS des ESXi-Hosts aktiviert ist. Informationen zu den unterstützten CPUs finden Sie unter https://kb.vmware.com/s/article/71367.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Sicherheitsgeräte**.
4. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
5. Geben Sie unter **Cachegröße der Enclave-Seite** einen neuen Wert in das Textfeld ein und wählen Sie im Dropdown-Menü die Größe in MB oder GB aus.

   Hinweis Die Cachegröße der Enclave-Seite muss ein Vielfaches von 2 sein.

6 Wählen Sie im Dropdown-Menü **Steuerungskonfiguration starten** den entsprechenden Modus aus.

Option	Aktion
Gesperrt	Aktiviert die Konfiguration für Start-Enclave. Geben Sie unter **Public-Key-Hash für Start-Enclave** einen gültigen SHA256-Hash ein. Der SHA256-Hashschlüssel muss 64 Zeichen enthalten.
Entsperrt	Aktiviert die Konfiguration für Start-Enclave des Gastbetriebssystems.

7 Klicken Sie auf **Speichern**.

Deaktivieren von vSGX auf einer virtuellen Maschine im VMware Host Client

Zum Deaktivieren von vSGX auf einer virtuellen Maschine können Sie den VMware Host Client verwenden.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Sicherheitsgeräte**.

4 Deaktivieren Sie das Kontrollkästchen **Aktivieren** und klicken Sie auf **Speichern**.

Ergebnisse

vSGX ist auf der virtuellen Maschine deaktiviert.

Verwalten von virtuellen Maschinen im VMware Host Client

Nachdem Sie eine virtuelle Maschine im VMware Host Client erstellt haben, können Sie daran verschiedene Verwaltungsaufgaben wie Löschen der VM vom Host, Entfernen aus dem und erneutes Registrieren im Datenspeicher uvm. durchführen. Sie können die virtuelle Maschine auch zurück auf den Host verschieben.

Zugreifen auf eine virtuelle Maschine im VMware Host Client

Sie können auf die virtuellen Maschinen auf dem Host, bei dem Sie angemeldet sind, zugreifen, um deren Hardware und Optionen zu konfigurieren und administrative und einfache Fehlerbehebungsaufgaben durchzuführen.

Schalten Sie die virtuelle Maschine, die in der VMware Host Client-Bestandsliste angezeigt werden soll, ein.

Verfahren

- Für den Zugriff auf die virtuellen Maschinen auf dem Host, bei dem Sie angemeldet sind, klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

Ergebnisse

Die Liste der verfügbaren virtuellen Maschinen wird unter **Virtuelle Maschinen** angezeigt.

Sie können nun die Einstellungen der virtuellen Maschinen in der Liste bearbeiten und verschiedene administrative und Fehlerbehebungsaufgaben daran durchführen.

Betriebszustände einer virtuellen Maschine im VMware Host Client

Zu den grundlegenden Betriebsvorgängen einer virtuellen Maschine gehören das Einschalten, Ausschalten, Anhalten und Zurücksetzen.

Informationen zum Ändern des Betriebsstatus einer virtuellen Maschine finden Sie unter Konfigurieren der Betriebszustände der virtuellen Maschine im VMware Host Client.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über das Recht **VirtualMachine.Interaction.PowerOn** verfügen.
- Vergewissern Sie sich, dass Sie über das Recht **VirtualMachine.Interaction.PowerOff** verfügen.
- Vergewissern Sie sich, dass Sie über das Recht **VirtualMachine.Interaction.Suspend** verfügen.
- Vergewissern Sie sich, dass Sie über das Recht **VirtualMachine.Interaction.Reset** verfügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie einen Vorgang zum Ändern des Betriebszustands aus.

Option	Beschreibung
Einschalten ( )	Schaltet eine virtuelle Maschine ein, wenn sie angehalten wurde.
Ausschalten ( )	Schaltet eine virtuelle Maschine aus und fährt das Gastbetriebssystem herunter. Das Ausschalten einer virtuellen Maschine kann zu Datenverlusten führen.

Option	Beschreibung
Anhalten ( )	Hält eine ausgeführte virtuelle Maschine an und behält die Verbindung zum Netzwerk bei. Wenn Sie eine angehaltene virtuelle Maschine fortsetzen, wird der Betrieb der virtuellen Maschine an genau dem Punkt fortgesetzt, an dem sie angehalten wurde.
Zurücksetzen ( )	Das Gastbetriebssystem wird heruntergefahren und neu gestartet, ohne dass die virtuelle Maschine ausgeschaltet wird.

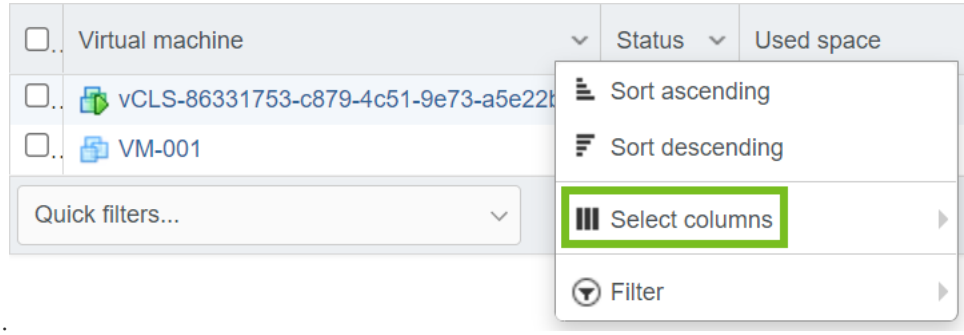
Verwenden der Spaltenkonfiguration von Controllern für virtuelle Maschinen im VMware Host Client

Über den Bereich „Virtuelle Maschinen“ im VMware Host Client können Sie die anzuzeigenden Informationen konfigurieren. Sie können verschiedene Spalten anzeigen oder ausblenden, wie z. B. Status, Verwendeter Speicherplatz, Hostname, Host-CPU usw.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie in der Liste der virtuellen Maschinen auf den nach unten weisenden Pfeil neben einem beliebigen Spaltentitel und wählen Sie **Spalten auswählen**



aus.

Die Liste mit allen verfügbaren Spalten wird angezeigt.

3 Wählen Sie die Informationen aus, die im Bereich „Virtuelle Maschinen“ angezeigt werden sollen.

Entfernen von virtuellen Maschinen von einem Host im VMware Host Client

Sie können die Registrierung einer virtuellen Maschine aufheben, wenn sie im Datenspeicher verbleiben, jedoch nicht mehr in der VMware Host Client-Bestandsliste angezeigt werden soll.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Bestandsliste und wählen Sie **Registrierung aufheben**.

3 Klicken Sie auf **Ja**, um zu bestätigen, dass die virtuelle Maschine aus der Bestandsliste entfernt werden soll.

Ergebnisse

Der Host entfernt die virtuelle Maschine aus der Bestandsliste und verfolgt ihren Status nicht mehr.

Entfernen von virtuellen Maschinen aus einem Datenspeicher im VMware Host Client

Zum Freigeben von Speicherplatz auf dem Datenspeicher können Sie die nicht mehr benötigten virtuellen Maschinen entfernen. Durch Entfernen einer virtuellen Maschine aus der VMware Host Client-Bestandsliste werden alle VM-Dateien aus dem Datenspeicher gelöscht, einschließlich der Konfigurationsdatei und der virtuellen Festplattendateien. Sie können mehrere virtuelle Maschinen löschen.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Vergewissern Sie sich, dass die virtuelle Maschine die Festplatte nicht zusammen mit einer anderen virtuellen Maschine verwendet. Wenn zwei virtuelle Maschinen dieselbe Festplatte gemeinsam verwenden, werden die Festplattendateien nicht entfernt.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Aktivieren Sie ein oder mehrere Kontrollkästchen neben den zu entfernenden virtuellen Maschinen und wählen Sie **Aktionen > Löschen** aus.

   Das Dialogfeld **VMs löschen** wird geöffnet.

3 Klicken Sie auf **Löschen**.

Registrieren einer virtuellen Maschine im VMware Host Client

Wenn Sie eine virtuelle Maschine oder eine Vorlage von einem Host, aber nicht aus dem Datenspeicher des Hosts entfernen, können Sie sie erneut in der Bestandsliste des Hosts wiederherstellen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher**.

2 Klicken Sie mit der rechten Maustaste auf einen Datenspeicher in der Liste und wählen Sie **VM registrieren**.

3 Wählen Sie die zu registrierende virtuelle Maschine aus der Liste aus und klicken Sie auf **Registrieren**.

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. Die virtuelle Maschine wird von der Erstellung eines Snapshots nicht betroffen. Es wird lediglich ein Bild der virtuellen Maschine in einem bestimmten Zustand kopiert und gespeichert. 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 durchzuführen. Snapshots werden immer für eine einzelne virtuelle Maschine erstellt. Um Snapshots von mehreren virtuelle 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 Shapshot 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 Änderungen an einer virtuellen Maschine in der Snapshot-Struktur vornehmen.

Im Snapshot-Manager im VMware Host Clientstehen mehrere Vorgänge zum Erstellen und Verwalten von Snapshots und Snapshot-Strukturen für virtuelle Maschinen zur Verfügung. Mit diesen Vorgängen können Sie Snapshots erstellen, alle Snapshots in der Snapshot-Hierarchie wiederherstellen, Snapshots löschen usw. Darüber hinaus können Sie den Zustand einer 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 Snapshots in der Hierarchie sind übergeordnet und untergeordnet angelegt. 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 einer virtuellen Maschine, der nach dem übergeordneten Snapshot erstellt wurde. 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.

Snapshot-Dateien

Wenn Sie einen Snapshot erstellen, erfassen Sie den Status der VM-Einstellungen und den Status der virtuellen Festplatte. Wenn Sie einen Speicher-Snapshot erstellen, erfassen Sie ebenfalls den Speicherstatus der virtuellen Maschine. Diese Statusangaben werden in Dateien gespeichert, die sich in Verzeichnissen befinden, in denen auch die Basisdateien der virtuellen Maschine gespeichert sind.

Snapshot-Dateien

Ein Snapshot besteht aus Dateien, die auf einem unterstützten Speichergerät abgelegt werden. Beim Erstellen eins Snapshots werden die Dateien `.vmdk`, `-delta.vmdk`, `.vmsd` und `.vmsn` erstellt. Standardmäßig werden die erste und alle Delta-Festplatten mit der `.vmdk`-Basisdatei gespeichert. Die Dateien der Typen `.vmsd` und `.vmsn` werden im Verzeichnis der virtuellen Maschine gespeichert.

Delta-Festplattendateien

Eine `.vmdk`-Datei, in die das Gastbetriebssystem schreiben kann. 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. Beim Erstellen eines Snapshots wird der Status der virtuellen Festplatte beibehalten, wodurch sie vom Gastbetriebssystem nicht mehr beschrieben werden kann, und eine Delta- oder untergeordnete Festplatte wird erstellt.

Eine Delta-Festplatte verfügt über zwei Dateien. Eine ist eine kleine Deskriptordatei, die Informationen über die virtuelle Festplatte enthält, wie z. B. Informationen zur Geometrie und zu Beziehungen zwischen untergeordneten und übergeordneten Elementen. Die zweite Instanz ist eine entsprechende Datei, die Raw-Daten enthält.

Die Dateien, die die Delta-Festplatte bilden, werden als untergeordnete Festplatten oder Redo-Protokolle bezeichnet.

Flache Datei

Eine `-flat.vmdk`-Datei, bei der es sich um eine der beiden Dateien der Basisfestplatte handelt. Die Festplatte im Flat-Format enthält Raw-Daten für die Basisfestplatte. Diese Datei wird nicht als separate Datei im Datenspeicherbrowser angezeigt.

Datenbankdatei

Eine `.vmsd`-Datei, die die Snapshot-Informationen der virtuellen Maschine enthält und die primäre Quelle der Informationen für den Snapshot-Manager ist. Diese Datei enthält Zeileneinträge, die die Beziehungen zwischen Snapshots und den untergeordneten Festplatten für jeden einzelnen Snapshot festlegen.

Speicherdatei

Eine `.vmsn`-Datei, die den aktiven Status der virtuellen Maschine beinhaltet. Wenn Sie den Speicherstatus der virtuellen Maschine erfassen, können Sie in den Zustand wechseln, dass die virtuelle Maschine eingeschaltet ist. Bei Snapshots ohne Speicherfunktion können Sie nur in den Zustand der ausgeschalteten virtuellen Maschine wechseln. Das Erstellen von Speicher-Snapshots nimmt im Vergleich zum Speichern von Snapshots ohne Speicherfunktion mehr Zeit in Anspruch. Die Zeit, die der ESXi-Host benötigt, um den Arbeitsspeicher auf die Festplatte zu schreiben, richtet sich nach der auf der virtuellen Maschine konfigurierten Arbeitsspeichermenge.

Ein **Snapshot erstellen**-Vorgang erstellt die Dateien `.vmdk`, `-delta.vmdk`, `vmsd` und `vmsn`.

Datei	Beschreibung
vmname`-`*number*`.vmdk` und *vmname*`-`*number*`-delta.vmdk`	Snapshot-Datei, die den Unterschied zwischen dem aktuellen Status der virtuellen Festplatte und dem Status darstellt, der zum Zeitpunkt der vorherigen Snapshot-Erstellung vorlag. Der Dateiname verwendet die folgende Syntax: `S1vm-000001.vmdk`, wobei `S1vm` der Name der virtuellen Maschine ist und die sechsstellige Nummer `000001` auf den Dateien basiert, die im Verzeichnis bereits vorhanden sind. Die Nummer gibt nicht die Anzahl der Festplatten an, die mit der virtuellen Maschine verbunden sind.
vmname`.vmsd`	Datenbank der Snapshot-Informationen für die virtuelle Maschine und die primäre Informationsquelle für den Snapshot-Manager.
vmname`.Snapshot`*number*`.vmsn`	Speicherstatus der virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung. Der Dateiname weist die folgende Syntax auf: `S1vm.snapshot1.vmsn`, wobei `S1vm` der Name der virtuellen Maschine und `snapshot1` der erste Snapshot ist. **Hinweis** Eine `.vmsn`-Datei wird jedes Mal angelegt, wenn ein Snapshot erstellt wird. Die Speicherauswahl ist dabei unerheblich. Eine `.vmsn`-Datei ohne Speicher ist wesentlich kleiner als eine mit Speicher.

Snapshot-Einschränkungen

Snapshots können sich auf die VM-Leistung auswirken und bieten keine Unterstützung für bestimmte Festplattentypen oder virtuelle Maschinen, die mit gemeinsamer Busverwendung konfiguriert sind. Snapshots sind nützlich als kurzfristige Lösungen für Momentaufnahmen des Status virtueller Maschinen, eignen sich jedoch nicht als langfristige Sicherung von virtuelle Maschinen.

- VMware unterstützt keine Snapshots von Raw-Festplatten, RDM-Festplatten im physischen Modus oder Gastbetriebssystemen, die einen iSCSI-Initiator verwenden.
- Virtuelle Maschinen mit unabhängigen Festplatten müssen vor dem Erstellen eines Snapshots ausgeschaltet werden.
- Stillgelegte Snapshots erfordern die Installation von VMware Tools und Unterstützung für Gastbetriebssysteme.
- Snapshots mit PCI vSphere DirectPath I/O-Geräten werden nicht unterstützt.
- VMware unterstützt keine Snapshots von virtuelle Maschinen, die für die gemeinsame Bus-Nutzung konfiguriert sind. Wenn Sie die gemeinsame Bus-Nutzung benötigen, sollten Sie als Alternativlösung in Betracht ziehen, Sicherungssoftware innerhalb des Gastbetriebssystems auszuführen. Wenn Ihre virtuelle Maschine zurzeit über Snapshots verfügt, die Sie daran hindern, die gemeinsame Bus-Nutzung zu konfigurieren, löschen (konsolidieren) Sie die Snapshots.
- Mit Snapshots wird eine „Momentaufnahme“ der Festplatte erstellt, die von Sicherungslösungen verwendet werden kann, sie stellen jedoch keine robuste Methode zur Sicherung und Wiederherstellung dar. Die Dateien mit einer virtuellen Maschine sowie deren Snapshot-Dateien gehen verloren. Zudem sind zahlreiche Snapshots schwer zu verwalten. Sie beanspruchen große Mengen an Festplattenspeicher und sind bei einem Hardwareausfall nicht geschützt.
- Snapshots können sich negativ auf die Leistung einer virtuellen Maschine auswirken. Diese Leistungsbeeinträchtigung basiert darauf, wie lange der Snapshot oder die Snapshot-Struktur beibehalten wird, welche Tiefe die Struktur aufweist und welche Änderungen an der virtuellen Maschine und ihrem Gastbetriebssystem seit dem Erstellen des Snapshots stattgefunden haben. Weiterhin kann es beim Einschalten der virtuellen Maschine zu Verzögerungen kommen. Führen Sie virtuelle Maschinen des Produktionssystems nicht dauerhaft über Snapshots aus.
- Wenn eine virtuelle Maschine virtuelle Festplatten mit mehr als 2 TB aufweist, kann die Ausführung von Snapshot-Vorgängen wesentlich länger dauern.

Erstellen von Snapshots einer virtuellen Maschine

Sie können einen oder mehrere Snapshots einer virtuellen Maschine erstellen, um den Einstellungs-, Festplatten- und Speicherstatus zu bestimmten 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 zur 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 `Quiesce` 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.

Anfertigen eines Snapshots im VMware Host 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 einen Snapshot von einer inaktiven virtuellen Maschine anfertigen möchten, warten Sie damit, bis dieser Vorgang abgeschlossen ist.

Wenn Sie einen Speicher-Snapshot erstellen, erfasst der Snapshot den Speicherstatus und die Energieeinstellungen der virtuellen Maschine. Die Fertigstellung von Snapshots, mit denen der Arbeitsspeicherstatus einer virtuellen Maschine erfasst wird, nimmt mehr Zeit in Anspruch. 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.

Die Außerbetriebnahme mit Anwendungskonsistenz wird für virtuelle Maschinen mit IDE- oder SATA-Festplatten nicht unterstützt.

Hinweis Wenn Sie von einer dynamischen Festplatte (Microsoft-spezifischer Festplattentyp) einen Snapshot erstellen, behält die Snapshot-Technologie zwar den stillgelegten Status des Dateisystems, jedoch nicht den stillgelegten Status der Anwendung bei.

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.
- Stellen Sie sicher, dass Sie die Berechtigung **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen** auf der virtuellen Maschine besitzen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Snapshots > Snapshot erstellen** aus.
3. Geben Sie einen Namen für den Snapshot ein.
4. (Optional) Geben Sie eine Beschreibung für den Snapshot ein.

5 (Optional) Aktivieren Sie das Kontrollkästchen **Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen**, wenn Sie den Arbeitsspeicher der virtuellen Maschine mit einbeziehen möchten.

6 (Optional) Heben Sie die Auswahl von **Snapshot des Arbeitsspeichers der virtuellen Maschine erstellen** auf und aktivieren Sie das Kontrollkästchen **Gast-Dateisystem stilllegen (VMware Tools müssen installiert sein)**, um laufende Prozesse auf dem Gastbetriebssystem anzuhalten, damit sich der Inhalt des Dateisystems in einem bekannten, konsistenten Zustand befindet, wenn Sie den Snapshot erstellen.

   Legen Sie die Dateien der virtuellen Maschine nur still, wenn die virtuelle Maschine eingeschaltet ist und Sie den Speicher der virtuellen Maschine nicht erfassen möchten.

7 Klicken Sie auf **Snapshot erstellen**.

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.

Sie können Snapshots folgendermaßen 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 3-4. 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 des letzten Snapshots im VMware Host Client

Stellen Sie einen Snapshot wieder her, um den Status der virtuellen Maschine wiederherzustellen, der dem Snapshot entspricht.

Voraussetzungen

Vergewissern Sie sich, dass Sie über die Berechtigungen **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot wiederherstellen** auf der virtuellen Maschine verfügen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine in der Liste und wählen Sie **Snapshots > Snapshot wiederherstellen** aus.

   Hinweis Der aktuelle Status der virtuellen Maschine geht verloren, wenn er nicht in einem Snapshot gespeichert wurde.
3. Klicken Sie auf **Wiederherstellen**, um die virtuelle Maschine auf den aktuellen Snapshot zurückzusetzen.

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.

Durch Löschen eines Snapshots werden weder die virtuelle Maschine noch andere Snapshots verändert. 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.

Zum Löschen eines Snapshots müssen zahlreiche Informationen gelesen und auf eine Festplatte geschrieben werden. Dieser Vorgang kann die Leistung der virtuellen Maschine beeinträchtigen, bis die Konsolidierung 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.

Wenn die Festplatte nicht konsolidiert wird, kann sich dies negativ auf die Leistung virtueller Maschinen auswirken. Sie können überprüfen, ob es virtuelle Maschinen gibt, die einer separaten Konsolidierung bedürfen, indem Sie eine Liste anzeigen. Weitere Informationen zum Feststellen und Anzeigen des Konsolidierungsstatus von mehreren virtuellen Maschinen und zum Ausführen eines separaten Konsolidierungsvorgangs finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Löschen

Verwenden Sie die Option **Löschen**, um einen einzelnen übergeordneten oder untergeordneten Snapshot aus der Snapshot-Struktur zu entfernen. Mit **Löschen** werden Änderungen auf der Festplatte, die zwischen dem Status des Snapshots und dem vorherigen Festplattenstatus auftreten, in den untergeordneten Snapshot geschrieben.

Hinweis Beim Löschen eines einzelnen Snapshots wird der aktuelle Status der virtuellen Maschine beibehalten, ohne Auswirkung auf andere Snapshots.

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. Mit **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 **Wiederherstellen**, 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 VMware Host Client

Sie können den Snapshot-Manager zum Löschen eines einzigen Snapshots oder aller Snapshots in der Snapshot-Struktur verwenden.

Achten Sie darauf, keine Snapshots zu löschen, die Sie benötigen. Sie können ein gelöschtes 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 so genannte 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.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie in der Liste mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Snapshots > Snapshots verwalten** aus.
3. Wählen Sie den Snapshot aus, den Sie löschen möchten, und klicken Sie auf **Snapshot löschen**.
4. (Optional) Aktivieren Sie im Dialogfeld **Snapshot löschen** das Kontrollkästchen **Alle untergeordneten Snapshots entfernen**, um den ausgewählten Snapshot sowie alle untergeordneten Snapshots zu löschen.
5. Klicken Sie auf **Entfernen**, um die Löschung zu bestätigen.
6. Klicken Sie auf **Schließen**, um den Snapshot-Manager zu schließen.

Verwalten von Snapshots mit dem VMware Host Client

Sie können alle Snapshots Ihrer virtuellen Maschinen überprüfen und sie mithilfe des Snapshot-Managers verwalten.

Nach dem Anfertigen eines Snapshots können Sie mit der rechten Maustaste auf eine virtuelle Maschine klicken und diese durch Klicken auf **Snapshot wiederherstellen** jederzeit in den Zustand zurückversetzen, in dem sie sich zum Zeitpunkt des Snapshots befand.

Bei mehreren Snapshots können Sie mithilfe des Snapshot-Managers einen beliebigen übergeordneten oder untergeordneten Snapshot wiederherstellen. Für alle nachfolgenden untergeordneten Snapshots, die Sie aus dem wiederhergestellten Snapshot erstellen, wird eine untergeordnete Struktur in der Snapshot-Struktur angelegt. Außerdem können Sie mit dem Snapshot-Manager Snapshots aus der Struktur löschen.

Tabelle 3-5. Snapshot-Manager

Option	Beschreibung
Snapshot-Struktur	Zeigt alle Snapshots für die virtuelle Maschine an.
Symbol **Sie befinden sich hier**	Das Symbol **Sie befinden sich hier** stellt den aktuellen und aktiven Status der virtuellen Maschine dar. Die Optionen **Wiederherstellen**, **Löschen** und **Bearbeiten** sind für den Status **Sie befinden sich hier** deaktiviert.
Übernehmen, **Wiederherstellen**, **Löschen**, **Bearbeiten**	Snapshot-Optionen.
Details	Zeigt den Namen und die Beschreibung des Snapshots und dessen Erstellungsdatum an. Die Konsole zeigt den Betriebszustand der virtuellen Maschine, wenn ein Snapshot erstellt wurde. Die Textfelder „Name“, „Beschreibung“ und „Erstellt“ sind leer, wenn Sie keinen Snapshot auswählen.

Überwachen einer virtuellen Maschine im VMware Host Client

Sie können verschiedene Leistungsaspekte überwachen und Aktionen verfolgen, die auf im VMware Host Client erstellten virtuellen Maschinen durchgeführt werden.

Anzeigen von Leistungsdiagrammen zu virtuellen Maschinen im VMware Host Client

Sie können Liniendiagramme mit Informationen zur Ressourcennutzung virtueller Maschinen anzeigen, die Sie im VMware Host Client erstellen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Wählen Sie eine virtuelle Maschine aus der Liste aus.
3. Erweitern Sie die virtuelle Maschine in der VMware Host Client-Bestandsliste und klicken Sie auf **Überwachen**.
4. Klicken Sie auf **Leistung**.

5 Wählen Sie zur Anzeige der Ressourcennutzung der virtuellen Maschine in der vergangenen Stunde eine Option aus dem Dropdown-Menü aus.

- Zur Anzeige der CPU-Auslastung der virtuellen Maschine in der vergangenen Stunde wählen Sie **CPU-Nutzung**.
- Zur Anzeige der Arbeitsspeichernutzung des Hosts in der vergangenen Stunde wählen Sie **Arbeitsspeichernutzung**.

Anzeigen von Ereignissen in virtuellen Maschinen im VMware Host Client

Ereignisse sind Aufzeichnungen der Aktionen, die ein Benutzer auf einer virtuellen Maschine durchführt. Wenn Sie eine virtuelle Maschine im VMware Host Client erstellen, können Sie die damit verbundenen Ereignisse anzeigen.

Voraussetzungen

Erforderliche Berechtigung: **Nur-Lesen**.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Wählen Sie eine virtuelle Maschine aus der Liste aus.

3 Erweitern Sie die virtuelle Maschine in der VMware Host Client-Bestandsliste und klicken Sie auf **Überwachen**.

4 Klicken Sie auf **Ereignisse**.

Es wird eine Liste aller Ereignisse auf der virtuellen Maschine angezeigt.

5 (Optional) Klicken Sie in der Liste auf ein Ereignis, um Details dazu anzuzeigen.

6 (Optional) Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.

7 (Optional) Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen von Aufgaben in virtuellen Maschinen im VMware Host Client

Wenn Sie eine virtuelle Maschine im VMware Host Client erstellen, können Sie alle ihre Aufgaben sowie Informationen zu Aufgabenziel, Initiator, Warteschlangenzeit, Startzeit, Ergebnis und Fertigstellungszeit anzeigen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Wählen Sie eine virtuelle Maschine aus der Liste aus.

3 Erweitern Sie die virtuelle Maschine in der VMware Host Client-Bestandsliste und klicken Sie auf **Überwachen**.

4 Klicken Sie auf **Aufgaben**.

5 (Optional) Klicken Sie in der Liste auf eine Aufgabe, um Details dazu anzuzeigen.

6 (Optional) Verwenden Sie zum Filtern der Liste die Filtersteuerelemente oberhalb der Liste.

7 (Optional) Klicken Sie auf eine Spaltenüberschrift, um die Liste zu sortieren.

Anzeigen des Protokollbrowsers zu virtuellen Maschinen im VMware Host Client

Sie können im VMware Host Client Protokolle zum verwalteten Host generieren und überwachen. Diese Protokolle können Sie anschließend zum Diagnostizieren und Beheben zahlreicher Probleme mit der Hostumgebung verwenden.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Wählen Sie eine virtuelle Maschine aus der Liste aus.

3 Erweitern Sie die virtuelle Maschine in der VMware Host Client-Bestandsliste und klicken Sie auf **Überwachen**.

4 Klicken Sie auf **Protokolle**.

5 (Optional) Klicken Sie auf **Support-Paket generieren**, um alle Protokolle für die Fehlerbehebung zusammenzufassen.

6 Klicken Sie mit der rechten Maustaste auf ein Protokoll in der Liste und wählen Sie **In neuem Fenster öffnen**, um das Protokoll anzuzeigen.

Anzeigen von Benachrichtigungen zu virtuellen Maschinen im VMware Host Client

Sie können im VMware Host Client Benachrichtigungen zu virtuellen Maschinen und Information zu verbundenen Aufgaben, die Sie auf virtuellen Maschinen durchführen können, anzeigen

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Wählen Sie eine virtuelle Maschine aus der Liste aus.

3 Erweitern Sie die virtuelle Maschine in der VMware Host Client-Bestandsliste und klicken Sie auf **Überwachen**.

4 Klicken Sie auf **Benachrichtigungen**.

Es wird eine Liste aller Benachrichtigungen zu virtuellen Maschinen angezeigt.

5 (Optional) Klicken Sie auf eine Benachrichtigung, um Details dazu anzuzeigen.

6 (Optional) Klicken Sie auf eine Benachrichtigung und anschließend auf **Aktionen**, um die vorgeschlagenen Aufgaben anzuzeigen.

Sichern von virtuellen Maschinen im VMware Host Client

Das auf der virtuellen Maschine ausgeführte Gastbetriebssystem ist denselben Sicherheitsrisiken ausgesetzt wie ein physisches System. Zur Verbesserung der Sicherheit in Ihrer virtuellen Umgebung können Sie ein virtuelles Trusted Platform Module (vTPM) zu Ihren ESXi-Hosts hinzufügen. Sie können auch virtualisierungsbasierte Sicherheit (VBS) für die virtuellen Maschinen aktivieren, auf denen die aktuellen Windows 10- und Windows Server 2016-Betriebssysteme ausgeführt werden.

Verwenden des virtuellen TPM im VMware Host Client

Das Trusted Platform Module (TPM) ist ein spezieller Chip, auf dem hostspezifische vertrauliche Informationen gespeichert werden, wie z. B. private Schlüssel und Betriebssystemgeheimnisse. Der TPM-Chip wird auch verwendet, um kryptografische Aufgaben durchzuführen und die Integrität der Plattform zu bestätigen.

Das virtuelle TPM-Gerät stellt eine Softwareemulation der TPM-Funktion dar. Sie können den virtuellen Maschinen in Ihrer Umgebung ein virtuelles TPM-Gerät hinzufügen. Die vTPM-Implementierung benötigt keinen physischen TPM-Chip auf dem Host. ESXi verwendet das vTPM-Gerät, um die TPM-Funktionen in Ihrer vSphere-Umgebung anzuwenden.

vTPM steht für virtuelle Maschinen unter Windows 10 oder Windows Server 2016 zur Verfügung. Die virtuelle Maschine muss die Hardwareversion 14 oder höher aufweisen.

Sie können ein virtuelles TPM-Gerät nur in der vCenter Server-Instanz einer virtuellen Maschine hinzufügen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Im VMware Host Client können Sie das virtuelle TPM-Gerät ausschließlich aus einer virtuellen Maschine entfernen.

Verwenden von VBS im VMware Host Client

Virtualisierungsbasierte Sicherheit (VBS) verwendet die auf Microsoft Hyper-V basierende Virtualisierungstechnologie, um Kerndienste des Windows-Betriebssystems in einer separaten virtualisierten Umgebung zu isolieren. Diese Isolation bietet zusätzlichen Schutz, da sie verhindert, dass Schlüsseldienste in Ihrer Umgebung manipuliert werden.

Durch Aktivierung von VBS auf einer virtuellen Maschine wird automatisch auch die virtuelle Hardware aktiviert, die von Windows für die VBS-Funktion benötigt wird. Durch Aktivierung von VBS startet eine Variante von Hyper-V in der virtuellen Maschine und Windows wird innerhalb der Hyper-V-Root-Partition ausgeführt.

VBS steht in den aktuellen Versionen der Windows-Betriebssysteme zur Verfügung, z. B. Windows 10 und Windows Server 2016. Zur Verwendung von VBS auf einer virtuellen Maschine muss diese mit ESXi 6.7 und höher kompatibel sein.

Sie können VBS während der Erstellung einer virtuellen Maschine im VMware Host Client aktivieren. Alternativ können Sie VBS für eine vorhandene virtuelle Maschine aktivieren oder deaktivieren.

Hinweis Sie können VBS nur dann auf einer virtuellen Maschine aktivieren, wenn die TPM-Validierung des Hosts erfolgreich verläuft.

Entfernen eines vTPM-Geräts von einer VM im VMware Host Client

In VMware Host Client können Sie das virtuelle vTPM-Gerät lediglich von einer virtuellen Maschine entfernen.

Voraussetzungen

- Die virtuelle Maschine muss die Hardwareversion 14 oder höher aufweisen.
- Auf dem Gastbetriebssystem muss Windows 10 oder Windows Server 2016 und höher installiert sein.
- Die virtuelle Maschine muss ausgeschaltet sein.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Suchen Sie auf der Registerkarte **Virtuelle Hardware** nach dem TPM-Gerät und klicken Sie auf das Symbol **Entfernen**.

   Das virtuelle TPM-Gerät wird von der virtuellen Maschine entfernt.
4. Klicken Sie auf **Speichern**, um den Assistenten zu schließen.

Aktivieren oder Deaktivieren von virtualisierungsbasierter Sicherheit für eine vorhandene VM im VMware Host Client

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft auf vorhandenen virtuellen Maschinen für unterstützte Windows-Gastbetriebssysteme aktivieren.

Voraussetzungen

Die Aktivierung von VBS ist ein Prozess, bei dem VBS zuerst in der virtuellen Maschine und anschließend im Gastbetriebssystem aktiviert wird.

Hinweis Neue virtuelle Maschinen, die in niedrigeren Hardwareversionen als Version 14 für Windows 10, Windows Server 2016 und Windows Server 2019 konfiguriert werden, werden standardmäßig mit dem Legacy-BIOS erstellt. Wenn Sie den Firmwaretyp der virtuellen Maschine von Legacy-BIOS in UEFI ändern, müssen Sie das Gastbetriebssystem neu installieren.

Weitere Informationen zu geeigneten CPUs und Best Practices für VBS finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 14 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit) oder höhere Versionen
- Windows Server 2016 (64 Bit) oder höhere Versionen

Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 19 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit), Version 1809 oder höhere Versionen
- Windows Server 2019 (64 Bit) oder höhere Versionen

Stellen Sie sicher, dass Sie die neuesten Patches für Windows 10, Version 1809, und Windows Server 2019 installieren, bevor Sie VBS aktivieren.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.
3. Aktivieren bzw. deaktivieren Sie VBS für die virtuelle Maschine auf der Registerkarte **VM-Optionen**.
   - Wenn Sie VBS für die virtuelle Maschine aktivieren möchten, aktivieren Sie das Kontrollkästchen **Virtualisierungsbasierte Sicherheit aktivieren**.
   - Wenn Sie VBS für die virtuelle Maschine deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Virtualisierungsbasierte Sicherheit aktivieren**.

   Wenn Sie VBS aktivieren, werden verschiedene Optionen automatisch ausgewählt und im Assistenten abgeblendet angezeigt.
4. Klicken Sie auf **Speichern**, um den Assistenten zu schließen.

Verwalten von Speichern im VMware Host Client

4

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie auf dem ESXi-Host verschiedene Speicherverwaltungsaufgaben wie Konfigurieren von Adaptern, Erstellen von Datenspeichern und Anzeigen von Informationen zu Speichergeräten durchführen.

Dieses Kapitel enthält die folgenden Themen:

Arbeiten mit Datenspeichern im VMware Host Client

Datenspeicher sind logische Container ähnlich wie Dateisysteme, die spezielle Informationen zu den einzelnen Speichergeräten enthalten und ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Datenspeicher können auch zum Speichern von ISO-Images, Vorlagen virtueller Maschinen und Disketten-Images genutzt werden.

Je nach Art des verwendeten Speichers können Datenspeicher folgende Typen aufweisen:

- Virtual Machine File System (VMFS)
- Network File System (NFS)

Sie können die Kapazität von Datenspeichern nach deren Erstellung erhöhen, jedoch nur, wenn es sich um VMFS-Datenspeicher handelt.

Anzeigen von Informationen zu Datenspeichern im VMware Host Client

Verwenden Sie den VMware Host Client, um die auf den Hosts verfügbaren Datenspeicher anzuzeigen und deren Eigenschaften zu analysieren.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Wählen Sie den Datenspeicher in der Liste aus, um Details dazu anzuzeigen.

Erstellen eines VMFS-Datenspeichers im VMware Host Client

VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte. Sie können Datenspeicher mit dem **Assistenten für neue Datenspeicher** im VMware Host Client erstellen.

Voraussetzungen

Installieren und konfigurieren Sie alle Adapter, die vom Speicher benötigt werden. Scannen Sie alle Adapter erneut auf neu hinzugefügte Speicher.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie auf **Neuer Datenspeicher**.

Der **Assistent für neue Datenspeicher** wird angezeigt.

3 Wählen Sie auf der Seite „Erstellungstyp auswählen“ die Option **Neuen VMFS-Datenspeicher erstellen** aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Neuen VMFS-Datenspeicher erstellen	Erstellt einen neuen VMFS-Datenspeicher auf einem lokalen Festplattengerät.
Vorhandenem VMFS-Datenspeicher eine Erweiterung hinzufügen	Erhöht die Größe eines vorhandenen Datenspeichers durch Hinzufügen eines neuen Umfangs auf einer anderen Festplatte.
Vorhandene VMFS-Datenspeichererweiterung erweitern	Erhöht die Größe eines vorhandenen VMFS-Datenspeichers.
NFS-Datenspeicher mounten	Erstellt einen neuen Datenspeicher durch Mounten eines Remote-NFS-Volumes.

4 Wählen Sie auf der Seite „Gerät auswählen“ das Gerät aus, in dem die VMFS-Partition erstellt werden soll.

a Geben Sie einen Namen für den neuen Datenspeicher ein.

b Wählen Sie ein Gerät aus, dem der Datenspeicher hinzugefügt werden soll.

Die Liste enthält nur Geräte, die über ausreichend Speicherplatz verfügen.

c Klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite „Partitionierungsoptionen auswählen“ aus, wie das Gerät partitioniert werden soll, und klicken Sie auf **Weiter**.

Option	Beschreibung
Vollständige Festplatte nutzen	Zeigt den auf dem Gerät verfügbaren Speicherplatz.
Benutzerdefiniert	Klicken Sie auf die Leiste **Freier Speicherplatz** und partitionieren Sie das Gerät mithilfe des senkrechten Scrollers.

6 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Konfigurationsdetails und klicken Sie auf **Beenden**.

Erhöhen der VMFS-Datenspeicherkapazität

Wenn Ihr VMFS-Datenspeicher mehr Speicherplatz benötigt, erhöhen Sie die Datenspeicherkapazität. Sie können die Kapazität dynamisch erhöhen, indem Sie eine Datenspeichererweiterung vergrößern oder eine Erweiterung hinzufügen.

Erhöhen Sie die Datenspeicherkapazität mit einer der folgenden Methoden:

- Erweitern Sie dynamisch eine vergrößerbare Datenspeichererweiterung, damit der Datenspeicher die benachbarte Kapazität belegt. Die Erweiterung wird als vergrößerbar angesehen, wenn das zugrunde liegende Speichergerät unmittelbar hinter der Erweiterung über freien Speicherplatz verfügt.
- Fügen Sie die neue Erweiterung dynamisch hinzu. Der Datenspeicher kann sich über bis zu 32 Erweiterungen mit einer Größe von jeweils mehr als 2 TB erstrecken und dennoch als ein einziges Volume erscheinen. Der übergreifende VMFS-Datenspeicher kann jederzeit jede einzelne oder alle seiner Erweiterungen verwenden. Es ist nicht notwendig, dass eine bestimmte Erweiterung aufgefüllt wird, bevor die nächste Erweiterung verwendet werden kann.

  Hinweis Datenspeicher, die nur hardwaregestützte Sperren unterstützen, die auch als Atomic Test and Set-Mechanismus (ATS) bezeichnet werden, können sich nicht über Nicht-ATS-Geräte erstrecken. Weitere Informationen finden Sie unter *vSphere-Speicher*.

Erweitern eines bestehenden VMFS-Datenspeichers im VMware Host Client

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

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

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie auf **Neuer Datenspeicher**.

3 Klicken Sie auf der Seite „Erstellungstyp auswählen“ auf **Vorhandenem VMFS-Datenspeicher eine Erweiterung hinzufügen** und dann auf **Weiter**.

4 Wählen Sie auf der Seite „Datenspeicher auswählen“ den zu erweiternden Datenspeicher aus und klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite „Gerät auswählen“ ein Gerät aus, auf dem die neue VMFS-Partition erstellt werden soll, und klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite „Partitionierungsoptionen auswählen“ aus, wie das Gerät partitioniert werden soll, und klicken Sie auf **Weiter**.

Option	Beschreibung
Vollständige Festplatte nutzen	Zeigt den auf dem Gerät verfügbaren Speicherplatz.
Benutzerdefiniert	Klicken Sie auf die Leiste **Freier Speicherplatz** und partitionieren Sie das Gerät mithilfe des senkrechten Scrollers.

7 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Konfigurationsdetails und klicken Sie auf **Beenden**.

Mounten eines Network File System-Datenspeichers im VMware Host Client

Mit dem VMware Host Client können Sie einen NFS (Network File System)-Datenspeicher erstellen, in dem virtuelle Festplatten gespeichert werden und das als zentrales Repository für ISO-Images und für Vorlagen virtueller Maschinen genutzt wird. In ESXi integrierte NFS-Clients verwenden das Network File System-Protokoll (NFS) über TCP/IP, um auf ein ausgewähltes NFS-Volume auf einem NAS-Server zuzugreifen. vSphere unterstützt die Versionen 3 und 4.1 des NFS-Protokolls.

Der ESXi-Host kann ein NFS-Volume mounten und es zur Deckung seines Speicherbedarfs verwenden.

Das NFS-Volume bzw. NFS-Verzeichnis wird von einem Speicheradministrator erstellt und vom NFS-Server exportiert. Das NFS-Volume muss nicht mit einem lokalen Dateisystem wie VMFS formatiert werden. Stattdessen mounten Sie das Volume direkt auf den ESXi-Hosts und verwenden es auf die gleiche Weise zum Speichern und Starten der virtuellen Maschinen wie die VMFS-Datenspeicher.

Neben der Speicherung von virtuellen Festplatten in NFS-Datenspeichern können Sie NFS als zentrales Repository für ISO-Images, VM-Vorlagen usw. nutzen. Wenn Sie den Datenspeicher für die ISO-Images verwenden möchten, können Sie das CD-ROM-Laufwerk der virtuellen Maschine mit einer ISO-Datei auf dem Datenspeicher verbinden. Anschließend können Sie ein Gastbetriebssystem von der ISO-Datei installieren.

Bei Verwendung des NFS-Speichers müssen Sie die spezifischen Richtlinien zur NFS-Serverkonfiguration, zum Netzwerk, zu NFS-Datenspeichern usw. befolgen.

Verfahren

1 Mounten eines NFS-Datenspeichers im VMware Host Client

  Verwenden Sie den **Assistenten für neue Datenspeicher** zum Mounten eines NFS (Network File System)-Datenspeichers im VMware Host Client.

Mounten eines NFS-Datenspeichers im VMware Host Client

Verwenden Sie den **Assistenten für neue Datenspeicher** zum Mounten eines NFS (Network File System)-Datenspeichers im VMware Host Client.

Voraussetzungen

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

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie auf **Neuer Datenspeicher**.

  Der **Assistent für neue Datenspeicher** wird angezeigt.

3 Klicken Sie auf der Seite „Erstellungstyp auswählen“ auf **NFS-Datenspeicher mounten** und dann auf **Weiter**.

4 Geben Sie auf der Seite „NFS-Mount-Details angeben“ die Details für das NFS an, das Sie mounten.

   a Geben Sie einen Namen für den NFS-Datenspeicher ein.

   b Geben Sie den NFS-Servernamen 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 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 ist es, wenn Sie **`filer`** als Servernamen auf einem Host und **`filer.domain.com`** auf dem anderen Host eingeben.

   c Geben Sie die NFS-Freigabe an.

   d Geben Sie die NFS-Version an.

   e Klicken Sie auf **Weiter**.

5 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Konfigurationseinstellungen für den NFS-Datenspeicher und klicken Sie auf **Beenden**.

Unmounten eines Datenspeichers im VMware Host Client

Wenn ein Datenspeicher im VMware Host Client ungemountet wird, bleibt dieser intakt, er wird jedoch nicht mehr in der Bestandsliste des verwalteten Hosts angezeigt. Der Datenspeicher wird weiterhin auf anderen Hosts angezeigt, auf denen er gemountet bleibt.

Führen Sie keine Konfigurationsvorgänge durch, die zu E/A des Datenspeichers führen können, während das Unmounten ausgeführt wird.

Voraussetzungen

Hinweis Stellen Sie sicher, dass der Datenspeicher nicht für vSphere HA-Taktsignale verwendet wird. vSphere HA-Taktsignale verhindern das Unmounten des Datenspeichers nicht. Wenn jedoch der Datenspeicher für das Taktsignal verwendet wird, kann das Unmounten des Datenspeichers dazu führen, dass der Host ausfällt und alle aktiven virtuellen Maschinen neu gestartet werden.

Stellen Sie vor dem Unmounten von Datenspeichern sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Es dürfen sich keine virtuelle Maschinen im Datenspeicher befinden.
- Speicher-DRS verwaltet den Datenspeicher nicht.
- Storage I/O Control ist für diesen Datenspeicher deaktiviert.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie in der Liste mit der rechten Maustaste auf den Datenspeicher, der unmountet werden soll, und klicken Sie auf **Unmounten**.

3 Bestätigen Sie, dass Sie den Datenspeicher unmounten möchten.

Das Unmounten oder Entfernen eines Datenspeichers schlägt fehl

Wenn Sie versuchen, ein Unmounten oder Entfernen eines Datenspeichers durchzuführen, schlägt der Vorgang fehl.

Problem

Das Unmounten oder Entfernen eines Datenspeichers schlägt fehl, wenn im Datenspeicher geöffnete Dateien vorhanden sind. Für diese Benutzervorgänge schließt der vSphere HA-Agent alle Dateien, die er geöffnet hat, beispielsweise die Taktsignal-Dateien. Falls der Agent nicht von vCenter Server erreicht werden kann oder der Agent ausstehende E/A-Vorgänge nicht auf die Festplatte schreiben kann, um die Dateien zu schließen, wird der Fehler `Der vSphere HA-Agent auf Host '{hostName}' konnte die Dateiaktivitäten auf dem Datenspeicher '{dsName}' nicht stilllegen` ausgelöst.

Ursache

Wenn der Datenspeicher, für den ein Unmounten durchgeführt oder der entfernt werden soll, für Taktsignale verwendet wird, schließt vCenter Server ihn als Taktsignal-Datenspeicher aus und wählt dafür einen neuen Datenspeicher aus. Allerdings empfängt der Agent nicht die aktualisierten Taktsignal-Datenspeicher, wenn er nicht erreichbar ist. Dies ist der Fall, wenn der Host isoliert ist oder sich in einer Netzwerkpartition befindet. In diesen Fällen werden die Taktsignal-Dateien nicht geschlossen und der Benutzervorgang schlägt fehl. Der Vorgang kann auch fehlschlagen, wenn der Datenspeicher aufgrund von Speicherausfällen, z. B. „Keine Pfade verfügbar“, nicht zugänglich ist.

Hinweis Wenn Sie einen VMFS-Datenspeicher entfernen, wird der Datenspeicher von allen Hosts in der Bestandsliste entfernt. Wenn also Hosts in einem vSphere HA-Cluster nicht erreichbar sind oder Hosts nicht auf den Datenspeicher zugreifen können, schlägt der Vorgang fehl.

Lösung

Stellen Sie sicher, dass der Datenspeicher zugänglich ist und die betreffenden Hosts erreichbar sind.

Verwenden des Datenspeicher-Dateibrowsers im VMware Host Client

Verwenden Sie den Datenspeicherbrowser zum Verwalten des Inhalts des Datenspeichers. Sie können zahlreiche Aufgaben wie Hochladen von Dateien in den Datenspeicher, Herunterladen

von Dateien aus dem Datenspeicher in Ihr System, Verschieben und Kopieren von Dateien oder Ordnern sowie Erstellen neuer Verzeichnisse im Datenspeicher durchführen.

Hochladen von Dateien in einen Datenspeicher im VMware Host Client

Verwenden Sie den Datenspeicher-Dateibrowser zum Hochladen von Dateien in Datenspeicher, auf dem Host.

Hinweis Das direkte Hochladen von Dateien in die virtuellen Datenspeicher wird von Virtual Volumes nicht unterstützt. Sie müssen zuerst einen Ordner im virtuellen Datenspeicher erstellen und dann die Dateien in den Ordner hochladen.

Zusätzlich zur herkömmlichen Verwendung als Speicher für VM-Dateien können Daten oder im Zusammenhang mit virtuellen Maschinen stehende Dateien in Datenspeichern gespeichert werden. Beispiel: Sie können ISO-Images von Betriebssystemen von einem lokalen Computer in einen Datenspeicher auf dem Host hochladen. Anschließend können Sie diese Images zum Installieren von Gastbetriebssystemen auf den neuen virtuellen Maschinen verwenden.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie auf **Datenspeicherbrowser**.
3. Wählen Sie den Datenspeicher aus, in dem die Datei gespeichert werden soll.
4. (Optional) Klicken Sie auf **Verzeichnis erstellen**, um ein neues Datenspeicherverzeichnis zum Speichern der Datei zu erstellen.
5. Wählen Sie den Zielordner aus und klicken Sie auf **Hochladen**.
6. Suchen Sie das Element, das Sie vom lokalen Computer aus hochladen möchten, und klicken Sie auf **Öffnen**.

   Die Datei wird in den ausgewählten Datenspeicher hochgeladen.
7. (Optional) Aktualisieren Sie den Dateibrowser des Datenspeichers, damit die hochgeladene Datei in der Liste angezeigt wird.
8. Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Herunterladen von Dateien aus einem Datenspeicher in das System im VMware Host Client

Laden Sie mit dem Datenspeicherbrowser Dateien aus den verfügbaren Datenspeichern auf dem verwalteten Host auf das lokale System herunter.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie auf **Datenspeicherbrowser**.
3. Wählen Sie den Zieldatenspeicher aus.
4. Wählen Sie den Ordner mit der herunterzuladenden Datei aus.

   Die im Ordner verfügbaren Dateien werden angezeigt.
5. Klicken Sie auf die herunterzuladende Datei.
6. Klicken Sie auf **Herunterladen**.

   Die Datei wird auf Ihr System heruntergeladen.
7. Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Löschen von Dateien aus einem Datenspeicher im VMware Host Client

Sie können nicht mehr benötigte Dateien dauerhaft aus jedem beliebigen Datenspeicher löschen.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie auf **Datenspeicherbrowser**.
3. Wählen Sie den Zieldatenspeicher aus.
4. Wählen Sie den Ordner mit der zu löschenden Datei aus.

   Die im Ordner verfügbaren Dateien werden angezeigt.
5. Wählen Sie die Datei aus, die aus dem Datenspeicher entfernt werden soll, und klicken Sie auf **Löschen** und anschließend nochmals auf **Löschen**.
6. Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Verschieben von Ordnern oder Dateien im Datenspeicher im VMware Host Client

Verschieben Sie Ordner oder Dateien mit dem Datenspeicherbrowser an einen neuen Speicherort im selben oder einem anderen Datenspeicher.

Hinweis Virtuelle Festplattendateien werden ohne Formatkonvertierung verschoben und kopiert. Wenn Sie eine virtuelle Festplatte in einen Datenspeicher eines Hosttyps verschieben, der sich vom Quellhost unterscheidet, müssen die virtuellen Festplatten u. U. konvertiert werden, bevor Sie diese verwenden können.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie auf **Datenspeicherbrowser**.
3. Wählen Sie den Zieldatenspeicher aus.
4. Wählen Sie die Datei oder den Ordner, die bzw. den Sie an einen anderen Speicherort verschieben möchten, aus und klicken Sie auf **Verschieben**.
5. Wählen Sie den Zielspeicherort aus und klicken Sie auf **Verschieben**.
6. Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Kopieren von Ordnern oder Dateien im Datenspeicher im VMware Host Client

Verwenden Sie den Datenspeicherbrowser zum Kopieren von Ordnern oder Dateien an einen neuen Speicherort auf demselben oder einem anderen Datenspeicher.

Hinweis Virtuelle Festplattendateien werden ohne Formatkonvertierung verschoben und kopiert. Wenn Sie eine virtuelle Festplatte in einen Datenspeicher eines Hosttyps verschieben, der sich vom Quellhost unterscheidet, müssen die virtuellen Festplatten u. U. konvertiert werden.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie auf **Datenspeicherbrowser**.
3. Wählen Sie den Zieldatenspeicher aus.

4 Wählen Sie die Datei oder den Ordner, die bzw. den Sie an einen anderen Speicherort verschieben möchten, aus und klicken Sie auf **Kopieren**.

5 Wählen Sie den Zielspeicherort aus und klicken Sie auf **Kopieren**.

6 Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Erstellen eines neuen Datenspeichers im VMware Host Client

Sie können neue Datenspeicherverzeichnisse erstellen, wenn Sie Dateien an einem bestimmten Ort speichern möchten.

Voraussetzungen

Erforderliche Berechtigung:**Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie auf **Datenspeicherbrowser**.

3 Klicken Sie auf **Verzeichnis erstellen**.

4 Wählen Sie den Zieldatenspeicher aus.

5 (Optional) Geben Sie einen Namen für das neue Verzeichnis ein.

6 Klicken Sie auf **Verzeichnis erstellen**.

7 Klicken Sie auf **Schließen**, um den Dateibrowser zu beenden.

Umbenennen eines Datenspeichers im VMware Host Client

Sie können den Anzeigenamen eines Datenspeichers im VMware Host Client ändern.

Hinweis Wenn der Host von vCenter Server verwaltet wird, können Sie den Datenspeicher aus VMware Host Client nicht umbenennen. Sie können die Aufgabe nur von der vCenter Server-Instanz aus ausführen, die den Host verwaltet.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.

2 Klicken Sie mit der rechten Maustaste auf einen Datenspeicher in der Liste und wählen Sie **Umbenennen** im Dropdown-Menü aus.

3 Geben Sie einen neuen Namen für den Datenspeicher ein und klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

4 (Optional) Durch Klicken auf **Aktualisieren** wird der Name des neuen Datenspeichers in der Liste der verfügbaren Datenspeicher angezeigt.

Löschen eines VMFS-Datenspeichers im VMware Host Client

Sie können jede Art von VMFS-Datenspeicher löschen, einschließlich Kopien, die Sie gemountet haben, ohne sie neu zu signieren. Beim Löschen eines Datenspeichers werden alle mit ihm verbundenen Dateien vom Host entfernt.

Hinweis Der Datenspeicher-Löschvorgang löscht alle Dateien permanent, die virtuelle Maschinen auf dem Datenspeicher zugeordnet sind. Obwohl Sie den Datenspeicher ohne Unmounten löschen können, empfiehlt es sich, zuerst den Datenspeicher zu unmounten.

Voraussetzungen

Entfernen Sie alle virtuelle Maschinen aus dem Datenspeicher.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Datenspeicher**.
2. Klicken Sie mit der rechten Maustaste auf den Datenspeicher in der Liste und wählen Sie **Löschen** im Dropdown-Menü aus.
3. Klicken Sie auf **Bestätigen**, um den Datenspeicher zu löschen.

Speicherhardware-Beschleunigung

Mithilfe der Hardwarebeschleunigung kann der ESXi-Host in konforme Speichersysteme integriert werden. Der Host kann bestimmte VM- und Speicherverwaltungsvorgänge auf die Speichersysteme auslagern. 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 im VMware Host Client

Die Host-Hardwarebeschleunigung für Blockspeichergeräte ist standardmäßig auf allen Hosts aktiviert. Sie können die erweiterten Einstellungen des VMware Host Client verwenden, um die Hardwarebeschleunigung zu deaktivieren.

Das Ändern der erweiterten Einstellungen wird nicht unterstützt, es sei denn, der technische Support von VMware weist Sie an, dies zu tun.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Virtuelle Maschinen**.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine in der Liste und wählen Sie **Einstellungen bearbeiten** im Dropdown-Menü aus.

3 Erweitern Sie auf der Registerkarte **VM-Optionen** die Option **Erweitert**.

4 Wählen Sie unter **Einstellungen** die Option **Beschleunigung deaktivieren**.

5 Klicken Sie auf **Speichern**.

Thin-Bereitstellung des Speichers in VMware Host Client

Mit ESXi können Sie zwei Modelle der Thin-Bereitstellung verwenden: Thin-Bereitstellung auf Array-Ebene und Thin-Bereitstellung auf der Ebene der virtuellen Festplatte.

Thin-Bereitstellung ist eine Methode, die die Speichernutzung optimiert, indem Speicherplatz auf flexible Weise nach Bedarf zugeteilt wird. Thin-Bereitstellung 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-Bereitstellungsfunktionen 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 im VMware Host Client

Um Speicherplatz zu sparen, können Sie Thin-bereitgestellte virtuelle Festplatten erstellen. Die Größe der virtuellen Thin-bereitgestellten Festplatte ist zunächst gering und steigt an, sobald mehr virtueller Festplattenspeicher erforderlich ist. Sie können Thin-Festplatten nur auf Datenspeichern erstellen, die Thin Provisioning auf Festplattenebene unterstützen.

Beim nachfolgenden Verfahren wird davon ausgegangen, dass Sie eine neue virtuelle Maschine erstellen. Weitere Informationen finden Sie unter Erstellen einer virtuellen Maschine im VMware Host Client.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Host** und wählen Sie **VM erstellen/registrieren**.

   Der Assistent zum **Erstellen neuer virtueller Maschinen** wird angezeigt.

2 Wählen Sie eine Methode für das Hinzufügen einer virtuellen Maschine auf dem Host aus und klicken Sie auf **Weiter**.

3 Geben Sie einen Namen für die virtuelle Maschine ein.

4 Wählen Sie die Kompatibilität der virtuellen Maschine aus dem Dropdown-Menü **Kompatibilität** aus.

5 Wählen Sie im Dropdown-Menü **Version des Gastbetriebssystems** die Version des Gastbetriebssystems aus und klicken Sie auf **Weiter**.

6 Wählen Sie in der Liste der verfügbaren Datenspeicher auf der Seite „Speicher auswählen“ im Assistenten zum **Erstellen neuer virtueller Maschinen** den Zieldatenspeicher für die Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus.

7 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte**.

8 Klicken Sie unter **Festplattenbereitstellung** auf das Optionsfeld **Thin-bereitgestellt** und klicken Sie auf **Weiter**.

9 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ des Assistenten zum **Erstellen neuer virtueller Maschinen** die Konfigurationseinstellungen für die virtuelle Maschine und klicken Sie auf **Beenden**, um die Einstellungen zu speichern.

Anzeigen von Speicherressourcen virtueller Maschinen im VMware Host Client

Sie können anzeigen, wie Speicherplatz von Datenspeichern Ihren virtuellen Maschinen im VMware Host Client zugeteilt ist.

Die Anzeige des Ressourcenverbrauchs bietet Aufschluss über den Datenspeicherplatz, der von den Dateien der virtuellen Maschine, z. B. Konfigurations- und Protokolldateien, Snapshots, virtuellen Festplatten usw., beansprucht wird. Wenn die virtuelle Maschine läuft, werden im verwendeten Speicherplatz auch die Auslagerungsdateien berücksichtigt.

Für virtuelle Maschinen mit Thin-Festplatten kann der tatsächliche Speichernutzungswert geringer als die Größe der virtuellen Festplatte sein.

Verfahren

1 Klicken Sie auf die virtuelle Maschine in der VMware Host Client-Bestandsliste.

2 Überprüfen Sie die Informationen zum Ressourcenverbrauch im unteren rechten Bereich der Übersichtsseite zur virtuellen Maschine.

Festlegen des Festplattenformats für eine virtuelle Maschine im VMware Host Client

Sie können festlegen, ob Ihre virtuelle Festplatte im Thick- oder im Thin-Format bereitgestellt werden soll.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

2 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte**.

Im Textfeld **Typ** wird das Format Ihrer virtuellen Festplatte angezeigt.

Verwalten von Speicheradaptern im VMware Host Client

Wenn Sie über den VMware Host Client eine Verbindung zu einem Host oder zu vCenter Server herstellen, können Sie verschiedene Aufgaben auf Ihren Speicheradaptern durchführen, wie z. B. das Konfigurieren unterschiedlicher iSCSI-Komponenten.

Wenn Sie iSCSI auf dem Host aktivieren, den Sie in Ihrer VMware Host Client-Umgebung verwalten, können Sie Netzwerk-Port-Bindungen sowie statische und dynamische Ziele konfigurieren und neu hinzufügen, die CHAP-Authentifizierung verwalten und verschiedene erweiterte Einstellungen auf dem Hostspeicher konfigurieren.

Anzeigen von Speicheradaptern im VMware Host Client

Sie können die vom Host verwendeten Speicheradapter und damit verbundene Informationen anzeigen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter**.

   Alle auf dem Host verfügbaren Speicheradapter werden unter **Adapter** aufgeführt.
2. Wählen Sie einen Adapter in der Liste aus, um Details dazu anzuzeigen.

Konfigurieren von Software-iSCSI-Adaptern im VMware Host Client

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 kommuniziert über den Netzwerkstapel mit den physischen Netzwerkkarten.

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

Der Workflow für die Konfiguration des iSCSI-Adapters umfasst die folgenden Schritte:

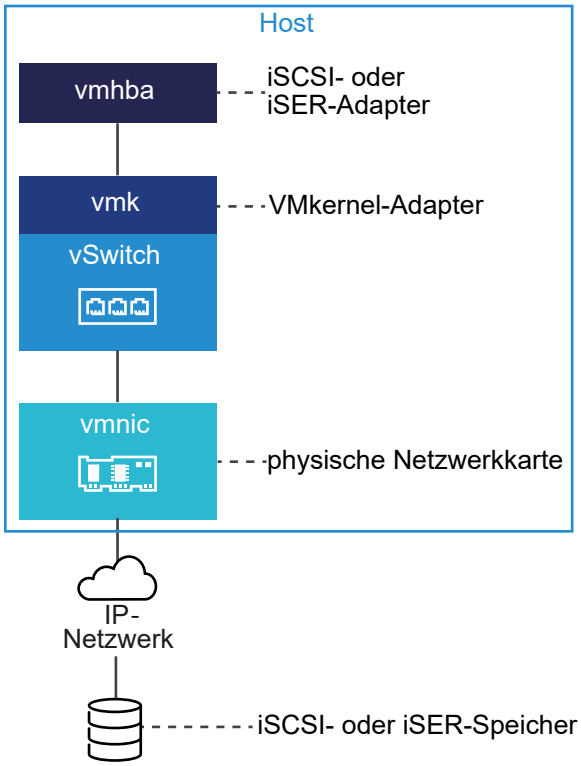
- Aktivieren von iSCSI auf Ihrem Host. Weitere Informationen hierzu finden Sie unter Aktivieren von iSCSI für einen ESXi-Host im VMware Host Client.
- Hinzufügen einer Port-Bindung. Weitere Informationen hierzu finden Sie unter Hinzufügen von Port-Bindungen im VMware Host Client.
- Entfernen einer Port-Bindung. Weitere Informationen hierzu finden Sie unter Entfernen von Port-Bindungen im VMware Host Client.

Einrichten eines Netzwerks für iSCSI und iSER

Bestimmte iSCSI-Adaptertypen hängen vom VMkernel-Netzwerk ab. Diese Adapter umfassen den Software- oder abhängigen Hardware-iSCSI-Adapter und den VMware-iSCSI über RDMA (iSER)-Adapter. Wenn Ihre Umgebung einen dieser Adapter enthält, müssen Sie Verbindungen für den

Datenverkehr zwischen der iSCSI- oder iSER-Komponente und den physischen Netzwerkadaptern konfigurieren.

Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter. Anschließend muss der VMkernel-Adapter mit einem entsprechenden iSCSI- oder iSER-Adapter verknüpft werden. Dieser Vorgang wird Port-Bindung genannt.



Befolgen Sie diese Regeln beim Konfigurieren der Port-Bindung:

- 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.
- Sie dürfen den iSER-Adapter nur mit dem RDMA-fähigen Netzwerkadapter verbinden.

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

Aktivieren von iSCSI für einen ESXi-Host im VMware Host Client

Aktivieren Sie iSCSI für Ihren Host in der VMware Host Client-Umgebung, um Parameter für Speicheradapter zu konfigurieren, wie z. B. die CHAP-Authentifizierung, Netzwerk-Port-Bindungen, statische und dynamische Ziele sowie verschiedene erweiterte Einstellungen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.

2 Wählen Sie das Optionsfeld **Aktiviert** aus.

3 (Optional) Konfigurieren Sie die zu ändernden Parameter und Komponenten.

4 Klicken Sie auf **Konfiguration speichern**.

Best Practices für die Konfiguration des Netzwerks mit Software-iSCSI

Berücksichtigen Sie bei der Konfiguration des Netzwerks mit Software-iSCSI verschiedene Best Practices.

Software-iSCSI-Port-Bindung

Sie können den Software-iSCSI-Initiator auf dem ESXi-Host an einen einzelnen oder mehrere VMkernel-Ports binden, sodass der iSCSI-Datenverkehr nur über die gebundenen Ports fließt. Ungebundene Ports werden nicht für iSCSI-Datenverkehr verwendet.

Wenn die Port-Bindung konfiguriert ist, erstellt der iSCSI-Initiator iSCSI-Sitzungen von allen gebundenen Ports zu allen konfigurierten Zielportalen.

Nachfolgend finden Sie Beispiele.

VMkernel-Ports	Zielportale	iSCSI-Sitzungen
2 gebundene VMkernel-Ports	2 Zielportale	4 Sitzungen (2 x 2)
4 gebundene VMkernel-Ports	1 Zielportal	4 Sitzungen (4 x 1)
2 gebundene VMkernel-Ports	4 Zielportale	8 Sitzungen (2 x 4)

Hinweis Stellen Sie sicher, dass alle Zielportale von allen VMkernel-Ports erreicht werden können, wenn die Port-Bindung verwendet wird. Andernfalls können iSCSI-Sitzungen möglicherweise nicht erstellt werden. Infolgedessen wird für die erneute Prüfung möglicherweise mehr Zeit benötigt als erwartet.

Keine Port-Bindung

Wird keine Port-Bindung verwendet, wird auf der ESXi-Netzwerkebene der beste VMkernel-Port basierend auf seiner Routing-Tabelle ausgewählt. Der Host nutzt den Port zum Erstellen einer iSCSI-Sitzung mit dem Zielportal. Ohne die Port-Bindung wird nur eine Sitzung pro Zielportal erstellt.

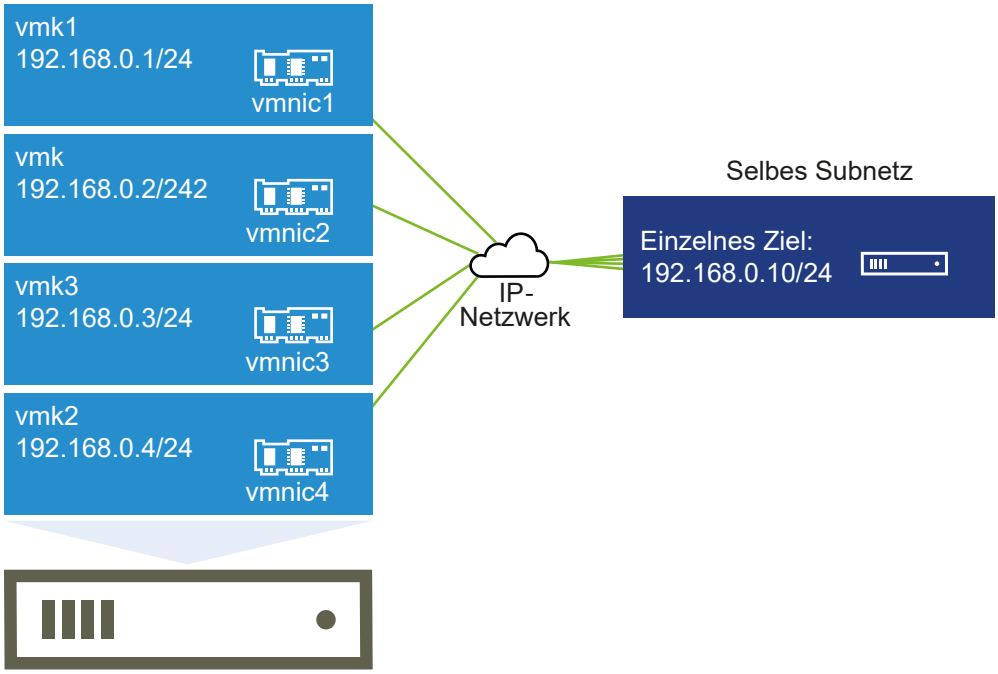
Nachfolgend finden Sie Beispiele.

VMkernel-Ports	Zielportale	iSCSI-Sitzungen
2 ungebundene VMkernel-Ports	2 Zielportale	2 Sitzungen
4 ungebundene VMkernel-Ports	1 Zielportal	1 Sitzung
2 ungebundene VMkernel-Ports	4 Zielportale	4 Sitzungen

Software-iSCSI-Multipathing

Beispiel 1: Mehrere Pfade für ein iSCSI-Ziel mit einem einzelnen Netzwerkportal

Wenn das Ziel nur über ein Netzwerkportal verfügt, können Sie mehrere Pfade zu dem Ziel erstellen, indem Sie mehrere VMkernel-Ports auf dem ESXi-Host hinzufügen und diese an den iSCSI-Initiator binden.

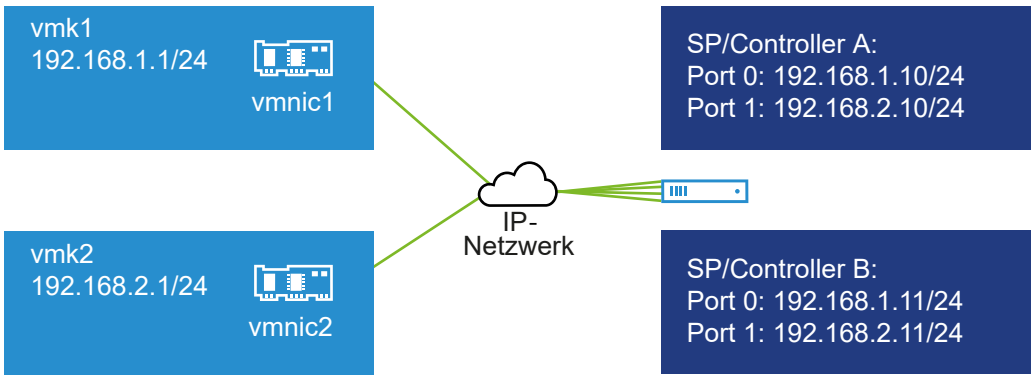


In diesem Beispiel werden alle Initiator-Ports und das Zielportal im selben Subnetz konfiguriert. Das Ziel kann über alle gebundenen Ports erreicht werden. Sie haben vier VMkernel-Ports und ein Zielportal. Es werden also insgesamt vier Pfade erstellt.

Ohne die Port-Bindung wird nur ein Pfad erstellt.

Beispiel 2: Mehrere Pfade mit VMkernel-Ports in verschiedenen Subnetzen

Sie können mehrere Pfade erstellen, indem Sie mehrere Ports und Zielportale in verschiedenen IP-Subnetzen konfigurieren. Indem Initiator- und Zielports in verschiedenen Subnetzen beibehalten werden, können Sie erzwingen, dass ESXi Pfade über bestimmte Ports erstellt. Bei dieser Konfiguration wird keine Port-Bindung verwendet, da für die Port-Bindung erforderlich ist, dass sich alle Initiator- und Zielports im selben Subnetz befinden.



ESXi wählt vmk1 aus, wenn eine Verbindung zu Port 0 von Controller A und Controller B hergestellt wird, da sich alle drei Ports im selben Subnetz befinden. Ebenso wird vmk2 ausgewählt, wenn eine Verbindung zu Port 1 von Controller A und B hergestellt wird. Bei dieser Konfiguration kann die NIC-Gruppierung verwendet werden.

Es werden insgesamt vier Pfade erstellt.

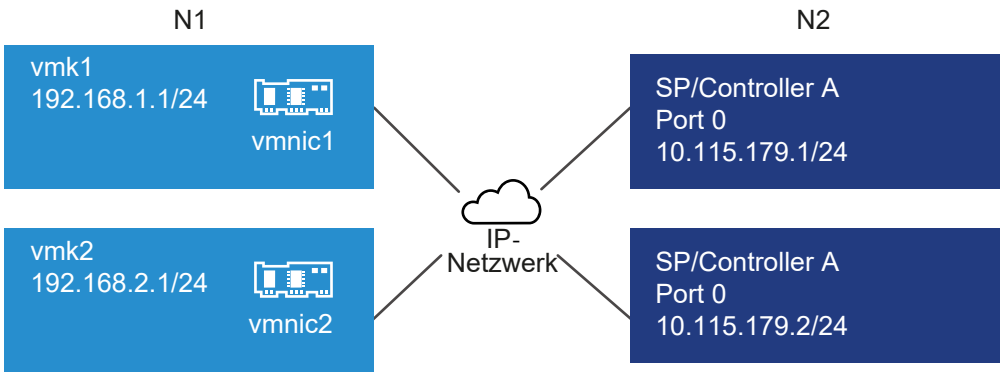
Pfade	Beschreibung
Pfad 1	vmk1 und Port 0 von Controller A
Pfad 2	vmk1 und Port 0 von Controller B
Pfad 3	vmk2 und Port 1 von Controller A
Pfad 4	vmk2 und Port 1 von Controller B

Routing mit Software-iSCSI

Mit dem Befehl `esxcli` können Sie statische Routen für Ihren iSCSI-Datenverkehr hinzufügen. Nachdem die statischen Routen konfiguriert wurden, können die Initiator- und Zielports in verschiedenen Subnetzen miteinander kommunizieren.

Beispiel 1: Verwenden von statischen Routen mit Port-Bindung

In diesem Beispiel werden alle gebundenen VMkernel-Ports in einem Subnetz (N1) beibehalten und alle Zielportale in einem anderen Subnetz (N2) konfiguriert. Sie können dann eine statische Route für das Zielsubnetz (N2) hinzufügen.

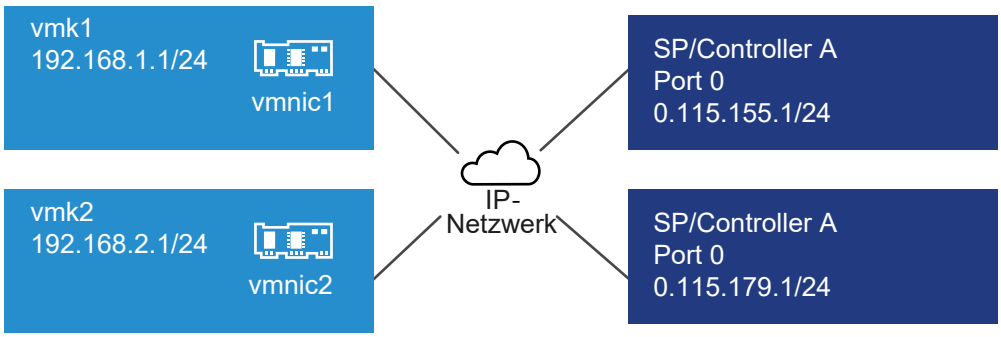


Verwenden Sie den folgenden Befehl:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Beispiel 2: Verwenden von statischen Routen, um mehrere Pfade zu erstellen

Bei dieser Konfiguration verwenden Sie statische Routen und verschiedene Subnetze. Bei dieser Konfiguration kann die Port-Bindung nicht verwendet werden.



Sie konfigurieren vmk1 und vmk2 in separaten Subnetzen: 192.168.1.0 und 192.168.2.0. Ihre Zielportale befinden sich also in separaten Subnetzen: 10.115.155.0 und 10.155.179.0.

Sie können die statische Route für 10.115.155.0 von vmk1 hinzufügen. Stellen Sie sicher, dass das Gateway von vmk1 aus erreicht werden kann.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.155.0/24
```

Anschließend fügen Sie die statische Route für 10.115.179.0 von vmk2 hinzu. Stellen Sie sicher, dass das Gateway von vmk2 aus erreicht werden kann.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network
10.115.179.0/24
```

Beim Herstellen der Verbindung mit Port 0 von Controller A wird vmk1 verwendet.

Beim Herstellen der Verbindung mit Port 0 von Controller B wird vmk2 verwendet.

Beispiel 3: Routing mit einem separaten Gateway pro vmkernel-Port

Ab vSphere 6.5 können Sie ein separates Gateway pro VMkernel-Port konfigurieren. Wenn Sie DHCP zum Abrufen der IP-Konfiguration für einen VMkernel-Port verwenden, können Gateway-Informationen ebenfalls über DHCP abgerufen werden.

Verwenden Sie den folgenden Befehl, um Gateway-Informationen pro VMkernel-Port anzuzeigen:

```
# esxcli network ip interface ipv4 address list
```

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

Bei separaten Gateways pro VMkernel-Port nutzen Sie die Port-Bindung, um Ziele in verschiedenen Subnetzen zu erreichen.

Hinzufügen von Port-Bindungen im VMware Host Client

Verwenden Sie den VMware Host Client, um einen iSCSI-Adapter mit einem VMkernel-Adapter an Ihren Host zu binden.

Voraussetzungen

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

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.
2. Klicken Sie im Abschnitt **Netzwerk-Port-Bindungen** auf **Port-Bindung hinzufügen**.
3. Wählen Sie einen VMkernel-Adapter zur Bindung mit dem iSCSI-Adapter aus.

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

   Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter ist nur ein VMkernel-Adapter verfügbar, der mit der richtigen physischen Netzwerkkarte verknüpft ist.
4. Klicken Sie auf **Auswählen**.
5. Klicken Sie auf **Konfiguration speichern**.

Entfernen von Port-Bindungen im VMware Host Client

Bearbeiten Sie die iSCSI-Konfiguration auf Ihrem Host, um eine Port-Bindung zu entfernen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.
2. Wählen Sie im Abschnitt **Netzwerk-Port-Bindungen** eine VMkernel-Netzwerkkarte aus der Liste aus.
3. Klicken Sie auf **Port-Bindung entfernen**.
4. Klicken Sie auf **Konfiguration speichern**.

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 eines statischen Ziels im VMware Host Client

Mithilfe von iSCSI-Initiatoren können Sie die statische Erkennung verwenden, um Informationen für die Ziele manuell einzugeben.

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.

Voraussetzungen

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

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.

2 Klicken Sie auf **Statisches Ziel hinzufügen**.

   Das neue statische Ziel wird in der Liste angezeigt.

3 Klicken Sie zum Hinzufügen eines Namens für das neue statische Ziel auf das Ziel in der Liste und geben Sie den Namen ein.

4 Klicken Sie zum Hinzufügen einer Adresse für das neue statische Ziel auf das Ziel in der Liste und geben Sie die Adresse ein.

5 (Optional) Sie können die Portnummer des neuen statischen Ziels ändern, indem Sie auf das Textfeld **Port** des Ziels klicken und die neue Portnummer eingeben.

6 (Optional) Sie können die Einstellungen für das statische Ziel bearbeiten, indem Sie das neue Ziel aus der Liste mit den verfügbaren Zielen auswählen, auf **Einstellungen bearbeiten** klicken, die zu ändernden Parameter konfigurieren und auf **Speichern** klicken.

7 (Optional) Sie können ein bestimmtes Ziel löschen, indem Sie das Ziel auswählen und auf **Statisches Ziel entfernen** klicken.

   Das Ziel wird nun nicht mehr in der Liste mit den vorhandenen statischen Zielen angezeigt.

8 Klicken Sie auf **Konfiguration speichern**.

Einrichten eines dynamischen Ziels im VMware Host Client

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

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 die Parameter ändern möchten, entfernen Sie das vorhandene System und fügen Sie ein neues hinzu.

Voraussetzungen

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

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.

2 Klicken Sie auf **Dynamisches Ziel hinzufügen**.

   Das neue dynamische Ziel wird in der Liste angezeigt.

3 Klicken Sie zum Hinzufügen einer Adresse für das neue dynamische Ziel auf das Ziel in der Liste und geben Sie die Adresse ein.

4 (Optional) Sie können die Portnummer des neuen dynamischen Ziels ändern, indem Sie auf das Textfeld **Port** des Ziels klicken und die neue Portnummer eingeben.

5 (Optional) Sie können die Einstellungen für das dynamische Ziel bearbeiten, indem Sie das neue Ziel aus der Liste mit den verfügbaren Zielen auswählen, auf **Einstellungen bearbeiten** klicken, die zu ändernden Parameter konfigurieren und auf **Speichern** klicken.

6 (Optional) Sie können ein bestimmtes Ziel löschen, indem Sie das Ziel auswählen und auf **Dynamisches Ziel entfernen** klicken.

   Das Ziel wird nun nicht mehr in der Liste mit den vorhandenen dynamischen Zielen angezeigt.

7 Klicken Sie auf **Konfiguration speichern**.

Bearbeiten erweiterter Einstellungen für iSCSI im VMware Host 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 Einstellungsänderungen verfügen.

Voraussetzungen

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

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.

2 Klicken Sie auf **Erweiterte Einstellungen**, um die gesamte Liste der Einstellungen anzuzeigen.

3 Bearbeiten Sie die zu ändernden Parameter und klicken Sie auf **Konfiguration speichern**.

Einrichten der CHAP-Authentifizierung für einen iSCSI-Adapter im VMware Host 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 die Anzahl von 511 alphanumerischen Zeichen nicht überschreiten und der CHAP-Schlüssel darf die Anzahl von 255 alphanumerischen Zeichen nicht überschreiten. Einige Adapter, z. B. der QLogic-Adapter, haben möglicherweise niedrigere Grenzen: 255 für den CHAP-Namen und 100 für den CHAP-Schlüssel.

Voraussetzungen

- Legen Sie fest, ob Sie unidirektionales CHAP, auch als normales CHAP bezeichnet, oder wechselseitiges CHAP konfigurieren, bevor Sie die CHAP-Parameter für Software-iSCSI oder abhängige Hardware-iSCSI einrichten. Abhängige Hardware-iSCSI-Adapter unterstützen das wechselseitige 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 wechselseitiges CHAP verschiedene Schlüssel.

  Stellen Sie beim Konfigurieren von CHAP-Parametern sicher, dass sie mit den Parametern auf der Speicherseite übereinstimmen.
- Erforderliche Berechtigungen: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter** und auf **iSCSI konfigurieren**.
2. Erweitern Sie zur Konfiguration von unidirektionalem CHAP die Option **CHAP-Authentifizierung**, um alle Parameter anzuzeigen.
   a. Wählen Sie die CHAP-Sicherheitsstufe.
   b. Geben Sie den CHAP-Namen ein.

      Stellen Sie sicher, dass der Name, den Sie eingeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.
   c. Geben Sie einen Schlüssel für das unidirektionale CHAP ein, der für die Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.
3. Wählen Sie für die Konfiguration von wechselseitigem CHAP die Option **CHAP verwenden** für den unidirektionalen CHAP aus. Erweitern Sie **Wechselseitige CHAP-Authentifizierung**, um alle Parameter anzuzeigen.
   a. Wählen Sie die Option **CHAP verwenden** aus.
   b. Geben Sie den Namen für wechselseitiges CHAP ein.
   c. Geben Sie den Schlüssel für wechselseitiges CHAP an.

      Verwenden Sie für unidirektionales CHAP und wechselseitiges CHAP verschiedene Schlüssel.
4. Klicken Sie auf **Konfiguration speichern**.

Ergebnisse

Wenn Sie die Authentifizierungseinstellungen für einen iSCSI-Adapter ändern, verwenden Sie nur die aktualisierten Anmeldedaten für neue iSCSI-Sitzungen. Bereits vorhandene Sitzungen bleiben

bestehen, bis die Verbindung aufgrund eines äußeren Einflusses wie etwa eine erzwungene erneute Authentifizierung verloren geht oder bis Sie die iSCSI-Ziele des Adapters entfernen und hinzufügen.

Verwalten von Speichergeräten im VMware Host Client

Sie können mit dem VMware Host Client die lokalen und Netzwerkspeichergeräte verwalten, auf die der verwaltete ESXi-Host Zugriff hat.

Anzeigen von Speichergeräten im VMware Host Client

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

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

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Geräte**.

   Alle für den Host verfügbaren Speichergeräte werden unter **Speichergeräte** aufgeführt.
2. Wählen Sie ein Gerät in der Liste aus, um Details zu diesem Gerät anzuzeigen.

Löschen einer Gerätepartitionstabelle im VMware Host Client

Wenn Sie mit dem VMware Host Client bei einem ESXi-Host angemeldet sind, können Sie die Partitionstabelle eines Festplattengeräts löschen, auf die vom Host aus zugegriffen werden kann.

Voraussetzungen

Vergewissern Sie sich, dass das Gerät nicht von ESXi als Startfestplatte, VMFS-Datenspeicher oder vSAN verwendet wird.

Verfahren

1. Klicken Sie im VMware Host Client auf **Speicher** und anschließend auf **Geräte**.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät in der Liste und klicken Sie anschließend auf **Partitionstabelle löschen** und **Ja**.

   Durch Löschen der Partitionstabelle können Daten verloren gehen.

Bearbeiten einzelner Gerätepartitionen im VMware Host Client

Wenn Sie sich mit dem VMware Host Client bei einem ESXi-Host anmelden, können Sie einzelne Partitionen eines Geräts mithilfe des Partitions-Editors entfernen.

Voraussetzungen

Vergewissern Sie sich, dass das Gerät nicht von ESXi als Startfestplatte, VMFS-Datenspeicher oder vSAN verwendet wird.

Verfahren

1. Klicken Sie im VMware Host Client auf **Speicher** und anschließend auf **Geräte**.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät in der Liste und wählen Sie **Partitionen bearbeiten**.
3. Wählen Sie eine Partition aus und klicken Sie auf **Partition löschen**.
4. (Optional) Klicken Sie auf **Zurücksetzen**, um die ursprünglichen Partitionen wiederherzustellen.
5. Klicken Sie auf **Partitionen speichern**.
6. Bestätigen Sie, dass Sie die Partition ändern möchten.

Verwalten von persistentem Arbeitsspeicher

ESXi 6.5 unterstützt die neueste Technologie für den Arbeitsspeicher des Computers, die als nicht flüchtiger Arbeitsspeicher (Non-Volatile Memory, NVM) oder persistenter Arbeitsspeicher (PMem) bezeichnet wird. Bei PMem wird die hohe Datenübertragungsrate des flüchtigen Arbeitsspeichers des Computers mit der Persistenz und Stabilität des herkömmlichen Speichers kombiniert. PMem-Geräte weisen eine niedrige Zugriffslatenz auf und können gespeicherte Daten über Neustarts oder Stromausfälle hinweg beibehalten.

Modi des Verbrauchs der persistenten Arbeitsspeicherressourcen des Hosts

Wenn Sie einem Host ein physisches PMem-Gerät hinzufügen, erkennt ESXi die PMem-Ressource und macht sie als hostlokalen PMem-Datenspeicher für die virtuellen Maschinen verfügbar, die auf dem Host ausgeführt werden. Je nach Gastbetriebssystem können virtuelle Maschinen direkt auf die PMem-Ressourcen zugreifen.

Jeder Host kann nur über einen lokalen PMem-Datenspeicher verfügen, der alle PMem-Ressourcen des Hosts zusammenlegt und darstellt.

Persistenter Arbeitsspeicher kombiniert die Eigenschaften von Arbeitsspeicher und Speicher. Daher können virtuelle Maschinen die PMem-Ressourcen des ESXi-Hosts als Arbeitsspeicher (über virtuelle NVDIMM-Geräte) oder als Speicher (über virtuelle PMem-Festplatten) verbrauchen.

Der hostlokale PMem-Datenspeicher speichert alle NVDIMM-Geräte mit direktem Zugriff und alle virtuellen PMem-Festplatten.

Virtueller PMem (vPMem)

Wenn das Gastbetriebssystem in diesem Modus PMem-fähig ist, kann die virtuelle Maschine direkten Zugriff auf die physischen PMem-Ressourcen des Hosts haben und diese als standardmäßigen byteaddressierbaren Arbeitsspeicher verwenden.

Virtuelle Maschinen verwenden NVDIMMs für den direkten Zugriff auf PMem. Das NVDIMM ist ein Arbeitsspeichergerät, das sich auf einem normalen Speicherkanal befindet, aber nicht flüchtigen Arbeitsspeicher enthält. In vSphere 6.5 handelt es sich bei virtuellem NVDIMM um einen neuen Gerätetyp, der die physischen PMem-Regionen des Hosts darstellt. Eine einzelne virtuelle Maschine kann über maximal 64 virtuelle NVDIMM-Geräte verfügen. Jedes NVDIMM-Gerät ist in einem hostlokalen PMem-Datenspeicher gespeichert.

Hinweis Zum Zuweisen einer virtuellen Maschine zu einem NVDIMM-Gerät muss die virtuelle Maschine Hardwareversion 14 aufweisen, und das Gastbetriebssystem muss persistenten Arbeitsspeicher unterstützen. Wenn das Gastbetriebssystem nicht PMem-fähig ist, können Sie PMem weiterhin verwenden. Der virtuellen Maschine kann jedoch kein NVDIMM-Gerät hinzugefügt werden.

Virtuelle PMem-Festplatten (vPMemDisk)

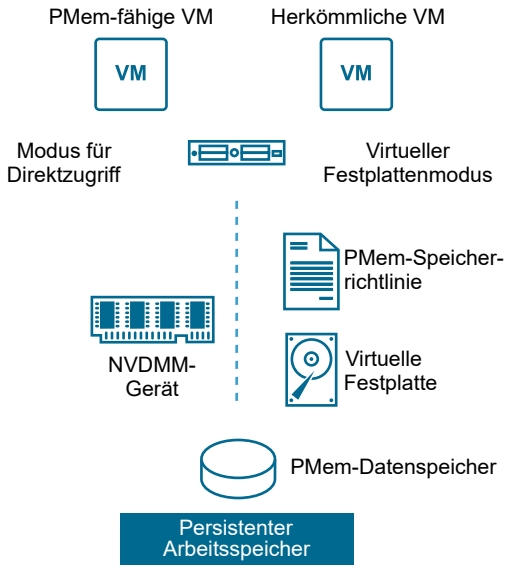
In diesem Modus verfügt die virtuelle Maschine nicht über direkten Zugriff auf die PMem-Ressourcen des Hosts.

Sie müssen der virtuellen Maschine eine virtuelle PMem-Festplatte hinzufügen. Eine virtuelle PMem-Festplatte ist eine herkömmliche SCSI-Festplatte, auf die die PMem-Speicherrichtlinie angewendet wird. Die Richtlinie platziert die Festplatte automatisch im hostlokalen PMem-Datenspeicher.

In diesem Nutzungsmodus sind keine Anforderungen für die Hardwareversion der virtuellen Maschine und des Gastbetriebssystems vorhanden.

Hinweis Wenn das Gastbetriebssystem nicht PMem-fähig ist, können virtuelle Maschinen PMem nur über vPMemDisks verwenden.

Das folgende Diagramm veranschaulicht, wie die Komponenten des persistenten Arbeitsspeichers interagieren.



Weitere Informationen zum Konfigurieren und Verwalten von virtuellen Maschinen mit NVDIMMs oder virtuellen Festplatten für persistenten Arbeitsspeicher finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Struktur des PMem-Datenspeichers

Die VMware Host Client-Benutzerschnittstelle enthält Informationen über die komplexe Struktur des lokalen PMem-Datenspeichers auf dem Host. Um diese Informationen zu analysieren und zu Fehlerbehebungs- und Verwaltungszwecken zu nutzen, müssen Sie sich mit den Konzepten dieser komplexen Infrastruktur auskennen.

Module

Auf der VMware Host Client-Benutzeroberfläche stellen Module die physischen NVDIMMs dar, die mit der Hauptplatine des Hosts verbunden sind.

Im VMware Host Client können Sie den Systemzustand aller Module überprüfen und fehlerhafte NVDIMM-Module erkennen.

Interleave-Sätze

Interleave-Sätze sind logische Gruppierungen eines oder mehrerer Module. Interleave-Sätze geben an, wie Informationen über die physischen DIMMs verteilt werden und wie ESXi die Informationen aus den Modulen liest. Da ESXi abwechselnd aus jedem Interleave-Satz liest, garantieren Interleave-Sätze einen höheren Speicherdurchsatz.

Besteht ein Interleave-Satz beispielsweise aus zwei Modulen, liest ESXi die Informationen gleichzeitig aus beiden physischen DIMMs und fährt dann mit dem nächsten Interleave-Satz fort.

Die VMware Host Client-Benutzerschnittstelle enthält Informationen darüber, wie NVDIMMs in Interleave-Sätzen zusammengefasst werden.

Namespaces

Namespaces sind Bereiche zusammenhängend angesprochenen Speichers im NVDIMM. Namespaces können Interleave-Sätze überlappen. Der PMem-Datenspeicher wird zusätzlich zu den Namespaces erstellt.

Im VMware Host Client können Sie die Kapazität, den Systemzustand und die Speicherort-ID aller Namespaces anzeigen.

Anzeigen von Informationen zu Modulen, Interleave-Sätzen und Namespaces im VMware Host Client

Im VMware Host Client können Sie Informationen zu den Modulen, Interleave-Sätzen und Namespaces des lokalen PMem-Datenspeichers des Hosts anzeigen. Folglich können Sie ein problembehaftetes Modul schnell erkennen und eine Fehlerbehebung durchführen.

Die meisten herkömmlichen Datenspeicherverwaltungsaufgaben können im PMem-Datenspeicher des lokalen Hosts nicht durchgeführt werden. Zu Fehlerbehebungszwecken können Sie die Informationen über Module, Interleave-Sätze und Namespaces jedoch verwenden.

Voraussetzungen

Stellen Sie sicher, dass der Host über mindestens ein physisches NVDIMM-Gerät verfügt.

Verfahren

1. Klicken Sie im Fensterbereich **Navigator** auf **Speicher**.
2. Zeigen Sie auf der Registerkarte **Persistenter Speicher** Informationen über den PMem-Datenspeicher des lokalen Hosts an.
   - Klicken Sie auf **Module**, um Informationen zu den NVDIMMs anzuzeigen, aus denen sich der PMem-Datenspeicher zusammensetzt.
   - Klicken Sie auf **Namespaces**, um Informationen zu Namespaces auf den NVDIMMs anzuzeigen.
   - Klicken Sie auf **Interleave-Sätze**, um anzuzeigen, wie die Module oder physischen NVDIMMs in Interleave-Sätzen zusammengefasst werden.

Löschen eines Namespace im VMware Host Client

Im VMware Host Client können Sie Namespaces löschen, die nicht von ESXi, sondern von einem Betriebssystem erstellt wurden, das zuvor auf der Hostmaschine installiert war.

Voraussetzungen

- Versetzen Sie den Host in den Wartungsmodus.
- Sichern Sie den Inhalt des Namespace, wenn Sie diesen Inhalt zu einem späteren Zeitpunkt benötigen.

Verfahren

1 Klicken Sie im VMware Host Client auf **Speicher**.

2 Klicken Sie auf der Registerkarte **Persistenter Arbeitsspeicher** auf **Namespaces**.

3 (Optional) Überprüfen Sie in der Liste der Namespaces die Spalte „Status“, um die derzeit von ESXi verwendeten Namespaces zu ermitteln.

   Zur Freigabe von Speicherplatz müssen Sie Namespaces löschen, deren Status „In Gebrauch“ lautet.

4 Wählen Sie einen Namespace aus und klicken Sie auf das Symbol **Löschen**.

   Wichtig Durch Löschen eines Namespace wird Speicherplatz im Datenspeicher freigegeben. Sie können den freien Speicherplatz jedoch erst nutzen, wenn Sie den Host neu starten.

5 Klicken Sie auf das Symbol **Host neu starten**, um den Host neu starten.

Ergebnisse

Der ausgewählte Namespace wird aus dem PMem-Datenspeicher gelöscht. ESXi erstellt automatisch einen neuen Namespace, der vom PMem-Datenspeicher verwendet werden kann. Der neue Namespace verfügt über dieselbe Kapazität, denselben Typ und dieselbe Speicherort-ID wie der gelöschte Namespace.

Überwachen des Speichers im VMware Host Client

Sie können im VMware Host Client, den Speicherzustand des ESXi-Hosts überwachen, den Sie verwalten. Des Weiteren können Sie Ereignisse und Aufgaben im Zusammenhang mit den verschiedenen Datenspeichern, Speicheradaptern und Speichergeräten auf dem verwalteten Host anzeigen.

Überwachen von Datenspeichern im VMware Host Client

Sie können in VMware Host Client den Zustand eines Datenspeichers und damit verbundene Ereignisse und Aufgaben überwachen. Ab vSphere 6.5 Update 1 und nach der Aktivierung des vSAN-Diensts im vSphere Client können Sie auch Ihre vSAN-Umgebung überwachen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher**.

2 Klicken Sie auf **Datenspeicher**.

3 Wählen Sie einen Datenspeicher aus der Liste aus.

   Der Datenspeicher wird in der VMware Host Client-Bestandsliste erweitert.

4 Klicken Sie unter dem Namen des Datenspeichers auf **Überwachen**.

5 (Optional) Klicken Sie auf **Ereignisse**, um Ereignisse zum Datenspeicher anzuzeigen.

6 (Optional) Klicken Sie auf **vSAN**, um die Konfigurationsparameter der vSAN-Umgebung Ihres Hosts anzuzeigen.

7 (Optional) Klicken Sie auf **Hosts**, um die in diesem Datenspeicher enthaltenen Hosts anzuzeigen.

8 (Optional) Klicken Sie auf **Systemzustand**, um Details zum Status verschiedener Parameter anzuzeigen, wie z. B. **Leistungsdienst**, **Netzwerk**, **Physische Festplatte**, **Daten**, **Cluster** und **Grenzwerte**.

Überwachen von vSAN auf dem VMware Host Client

Sie können den VMware Host Client zur Überwachung der vSAN-Umgebung des ESXi-Hosts verwenden.

vSAN-Konzepte

VMware vSAN verwendet einen softwaredefinierten Ansatz zum Erstellen von gemeinsam genutztem Speicher für virtuelle Maschinen. Die Lösung virtualisiert die lokalen physischen Speicherressourcen der ESXi-Hosts. Sie wandelt diese auch in Speicherpools um, die aufgeteilt und virtuellen Maschinen und Anwendungen gemäß deren Quality-of-Service-Anforderungen zugewiesen werden können. vSAN wird direkt in den ESXi-Hypervisor implementiert.

Sie können vSAN so konfigurieren, dass es als Hybrid- oder All-Flash-Cluster verwendet wird. In Hybrid-Clustern werden Flash-Geräte für die Cache-Ebene verwendet. Magnetische Festplatten werden hingegen für die Speicherkapazitätsschicht verwendet. In Alle-Flash-Clustern werden Flash-Geräte als Zwischenspeicher und Kapazität verwendet.

Sie können vSAN auf Ihren vorhandenen Host-Clustern und beim Erstellen neuer Cluster aktivieren.

Wenn vSAN auf den automatischen Modus eingestellt ist, fasst vSAN alle freien lokalen Kapazitätsgeräte zu einem einzigen Datenspeicher zusammen, der von allen Hosts im vSAN-Cluster gemeinsam genutzt wird. vSAN kann keine Geräte verwenden, die formatiert sind und bereits einige Informationen enthalten.

Wenn vSAN auf den manuellen Modus eingestellt ist, verwendet vSAN die lokalen Kapazitätsgeräte, die Sie mithilfe von vSphere Client beansprucht haben. Wenn Sie keine Geräte über den vSphere Client beansprucht haben, beträgt die Größe des vSAN-Datenspeichers 0 MB.

Sie können den Datenspeicher erweitern, indem Sie dem Cluster Kapazitätsgeräte oder Hosts mit Kapazitätsgeräten hinzufügen. vSAN funktioniert am besten, wenn alle ESXi-Hosts im Cluster bei allen Clustermitgliedern ähnliche oder identische Konfigurationen verwenden, einschließlich ähnlicher oder identischer Speicherkonfigurationen. Mit dieser konsistenten Konfiguration werden ausgeglichene Speicherkomponenten der virtuellen Maschine auf allen Geräten und Hosts im Cluster sichergestellt. Auch Hosts ohne lokale Geräte können teilnehmen und ihre virtuellen Maschinen im Datenspeicher von vSAN ausführen.

Wenn ein Host seine lokalen Speichergeräte zum vSAN-Datenspeicher beiträgt, muss der Host mindestens ein Gerät für Flash-Cache und mindestens ein Gerät für Kapazität bereitstellen. Kapazitätsgeräte werden auch als Datenfestplatten bezeichnet.

Die Geräte auf dem beitragenden Host bilden eine oder mehrere Festplattengruppen. Jede Festplattengruppe enthält ein Flash-Zwischenspeichergerät und ein oder mehrere Kapazitätsgeräte für dauerhaften Speicher. Jeder Host kann für die Verwendung mehrerer Festplattengruppen konfiguriert werden.

Informationen zu Best Practices, Überlegungen zur Kapazität und allgemeine Empfehlungen in Bezug auf das Entwerfen und Dimensionieren eines vSAN-Clusters finden Sie im *Handbuch für VMware Virtual SAN Design und Sizing*.

Merkmale von vSAN

In diesem Kapitel werden die Merkmale von vSAN, den zugehörigen Clustern und Datenspeichern zusammengefasst.

vSAN bietet zahlreiche Vorteile für Ihre Umgebung.

Tabelle 4-1. Funktionen von vSAN

Unterstützte Funktionen	Beschreibung
Unterstützung von gemeinsam genutztem Speicher	vSAN unterstützt VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, wie HA, vMotion und DRS. Beispiel: Wenn ein Host überlastet wird, kann DRS die virtuellen Maschinen zu anderen Hosts im Cluster migrieren.
On-Disk-Format	Das vSAN-Format für virtuelle Festplattendateien unterstützt für jeden vSAN-Cluster eine stark skalierbare Snapshot- und Klonverwaltung. Informationen zur Anzahl der je vSAN-Cluster unterstützten VM-Snapshots und -Klone finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*.
Reine Flash- und Hybrid-Konfigurationen	vSAN kann für reine Flash- oder Hybrid-Cluster konfiguriert werden.
Fehlerdomänen	vSAN unterstützt das Konfigurieren von Fehlerdomänen, um Hosts vor Rack- oder Gehäuseausfällen zu schützen, wenn der vSAN-Cluster sich über mehrere Racks oder Blade-Server-Gehäuse in einem Datencenter erstreckt.
iSCSI-Zieldienst	Mit dem iSCSI-Zieldienst von vSAN können Hosts und physische Arbeitslasten, die sich außerhalb des vSAN-Clusters befinden, auf den vSAN-Datenspeicher zugreifen.
Stretched Cluster	vSAN unterstützt Stretched Cluster, die sich über zwei geografische Standorte erstrecken.

Tabelle 4-1. Funktionen von vSAN (Fortsetzung)

Unterstützte Funktionen	Beschreibung
Unterstützung für Windows Server Failover Cluster (WSFC)	vSAN 6.7 Update 3 und höher bietet Unterstützung für dauerhafte SCSI-3-Reservierungen (SCSI-3 Persistent Reservations, SCSI3-PR) auf der Ebene einer virtuellen Festplatte, die von Windows Server Failover Cluster (WSFC) benötigt wird, um Zugriff auf eine gemeinsame Festplatte zwischen Knoten zu vermitteln. Aufgrund der Unterstützung von SCSI-3 PRs kann WSFC mit einer Festplattenressource konfiguriert werden, die zwischen VMs auf vSAN-Datenspeichern nativ freigegeben wird. Aktuell werden die folgenden Konfigurationen unterstützt: ■ Maximal 6 Anwendungsknoten pro Cluster. ■ Maximal 64 freigegebene virtuelle Festplatten pro Knoten. **Hinweis** Microsoft SQL Server 2012 oder höher unter Microsoft Windows Server 2012 oder höher wurde für vSAN qualifiziert.
vSAN-Integritätsdienst	Der vSAN-Integritätsdienst enthält vorkonfigurierte Tests zur Systemdiagnoseprüfung, um die Ursache von Problemen bei Clusterkomponenten zu überwachen, zu beheben und zu diagnostizieren und um potenzielle Risiken zu erkennen.
vSAN-Leistungsdienst	Der vSAN-Leistungsdienst beinhaltet statistische Diagramme, die zum Überwachen von IOPS, Durchsatz, Latenz und Überlastung verwendet werden. Sie können die Leistung eines Clusters, Hosts, einer Festplattengruppe, einer Festplatte und von VMs von vSAN überwachen.
Integration in vSphere-Speicherfunktionen	vSAN ist in den vSphere-Datenverwaltungsfunktionen integriert, die ursprünglich mit dem VMFS- und NFS-Speicher verwendet wurden. Zu diesen Funktionen gehören Snapshots, verknüpfte Klone und vSphere Replication.
VM-Speicherrichtlinien	vSAN arbeitet mit VM-Speicherrichtlinien, um einen VM-zentrierten Ansatz für die Speicherverwaltung zu unterstützen. Wenn Sie während der Bereitstellung keine Speicherrichtlinie zuweisen, wird der VM automatisch die Standardspeicherrichtlinie für vSAN zugewiesen.
Schnelle Bereitstellung	vSAN ermöglicht eine schnelle Bereitstellung von Speicher in vCenter Server® während der Erstellung und Bereitstellung einer virtuellen Maschine.
Deduplizierung und Komprimierung	vSAN führt Deduplizierung und Komprimierung auf Blockebene durch, um Speicherplatz zu sparen. Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-All-Flash-Cluster aktivieren, werden redundante Daten innerhalb jeder Festplattengruppe reduziert. Deduplizierung und Komprimierung sind als clusterweite Einstellung aktiviert, die Anwendung der Funktionen erfolgt jedoch auf Festplattengruppenbasis. vSAN nur mit Komprimierung wird auf Festplattenebene angewendet.

Tabelle 4-1. Funktionen von vSAN (Fortsetzung)

Unterstützte Funktionen	Beschreibung
Verschlüsselung ruhender Daten	vSAN bietet Verschlüsselung ruhender Daten. Die Daten werden verschlüsselt, nachdem alle anderen Verarbeitungsvorgänge, z. B. die Deduplizierung, durchgeführt wurden. Die Verschlüsselung ruhender Daten schützt Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.
SDK-Unterstützung	Das VMware vSAN SDK für Java stellt eine Erweiterung des VMware vSphere Management SDK dar. Es enthält die Dokumentation, Bibliotheken und Codebeispiele, mit denen Entwickler die Installation, Konfiguration, Überwachung und Fehlerbehebung von vSAN automatisieren können.

Überwachen von vSAN im VMware Host Client

Sie können den VMware Host Client zur Überwachung der vSAN-Umgebung des ESXi-Hosts verwenden.

Voraussetzungen

Der vSAN-Dienst muss im vSphere Client aktiviert werden, bevor Sie die vSAN-bezogenen Bildschirme für einen Datenspeicher anschauen können.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher**.
2. Klicken Sie auf der Registerkarte **Datenspeicher** auf **vSAN-Datenspeicher**.

   Der vSAN-Datenspeicher wird im VMware Host Client-Navigator erweitert.
3. Klicken Sie auf **Überwachen**.

   Die Registerkarten **vSAN**, **Host** und **Systemzustand** werden auf der Benutzeroberfläche angezeigt.

Option	Beschreibung
vSAN	Zeigt die Konfigurationen für den aktuellen Host an. Sie können die Einstellungen für den Beanspruchungsmodus und die Deduplizierung ändern. Zudem können Sie die folgenden Einstellungen ansehen: ■ Verschlüsselung – vSAN unterstützt die Verschlüsselung der Informationen für den gesamten vSAN-Datenspeicher. ■ ISCSI-Dienst – Zusätzlicher Dienst über den iSCSI-Dienst. ■ Leistungsdienst - Sammelt Daten zur Funktionsweise des Datenspeichers. Beispiel: die Geschwindigkeit eines Lese-/Schreibvorgangs.
Hosts	Zeigt eine Liste aller Hosts auf dem vSAN-Server zusammen mit der jeweiligen IP-Adresse und der Fault Domain, der der Host angehört.
Systemzustand	Die Registerkarte **Systemzustand** enthält Tests, die in Gruppen organisiert sind. Die folgenden Gruppen werden angezeigt: ■ Leistungsdienst ■ Netzwerk ■ Physische Festplatte ■ Daten ■ Cluster ■ Grenzwerte Jede Gruppe weist eines der folgenden Statussymbole auf: Fehler, Warnung, Unbekannt oder ordnungsgemäßer Zustand. Der Status der Gruppe stellt den schwerwiegendsten Zustand des Tests dieser Gruppe dar. Um die Tests und ihre Beschreibungen anzuzeigen, klicken Sie auf das Erweiterungssymbol in der oberen rechten Ecke der jeweiligen Gruppe. Auf der erweiterten Karte können Sie alle Tests der Gruppe und deren Ergebnisse überprüfen und weitere Informationen darüber anzeigen lassen, was bei jedem Test auf dem System untersucht wird.

4 Wählen Sie den vSAN-Parameter aus, den Sie überwachen möchten.

Bearbeiten der Einstellungen für einen vSAN-Datenspeicher

Sie können die Einstellungen für einen vSAN-Datenspeicher bearbeiten, wenn Sie einen fehlkonfigurierten Status des aktuellen Hosts beenden müssen.

Sie können nur die vSAN-Datenspeichereinstellungen **Beanspruchungsmodus** und **Deduplizierung** bearbeiten. Diese Änderungen werden nur auf dem aktuellem Host wirksam. Sie sind nicht mit den anderen am vSAN-Cluster beteiligten Hosts synchronisiert.

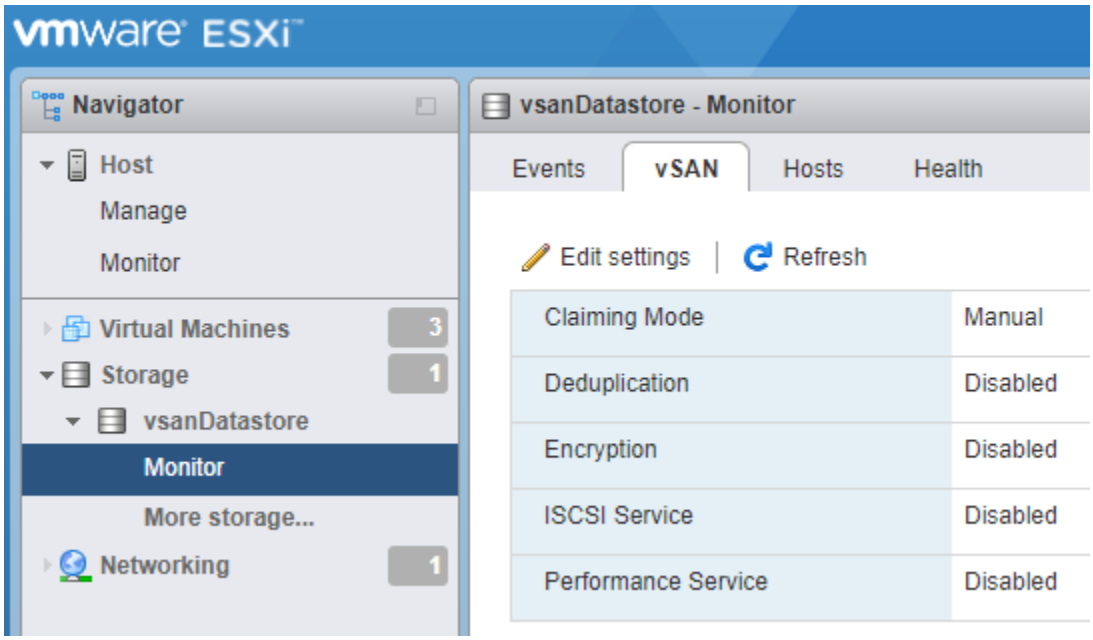
Hinweis Verwenden Sie diese Einstellungen nur für die Fehlerbehebung.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher**.

2 Klicken Sie auf der Registerkarte **Datenspeicher** auf einen vSAN-Datenspeicher in der Tabelle.

3 Klicken Sie auf **Überwachen** und dann auf die Registerkarte **vSAN**.



4 Klicken Sie auf **Einstellungen bearbeiten**.

Das Dialogfeld **Einstellungen bearbeiten** wird geöffnet.

5 Ändern Sie die Einstellungen. Wählen Sie **Auto** oder **Manuell** unter **Beanspruchungsmodus** aus.

Option	Aktion
Beanspruchungsmodus	a Wählen Sie unter **Beanspruchungsmodus** entweder **Auto** oder **Manuell** aus. ■ Wenn Sie **Auto** auswählen, werden automatisch alle Festplatten genommen und in einer Gruppe bzw. in Gruppen der gleichen Größe beansprucht. **Hinweis** Der Modus **Auto** ist veraltet. Er kann nur hybride Festplattengruppen belegen, die mit den meisten vSAN-Funktionen nicht kompatibel sind. ■ Wenn Sie die Option **Manuell** auswählen, müssen Sie die Festplatten in Gruppen manuell organisieren und sie mit dem vSphere Web Client zurückfordern. Beispielsweise ist die Auswahl des manuellen Beanspruchungsmodus geeignet, wenn der vCenter Server nicht verfügbar ist.
Deduplizierung	a Wählen Sie unter **Deduplizierung** entweder **Aktiviert** oder **Deaktiviert** aus.

6 Klicken Sie auf **Speichern**.

Durchführen von Vorgängen zum Aktualisieren und zum erneuten Scannen im VMware Host Client

Mit dem Aktualisierungsvorgang für Datenspeicher, Speichergeräte und Speicheradapter werden die Listen und Speicherinformationen im VMware Host Client aktualisiert. Es werden Informationen wie beispielsweise die Kapazität des Datenspeichers aktualisiert. Wenn Sie Datenspeichermanagementaufgaben durchführen oder Änderungen an der SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut scannen.

Durchführen eines erneuten Scans von Adaptern im VMware Host Client

Wenn Sie Änderungen an Ihrer SAN-Konfiguration vornehmen und diese Änderungen auf Speicher beschränken, auf die über einen bestimmten Adapter zugegriffen wird, führen Sie einen erneuten Scan nur dieses Adapters durch. Wenn Sie einen Adapter neu scannen, finden Sie neue LUNs, die darin verfügbar sind.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Adapter**.
2. Klicken Sie auf **Erneut scannen**.

Durchführen eines erneuten Scans von Geräten im VMware Host Client

Wenn Sie ein Gerät neu scannen, finden Sie neue VMFS-Volumes, die darauf verfügbar sind.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Speicher** und anschließend auf **Geräte**.
2. Klicken Sie auf **Erneut scannen**.

Ändern der Anzahl gescannter Speichergeräte im VMware Host Client

Der Bereich gescannter LUN-IDs für einen ESXi-Host liegt zwischen 0 und 16.383. ESXi ignoriert LUN-IDs ab 16.383. Der konfigurierbare Parameter `Disk.MaxLUN` steuert den Bereich gescannter LUN-IDs. Der Parameter hat den Standardwert 1024.

Der Parameter `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 1 und 100 vorhanden sind, legen Sie den Wert auf 101 fest. Folglich können Sie die Geschwindigkeit der Geräteerkennung für Ziele ohne Unterstützung von REPORT_LUNS 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 und der Auslastung des Speichersystems.

In anderen Situationen müssen Sie möglicherweise diesen Wert erhöhen, wenn in Ihrer Umgebung LUN-IDs über 1023 hinaus verwendet werden.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Verwalten** und anschließend auf **Erweiterte Einstellungen**.
2. Blättern Sie nach unten zu `Disk.MaxLUN`.
3. Klicken Sie mit der rechten Maustaste auf `Disk.MaxLUN` und klicken Sie dann auf **Option bearbeiten**.
4. Geben Sie einen neuen Wert ein und klicken Sie auf **Speichern**.

   Der SCSI-Scancode scannt keine LUNs mit IDs, die größer oder gleich dem eingegebenen Wert sind.

   Wenn Sie beispielsweise nach LUN-IDs von 0 bis 100 suchen möchten, setzen Sie `Disk.MaxLUN` auf „101.

Netzwerke im VMware Host Client

5

Wenn Sie mit dem VMware Host Client eine Verbindung zu einem ESXi-Host herstellen, können Sie vSphere Standard-Switches, Portgruppen, physische Netzwerkkarten, VMkernel-Netzwerkkarten und TCP/IP-Stacks anzeigen und konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

Verwalten von Portgruppen im VMware Host Client

Sie können Portgruppen-Einstellungen verwalten, um die Datenverkehrsverwaltung zu konfigurieren, die Netzwerksicherheit zu erhöhen und die Leistung zu verbessern. Mithilfe des VMware Host Client können Sie Portgruppen hinzufügen und entfernen. Sie können auch Portgruppeninformationen prüfen und Portgruppeneinstellungen bearbeiten, z. B. NIC-Gruppierung und Traffic Shaping.

Anzeigen von Informationen zu Portgruppen im VMware Host Client

Sie können im VMware Host Client Informationen zur Konfiguration von Portgruppen, Netzwerkdetails, der Topologie von virtuellen Switches, der Netzwerkkarten-Gruppierungsrichtlinien, Offload-Richtlinien und Sicherheitsrichtlinien anzeigen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Portgruppen**.

2 Klicken Sie in der Liste der verfügbaren Portgruppen auf ein Element.

Es werden Informationen zu Netzwerkdetails, der Topologie von virtuellen Switches, der Netzwerkkarten-Gruppierungsrichtlinien, Offload-Richtlinien und Sicherheitsrichtlinien angezeigt.

Hinzufügen einer Portgruppe für virtuellen Switch im VMware Host Client

Sie können einem virtuellen Switch im VMware Host Client eine Portgruppe hinzufügen. Portgruppen stellen virtuellen Maschinen das Netzwerk bereit.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Netzwerke** und wählen Sie im Popup-Menü **Portgruppe hinzufügen** aus.

2 Geben Sie einen Namen für die neue Portgruppe ein.

3 Legen Sie die VLAN-ID fest, um die VLAN-Handhabung in der Portgruppe zu konfigurieren.

Die VLAN-ID spiegelt auch den VLAN-Tagging-Modus in der Portgruppe wider.

VLAN-Tagging-Modus	VLAN-ID	Beschreibung
External Switch Tagging (EST)	0	Der virtuelle Switch übermittelt keinen Datenverkehr im Zusammenhang mit einem VLAN.
Virtual Switch Tagging (VST)	Zwischen 1 und 4094	Der virtuelle Switch kennzeichnet den Datenverkehr mit dem eingegebenen Tag.
Virtual Guest Tagging (VGT)	4095	VLANs werden von virtuellen Maschinen abgewickelt. Der virtuelle Switch ermöglicht Datenverkehr über jedes VLAN.

4 Wählen Sie im Dropdown-Menü einen virtuellen Switch aus.

5 Erweitern Sie **Sicherheit** und wählen Sie die Optionen aus, die Sie für den Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen aktivieren möchten.

6 Klicken Sie auf **Hinzufügen**.

Die Portgruppe wird erstellt.

7 (Optional) Durch Klicken auf **Aktualisieren** wird die neue Portgruppe in der Liste angezeigt.

Bearbeiten von Portgruppen-Einstellungen im VMware Host Client

Zur Erhöhung der Netzwerksicherheit und Verbesserung der Netzwerkleistung im VMware Host Client können Sie verschiedene Portgruppen-Einstellungen wie den Namen der Portgruppe, die VLAN-ID und den virtuellen Switch bearbeiten. Sie können auch Komponenten der Sicherheit, NIC-Gruppierung und des Traffic-Shaping konfigurieren.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Portgruppen**.

2 Klicken Sie mit der rechten Maustaste auf die Portgruppe in der Liste und wählen Sie **Einstellungen bearbeiten**.

3 (Optional) Geben Sie einen neuen Namen für die Portgruppen ein.

4 (Optional) Geben Sie einen neuen Wert für die VLAN-ID ein.

Die VLAN-ID spiegelt den VLAN-Tagging-Modus in der Portgruppe wider.

VLAN-Tagging-Modus	VLAN-ID	Beschreibung
External Switch Tagging (EST)	0	Der virtuelle Switch übermittelt keinen Datenverkehr im Zusammenhang mit einem VLAN.
Virtual Switch Tagging (VST)	Zwischen 1 und 4094	Der virtuelle Switch kennzeichnet den Datenverkehr mit dem eingegebenen Tag.
Virtual Guest Tagging (VGT)	4095	VLANs werden von virtuellen Maschinen abgewickelt. Der virtuelle Switch ermöglicht Datenverkehr über jedes VLAN.

5 (Optional) Wählen Sie im Dropdown-Menü einen virtuellen Switch aus.

6 (Optional) Erweitern Sie **Sicherheit** und geben Sie an, ob die Sicherheitsrichtlinienausnahmen abgelehnt, akzeptiert oder aus vSwitch übernommen werden sollen.

Option	Beschreibung
Promiscuous-Modus	■ **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. ■ **Aus vSwitch übernehmen**. Bei Aktivierung des Promiscuous-Modus für den Gastadapter wird die Konfiguration aus dem zugehörigen virtuellen Switch übernommen.
MAC-Adressänderungen	■ **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**. Das Ändern der MAC-Adresse vom Gastbetriebssystem hat die gewünschte Auswirkung: An die neue MAC-Adresse gesendete Frames werden empfangen. ■ **Aus vSwitch übernehmen**. Wenn Sie **MAC-Adressenänderungen** auf **Aus vSwitch übernehmen** einstellen, wird die MAC-Adresse in einen der zugehörigen virtuellen Switches geändert.
Gefälschte Übertragungen	■ **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. ■ **Aus vSwitch übernehmen**. Die Konfiguration für ausgehende Frames wird aus dem zugehörigen virtuellen Switch übernommen.

7 (Optional) Erweitern Sie **NIC-Gruppierung** und konfigurieren Sie die folgenden Komponenten.

Option	Beschreibung
Lastausgleich	Geben Sie an, wie ein Uplink ausgewählt werden soll. ■ **Aus vSwitch übernehmen**. Wählen Sie den Uplink, der für den zugeordneten virtuellen Switch ausgewählt 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. ■ **Anhand der Quelle der Port-ID routen**. Wählen Sie einen Uplink anhand der Quelle der Port-ID. ■ **Ausdrückliche Failover-Reihenfolge verwenden**. Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt. **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.
Netzwerk-Failover-Ermittlung	Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an. ■ ■ **Aus vSwitch übernehmen**. Übernimmt die jeweilige Konfiguration aus dem zugeordneten virtuellen Switch. ■ **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 ein STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ **Nur Signal**. Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können. **Hinweis** Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.

Option	Beschreibung
Switches benachrichtigen	Wählen Sie **Ja**, **Nein** oder **Aus vSwitch übernehmen** aus, um Switches bei einem Failover zu benachrichtigen. Wenn Sie **Ja** wählen, wird, 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 im Team geleitet wird, eine Benachrichtigung über das Netzwerk gesendet, um die Verweistabellen auf den physischen Switches zu aktualisieren. In fast allen Fällen wird dies empfohlen, um die Wartezeiten für Failover-Ereignisse und Migrationen mit vMotion zu minimieren. **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.
Failback	Wählen Sie **Ja**, **Nein** oder **Aus vSwitch übernehmen**, um Failback zu aktivieren bzw. zu deaktivieren. Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf die Standardeinstellung **Ja** gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit wieder 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.
Failover-Reihenfolge	Geben Sie an, wie die Arbeitslast 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: ■ **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. **Hinweis** Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks. Sie können die Failover-Reihenfolge nicht konfigurieren, wenn Portgruppen-Komponenten so konfiguriert sind, dass sie die Konfiguration aus dem zugehörigen virtuellen Switch übernehmen.

8 (Optional) Erweitern Sie zum Konfigurieren von Traffic-Shaping **Traffic-Shaping**, klicken Sie auf **Aktiviert** und geben Sie die folgenden Parameter an.

Option	Beschreibung
Durchschnittliche Bandbreite	Legt die 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 ist die maximale Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung **Durchschnittliche Bandbreite** angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter steht für die maximale Anzahl der Bytes, die im Burst-Bonus angesammelt und mit einer höheren Geschwindigkeit übertragen werden können.

Die Traffic-Shaping-Richtlinien werden auf den Datenverkehr jedes virtuellen Netzwerkadapters angewendet, der an den virtuellen Switch angeschlossen ist.

9 Klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

Entfernen einer Portgruppe für virtuelle Switches im VMware Host Client

Sie können Portgruppen von virtuellen Switches entfernen, wenn Sie die zugewiesenen bezeichneten Netzwerke nicht mehr benötigen.

Voraussetzungen

Stellen Sie sicher, dass keine VMkernel-Netzwerkkarten und keine eingeschalteten virtuellen Maschinen mit der Portgruppe verbunden sind, die Sie entfernen möchten.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf die Registerkarte **Portgruppen**.

2 Klicken Sie mit der rechten Maustaste auf die zu entfernende Portgruppe und wählen Sie **Entfernen** aus dem Popup-Menü aus.

3 Um die Portgruppe zu entfernen, klicken Sie auf **Entfernen**.

4 (Optional) Klicken Sie auf **Überprüfen**, um zu überprüfen, ob die Portgruppe entfernt wurde.

Verwalten von virtuellen Switches im VMware Host Client

Im VMware Host Client können Sie verschiedene Einstellungen für virtuelle Switches konfigurieren, wie etwa Verbindungserkennung, NIC-Gruppierung und Traffic-Shaping.

Anzeigen von Informationen zu virtuellen Switches im VMware Host Client

Sie können im VMware Host Client Informationen zu virtuellen Switches wie Konfiguration, Netzwerkdetails, Topologie virtueller Switches uvm. anzeigen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Virtuelle Switches**.
2. Klicken Sie in der Liste der verfügbaren virtuellen Switches auf einen Switch.

   Es werden Informationen zur Konfiguration, Netzwerkdetails und Topologie des virtuellen Switchs angezeigt.

Hinzufügen eines virtuellen Standard-Switches im VMware Host Client

In VMware Host Client können Sie einen virtuellen Standard-Switch hinzufügen, um Netzwerkkonnektivität für den von Ihnen verwalteten Host und für die virtuellen Maschinen auf diesem Host zu ermöglichen und den VMkernel-Datenverkehr zu regeln. Je nach dem Verbindungstyp, den Sie erstellen möchten, können Sie einen vSphere Standard-Switch mit einem VMkernel-Adapter erstellen, einen vorhandenen physischen Netzwerkadapter mit dem neuen Switch verbinden oder den Switch mit einer Portgruppe der virtuellen Maschine erstellen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Netzwerke** und wählen Sie im Popup-Menü die Option **Standard-vSwitch hinzufügen** aus.
2. (Optional) Klicken Sie auf **Uplink hinzufügen**, um dem virtuellen Switch einen neuen physischen Uplink hinzuzufügen.
3. Geben Sie einen Namen für den virtuellen Switch ein und klicken Sie auf **Virtuellen Switch erstellen**.
4. Wählen Sie einen Uplink für den virtuellen Switch.

5 Erweitern Sie **Verbindungserkennung** und wählen Sie eine Option für den Modus des virtuellen Switches aus.

Vorgang	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch-Port an, jedoch stehen dem Switch-Administrator keine Informationen zum vSphere Standard-Switch zur Verfügung.
Werben	ESXi stellt dem Switch-Administrator Informationen zum vSphere Standard-Switch zur Verfügung, ohne jedoch Informationen zum physischen Switch zu erkennen oder anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch an und stellt dem Switch-Administrator Informationen zum vSphere Standard-Switch zur Verfügung.
Keine	ESXi erkennt keinen verknüpften physischen Switch-Port und zeigt keine Informationen dazu an, und dem Switch-Administrator stehen keine Informationen zum vSphere Standard-Switch zur Verfügung.

6 Wählen Sie im Abschnitt „Protokoll“ im Dropdown-Menü die Option **Cisco Discovery-Protokoll** aus.

7 Erweitern Sie **Sicherheit** und akzeptieren Sie Promiscuous-Modus, MAC-Adressenänderungen und gefälschte Übertragungen für die an den Standard-Switch angeschlossenen virtuellen Maschinen bzw. lehnen Sie diese ab.

Option	Beschreibung
Promiscuous-Modus	■ **Ablehnen**. Der VM-Netzwerkadapter empfängt nur Frames, die an die virtuelle Maschine adressiert sind. ■ **Akzeptieren**. Der virtuelle Switch leitet alle Frames an die virtuellen Maschinen in Übereinstimmung mit der aktiven VLAN-Richtlinie für den Port weiter, mit dem der VM-Netzwerkadapter verbunden ist. **Hinweis** Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.
MAC-Adressänderungen	■ **Ablehnen**. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht (festgelegt in der `.vmx`-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames. ■ **Akzeptieren**. Wenn das Gastbetriebssystem die effektive MAC-Adresse einer virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht, lässt der Switch Frames zu der neuen Adresse passieren.
Gefälschte Übertragungen	■ **Ablehnen**. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine mit einer Quell-MAC-Adresse, die von der Adresse in der `.vmx`-Konfigurationsdatei abweicht. ■ **Akzeptieren**. Der Switch führt keine Filterung durch und lässt alle ausgehenden Frames zu.

8 Klicken Sie auf **Hinzufügen**.

Entfernen eines virtuellen Standard-Switches im VMware Host Client

Sie können den virtuellen Standard-Switch entfernen, wenn Sie ihn nicht mehr benötigen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf die Registerkarte **Virtuelle Switches**.

2 Klicken Sie mit der rechten Maustaste auf den virtuellen Switch, den Sie aus der Liste entfernen möchten, und wählen Sie **Entfernen**.

3 Klicken Sie auf **Ja**.

Hinzufügen eines physischen Uplinks zu einem virtuellen Switch im VMware Host Client

Sie können mit einem einzelnen vSphere Standard-Switch mehrere Adapter verbinden, um Netzwerkkarten-Gruppierung zu bewirken. Die Gruppe kann den Datenverkehr gemeinsam verarbeiten und Ausfallsicherheit gewährleisten.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Virtuelle Switches**.
2. Wählen Sie einen virtuellen Switch aus der Liste aus und klicken Sie auf **Uplink hinzufügen**.
3. Wählen Sie aus den verfügbaren Optionen eine physische Netzwerkkarte aus.
4. Klicken Sie auf **Speichern**.

Bearbeiten von Einstellungen zu virtuellen Switches im VMware Host Client

Im VMware Host Client können Sie Einstellungen von virtuellen Switches bearbeiten, beispielsweise Uplinks von virtuellen Switches.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Virtuelle Switches**.
2. Klicken Sie mit der rechten Maustaste auf den zu bearbeitenden virtuellen Switch und wählen Sie **Einstellungen bearbeiten**.
3. (Optional) Klicken Sie auf **Uplink hinzufügen**, um dem virtuellen Switch einen neuen physischen Uplink hinzuzufügen.
4. Ändern Sie die maximale Übertragungseinheit (Maximum Transmission Unit – MTU).

   Die MTU verbessert die Netzwerkeffizienz, indem die Menge der mit einem einzelnen Paket übertragenen Nutzlastdaten erhöht wird, d. h. Jumbo-Frames aktiviert werden.
5. (Optional) Klicken Sie auf das **Entfernen**-Symbol (⊗), um den alten Uplink aus dem virtuellen Switch zu entfernen.

6 Erweitern Sie **Verbindungserkennung** und wählen Sie eine Option für den Modus des virtuellen Switches aus.

Vorgang	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch-Port an, jedoch stehen dem Switch-Administrator keine Informationen zum vSphere Standard-Switch zur Verfügung.
Werben	ESXi stellt dem Switch-Administrator Informationen zum vSphere Standard-Switch zur Verfügung, ohne jedoch Informationen zum physischen Switch zu erkennen oder anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch an und stellt dem Switch-Administrator Informationen zum vSphere Standard-Switch zur Verfügung.
Keine	ESXi erkennt keinen verknüpften physischen Switch-Port und zeigt keine Informationen dazu an, und dem Switch-Administrator stehen keine Informationen zum vSphere Standard-Switch zur Verfügung.

7 Wählen Sie im Abschnitt „Protokoll“ im Dropdown-Menü die Option **Cisco Discovery-Protokoll** aus.

8 Erweitern Sie **Sicherheit** und akzeptieren Sie Promiscuous-Modus, MAC-Adressenänderungen und gefälschte Übertragungen für die an den Standard-Switch angeschlossenen virtuellen Maschinen bzw. lehnen Sie diese ab.

Option	Beschreibung
Promiscuous-Modus	■ **Ablehnen**. Der VM-Netzwerkadapter empfängt nur Frames, die an die virtuelle Maschine adressiert sind. ■ **Akzeptieren**. Der virtuelle Switch leitet alle Frames an die virtuellen Maschinen in Übereinstimmung mit der aktiven VLAN-Richtlinie für den Port weiter, mit dem der VM-Netzwerkadapter verbunden ist. **Hinweis** Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.
MAC-Adressänderungen	■ **Ablehnen**. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht (festgelegt in der `.vmx`-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames. ■ **Akzeptieren**. Wenn das Gastbetriebssystem die effektive MAC-Adresse einer virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht, lässt der Switch Frames zu der neuen Adresse passieren.
Gefälschte Übertragungen	■ **Ablehnen**. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine mit einer Quell-MAC-Adresse, die von der Adresse in der `.vmx`-Konfigurationsdatei abweicht. ■ **Akzeptieren**. Der Switch führt keine Filterung durch und lässt alle ausgehenden Frames zu.

9 (Optional) Erweitern Sie **NIC-Gruppierung** und konfigurieren Sie die folgenden Komponenten.

Option	Beschreibung
Lastausgleich	Geben Sie an, wie ein Uplink ausgewählt werden soll. ■ **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. ■ **Anhand der Quelle der Port-ID routen**. Wählen Sie einen Uplink anhand der Quelle der Port-ID. ■ **Ausdrückliche Failover-Reihenfolge verwenden**. Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungkriterien erfüllt. **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.
Netzwerk-Failover-Ermittlung	Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an. ■ **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. ■ **Nur Signal**. Sendet Signale, wartet auf Signalprüfpakete 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. **Hinweis** Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.
Switches benachrichtigen	Wählen Sie **Ja**, **Nein** oder **Aus vSwitch übernehmen** für die Benachrichtigung von Switches im Falle eines Failovers. 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, 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. **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.

Option	Beschreibung
Failback	Wählen Sie **Ja**, **Nein** oder **Aus vSwitch übernehmen**, um Failback zu aktivieren bzw. zu deaktivieren. 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.
Failover-Reihenfolge	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: ■ **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. **Hinweis** Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.

10 (Optional) Erweitern Sie zum Konfigurieren von Traffic-Shaping **Traffic-Shaping**, klicken Sie auf **Aktiviert** und geben Sie die folgenden Parameter an.

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 dann mit einer höheren Geschwindigkeit übertragen werden können.

Die Traffic-Shaping-Richtlinien werden auf den Datenverkehr jedes virtuellen Netzwerkadapters angewendet, der an den virtuellen Switch angeschlossen ist.

11 Klicken Sie auf **Speichern**.

Verwalten von physischen Netzwerkadaptern im VMware Host Client

Weisen Sie einem Standard-Switch einen physischen Adapter zu, um Konnektivität für virtuelle Maschinen und VMKernel-Adapter auf dem verwalteten Host bereitzustellen.

Anzeigen von Informationen zu physischen Netzwerkadaptern im VMware Host Client

Sie können im VMware Host Client verschiedene Informationen zu Konfiguration und Einstellungen von physischen Netzwerkadaptern anzeigen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Physische Netzwerkkarten**.
2. Klicken Sie auf den Netzwerkadapter, zu dem Sie Informationen wünschen.

Bearbeiten von physischen Netzwerkkarten im VMware Host Client

Sie können die Geschwindigkeit physischer Netzwerkkarten im VMware Host Client bearbeiten.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Physische Netzwerkkarten**.
2. Wählen Sie die zu bearbeitende Netzwerkkarte in der Tabelle aus.
3. Klicken Sie auf **Einstellungen bearbeiten** und wählen Sie eine Geschwindigkeit aus dem Dropdown-Menü aus.
4. Klicken Sie auf **Speichern**.

Verwalten von VMkernel-Netzwerkadaptern im VMware Host Client

Sie können im VMware Host Client VMkernel-Netzwerkadapter hinzufügen und entfernen und die Einstellungen zu VMkernel-Netzwerkkarten ändern.

Anzeigen von Informationen zu VMkernel-Netzwerkadaptern im VMware Host Client

Sie können im VMware Host Client Informationen zu VMkernel-Netzwerkadaptern (Netzwerkkarten) wie TCP/IP-Konfiguration, Netzwerkdetails, Topologie virtueller Switches uvm. anzeigen.

Verfahren

1 Klicken Sie in der Bestandsliste auf **Netzwerke** und VMware Host Client anschließend auf **VMkernel-Netzwerkkarten**.

2 Klicken Sie auf eine Netzwerkkarte in der Liste, um deren Konfiguration und Topologie-Details anzuzeigen.

Hinzufügen eines VMkernel-Netzwerkadapters im VMware Host Client

Sie können einen VMkernel-Netzwerkadapter (Netzwerkkarte) auf einem VMware vSphere® Standard Edition™-Switch hinzufügen, um die Netzwerkkonnektivität für Hosts bereitzustellen. Die VMkernel-Netzwerkkarte verarbeitet auch den Systemdatenverkehr für VMware vSphere® vMotion®, IP-Speicher, Fault Tolerance, Protokollierung, vSAN usw.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste mit der rechten Maustaste auf **Netzwerk** und anschließend auf **VMkernel-Netzwerkkarte hinzufügen**.

2 Konfigurieren Sie im Dialogfeld **VMkernel-Netzwerkkarte hinzufügen** die Einstellungen für den VMkernel-Adapter.

Option	Beschreibung
Bezeichnung für neue Portgruppe	Beim Hinzufügen einer VMkernel-Netzwerkkarte wird auch eine Portgruppe hinzugefügt. Legen Sie einen Namen für diese Portgruppe fest.
VLAN-ID	Geben Sie eine VLAN-ID zum Identifizieren des VLANs ein, das vom Netzwerkdatenverkehr des VMkernel-Adapters verwendet wird.
IP-Version	Wählen Sie IPv4, IPv6 oder beide aus. **Hinweis** Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.

3 Wählen Sie im Dropdown-Menü einen virtuellen Switch aus.

4 (Optional) Erweitern Sie den Abschnitt „IPv4-Einstellungen“, um eine Option zum Abrufen von IP-Adressen auszuwählen.

Option	Beschreibung
DHCP zum Abrufen der IP-Einstellungen verwenden	IP-Einstellungen werden automatisch abgerufen. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

5 (Optional) Erweitern Sie den Abschnitt „IPv6-Einstellungen“, um eine Option zum Abrufen von IPv6-Adressen auszuwählen.

Option	Beschreibung
DHCPv6	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
Automatische Konfiguration	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	a Klicken Sie auf **Adresse hinzufügen**, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein.

6 Wählen Sie im Dropdown-Menü einen TCP/IP-Stack aus.

Der TCP/IP-Stack, den Sie für den VMkernel-Adapter festlegen, kann später nicht mehr geändert werden. Wenn Sie den vMotion- oder den Bereitstellungs-TCP/IP-Stack auswählen, können Sie nur diesen Stack für vMotion- oder Bereitstellungsdatenverkehr auf dem Host verwenden. Alle VMkernel-Adapter für vMotion im Standard-TCP/IP-Stack werden für zukünftige vMotion-Sitzungen deaktiviert. Wenn Sie den Bereitstellungs-TCP/IP-Stack verwenden, sind die VMkernel-Adapter auf dem Standard-TCP/IP-Stack deaktiviert, und Sie können einige Vorgänge nicht ausführen. Zu diesen Vorgängen gehören die Bereitstellung von Datenverkehr, wie z. B. die VM-Cold-Migration, das Klonen und die Snapshot-Migration.

7 (Optional) Wählen Sie die Dienste aus, die für den Standard-TCP/IP-Stack auf dem Host aktiviert werden sollen.

vMotion ermöglicht es, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die vMotion-Datenverkehr gesendet wird. Die Migration mit vMotion zu ausgewählten Hosts ist nicht möglich, wenn der vMotion-Dienst für keinen VMkernel-Adapter im Standard-TCP/IP-Stack aktiviert ist oder wenn keine Adapter den vMotion-TCP/IP-Stack verwenden.

8 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Erstellen**.

Bearbeiten der VMkernel-Netzwerkadaptereinstellungen im VMware Host Client

Sie müssen möglicherweise den unterstützten Datenverkehrstyp für einen VMkernel-Netzwerkadapter oder die Art und Weise, wie IPv4- oder IPv6-Adressen abgerufen werden, ändern.

Verfahren

1 Klicken Sie in der Bestandsliste auf **Netzwerke** und VMware Host Client anschließend auf **VMkernel-Netzwerkkarten**.

2 Wählen Sie den VMkernel-Adapter aus, der sich im Ziel-Standard-Switch befindet, klicken Sie auf **Aktionen** und wählen Sie **Einstellungen bearbeiten** aus dem Dropdown-Menü aus.

3 (Optional) Bearbeiten Sie die VLAN-ID.

Die VLAN-ID legt das VLAN fest, das vom Netzwerkdatenverkehr des VMkernel-Adapters verwendet wird.

4 (Optional) Um die IP-Version zu bearbeiten, wählen Sie IPv4, IPv6 oder beide im Dropdown-Menü aus.

Hinweis Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.

5 (Optional) Erweitern Sie den Abschnitt „IPv4-Einstellungen“, um eine Option zum Abrufen von IP-Adressen auszuwählen.

Option	Beschreibung
DHCP zum Abrufen der IP-Einstellungen verwenden	IP-Einstellungen werden automatisch abgerufen. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

6 (Optional) Erweitern Sie den Abschnitt „IPv6-Einstellungen“, um eine Option zum Abrufen von IPv6-Adressen auszuwählen.

Option	Beschreibung
DHCPv6	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
Automatische Konfiguration	Verwenden Sie eine Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	a Klicken Sie auf **Adresse hinzufügen**, um eine IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein.

7 (Optional) Wählen Sie den Dienst aus, der für den Standard-TCP/IP-Stack auf dem Host aktiviert oder deaktiviert werden soll.

vMotion ermöglicht, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die der vMotion-Datenverkehr gesendet wird. Die Migration mit vMotion zu ausgewählten Hosts ist nicht möglich, wenn der vMotion-Dienst für keinen VMkernel-Adapter im Standard-TCP/IP-Stack aktiviert ist oder wenn keine Adapter den vMotion-TCP/IP-Stack verwenden.

8 Überprüfen Sie die Änderungen an den Einstellungen und klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Entfernen eines VMkernel-Netzwerkadapters im VMware Host Client

Sie können einen VMkernel-Netzwerkadapter im VMware Host Client entfernen, wenn Sie ihn nicht mehr benötigen.

Verfahren

1 Klicken Sie in der Bestandsliste auf **Netzwerke** und VMware Host Client anschließend auf **VMkernel-Netzwerkkarten**.

2 Klicken Sie mit der rechten Maustaste auf den VMkernel-Netzwerkadapter, den Sie entfernen möchten, und wählen Sie **Entfernen**.

3 Klicken Sie auf **Bestätigen**, um den Netzwerkadapter zu entfernen.

Anzeigen der TCP/IP-Stack-Konfiguration auf einem Host im VMware Host Client

Sie können das DNS und die Routingkonfiguration eines TCP/IP-Stack auf einem Host anzeigen. Sie können auch die IPv4- und IPv6-Routing-Tabellen, den Algorithmus zur Überlastungssteuerung und die maximale Anzahl zulässiger Verbindungen anzeigen.

Verfahren

1 Klicken Sie in der Host-Bestandsliste auf **Netzwerk** und anschließend auf **TCP/IP-Stacks**.

2 Wählen Sie einen Stack aus der Liste aus.

Die Konfigurationseinstellungen zum ausgewählten Stack werden angezeigt.

Ändern der Konfiguration eines TCP/IP-Stacks auf einem Host im VMware Host Client

Sie können das DNS und die Standard-Gatewaykonfiguration eines TCP/IP-Stack auf einem Host ändern. Sie können auch den Algorithmus zur Überlastungssteuerung, die maximale Anzahl der Verbindungen und den Namen der benutzerdefinierten TCP/IP-Stacks ändern.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk** und anschließend auf **TCP/IP-Stacks**.

2 Klicken Sie mit der rechten Maustaste auf einen Stack in der Liste und wählen Sie **Einstellungen bearbeiten**.

Das Dialogfeld „TCP/IP-Konfiguration - Bereitstellungs-Stack“ wird angezeigt.

3 Legen Sie fest, wie der Host seine Einstellungen für diesen TCP/IP-Stack erhalten soll.

- Klicken Sie auf die Optionsschaltfläche **DHCP-Dienste von folgendem Adapter verwenden** und wählen Sie einen Adapter aus, von dem die Konfiguration mit den Standardeinstellungen für den TCP/IP-Stack bezogen werden soll.

- Wählen Sie die Option **Einstellungen für diesen TCP/IP-Stack manuell konfigurieren**, um die Konfiguration der Einstellungen zu ändern.

Option	Beschreibung
Basiskonfiguration	**Hostname** Bearbeiten Sie den Namen des lokalen Hosts. **Domänenname** Geben Sie den Domänennamen ein. **Primärer DNS-Server** Geben Sie die IP-Adresse eines bevorzugten DNS-Servers ein. **Sekundärer DNS-Server** Geben Sie die IP-Adresse eines alternativen DNS-Servers ein. **Domänen durchsuchen** Geben Sie die DNS-Suffixe an, die in DNS-Suchvorgängen beim Auflösen unqualifizierter Domänennamen verwendet werden sollen.
Routing	Bearbeiten Sie die IPv4- und IPv6-Gateway-Informationen. **Hinweis** Durch Entfernen des Standard-Gateway geht möglicherweise die Verbindung zum Host verloren.
Erweiterte Einstellungen	Bearbeiten Sie den Algorithmus zur Überlastungssteuerung und die maximale Anzahl der Verbindungen.

4 Klicken Sie auf **Speichern**.

Konfigurieren der ESXi-Firewall im VMware Host Client

ESXi enthält eine Firewall, die standardmäßig aktiviert ist. Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme des Datenverkehrs für Dienste, die im Sicherheitsprofil des Hosts aktiviert sind, der ein- und ausgehende Datenverkehr blockiert wird.

Beim Öffnen der Ports in der Firewall müssen Sie sich bewusst sein, dass der uneingeschränkte Zugriff auf die Dienste eines ESXi-Hosts den Host für Angriffe von außen und nicht autorisierten Zugriff verwundbar machen. Reduzieren Sie dieses Risiko, indem Sie die ESXi-Firewall so konfigurieren, dass sie nur den Zugriff über autorisierte Netzwerke zulässt.

Hinweis Die Firewall lässt auch Internet Control Message Protocol oder ICMP, Pings und Kommunikation mit DHCP- und DNS- Clients (nur UDP) zu.

Verwalten von ESXi-Firewalleinstellungen mithilfe des VMware Host Client

Wenn Sie bei einem ESXi-Host mit dem VMware Host Client angemeldet sind, können Sie ein- und ausgehende Firewallverbindungen für einen Dienst- oder einen Verwaltungs-Agent konfigurieren.

Hinweis Wenn sich die Portregeln verschiedener Dienste überschneiden, kann das Aktivieren eines Diensts möglicherweise dazu führen, dass implizit weitere Dienste aktiviert werden. Sie können angeben, welche IP-Adressen auf jeden Dienst auf dem Host zugreifen können, um dieses Problem zu vermeiden.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.
2. Klicken Sie auf **Firewallregeln**.

   Der VMware Host Client zeigt eine Liste der aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.
3. Für einige Dienste können Dienstdetails verwaltet werden. Klicken Sie mit der rechten Maustaste auf einen Dienst und wählen Sie eine Option aus dem Popup-Menü.
   - Verwenden Sie die Schaltflächen Starten, Anhalten oder Neu starten, um den Status eines Dienstes vorübergehend zu ändern.
   - Ändern Sie die Startrichtlinie, um den Dienst so zu konfigurieren, dass er mit dem Host, den Firewallports oder manuell startet und stoppt.

Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host mit dem VMware Host Client

Standardmäßig lässt die Firewall für jeden Dienst den Zugriff auf alle IP-Adressen zu. Um den Datenverkehr einzuschränken, konfigurieren Sie jeden Dienst so, dass nur Datenverkehr aus Ihrem Verwaltungssubnetz zugelassen wird. Sie können auch einige Dienste deaktivieren, wenn diese in Ihrer Umgebung nicht verwendet werden.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerke** und anschließend auf **Firewallregeln**.
2. Wählen Sie einen Dienst aus der Liste aus und klicken Sie auf **Einstellungen bearbeiten**.

3 Klicken Sie im Abschnitt „Zulässige IP-Adressen“ auf **Nur Verbindungen von den folgenden Netzwerken zulassen** und geben Sie die IP-Adressen der Netzwerke ein, die eine Verbindung zum Host herstellen dürfen.

   Trennen Sie mehrere IP-Adressen durch Kommas. Sie können die folgenden Adressformate verwenden:

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64

4 Klicken Sie auf **OK**.

Überwachen von Netzwerkereignissen und Aufgaben im VMware Host Client

Sie können Details zu den Ereignissen und Aufgaben im Zusammenhang mit Portgruppen, virtuellen Switches, physischen Netzwerkadaptern, VMkernel-Netzwerkadaptern und TCP/IP-Stacks auf dem ESXi-Host anzeigen, den Sie verwalten.

Überwachen von Portgruppen im VMware Host Client

Durch Anzeigen der Ereignisse und Aufgaben der Portgruppen auf dem Host können Sie im VMware Host Client die Leistung von Portgruppen überwachen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.

2 Klicken Sie auf **Portgruppen**.

3 Wählen Sie eine Portgruppe aus der Liste aus.

   Die Portgruppe wird in der VMware Host Client-Bestandsliste erweitert.

4 Klicken Sie unter dem Namen der Portgruppe in der VMware Host Client-Bestandsliste auf **Überwachen**.

5 (Optional) Klicken Sie auf **Ereignisse**, um die Ereignisse zur Portgruppe anzuzeigen.

Überwachen von virtuellen Switches im VMware Host Client

Durch Anzeigen der Ereignisse und Aufgaben der virtuellen Switches auf dem Host können Sie im VMware Host Client die Leistung virtueller Switches überwachen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.

2 Klicken Sie auf **Virtuelle Switches**.

3 Wählen Sie einen virtuellen Switch aus der Liste aus.

   Der virtuelle Switch wird in der VMware Host Client-Bestandsliste erweitert.

4 Klicken Sie unter dem Namen des virtuellen Switchs in der VMware Host Client-Bestandsliste auf **Überwachen**.

5 (Optional) Klicken Sie auf **Ereignisse**, um die Ereignisse zum virtuellen Switch anzuzeigen.

Überwachen von physischen Netzwerkadaptern im VMware Host Client

Durch Anzeigen der Ereignisse und Aufgaben der physischen Netzwerkkarten auf dem Host können Sie im VMware Host Client die Leistung physischer Netzwerkadapter (Netzwerkkarten) überwachen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.

2 Klicken Sie auf **Physische Netzwerkkarten**.

3 Klicken Sie auf einen physischen Netzwerkadapter in der Liste.

   Der physische Netzwerkadapter wird in der VMware Host Client-Bestandsliste erweitert.

4 Klicken Sie unter dem Namen des physischen Netzwerkadapters in der VMware Host Client-Bestandsliste auf **Überwachen**.

5 (Optional) Klicken Sie auf **Ereignisse**, um die Ereignisse zum physischen Netzwerkadapter anzuzeigen.

Verwalten von VMkernel-Netzwerkadaptern im VMware Host Client

Durch Anzeigen der Ereignisse und Aufgaben der physischen Netzwerkkarten auf dem Host können Sie im VMware Host Client die Leistung von VMkernel Netzwerkadaptern überwachen.

Verfahren

1 Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.

2 Klicken Sie auf **VMkernel- Netzwerkkarten**.

3 Klicken Sie auf einen VMkernel-Netzwerkadapter in der Liste.

   Der VMkernel-Netzwerkadapter wird in der VMware Host Client-Bestandsliste erweitert.

4 Klicken Sie unter dem Namen des VMkernel-Netzwerkadapters in der VMware Host Client-Bestandsliste auf **Überwachen**.

5 (Optional) Klicken Sie auf **Ereignisse**, um die Ereignisse zum VMkernel-Netzwerkadapter anzuzeigen.

Überwachen von TCP/IP-Stacks im VMware Host Client

Durch Anzeigen der Ereignisse und Aufgaben der TCP/IP-Stacks auf dem Host können Sie im VMware Host Client die Leistung von TCP/IP-Stacks überwachen.

Verfahren

1. Klicken Sie in der VMware Host Client-Bestandsliste auf **Netzwerk**.
2. Klicken Sie auf **TCP/IP-Stacks**.
3. Wählen Sie einen TCP/IP-Stack aus der Liste aus.

   Der TCP/IP-Stack wird in der VMware Host Client-Bestandsliste erweitert.
4. Klicken Sie unter dem Namen des TCP/IP-Stacks in der VMware Host Client-Bestandsliste auf **Überwachen**.
5. (Optional) Klicken Sie auf **Ereignisse**, um die Ereignisse zum TCP/IP-Stack anzuzeigen.
6. (Optional) Klicken Sie auf **Aufgaben**, um die Aufgaben zum TCP/IP-Stack anzuzeigen.