

Handbuch zur Verfügbarkeit in vSphere

ESX 4.1

ESXi 4.1

vCenter Server 4.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-000316-00

vmware[®]

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

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

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

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

docfeedback@vmware.com

Copyright © 2009, 2010 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

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

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

Inhalt

Über dieses Handbuch	5
1 Business Continuity und Minimieren der Ausfallzeit	7
Reduzieren geplanter Ausfallzeiten	7
Verhindern ungeplanter Ausfallzeiten	8
VMware HA bietet eine schnelle Wiederherstellung nach Ausfällen	8
VMware-Fehlertoleranz bietet unterbrechungsfreie Verfügbarkeit	9
2 Erstellen und Verwenden von VMware HA-Clustern	11
Wie VMware HA funktioniert	11
VMware HA-Zugangssteuerung	13
VMware HA-Checkliste	20
Erstellen eines VMware HA-Clusters	21
Anpassen des VMware-HA-Verhaltens	26
Empfohlene Vorgehensweisen für VMware HA-Cluster	29
3 Aktivieren der Fehlertoleranz für virtuelle Maschinen	33
Wie die Fehlertoleranz funktioniert	33
Verwendung der Fehlertoleranz mit DRS	35
Beispiele für die Nutzen der Fehlertoleranz	35
Fehlertoleranz-Checkliste	36
Fehlertoleranzinteroperabilität	37
Vorbereiten Ihrer Cluster und Hosts für Fehlertoleranz	39
Aktivieren der Fehlertoleranz für virtuelle Maschinen	43
Anzeigen der Information zu fehlertoleranten virtuellen Maschinen	45
Best Practices für die Fehlertoleranz	47
VMware-Fehlertoleranz - Konfigurationsempfehlungen	50
Beheben von Problemen bei der Fehlertoleranz	50
 Anhang: Fehlertoleranz-Fehlermeldungen	 55
 Index	 61

Über dieses Handbuch

Das *Handbuch zur Verfügbarkeit in vSphere* beschreibt Lösungen, die Business Continuity bieten, einschließlich Informationen zum Einrichten von VMware® High Availability (HA) und VMware-Fehlertoleranz.

Zielgruppe

Dieses Buch ist an alle gerichtet, die mithilfe von VMware HA und Fehlertoleranz Business Continuity bieten möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datacenteroperationen vertraut sind.

VMware Technical Publications - Glossar

VMware Technical Publications stellt einen Glossar mit Begriffen zur Verfügung, die Ihnen möglicherweise nicht vertraut sind. Definitionen von Begriffen wie sie in der technischen Dokumentation von VMware genutzt werden finden Sie unter <http://www.vmware.com/support/pubs>.

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Falls Sie Anmerkungen haben, senden Sie diese bitte an: docfeedback@vmware.com.

vSphere-Dokumentation

Die Dokumentation zu vSphere® umfasst die kombinierte Dokumentation zu VMware vCenter Server und ESX/ESXi. Das *Handbuch zur Verfügbarkeit in vSphere* bezieht sich auf ESX®, ESXi und vCenter® Server.

Technischer Support und Schulungsressourcen

Ihnen stehen die folgenden Ressourcen für die technische Unterstützung zur Verfügung. Die aktuelle Version dieses Handbuchs sowie weiterer Handbücher finden Sie auf folgender Webseite:

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

Online- und Telefon-Support

Auf der folgenden Webseite können Sie über den Onlinesupport technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren: <http://www.vmware.com/support>.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support schnelle Hilfe bei Problemen der Prioritätsstufe 1. Rufen Sie die folgende Webseite auf:

http://www.vmware.com/support/phone_support.html.

Support-Angebote

Informationen zum Support-Angebot von VMware und dazu, wie es Ihre geschäftlichen Anforderungen erfüllen kann, finden Sie unter

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

VMware Professional Services

Die VMware Education Services-Kurse umfassen umfangreiche Praxisübungen, Fallbeispiele und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Kurse können vor Ort, im Unterrichtsraum und live online durchgeführt werden. Für Pilotprogramme vor Ort und die Best Practices für die Implementierung verfügt VMware Consulting Services über Angebote, die Sie bei der Beurteilung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung unterstützen. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting-Diensten finden Sie auf der folgenden Webseite: <http://www.vmware.com/services>.

Business Continuity und Minimieren der Ausfallzeit

1

Ausfallzeiten, ob geplant oder ungeplant, verursachen erhebliche Kosten. Bisherige Lösungen, die eine hohe Verfügbarkeit garantieren, sind jedoch teuer, schwer zu implementieren und umständlich zu verwalten gewesen.

VMware-Software macht das Bereitstellen von hoher Verfügbarkeit für wichtige Anwendungen einfacher und günstiger. Organisationen können mithilfe von vSphere die grundlegende Verfügbarkeit aller Anwendungen unschwer erhöhen und höhere Verfügbarkeitsebenen einfacher und kostengünstiger bereitstellen. Mit vSphere können Sie Folgendes erreichen:

- Eine höhere Verfügbarkeit, unabhängig von Hardware, Betriebssystem und Anwendungen.
- Eliminierung der geplanten Ausfallzeiten für allgemeine Wartungsvorgänge.
- Automatische Wiederherstellung bei Ausfällen.

vSphere ermöglicht das Reduzieren der geplanten Ausfallzeiten, das Verhindern ungeplanter Ausfallzeiten und das schnelle Wiederherstellen nach Ausfällen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Reduzieren geplanter Ausfallzeiten“](#), auf Seite 7
- [„Verhindern ungeplanter Ausfallzeiten“](#), auf Seite 8
- [„VMware HA bietet eine schnelle Wiederherstellung nach Ausfällen“](#), auf Seite 8
- [„VMware-Fehlertoleranz bietet unterbrechungsfreie Verfügbarkeit“](#), auf Seite 9

Reduzieren geplanter Ausfallzeiten

Geplante Ausfallzeiten sind in der Regel für 80 % der Datencenterausfallzeit verantwortlich. Hardwarewartung, Servermigration und Firmware-Updates erfordern das Herunterfahren physischer Server, was zu Ausfallzeiten führt. Organisationen werden zum Minimieren der Auswirkungen dieser Ausfallzeiten gezwungen, die Wartung in unpassende und schwer zu planende Ausfallzeitfenster zu verlegen.

vSphere ermöglicht Organisationen eine deutliche Reduzierung der geplanten Ausfallzeiten. Da Arbeitslasten in einer vSphere-Umgebung dynamisch und ohne Ausfallzeit oder Dienstunterbrechung auf andere physische Server verschoben werden können, kann die Serverwartung ausgeführt werden, ohne dass Anwendungs- und Dienstausfallzeiten erforderlich werden. Organisationen können unter Verwendung von vSphere Folgendes erreichen:

- Eliminierung der Ausfallzeiten für allgemeine Wartungsvorgänge.
- Eliminierung von geplanten Wartungsfenstern.
- Durchführung von Wartungsarbeiten zu jeder Zeit, ohne Benutzer und Dienste zu stören.

Die VMware vMotion[®]- und Storage vMotion-Funktionalität in vSphere ermöglicht Organisationen die Reduzierung von geplanten Ausfallzeiten, weil Arbeitslasten in einer VMware-Umgebung dynamisch und ohne Dienstunterbrechung auf andere physische Server oder auf anderen zugrunde liegenden Speicher verschoben werden können. Administratoren können schnellere und vollständig transparente Wartungsvorgänge durchführen, ohne unpassende Ausfallzeitfenster planen zu müssen.

Verhindern ungeplanter Ausfallzeiten

Ein ESX/ESXi-Host bietet zwar eine robuste Plattform für die Ausführung von Anwendungen, eine Organisation muss sich jedoch auch vor ungeplanten Ausfallzeiten schützen, die durch Hardware- oder Anwendungsfehler verursacht werden. vSphere integriert wichtige Funktionen in die Datacenterinfrastruktur, die Ihnen helfen können, ungeplante Ausfallzeiten zu verhindern.

Diese vSphere-Funktionen sind Teil der virtuellen Infrastruktur und sind somit für das Betriebssystem und für die Anwendungen sichtbar, die in virtuellen Maschinen ausgeführt werden. Diese Funktionen können auf allen virtuellen Maschinen eines physischen Systems konfiguriert und dort verwendet werden. Kosten und Aufwand, die üblicherweise mit der Bereitstellung einer hohen Verfügbarkeit verbunden sind, werden reduziert. Zu den Schlüsselfunktionen der in vSphere integrierten Fehlertoleranz gehören:

- **Gemeinsam genutzter Speicher.** Eliminieren Sie einzelne Fehlerstellen (single points of failure), indem Sie Dateien der virtuellen Maschine auf gemeinsam genutztem Speicher, z. B. Fibre-Channel, iSCSI-SAN oder NAS, ablegen. Sie können SAN-Spiegelung und Replizierungsfunktionen verwenden, um aktuelle Kopien der virtuellen Festplatte auf Notfallwiederherstellungs-Sites zu speichern.
- **NIC-Gruppierung.** Sie bietet Toleranz für einzelne Netzwerkkartenfehler.
- **Speicher-Multipathing.** Toleriert Speicherpfadfehler.

Zusätzlich zu diesen Funktionen können die Funktionen von VMware HA und Fehlertoleranz ungeplante Ausfallzeiten minimieren oder eliminieren, indem sie schnelle Wiederherstellung nach Ausfällen bzw. unterbrechungsfreie Verfügbarkeit bieten.

VMware HA bietet eine schnelle Wiederherstellung nach Ausfällen

VMware HA verwendet mehrere ESX/ESXi-Hosts, die als Cluster konfiguriert sind, um eine schnelle Wiederherstellung nach Ausfällen und kosteneffektive hohe Verfügbarkeit für Anwendungen zu bieten, die in virtuellen Maschinen ausgeführt werden.

VMware HA sorgt auf folgende Arten für die Verfügbarkeit von Anwendungen:

- Es schützt vor einem Serverausfall, indem es die virtuellen Maschinen auf anderen Hosts im Cluster neu startet.
- Es schützt vor Anwendungsfehlern, indem es die virtuelle Maschine kontinuierlich überwacht und sie zurücksetzt, wenn ein Fehler erkannt wird.

Im Gegensatz zu anderen Clusterlösungen bietet VMware HA die Infrastruktur, um alle Arbeitslasten zu schützen:

- Es muss keine spezielle Software in der Anwendung oder virtuellen Maschine installiert werden. Alle Arbeitslasten werden von VMware HA geschützt. Nachdem VMware HA konfiguriert wurde, sind keine weiteren Aktionen erforderlich, um neue virtuelle Maschinen zu schützen. Sie werden automatisch geschützt.
- Sie können VMware HA mit VMware Distributed Resource Scheduler (DRS) kombinieren, um gegen Ausfälle geschützt zu sein und um Lastausgleich zwischen den Hosts innerhalb eines Clusters zu bieten.

VMware HA bietet mehrere Vorteile gegenüber herkömmlichen Failover-Lösungen:

Minimalinstallation	Nachdem ein VMware HA-Cluster eingerichtet wurde, erhalten alle virtuellen Maschinen im Cluster Failover-Unterstützung ohne zusätzliche Konfiguration.
Geringere Hardwarekosten und geringerer Installationsaufwand	Die virtuelle Maschine fungiert wie ein portabler Container für Anwendungen, der von einem Host auf einen anderen verschoben werden kann. Administratoren vermeiden doppelte Konfigurationen auf mehreren Maschinen. Bei der Verwendung von VMware HA müssen ausreichend Ressourcen vorhanden sein, um die Failover-Funktion für die gewünschte Anzahl an Hosts zu gewährleisten, die Sie mit VMware HA schützen möchten. Allerdings verwaltet das vCenter Server-System Ressourcen und konfiguriert Cluster automatisch.
Erhöhte Anwendungs- verfügbarkeit	Für jede innerhalb einer virtuellen Maschine ausgeführte Anwendung besteht eine erhöhte Verfügbarkeit. Da die virtuelle Maschine nach einem Hardwareausfall wiederhergestellt werden kann, verfügen alle Anwendungen, die beim Starten der virtuellen Maschine gestartet werden, über eine erhöhte Verfügbarkeit ohne zusätzlichen CPU-Aufwand, sogar wenn die Anwendung selbst keine Clusteranwendung ist. Durch das Überwachen und Reagieren auf die Taktsignale von VMware Tools und das Zurücksetzen nicht-reagierender virtueller Maschinen besteht ein Schutz gegen Abstürze von Gastbetriebssystemen.
DRS- und VMotion-Integration	Wenn ein Host ausfällt und virtuelle Maschinen auf anderen Hosts neu gestartet werden, kann DRS Migrationsempfehlungen bieten oder die virtuelle Maschine für eine ausgeglichene Ressourcenzuteilung migrieren. Fällt bei der Migration der Quellhost und/oder der Zielhost aus, unterstützt VMware HA die Wiederherstellung nach dem Ausfall.

VMware-Fehlertoleranz bietet unterbrechungsfreie Verfügbarkeit

VMware HA bietet Ihren virtuellen Maschinen einen grundlegenden Schutz, indem sie virtuelle Maschinen im Fall eines Hostausfalls neu startet. VMware-Fehlertoleranz bietet einen höheren Grad der Verfügbarkeit, da Benutzern ermöglicht wird, jede virtuelle Maschine ohne Daten-, Transaktions- oder Verbindungsverlust vor Hostausfällen zu schützen.

Die Fehlertoleranz verwendet auf der ESX/ESXi-Hostplattform die vLockstep-Technologie von VMware, um unterbrechungsfreie Verfügbarkeit zu gewährleisten. Die permanente Verfügbarkeit wird dadurch sichergestellt, dass die Statuszustände der primären und sekundären virtuellen Maschine an jedem Punkt in der Anweisungsausführung der virtuellen Maschine identisch sind. vLockstep erreicht dies, indem es dafür sorgt, dass die primäre und sekundäre virtuelle Maschine identische Folgen von x86-Anweisungen ausführen. Die primäre virtuelle Maschine erfasst alle Eingaben und Ereignisse (vom Prozessor bis zu den virtuellen E/A-Geräten) und gibt sie auf der sekundären virtuellen Maschine wieder. Die sekundäre virtuelle Maschine führt dieselbe Reihenfolge von Anweisungen aus wie die primäre virtuelle Maschine, wobei die Arbeitslast nur auf einem VM-Image (der primären virtuellen Maschine) ausgeführt wird.

Wenn entweder der Host, auf dem die primäre virtuelle Maschine ausgeführt wird, oder der Host, auf dem sich die sekundäre virtuelle Maschine befindet, ausfällt, erfolgt ein transparentes Failover. Der funktionierende ESX/ESXi-Host wird nahtlos zum primären VM-Host, ohne dass Netzwerkverbindungen oder laufende Transaktionen verloren gehen. Bei einem transparenten Failover entsteht kein Datenverlust, auch Netzwerkverbindungen bleiben erhalten. Nachdem ein transparentes Failover aufgetreten ist, wird eine neue sekundäre virtuelle Maschine erzeugt und die Redundanz wiederhergestellt. Der gesamte Vorgang ist transparent und voll automatisiert. Er findet sogar dann statt, wenn vCenter Server nicht verfügbar ist.

Erstellen und Verwenden von VMware HA-Clustern

2

VMware HA Cluster ermöglichen einer Sammlung von ESX/ESXi-Hosts das Zusammenarbeiten in einer Gruppe und bieten virtuellen Maschinen dadurch eine höhere Verfügbarkeit, als es einzelne ESX/ESXi-Hosts könnten. Wenn Sie planen, einen neuen VMware HA-Cluster zu erstellen und zu verwenden, wirken sich die ausgewählten Optionen auf die Art und Weise aus, wie der Cluster auf Ausfälle von Hosts oder virtuellen Maschinen reagieren wird.

Vor dem Erstellen eines VMware HA-Clusters sollten Sie sich bewusst machen, wie VMware HA Hostausfälle und -isolierung identifiziert und auf solche Situationen reagiert. Darüber hinaus sollten Sie wissen, wie die Zugangssteuerung funktioniert, damit Sie die für Ihre Failover-Anforderungen am besten geeignete Richtlinie wählen können. Nach der Einrichtung eines Clusters können Sie mit erweiterten Attributen dessen Verhalten beeinflussen und seine Leistung optimieren, wenn Sie sich an die folgende empfohlene Vorgehensweise halten.

Dieses Kapitel behandelt die folgenden Themen:

- [„Wie VMware HA funktioniert“](#), auf Seite 11
- [„VMware HA-Zugangssteuerung“](#), auf Seite 13
- [„VMware HA-Checkliste“](#), auf Seite 20
- [„Erstellen eines VMware HA-Clusters“](#), auf Seite 21
- [„Anpassen des VMware-HA-Verhaltens“](#), auf Seite 26
- [„Empfohlene Vorgehensweisen für VMware HA-Cluster“](#), auf Seite 29

Wie VMware HA funktioniert

VMware HA bietet virtuellen Maschinen hohe Verfügbarkeit, indem sie die virtuellen Maschinen und die Hosts, auf denen diese sich befinden, zu einem Cluster zusammenfasst. Die Hosts im Cluster werden überwacht. Wenn einer der Hosts ausfällt, werden die auf dem ausgefallenen Host betriebenen virtuellen Maschinen auf anderen Hosts neu gestartet.

Primäre und sekundäre Hosts in einem VMware HA-Cluster

Wenn Sie einen Host zu einem VMware HA-Cluster hinzufügen, wird ein Agent auf den Host hochgeladen und für die Kommunikation mit anderen Agenten im Cluster konfiguriert. Die ersten fünf Hosts im Cluster sind als primäre Hosts festgelegt, alle weiteren Hosts als sekundäre Hosts. Die primären Hosts warten und replizieren alle Clusterzustände und werden zum Einleiten von Failover-Aktionen verwendet. Wenn ein primärer Host aus dem Cluster entfernt wird, sorgt VMware HA dafür, dass ein anderer Host (sekundär) zum primären Host wird. Wenn geplant ist, dass ein primärer Host für längere Zeit offline sein soll, sollten Sie ihn aus dem Cluster entfernen, sodass er durch einen sekundären Host ersetzt werden kann.

Jeder Host, der zum Cluster hinzugefügt wird, muss zum Abschließen seiner Konfiguration mit einem vorhandenen primären Host im Cluster kommunizieren (es sei denn, Sie fügen ihn als ersten Host zum Cluster hinzu). Mindestens ein primärer Host muss funktionieren, damit VMware HA ordnungsgemäß funktioniert. Wenn keiner der primären Hosts verfügbar ist (sie reagieren nicht), können auch keine Hosts für VMware HA konfiguriert werden. Sie sollten diesen Grenzwert von fünf primären Hosts pro Cluster beachten, wenn Sie die Größe Ihres Clusters planen. Wenn Ihr Cluster in einer Blade-Server-Umgebung implementiert ist, sollten Sie nach Möglichkeit nicht mehr als vier primäre Hosts in einem einzelnen Blade-Chassis platzieren. Wenn sich alle fünf primären Hosts in demselben Chassis befinden und das Chassis ausfällt, verliert Ihr Cluster den VMware HA-Schutz.

Zudem wird ein primärer Host als aktiver primärer Host ausgewählt. Dieser hat folgende Aufgaben:

- Er entscheidet, wo die virtuelle Maschine neu gestartet wird.
- Er protokolliert fehlgeschlagene Neustartversuche.
- Er versucht erneut, die virtuelle Maschine zu starten, wenn dies sinnvoll ist.

Falls der aktive primäre Host ausfällt, wird er durch einen anderen primären Host ersetzt.

Erkennen von Ausfällen und Hostnetzwerkisolierung

Die Agenten kommunizieren untereinander und verfolgen die Lebenszeichen der Hosts im Cluster. Dazu werden standardmäßig jede Sekunde Taktsignale ausgetauscht. Falls über einen Zeitraum von 15 Sekunden keine Taktsignale vom Host empfangen werden und der Host nicht angepingt werden kann, wird er als ausgefallen eingestuft. Wenn ein Host ausfällt, wird für die auf diesem Host ausgeführten virtuellen Maschinen ein Failover durchgeführt, d. h., sie werden auf anderen Hosts neu gestartet.

HINWEIS Wenn ein Host ausfällt, führt VMware HA kein Failover von virtuellen Maschinen auf einen Host im Wartungsmodus durch.

Hostnetzwerkisolierung findet statt, wenn ein Host noch ausgeführt wird, aber mit anderen Hosts im Cluster nicht mehr kommunizieren kann. Wenn ein Host mit Standardeinstellungen über einen Zeitraum von 12 Sekunden keine Taktsignale von allen anderen Hosts im Cluster empfängt, versucht er, seine Isolierungsadresse anzupingen. Falls dies ebenfalls fehlschlägt, deklariert er sich selbst als vom Netzwerk isoliert. Eine Isolierungsadresse wird nur dann angepingt, wenn keine Taktsignale von einem anderen Host im Cluster empfangen werden.

Wenn die Netzwerkverbindung des isolierten Hosts für 15 Sekunden oder länger nicht wiederhergestellt werden kann, behandeln die anderen Hosts im Cluster den isolierten Host als ausgefallen und es wird versucht, ein Failover der virtuellen Maschinen dieses Hosts durchzuführen. Falls ein isolierter Host jedoch weiterhin auf den gemeinsam genutzten Speicher zugreifen kann, behält er auch die Festplattensperre für die Dateien der virtuellen Maschine bei. Um eine potenzielle Beschädigung der Dateien zu vermeiden, verhindert die VMFS-Festplattensperre gleichzeitige Schreibvorgänge in den Festplattendateien der virtuellen Maschinen und Versuche, ein Failover der virtuellen Maschinen des isolierten Hosts durchzuführen, schlagen fehl. Standardmäßig fährt der isolierte Host seine virtuellen Maschinen herunter, aber Sie können die Hostisolierungsreaktion in **[Eingeschaltet lassen]** oder **[Ausschalten]** ändern. Siehe „[Optionen für virtuelle Maschinen](#)“, auf Seite 23.

HINWEIS Wenn Sie sicherstellen, dass die Netzwerkinfrastruktur ausreichend redundant ist, sodass mindestens ein Netzwerkpfad stets zur Verfügung steht, dürfte eine Netzwerkisolierung äußerst selten auftreten.

Gemeinsame Verwendung von VMware HA und DRS

Wenn Sie VMware HA mit Distributed Resource Scheduler (DRS) verwenden, werden die Funktionen des automatischen Failovers und des Lastausgleichs kombiniert. Diese Kombination kann zu einem schnellen Lastausgleich der virtuellen Maschinen führen, nachdem sie durch VMware HA auf andere Hosts verschoben wurden.

Wenn VMware HA ein Failover durchführt und virtuelle Maschinen auf anderen Hosts neu startet, ist die erste Priorität die unmittelbare Verfügbarkeit aller virtuellen Maschinen. Nachdem dem Neustart der virtuellen Maschinen kann es bei den betreffenden Hosts zu einer hohen Auslastung kommen, wohingegen andere Hosts eine relativ geringe Last aufweisen. VMware HA ermittelt anhand der CPU- und der Arbeitsspeicherreservierung der virtuellen Maschine, ob ein Host über genügend freie Kapazität verfügt, um die virtuelle Maschine aufzunehmen.

In einem Cluster, in dem DRS und VMware HA mit aktivierter HA-Zugangssteuerung verwendet wird, werden die virtuellen Maschinen möglicherweise nicht von Hosts evakuiert, die in den Wartungsmodus wechseln. Dieses Verhalten tritt aufgrund der Ressourcen auf, die im Falle eines Ausfalls zum Neustart der virtuellen Maschinen reserviert sind. Sie müssen die virtuellen Maschinen manuell unter Verwendung von VMotion von den Hosts migrieren.

In einigen Szenarien vermag VMware HA aufgrund von Ressourceneinschränkungen kein Failover der virtuellen Maschinen durchzuführen. Dies kann aus verschiedenen Gründen auftreten.

- Die HA-Zugangssteuerung ist deaktiviert und DPM (Distributed Power Management) ist aktiviert. Dies kann dazu führen, dass DPM virtuelle Maschinen auf weniger Hosts konsolidiert und die leeren Hosts in den Standby-Modus versetzt, was zur Folge hat, dass die Kapazitäten für das Durchführen eines Failovers nicht ausreichen.
- VM-Host-Affinitätsregeln (erforderlich) begrenzen möglicherweise die Anzahl an Hosts, auf denen bestimmte virtuelle Maschinen platziert werden können.
- Möglicherweise gibt es insgesamt ausreichende Ressourcen, aber sie können über mehrere Hosts hinweg fragmentiert sein, sodass sie nicht von virtuellen Maschinen zwecks Failover verwendet werden können.

In solchen Fällen verwendet VMware HA DRS, um zu versuchen, den Cluster anzupassen (z. B. indem Hosts veranlasst werden, den Standby-Modus zu verlassen, oder virtuelle Maschinen migriert werden, um die Clusterressourcen zu defragmentieren), damit HA Failover durchführen kann.

Wenn sich DPM im manuellen Modus befindet, müssen Sie möglicherweise die Empfehlungen zu Einschaltvorgängen des Hosts bestätigen. Sie müssen ebenso die Migrationsempfehlungen möglicherweise bestätigen, wenn DRS im manuellen Modus ist.

Achten Sie bei der Verwendung von erforderlichen VM-Host-Affinitätsregeln darauf, dass nicht gegen diese Regeln verstoßen werden darf. VMware HA führt kein Failover durch, wenn dies gegen eine solche Regel verstoßen würde.

Weitere Informationen zu DRS finden Sie im *Handbuch zur Ressourcenverwaltung*.

VMware HA-Zugangssteuerung

vCenter Server verwendet die Zugangssteuerung, um sicherzustellen, dass genügend Ressourcen in einem Cluster verfügbar sind, um Failover-Schutz zu bieten und um sicherzustellen, dass Ressourcenreservierungen eingehalten werden.

Es gibt drei Typen von Zugangssteuerungen:

Host	Stellt sicher, dass ein Host über genügend Ressourcen verfügt, um den Reservierungsanforderungen aller virtuellen Maschinen gerecht zu werden, die auf ihm ausgeführt werden.
Ressourcenpool	Stellt sicher, dass ein Ressourcenpool über genügend Ressourcen verfügt, um den Reservierungen, Freigaben und Einschränkungen aller virtuellen Maschinen gerecht zu werden, die ihm zugeordnet sind.
VMware HA	Stellt sicher, dass genügend Ressourcen im Cluster für die Wiederherstellung von virtuellen Maschinen im Fall eines Hostausfalls reserviert sind.

Die Zugangssteuerung schreibt Einschränkungen für die Ressourcennutzung vor und gestattet keine Aktion, die gegen diese Einschränkungen verstößt. Beispiele für Aktionen, die möglicherweise nicht gestattet werden:

- Das Einschalten einer virtuellen Maschine.
- Das Migrieren einer virtuellen Maschine auf einen Host oder in einen Cluster oder einen Ressourcenpool.
- Erhöhen der CPU- oder Arbeitsspeicherreservierung einer virtuellen Maschine.

Von den drei Typen der Zugangssteuerung kann nur die VMware HA-Zugangssteuerung deaktiviert werden. Es gibt jedoch keine Garantie dafür, dass nach einem Hostausfall alle virtuellen Maschinen im Cluster neu gestartet werden können. Es wird empfohlen, dass Sie die Zugangssteuerung nicht deaktivieren, es kann jedoch unter anderem folgende Gründe geben, dies vorübergehend zu tun:

- Wenn Sie gegen die Failover-Einschränkung verstoßen müssen, weil es nicht genügend Ressourcen gibt, um sie zu erfüllen (z. B. wenn Sie Hosts in den Standby-Modus versetzen, um sie für die Verwendung mit DPM zu testen).
- Wenn ein automatisierter Vorgang Aktionen ausführen muss, die vorübergehend gegen die Failover-Einschränkungen verstoßen (z. B. als Teil eines von VMware Update Manager durchgeführten Upgrades).
- Wenn Sie Test- oder Wartungsvorgänge durchführen müssen.

Zugangssteuerung mit der Richtlinie „Vom Cluster tolerierte Hostfehler“

Sie können VMware HA für das Tolerieren einer angegebenen Anzahl an Hostausfällen konfigurieren. VMware HA stellt unter Verwendung der Richtlinie „Vom Cluster tolerierte Hostfehler“ für die Zugangssteuerung sicher, dass eine angegebene Anzahl an Hosts ausfallen kann und genügend Ressourcen im Cluster verbleiben, um ein Failover aller virtuellen Maschinen der Hosts durchzuführen.

Mit der Richtlinie „Vom Cluster tolerierte Hostfehler“ führt VMware HA die Zugangssteuerung folgendermaßen aus:

- 1 Berechnet die Slotgröße.

Ein Slot ist eine logische Darstellung der Arbeitsspeicher- und CPU-Ressourcen. Seine Größe ist standardmäßig so eingestellt, dass die Anforderungen jeder eingeschalteten virtuellen Maschine im Cluster erfüllt werden.

- 2 Ermittelt, wie viele Slots jeder Host im Cluster aufnehmen kann.
- 3 Ermittelt die aktuelle Failover-Kapazität des Clusters.

Dies ist die Anzahl der Hosts, die ausfallen können und dennoch genügend Slots freilassen, um die Anforderungen aller eingeschalteten virtuellen Maschinen zu erfüllen.

- 4 Ermittelt, ob die aktuelle Failover-Kapazität geringer ist als die konfigurierte Failover-Kapazität (vom Benutzer zur Verfügung gestellt).

Wenn dies zutrifft, lässt die Zugangssteuerung den Vorgang nicht zu.

HINWEIS Die maximale konfigurierte Failover-Kapazität, die Sie einstellen können, ist vier. Jeder Cluster verfügt über bis zu fünf primäre Hosts. Wenn alle gleichzeitig ausfallen, kann es sein, dass das Failover nicht auf allen virtuellen Maschinen erfolgreich ist.

Slotgrößenberechnung

Die Slotgröße besteht aus zwei Komponenten: CPU und Arbeitsspeicher.

- VMware HA berechnet die CPU-Komponente, indem es die CPU-Reservierung von jeder eingeschalteten virtuellen Maschine abrufen und den größten Wert auswählt. Wenn Sie keinen Wert für die CPU-Reservierung einer virtuellen Maschine angegeben haben, wird ein Standardwert von 256 MHz zugewiesen. Sie können diesen Wert anhand des erweiterten Attributs „das.vmcpuminhz“ ändern.
- VMware HA berechnet die Arbeitsspeicherkomponente, indem es die Arbeitsspeicherreservierung (zuzüglich Arbeitsspeicher-Overhead) von jeder eingeschalteten virtuellen Maschine abrufen und den größten Wert auswählt. Es gibt keinen Standardwert für die Arbeitsspeicherreservierung.

Wenn Ihr Cluster virtuelle Maschinen enthält, die viel größere Reservierungen als andere haben, verzerren sie die Berechnung der Slotgröße. Um dies zu vermeiden, können Sie eine Obergrenze für die CPU- oder Arbeitsspeicherkomponente der Slotgröße festlegen, indem Sie jeweils die erweiterten Attribute „das.slotcpuinhz“ oder „das.slotmeminmb“ verwenden.

Verwenden von Slots zum Berechnen der aktuellen Failover-Kapazität

Wenn die Slotgröße berechnet wurde, ermittelt VMware HA, welche CPU- und Arbeitsspeicherressourcen von jedem Host für virtuelle Maschinen zur Verfügung stehen. Dies entspricht der Menge, die der Ressourcenpool des Hosts enthält, nicht den gesamten physischen Ressourcen des Hosts. Die für die Virtualisierung verwendeten Ressourcen sind nicht enthalten. Nur Hosts, die verbunden und nicht im Wartungsmodus sind sowie keine VMware HA-Fehler aufweisen, werden berücksichtigt.

Die maximale Anzahl an Slots, die jeder Host unterstützen kann, wird daraufhin ermittelt. Dazu wird die CPU-Ressourcenmenge des Hosts durch die CPU-Komponente der Slotgröße geteilt und das Ergebnis wird abgerundet. Dieselbe Berechnung wird für die Arbeitsspeicherressourcenmenge des Hosts durchgeführt. Diese zwei Zahlen werden verglichen. Die niedrigere Zahl stellt die Anzahl an Slots dar, die der Host unterstützen kann.

Die aktuelle Failover-Kapazität wird berechnet, indem ermittelt wird, wie viele Hosts (angefangen mit dem größten Host) ausfallen können, damit noch genug Slots zur Verfügung stehen, um den Anforderungen aller eingeschalteten virtuellen Maschinen gerecht zu werden.

Erweiterte Laufzeitinformationen

Wenn Sie die Richtlinie für die Zugangssteuerung „Vom Cluster tolerierte Hostfehler“ auswählen, wird im vSphere-Client im Abschnitt „VMware HA“ der Registerkarte **[Übersicht]** des Clusters der Link **[Erweiterte Laufzeitinformationen]** angezeigt. Klicken Sie auf diesen Link, um die folgenden Informationen über den Cluster anzuzeigen:

- Slotgröße.
- Gesamtzahl der Steckplätze im Cluster. Die Summe der Slots, die von den guten Hosts im Cluster unterstützt werden.
- Verwendete Steckplätze. Die Anzahl an Slots, die eingeschalteten virtuellen Maschinen zugewiesen wurden. Sie kann die Anzahl der eingeschalteten virtuellen Maschinen übersteigen, wenn Sie unter Verwendung der erweiterten Optionen eine Obergrenze für die Slotgröße festgelegt haben. Dies liegt daran, dass einige virtuelle Maschinen mehrere Slots einnehmen können.
- Verfügbare Slots. Die Anzahl an Slots, die zum Einschalten von zusätzlichen virtuellen Maschinen im Cluster zur Verfügung stehen. VMware HA reserviert die erforderliche Anzahl von Failover-Slots. Die verbleibenden Slots stehen für das Einschalten neuer virtueller Maschinen zur Verfügung.
- Die Gesamtzahl eingeschalteter virtueller Maschinen im Cluster.

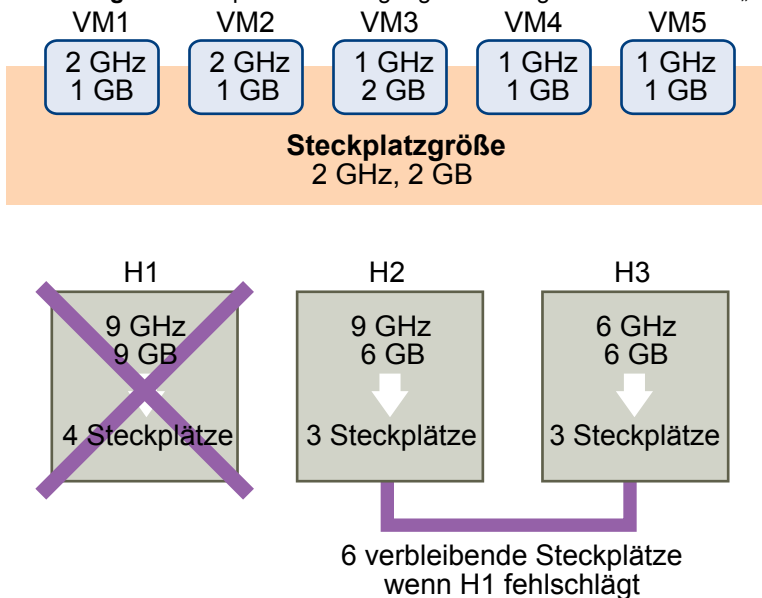
- Gesamtzahl an Hosts im Cluster.
- Gesamtzahl an guten Hosts im Cluster. Die Anzahl an Hosts, die verbunden und nicht im Wartungsmodus sind sowie keine VMware HA-Fehler aufweisen.

Beispiel 2-1. Zugangssteuerung, die die Richtlinie „Vom Cluster tolerierte Hostfehler“ verwendet

Die Art, wie die Slotgröße berechnet und mit dieser Zugangssteuerungsrichtlinie verwendet wird, wird anhand eines Beispiels dargestellt. Nehmen Sie Folgendes für einen Cluster an:

- Der Cluster besteht aus drei Hosts, jeder mit einer anderen Menge an verfügbaren CPU- und Arbeitsspeicherressourcen. Der erste Host (H1) hat 9 GHz verfügbarer CPU-Ressourcen und 9 GB verfügbaren Arbeitsspeichers, Host 2 (H2) verfügt über 9 GHz und 6 GB und Host 3 (H3) verfügt über 6 GHz und 6 GB.
- Es befinden sich fünf eingeschaltete virtuelle Maschinen im Cluster, mit unterschiedlichen CPU- und Arbeitsspeicheranforderungen. VM1 benötigt 2 GHz CPU-Ressourcen und 1 GB Arbeitsspeicher, VM2 benötigt 2 GHz und 1 GB, VM3 benötigt 1 GHz und 2 GB, VM4 benötigt 1 GHz und 1 GB und VM5 benötigt 1 GHz und 1 GB.
- Der Wert für „Vom Cluster tolerierte Hostfehler“ ist auf 1 festgelegt.

Abbildung 2-1. Beispiel für die Zugangssteuerung mit der Richtlinie „Vom Cluster tolerierte Hostfehler“



- 1 Die Slotgröße wird berechnet, indem die CPU- und Arbeitsspeicheranforderung der virtuellen Maschinen verglichen und die größte Anforderung ausgewählt wird.

Die größte CPU-Anforderung (die Anforderung von VM1 und VM2) beträgt 2 GHz, während die größte Arbeitsspeicheranforderung (die Anforderung von VM3) 2 GB beträgt. Darauf basierend wird die Slotgröße auf 2 GHz für die CPU und 2 GB für den Arbeitsspeicher festgelegt.

- 2 Die maximale Anzahl an Slots, die jeder Host unterstützen kann, wird ermittelt.

H1 unterstützt vier Slots. H2 unterstützt drei (der kleinere Wert von $9 \text{ GHz} / 2 \text{ GHz}$ und $6 \text{ GB} / 2 \text{ GB}$) und H3 unterstützt ebenfalls drei Slots.

- 3 Die aktuelle Failover-Kapazität wird berechnet.

Der größte Host ist H1. Wenn er ausfällt, verbleiben sechs Slots im Cluster, was für alle fünf eingeschalteten virtuellen Maschinen ausreicht. Wenn H1 und H2 ausfallen, verbleiben nur drei Slots, die nicht ausreichen. Deshalb ist die aktuelle Failover-Kapazität 1.

Der Cluster verfügt über einen verfügbaren Slot (die sechs Slots auf H2 und H3 minus den fünf verwendeten Slots).

Zugangssteuerung mit der Richtlinie „Prozentsatz der reservierten Clusterressourcen“

Sie können VMware HA konfigurieren, die Zugangssteuerung so durchzuführen, dass ein bestimmter Prozentsatz der Clusterressourcen für das Wiederherstellen nach einem Hostfehler reserviert wird.

Anhand der die Zugangssteuerungsrichtlinie für den Prozentsatz der reservierten Clusterressourcen stellt VMware HA sicher, dass ein bestimmter Prozentsatz der gesamten Clusterressourcen für das Failover reserviert wird.

Mit der Richtlinie für die Reservierung von Clusterressourcen führt VMware HA die Zugangssteuerung folgendermaßen aus:

- 1 Berechnet die gesamten Ressourcenanforderungen für alle eingeschalteten virtuellen Maschinen im Cluster.
- 2 Berechnet die gesamten Hostressourcen, die den virtuellen Maschinen zur Verfügung stehen.
- 3 Berechnet die aktuelle CPU-Failover-Kapazität und die aktuelle Arbeitsspeicher-Failover-Kapazität für den Cluster.
- 4 Stellt fest, ob entweder die aktuelle CPU-Failover-Kapazität oder die aktuelle Arbeitsspeicher-Failover-Kapazität weniger als die (vom Benutzer angegebene) konfigurierte Failover-Kapazität ist.

Ist dies der Fall, wird der Vorgang von der Zugangssteuerung nicht zugelassen.

VMware HA verwendet die tatsächlichen Reservierungen der virtuellen Maschinen. Verfügt eine virtuelle Maschine über keine Reservierungen, d. h., die Reservierung ist 0, werden standardmäßig 0 MB Arbeitsspeicher und 256 MHz CPU angesetzt.

Berechnen der aktuellen Failover-Kapazität

Die gesamten Ressourcenanforderungen für die eingeschalteten virtuellen Maschinen setzt sich aus zwei Komponenten zusammen: CPU und Arbeitsspeicher. VMware HA berechnet diese Werte.

- Die CPU-Komponente durch Addieren der CPU-Reservierungen der eingeschalteten virtuellen Maschinen. Wenn Sie keine Angabe zur CPU-Reservierung für eine virtuelle Maschine gemacht haben, wird ihr ein Standardwert von 256 MHz zugewiesen (dieser Wert kann durch Zuweisung des erweiterten Attributs „das.vmCpuMinMHz“ geändert werden).
- Die Arbeitsspeicherkomponente durch Addieren der Arbeitsspeicherreservierung (zzgl. Arbeitsspeicher-Overhead) einer jeden eingeschalteten virtuellen Maschine.

Die gesamten, für virtuellen Maschinen zur Verfügung stehenden Hostressourcen werden durch Addieren der CPU- und Arbeitsspeicherressourcen des Hosts berechnet. Dies entspricht der Menge, die der Ressourcenpool des Hosts enthält, nicht den gesamten physischen Ressourcen des Hosts. Die für die Virtualisierung verwendeten Ressourcen sind nicht enthalten. Nur Hosts, die verbunden und nicht im Wartungsmodus sind sowie keine VMware HA-Fehler aufweisen, werden berücksichtigt.

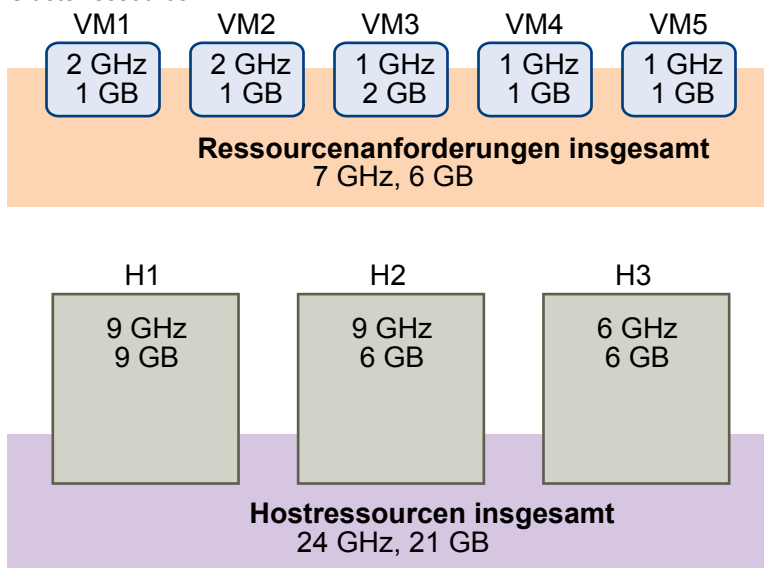
Die aktuelle CPU-Failover-Kapazität wird durch Subtrahieren der gesamten CPU-Ressourcenanforderungen von den gesamten Host-CPU-Ressourcen und Dividieren des Ergebnisses durch die gesamten Host-CPU-Ressourcen berechnet. Die aktuelle Arbeitsspeicher-Failover-Kapazität wird in gleicher Weise berechnet.

Beispiel 2-2. Zugangssteuerung mit der Richtlinie „Prozentsatz der reservierten Clusterressourcen“

Die Berechnung und Verwendung der aktuellen Failover-Kapazität durch diese Richtlinie für die Zugangssteuerung wird an einem Beispiel gezeigt. Nehmen Sie Folgendes für einen Cluster an:

- Der Cluster besteht aus drei Hosts, jeder mit einer anderen Menge an verfügbaren CPU- und Arbeitsspeicherressourcen. Der erste Host (H1) hat 9 GHz verfügbarer CPU-Ressourcen und 9 GB verfügbaren Arbeitsspeichers, Host 2 (H2) verfügt über 9 GHz und 6 GB und Host 3 (H3) verfügt über 6 GHz und 6 GB.
- Es befinden sich fünf eingeschaltete virtuelle Maschinen im Cluster, mit unterschiedlichen CPU- und Arbeitsspeicheranforderungen. VM1 benötigt 2 GHz CPU-Ressourcen und 1 GB Arbeitsspeicher, VM2 benötigt 2 GHz und 1 GB, VM3 benötigt 1 GHz und 2 GB, VM4 benötigt 1 GHz und 1 GB und VM5 benötigt 1 GHz und 1 GB.
- Die konfigurierte Failover-Kapazität ist auf 25 % festgelegt.

Abbildung 2-2. Zugangssteuerungsbeispiel mit der Richtlinie „Prozentsatz der reservierten Clusterressourcen“



Die gesamten Ressourcenanforderungen für die eingeschalteten virtuellen Maschinen sind 7 GHz und 6 GB. Die gesamten Hostressourcen, die den virtuellen Maschinen zur Verfügung stehen, sind 24 GHz und 21 GB. Demzufolge beläuft sich die aktuelle CPU-Failover-Kapazität auf 70 % $((24 \text{ GHz} - 7 \text{ GHz})/24 \text{ GHz})$. Auf die gleiche Weise beläuft sich die aktuelle Arbeitsspeicher-Failover-Kapazität auf 71 % $((21 \text{ GB} - 6 \text{ GB})/21 \text{ GB})$.

Da die konfigurierte Failover-Kapazität des Clusters auf 25 % festgelegt ist, stehen für das Einschalten zusätzlicher virtueller Maschinen noch 45 % der gesamten CPU-Ressourcen und 46 % der Arbeitsspeicherressourcen des Clusters zur Verfügung.

Zugangssteuerung mit der Richtlinie „Failover-Host angeben“

Sie können VMware HA für das Auswählen eines bestimmten Hosts als Failover-Host konfigurieren.

Wenn ein Host ausfällt, versucht VMware HA unter Verwendung der Richtlinie für die Zugangssteuerung „Failover-Host angeben“ seine virtuellen Maschinen auf einem angegebenen Failover-Host neu zu starten. Wenn dies nicht möglich ist, z. B. weil der Failover-Host selbst ausgefallen ist oder nicht über genügend Ressourcen verfügt, versucht VMware HA diese virtuellen Maschinen auf anderen Hosts im Cluster neu zu starten.

Es wird verhindert, dass Sie virtuelle Maschinen auf dem Failover-Host einschalten oder unter Verwendung von vMotion dorthin migrieren, um sicherzustellen, dass genügend Kapazität auf dem Failover-Host verfügbar bleibt. Außerdem verwendet DRS den Failover-Host nicht für den Lastausgleich.

Im vSphere-Client wird im Abschnitt „VMware HA“ der Registerkarte **[Übersicht]** des Clusters der aktuelle Failover-Host angezeigt. Das Statussymbol neben dem Host kann grün, gelb oder rot sein.

- Grün. Der Host ist verbunden, befindet sich nicht im Wartungsmodus und hat keine VMware HA-Fehler. Es befinden sich keine eingeschalteten virtuellen Maschinen auf dem Host.
- Gelb. Der Host ist verbunden, befindet sich nicht im Wartungsmodus und hat keine VMware HA-Fehler. Es befinden sich jedoch eingeschaltete virtuelle Maschinen auf dem Host.
- Rot. Der Host ist nicht verbunden, befindet sich im Wartungsmodus oder hat VMware HA-Fehler.

Auswählen einer Richtlinie für die Zugangssteuerung

Wählen Sie eine VMware HA-Richtlinie für die Zugangssteuerung basierend auf Ihren Verfügbarkeitsanforderungen und den Eigenschaften Ihres Clusters aus. Wenn Sie eine Richtlinie für die Zugangssteuerung auswählen, sollten Sie mehrere Faktoren berücksichtigen.

Vermeiden der Ressourcenfragmentierung

Von Ressourcenfragmentierung spricht man, wenn zwar insgesamt genug Ressourcen für das Failover einer virtuellen Maschine vorhanden sind, sich diese Slots jedoch auf mehreren Hosts befinden und nicht verwendet werden können, da eine virtuelle Maschine nicht gleichzeitig auf mehreren ESX/ESXi-Hosts ausgeführt werden kann. Die Richtlinie „Vom Cluster tolerierte Hostfehler“ vermeidet Ressourcenfragmentierung, indem sie ein Slot als die maximale Reservierung für eine virtuelle Maschine festlegt. Die Richtlinie „Prozentsatz der Cluster-Ressourcen“ befasst sich nicht mit der Ressourcenfragmentierung. Mit der Richtlinie „Failover-Host angeben“ werden Ressourcen nicht fragmentiert, weil ein einzelner Host für Failover reserviert wird.

Flexibilität bei der Ressourcenreservierung für das Failover

Die Richtlinien für die Zugangssteuerung unterscheiden sich im Grad der Kontrolle, die sie Ihnen geben, wenn Sie Clusterressourcen für den Failover-Schutz reservieren. Die Richtlinie „Vom Cluster tolerierte Hostfehler“ ermöglicht Ihnen das Festlegen der Failover-Ebene von einem bis zu vier Hosts. Die Richtlinie „Prozentsatz der Cluster-Ressourcen“ ermöglicht Ihnen das Auswählen von bis zu 50 % der Clusterressourcen für Failover. Die Richtlinie „Failover-Host angeben“ erlaubt nur die Angabe eines einzigen Failover-Hosts.

Heterogenität der Cluster

Cluster können im Bezug auf die Ressourcenreservierung der virtuellen Maschine und der gesamten Ressourcenkapazität des Hosts heterogen sein. In einem heterogenen Cluster kann die Richtlinie „Vom Cluster tolerierte Hostfehler“ zu konservativ sein, weil sie nur die größten Reservierungen der virtuellen Maschine beim Festlegen der Slotgröße berücksichtigt und annimmt, dass beim Berechnen der aktuellen Failover-Kapazität die größten Hosts ausfallen. Die anderen zwei Richtlinien für die Zugangssteuerung sind von der Clusterheterogenität nicht betroffen.

HINWEIS VMware HA bezieht bei der Durchführung von Zugangssteuerungsberechnungen die Ressourcennutzung von sekundären virtuellen Fehlertoleranz-Maschinen ein. Für die Richtlinie „Vom Cluster tolerierte Hostfehler“ wird einer sekundären virtuellen Maschine ein Slot zugewiesen und für die Richtlinie „Prozentsatz der Cluster-Ressourcen“ wird bei der Berechnung der nutzbaren Kapazität des Clusters die Ressourcennutzung der sekundären virtuellen Maschine berücksichtigt.

VMware HA-Checkliste

In der VMware HA-Checkliste sind die Anforderungen aufgeführt, die Ihnen bekannt sein müssen, bevor Sie einen VMware HA-Cluster erstellen und verwenden.

Anforderungen eines VMware HA-Clusters

Überprüfen Sie diese Liste, bevor Sie einen VMware HA-Cluster einrichten. Weitere Informationen erhalten Sie in den entsprechenden Querverweisen oder unter „[Erstellen eines VMware HA-Clusters](#)“, auf Seite 21.

- Alle Hosts müssen für VMware HA lizenziert sein.
- Sie benötigen mindestens zwei Hosts im Cluster.
- Alle Hosts benötigen einen eindeutigen Hostnamen.
- Alle Hosts müssen mit statischen IP-Adressen konfiguriert werden. Wenn Sie DHCP verwenden, müssen Sie sichergehen, dass nach jedem Neustart die Adresse eines jeden Hosts beibehalten wird.
- Alle Hosts müssen über Zugriff auf dieselben Management-Netzwerke verfügen. Es muss unter allen Hosts mindestens ein gemeinsames Management-Netzwerk geben und es ist Best Practice, mindestens zwei davon zu haben. Verwaltungsnetze unterscheiden sich je nach der Version des Hosts, den Sie verwenden.
 - ESX-Hosts - Servicekonsolennetzwerk.
 - ESXi-Hosts vor Version 4.0 - VMkernel-Netzwerk.
 - ESXi-Hosts der Version 4.0 und höher - VMkernel-Netzwerk mit aktiviertem Kontrollkästchen **[Verwaltungsnetzwerk]** .

Weitere Informationen hierzu finden Sie unter „[Optimale Vorgehensweisen für Netzwerke](#)“, auf Seite 30.

- Alle Hosts sollten auf dieselben VM-Netzwerke und -Datenspeicher zugreifen können, um sicherzustellen, dass jede virtuelle Maschine auf jedem Host im Cluster ausgeführt werden kann. In gleicher Weise müssen sich virtuelle Maschinen auf gemeinsam genutztem, nicht lokalem Speicher befinden. Anderenfalls kann im Falle eines Hostsausfalls kein Failover erfolgen.
- VMware Tools muss installiert sein, damit die VM-Überwachung funktionieren kann. Weitere Informationen hierzu finden Sie unter „[VM und Anwendungsüberwachung](#)“, auf Seite 25.
- Für alle Hosts in einem VMware HA-Cluster muss DNS konfiguriert sein, sodass der kurze Hostname (ohne Domänensuffix) jedes Hosts im Cluster in die entsprechende IP-Adresse eines beliebigen anderen Hosts im Cluster aufgelöst werden kann. Anderenfalls kann die Aufgabe „HA konfigurieren“ (Configuring HA) fehlschlagen. Wenn Sie den Host über die IP-Adresse hinzufügen, aktivieren Sie ebenfalls die umgekehrte DNS-Suche (die IP-Adresse sollte auf den Kurznamen des Hosts aufgelöst werden können).

HINWEIS VMware HA unterstützt IPv6 nicht.

Erstellen eines VMware HA-Clusters

VMware HA arbeitet im Kontext eines Clusters von ESX/ESXi-Hosts. Sie müssen ein Cluster erstellen, Hosts hinzufügen und VMware HA-Einstellungen konfigurieren, bevor der Failover-Schutz eingerichtet werden kann.

Wenn Sie einen VMware HA-Cluster erstellen, müssen Sie mehrere Einstellungen konfigurieren, die festlegen, wie es funktioniert. Identifizieren Sie zuvor die Knoten Ihres Clusters. Diese Knoten sind die ESX/ESXi-Hosts, die die Ressourcen für virtuelle Maschinen bereitstellen werden und die von VMware HA verwendet werden, um Failover-Schutz zu bieten. Legen Sie daraufhin fest, wie diese Knoten miteinander und mit dem gemeinsam genutzten Speicher verbunden werden sollen, auf dem sich die Daten Ihrer virtuellen Maschine befinden. Wenn sich diese Netzwerkarchitektur an Ort und Stelle befindet, können Sie die Hosts zum Cluster hinzufügen und das Konfigurieren von VMware HA abschließen.

Sie können VMware HA aktivieren und konfigurieren, bevor Sie Hostknoten zum Cluster hinzufügen. Ihr Cluster ist jedoch vor dem Hinzufügen der Hosts nicht voll funktionsfähig und manche Clustereinstellungen sind nicht verfügbar. Beispielsweise ist die Richtlinie für die Zugangssteuerung „Failover-Host angeben“ nicht verfügbar, bis es einen Host gibt, der als Failover-Host ausgewählt werden kann.

HINWEIS Die Funktion „Starten und Herunterfahren von virtuellen Maschinen“ (automatischer Start) ist für alle virtuellen Maschinen deaktiviert, die sich auf den in einem VMware HA-Cluster verfügbaren Hosts sind (oder dorthin verschoben werden). Es wird empfohlen, dass Sie diese Einstellung für keine der virtuellen Maschinen manuell reaktivieren. Dies kann die Aktionen der Clusterfunktionen, wie z. B. VMware HA oder Fehlertoleranz, beeinträchtigen.

Erstellen eines VMware HA-Clusters

Ihr Cluster kann für VMware HA aktiviert werden. Ein VMware HA-aktivierter Cluster ist eine Voraussetzung zur Verwendung der Fehlertoleranz. VMware empfiehlt, dass Sie zunächst einen leeren Cluster erstellen. Nachdem Sie die Planung der Ressourcen und der Netzwerkarchitektur für Ihren Cluster abgeschlossen haben, können Sie mithilfe des vSphere-Clients Hosts zum Cluster hinzufügen und die Einstellungen für VMware HA festlegen.

Verbinden Sie den vSphere-Client unter Verwendung eines Kontos mit Clusteradministratorberechtigungen mit vCenter Server.

Voraussetzungen

Stellen Sie sicher, dass sich alle virtuellen Maschinen und deren Konfigurationsdateien auf gemeinsam genutztem Speicher befinden. Stellen Sie sicher, dass die Hosts so konfiguriert sind, dass sie Zugriff auf diesen gemeinsam genutzten Speicher haben, damit Sie die virtuellen Maschinen mithilfe verschiedener Hosts im Cluster einschalten können.

Stellen Sie sicher, dass jeder Host in einem VMware HA-Cluster über einen zugewiesenen Hostnamen (mit maximal 26 Zeichen) verfügt und jeder der virtuellen Netzwerkkarten eine statische IP-Adresse zugewiesen wurde.

Stellen Sie sicher, dass Hosts für den Zugriff auf das Netzwerk virtueller Maschinen konfiguriert sind.

HINWEIS Für VMware HA werden redundante Management-Netzwerkverbindungen empfohlen. Weitere Informationen zur Einrichtung von Netzwerkredundanz finden Sie unter „[Netzwerkpfadredundanz](#)“, auf Seite 31.

Vorgehensweise

- 1 Wählen Sie die Ansicht „Hosts & Cluster“ aus.
- 2 Klicken Sie mit der rechten Maustaste auf ein Datacenter in der Bestandslistenstruktur und klicken Sie auf **[Neuer Cluster]** .
- 3 Führen Sie den Assistenten für Neue Cluster aus.
Aktivieren Sie VMware HA (oder DRS) zu diesem Zeitpunkt nicht.
- 4 Klicken Sie auf **[Beenden]** , um den Assistenten zu schließen und den Cluster zu erstellen.
Sie haben einen leeren Cluster erstellt.
- 5 Fügen Sie basierend auf Ihrer Ressourcen- und Netzwerkarchitekturplanung mithilfe des vSphere-Clients Hosts zum Cluster hinzu.
- 6 Klicken Sie mit der rechten Maustaste auf den Cluster, und wählen Sie **[Einstellungen bearbeiten]** .
Im Dialogfeld Einstellungen des Clusters können Sie die Einstellungen für VMware HA und andere Clustereinstellungen ändern.
- 7 Wählen Sie auf der Seite „Clusterfunktionen“ die Option **[VMware HA einschalten]** .
- 8 Konfigurieren Sie dann die VMware HA-Einstellungen gemäß den Anforderungen Ihres Clusters.
 - Hostüberwachungsstatus
 - Zugangssteuerung
 - Optionen für virtuelle Maschinen
 - VM-Überwachung
- 9 Klicken Sie auf **[OK]** , um das Dialogfeld Einstellungen zu schließen.
Ein konfigurierter VMware HA-Cluster mit den angegebenen Hosts steht zur Verfügung.

Clusterfunktionen

Das erste Fenster im Assistenten für Neue Cluster ermöglicht Ihnen das Angeben von grundlegenden Optionen für den Cluster.

Geben Sie in diesem Fenster den Clusternamen an und wählen Sie mindestens eine der beiden Clusterfunktionen.

Name	Name des Clusters. Dieser Name wird im Bestandslistenbereich des vSphere-Clients angezeigt. Sie müssen zuerst einen Namen festlegen, damit Sie mit der Erstellung des Clusters fortfahren können.
VMware HA einschalten	Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Maschinen bei Ausfall des Hosts auf einem anderen Host im Cluster neu gestartet. Sie müssen VMware HA einschalten, wenn Sie die VMware-Fehlertoleranz auf einer virtuellen Maschine im Cluster aktivieren möchten.
VMware HA DRS einschalten	Wenn dieses Kontrollkästchen aktiviert ist, gleicht DRS die Last der virtuellen Maschinen im Cluster aus. DRS platziert und migriert virtuelle Maschinen auch dann, wenn sie mit HA geschützt sind.

Sie können jede dieser Clusterfunktionen später ändern.

Hostüberwachungsstatus

Nachdem Sie einen Cluster erstellt haben, aktivieren Sie die Hostüberwachung, sodass VMware HA Taktsignale überwachen kann, die vom VMware HA-Agenten auf jeden Host im Cluster gesendet werden.

Wenn **[Hostüberwachung aktivieren]** ausgewählt ist, wird bei jedem ESX/ESXi-Host im Cluster geprüft, ob er ausgeführt wird. Bei einem Hostausfall werden die virtuellen Maschinen auf eine anderen Host neu gestartet. Die Hostüberwachung ist auch erforderlich, damit der VMware-Fehlertoleranzprozess ordnungsgemäß ausgeführt wird.

HINWEIS Falls Sie Netzwerkwartungsmaßnahmen durchführen müssen, die Hostisolierungsreaktionen auslösen könnten, empfiehlt VMware, dass Sie zuerst VMware HA anhalten, indem Sie die Hostüberwachung deaktivieren. Aktivieren Sie die Hostüberwachung wieder, wenn die Wartungsarbeiten abgeschlossen sind.

Aktivieren und Deaktivieren der Zugangssteuerung

Mithilfe des Assistenten für neue Cluster können Sie die Zugangssteuerung für das VMware HA-Cluster aktivieren oder deaktivieren und eine Richtlinie für die Erzwingung auswählen.

Die Zugangssteuerung für das HA-Cluster kann aktiviert oder deaktiviert werden.

Aktivieren: VMs nicht einschalten, die gegen die Verfügbarkeitseinschränkungen verstoßen

Aktiviert die Zugangssteuerung, setzt Verfügbarkeitseinschränkungen durch und behält die Failover-Kapazität bei. Ein Vorgang auf einer virtuellen Maschine, der die nicht reservierten Ressourcen im Cluster reduziert und gegen Verfügbarkeitseinschränkungen verstößt, ist nicht zulässig.

Deaktivieren: VMs einschalten, die gegen die Verfügbarkeitseinschränkungen verstoßen

Deaktiviert die Zugangssteuerung. Virtuelle Maschinen können z. B. sogar dann eingeschaltet werden, wenn dies zu ungenügender Failover-Kapazität führt. Wenn Sie dies tun, werden keine Warnungen angezeigt und der Cluster wird nicht rot gekennzeichnet. Wenn ein Cluster über eine ungenügende Failover-Kapazität verfügt, kann VMware HA trotzdem Failover durchführen. High Availability verwendet die Einstellung „VM-Neustartpriorität“, um zu ermitteln, welche virtuellen Maschinen zuerst eingeschaltet werden sollen.

VMware HA bietet drei Richtlinien zur Erzwingung der Zugangssteuerung, wenn sie aktiviert ist.

- Vom Cluster tolerierte Hostfehler
- Prozentsatz der Cluster-Ressourcen, die als Failover-Ersatzkapazität reserviert sind
- Angeben eines Failover-Hosts

HINWEIS Weitere Informationen dazu, wie die Zugangssteuerung in VMware HA funktioniert, finden Sie unter [„Auswählen einer Richtlinie für die Zugangssteuerung“](#), auf Seite 19.

Optionen für virtuelle Maschinen

Die Standardeinstellungen der virtuellen Maschine steuern die Reihenfolge, in der virtuelle Maschinen neu gestartet werden (VM-Neustartpriorität), und wie VMware HA reagiert, wenn Hosts über keine Netzwerkverbindung mehr zu anderen Hosts (Hostisolierungsreaktion) verfügen.

Diese Einstellungen gelten für alle virtuellen Maschinen im Cluster im Falle eines Hostausfalls oder einer Hostisolation. Sie können zudem Ausnahmen für bestimmte virtuelle Maschinen konfigurieren. Weitere Informationen hierzu finden Sie unter [„Anpassen des VMware-HA-Verhaltens für eine einzelne virtuelle Maschine“](#), auf Seite 28.

VM-Neustartpriorität, Einstellung

Mithilfe der VM-Neustartpriorität legen Sie die relative Reihenfolge fest, in der die virtuellen Maschinen nach einem Hostausfall neu gestartet werden. Auf diese Weise werden virtuelle Maschinen auf neuen Hosts der Reihe nach neu gestartet. Dabei wird die virtuelle Maschine mit der höchsten Priorität zuerst und die mit der niedrigsten zuletzt gestartet, bis alle virtuellen Maschinen neu gestartet sind oder keine Clusterressourcen mehr zur Verfügung stehen. Wenn die Anzahl der Hostausfälle den von der Zugangssteuerung festgelegten Schwellenwert übersteigt, werden die virtuellen Maschinen mit einer niedrigen Priorität möglicherweise erst dann neu gestartet, wenn mehr Ressourcen zur Verfügung stehen. Virtuelle Maschinen werden auf dem Failover-Host neu gestartet, falls einer angegeben ist.

Die Werte für diese Einstellung sind: Deaktiviert, Niedrig, Mittel (Standardeinstellung) und Hoch. Falls Sie „Deaktiviert“ auswählen, ist VMware HA für die virtuelle Maschine deaktiviert, d. h., dass sie nicht auf einem anderen ESX/ESXi-Host neu gestartet wird, wenn ihr ESX/ESXi-Host ausfällt. Die Einstellung „Deaktiviert“ hat keine Auswirkung auf die Überwachung von virtuellen Maschinen. Wenn nämlich eine virtuelle Maschine auf einem Host, der ordnungsgemäß funktioniert, ausfällt, wird die virtuelle Maschine auf demselben Host zurückgesetzt. Diese Einstellung kann für einzelne virtuelle Maschinen geändert werden.

Die Neustartprioritätseinstellungen für virtuelle Maschinen sind je nach Benutzererfordnissen unterschiedlich. VMware empfiehlt, dass Sie denjenigen virtuellen Maschinen, die die wichtigsten Dienste verrichten, eine höhere Neustartpriorität zuweisen.

Im Falle einer Multi-Tier-Anwendung könnten Sie beispielsweise die Prioritäten abhängig von den auf den virtuellen Maschinen gehosteten Funktionen festlegen:

- Hoch Datenbankserver, die Daten für Anwendungen bereitstellen.
- Mittel Anwendungsserver, die in der Datenbank Daten konsumieren und die Ergebnisse auf Webseiten präsentieren.
- Niedrig Webserver, die Benutzeranforderungen empfangen, Abfragen an Anwendungsserver übertragen und die Ergebnisse an die Benutzer zurücksenden.

Hostisolierungsreaktionseinstellung

Die Hostisolierungsreaktion legt fest, was geschieht, wenn die Verbindungen des Hosts in einem VMware HA-Cluster zum Verwaltungsnetzwerk verloren gehen, dieser aber weiter ausgeführt wird. Hostisolierungsreaktionen setzen voraus, dass der Hostüberwachungsstatus aktiviert ist. Wenn der Hostüberwachungsstatus deaktiviert ist, werden die Hostisolierungsreaktionen ebenfalls angehalten. Ein Host stellt fest, dass er isoliert ist, wenn er keine weiteren Taktsignale von allen anderen Hosts empfängt und seine Isolationsadressen nicht anpingen kann. Tritt dies ein, führt der Host seine Isolierungsreaktion aus. Die Antworten lauten: Eingeschaltet lassen, Ausschalten und Herunterfahren (Standardeinstellung). Diese Eigenschaft kann für einzelne virtuelle Maschinen geändert werden.

Sie müssen zum Verwenden der Einstellung „VM herunterfahren“ VMware Tools auf dem Gastbetriebssystem der virtuellen Maschine installieren. Das Herunterfahren der virtuellen Maschine hat den Vorteil, dass ihr Zustand beibehalten wird. Es ist besser, die virtuelle Maschine herunterzufahren als sie auszuschalten, da beim Ausschalten die neuesten Änderungen nicht auf die Festplatte geschrieben und Transaktionen nicht übernommen werden. Virtuelle Maschinen, die heruntergefahren werden, benötigen während der Zeit des Herunterfahrens länger für ein Failover. Virtuelle Maschinen, die nicht innerhalb von 300 Sekunden oder in dem Zeitraum, der in dem erweiterten Attribut „das.isolationShutdownTimeout“ in Sekunden angegeben ist, heruntergefahren werden, werden ausgeschaltet.

HINWEIS Nach dem Erstellen eines VMware HA-Clusters können Sie für bestimmte virtuelle Maschinen die Standardclustereinstellungen „Neustartpriorität“ und „Isolierungsreaktion“ überschreiben. Dies ist nützlich bei virtuellen Maschinen, die zu speziellen Zwecken eingesetzt werden. Virtuelle Maschinen, die beispielsweise Infrastrukturdienste wie DNS oder DHCP bereitstellen, müssen möglicherweise vor anderen virtuellen Maschinen im Cluster eingeschaltet werden.

VM und Anwendungsüberwachung

Die VM-Überwachung sorgt dafür, dass individuelle virtuelle Maschinen neu gestartet werden, falls ihre VMware Tools-Taktsignale nicht innerhalb einer festgelegten Zeitspanne empfangen werden. In ähnlicher Weise kann die Anwendungsüberwachung eine virtuelle Maschine neu starten, falls die Taktsignale für eine Anwendung, die sie ausführt, nicht erhalten werden. Sie können diese Funktionen aktivieren und die Empfindlichkeit konfigurieren, mit der VMware HA die Nichtansprechbarkeit überwacht.

Wenn Sie die VM-Überwachung aktivieren, prüft der VM-Überwachungsdienst (mithilfe von VMware Tools) anhand der Regelmäßigkeit der Taktsignale und der E/A-Aktivität des VMware Tools-Prozesses, der im Gastbetriebssystem läuft, ob die einzelnen virtuellen Maschinen im Cluster ausgeführt werden. Werden keine Taktsignale oder E/A-Aktivitäten empfangen, liegt dies wahrscheinlich daran, dass das Gastbetriebssystem ausgefallen ist oder VMware Tools keine Rechenzeit zum Abschließen von Aufgaben zugeteilt wurde. In einem solchen Fall stellt der VM-Überwachungsdienst fest, dass die virtuelle Maschine ausgefallen ist. Die virtuelle Maschine wird dann neu gestartet.

Manchmal hören virtuelle Maschinen oder Anwendungen, die noch ordnungsgemäß ausgeführt werden, auf, Taktsignale zu senden. Um das unnötige Zurücksetzen zu verhindern, überwacht der VM-Überwachungsdienst außerdem die E/A-Aktivität einer virtuellen Maschine. Falls innerhalb des Fehlerintervalls keine Taktsignale empfangen werden, wird das E/A-Statistikintervall (ein Attribut auf Clusterebene) geprüft. Das E/A-Statistikintervall ermittelt, ob während der vergangenen 2 Minuten (120 Sekunden) von der virtuellen Maschine eine Festplatten- oder Netzwerkaktivität ausgegangen ist. Ist dies nicht der Fall, wird die virtuelle Maschine zurückgesetzt. Dieser Standardwert (120 Sekunden) kann über das erweiterte Attribut „das.iostatInterval“ geändert werden.

Sie müssen sich zum Aktivieren der Anwendungsüberwachung zunächst das entsprechende SDK besorgen (oder eine Anwendung verwenden, die VMware Application Monitoring unterstützt) und es zum Einrichten von benutzerdefinierten Taktsignalen für die Anwendungen, die Sie überwachen möchten, verwenden. Danach arbeitet die Anwendungsüberwachung ähnlich wie die VM-Überwachung. Wenn die Taktsignale für eine Anwendung nicht innerhalb einer angegebenen Frist empfangen werden, wird deren virtuelle Maschine neu gestartet.

Sie können die Überwachungsempfindlichkeitsstufe konfigurieren. Bei einer hohen Überwachungsstufe werden Ausfälle schneller ermittelt. Obgleich es unwahrscheinlich ist, kann eine überempfindliche Überwachung dazu führen, dass fälschlicherweise Ausfälle ermittelt werden, falls die betroffene virtuelle Maschine oder Anwendung funktionsfähig ist, jedoch aufgrund von Faktoren wie Ressourceneinschränkungen keine Taktsignale empfangen wurden. Eine niedrige Überwachungsstufe führt zu längeren Dienstunterbrechungen zwischen tatsächlichen Ausfällen und dem Zurücksetzen von virtuellen Maschinen. Wählen Sie eine Option, die einen effektiven Kompromiss für Ihre Anforderungen darstellt.

Die Standardeinstellungen für die Überwachungsempfindlichkeit werden unter [Tabelle 2-1](#) beschrieben. Sie können auch benutzerdefinierte Werte sowohl für die Empfindlichkeit der VM-Überwachung als auch für das E/A-Statistikintervall angeben, indem Sie das Kontrollkästchen **[Benutzerdefiniert]** aktivieren.

Tabelle 2-1. VM-Überwachungseinstellungen

Einstellen	Ausfallintervall (Sekunden)	Zurücksetzungszeitraum
Hoch	30	1 Stunde:
Mittel	60	24 Stunden
Niedrig	120	7 Tage

Nachdem Ausfälle festgestellt wurden, sorgt VMware HA für das Zurücksetzen der virtuellen Maschinen. Das Reset stellt sicher, dass die Dienste verfügbar bleiben. Um zu verhindern, dass bei flüchtigen Fehlern virtuelle Maschinen wiederholt zurückgesetzt werden, werden standardmäßig während einer bestimmten, konfigurierbaren Zeitspanne virtuelle Maschinen nur drei Mal zurückgesetzt. Nachdem virtuelle Maschinen

drei Mal zurückgesetzt wurden, unternimmt VMware HA keine weiteren Versuche, sie infolge von weiteren Ausfällen oder nach Ablauf der angegebenen Zeitspanne zurückzusetzen. Sie können die Anzahl der Rücksetzungen unter Verwendung der benutzerdefinierten Einstellung **[Maximale Rücksetzungen pro VM]** konfigurieren.

Anpassen des VMware-HA-Verhaltens

Nachdem Sie einen Cluster eingerichtet haben, können Sie die spezifischen Attribute ändern, die das Verhalten von VMware HA beeinflussen. Sie können die von den virtuellen Maschinen übernommenen Standard-Clustereinstellungen ändern.

Überprüfen Sie die erweiterten Einstellungen, die Sie zum Optimieren der VMware HA-Cluster in Ihrer Umgebung verwenden können. Da sich diese Attribute auf die Funktionsweise von HA auswirken, sollten Sie diese mit Bedacht ändern.

Festlegen von erweiterten VMware HA-Optionen

Legen Sie erweiterte VMware HA-Optionen fest, um das VMware HA-Verhalten anzupassen.

Voraussetzungen

Ein VMware HA-Cluster, dessen Einstellungen geändert werden sollen.

Clusteradministratorrechte.

Vorgehensweise

- 1 Wählen Sie im Dialogfeld **[Clustereinstellungen (Cluster Settings)]** die Option **[VMware HA]**.
- 2 Klicken Sie auf die Schaltfläche **[Erweiterte Optionen (Advanced Options)]**, um das Dialogfeld **[Erweiterte Optionen (HA) (Advanced Options (HA))]** zu öffnen.
- 3 Geben Sie alle zu ändernden erweiterten Attribute in einem Textfeld in der Spalte **[Option]** ein und legen Sie in der Spalte **[Wert]** den zugehörigen Wert fest.
- 4 Klicken Sie auf **[OK]**.

Der Cluster verwendet Optionen, die Sie hinzugefügt oder geändert haben.

VMware HA - erweiterte Attribute

Sie können erweiterte Attribute festlegen, die das Verhalten Ihres VMware HA-Clusters beeinflussen.

Tabelle 2-2. VMware HA - erweiterte Attribute

Attribut	Beschreibung
das.isolationaddress[...]	Legt die Adresse für den Ping-Test fest, über den geprüft wird, ob ein Host vom Netzwerk isoliert ist. Diese Adresse wird nur dann angepingt, wenn keine Taktsignale von einem anderen Host im Cluster empfangen werden. Falls nicht angegeben, wird das Standard-Gateway des Management-Netzwerks verwendet. Das Standard-Gateway muss eine zuverlässige Adresse sein, die sicher verfügbar ist, sodass der Host ermitteln kann, ob er vom Netzwerk isoliert ist. Sie können mehrere Isolierungsadressen (max. 10) für den Cluster angeben: das.isolationaddressX, wobei X = 1-10. In der Regel sollten Sie eine Adresse pro Management-Netzwerk angeben. Die Angabe zu vieler Adressen führt dazu, dass die Isolationserkennung zu lange dauert.
das.usedefaultisolationaddress	Standardmäßig verwendet VMware HA das Standard-Gateway des Konsolennetzwerks als Prüfadresse, um eine Isolierung festzustellen. Dieses Attribut legt fest, ob dieser Standardwert verwendet wird (true false).
das.failedetectiontime	Ändert die Standardzeitdauer für das Erkennen eines Hostausfalls. Der Standardwert beträgt 15000 Millisekunden (15 Sekunden). Dies ist die Zeitspanne, innerhalb der ein Host kein Taktsignal von einem anderen Host empfängt und den Host als ausgefallen betrachtet.
das.failedetectioninterval	Ändert das Taktsignalintervall zwischen VMware HA-Hosts. Standardmäßig erfolgt dies alle 1000 Millisekunden (1 Sekunde).
das.isolationshutdowntimeout	Der Zeitraum, in dem das System auf das Herunterfahren einer virtuellen Maschine wartet, bevor es sie ausschaltet. Dies gilt nur, wenn die Isolierungsreaktion des Hosts „VM herunterfahren“ ist. Der Standardwert beträgt 300 Sekunden.
das.slotmeminmb	Definiert die Obergrenze der Arbeitsspeicher-Slotgröße. Wenn diese Option verwendet wird, ist die Slotgröße dieser Wert, sofern sie kleiner als die maximale Arbeitsspeicherreservierung zuzüglich Arbeitsspeicher-Overhead einer beliebigen eingeschalteten virtuellen Maschine im Cluster ist.
das.slotcpuinmhz	Definiert die Obergrenze der CPU-Slotgröße. Wenn diese Option verwendet wird, ist die Slotgröße dieser Wert, sofern sie geringer als die maximale CPU-Reservierung einer beliebigen eingeschalteten virtuellen Maschine im Cluster ist.
das.vmMemoryMinMB	Definiert den Standardwert der der virtuellen Maschine zugewiesenen Arbeitsspeicherressource, falls ihre Arbeitsspeicherreservierung Null oder nicht angegeben ist. Dieser Wert wird für die Richtlinie „Vom Cluster tolerierte Hostfehler“ verwendet. Falls kein Wert angegeben wird, gilt der Standardwert von 0 MB.

Tabelle 2-2. VMware HA - erweiterte Attribute (Fortsetzung)

Attribut	Beschreibung
das.vmcpuminhz	Definiert den Standardwert der der virtuellen Maschine zugewiesenen CPU-Ressource, falls ihre CPU-Reservierung Null oder nicht angegeben ist. Dieser Wert wird für die Richtlinie „Vom Cluster tolerierte Hostfehler“ verwendet. Falls kein Wert festgelegt wird, lautet der Standardwert 256 MHz.
das.iostatsinterval	Ändert das E/A-Statistikintervall für die VM-Überwachungsempfindlichkeit. Die Standardeinstellung lautet 120 Sekunden. Kann auf jeden Wert größer gleich Null eingestellt werden. Bei einem Wert von 0 wird die Prüfung deaktiviert.

HINWEIS Wenn Sie den Wert eines der folgenden erweiterten Attribute ändern, müssen Sie VMware HA deaktivieren und neu aktivieren, damit Ihre Änderungen wirksam werden.

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.failedetectiontime
- das.failedetectioninterval
- das.isolationshutdowntimeout

Anpassen des VMware-HA-Verhaltens für eine einzelne virtuelle Maschine

In einem VMware HA-Cluster wird allen virtuellen Maschinen die Standard-Clustereinstellungen für die VM-Neustartpriorität, die Hostisolierungsreaktion und die VM-Überwachung zugewiesen. Sie können ein bestimmtes Verhalten für jede virtuelle Maschine festlegen, indem Sie diese Standardeinstellungen ändern. Wenn die virtuelle Maschine aus dem Cluster entfernt wird, gehen diese Einstellungen verloren.

Vorgehensweise

- 1 Wählen Sie den Cluster, und klicken Sie im Kontextmenü auf die Option **[Einstellungen bearbeiten]**.
- 2 Klicken Sie unter VMware HA auf **[Optionen für virtuelle Maschinen]**.
- 3 Wählen Sie im Fenster „Einstellungen der virtuellen Maschine“ eine virtuelle Maschine aus und ändern Sie die Einstellung für die **[VM-Neustartpriorität]** oder die **[Hostisolierungsreaktion]**.
- 4 Wählen Sie **[VM-Überwachung]** unter „VMware HA“ aus.
- 5 Wählen Sie im Fenster „Einstellungen der virtuellen Maschine“ eine virtuelle Maschine aus und ändern Sie die Einstellung für die **[VM-Überwachung]**.
- 6 Klicken Sie auf **[OK]**.

Das Verhalten der virtuellen Maschine wird jetzt gemäß den geänderten Einstellungen angepasst.

Empfohlene Vorgehensweisen für VMware HA-Cluster

Um die optimale Leistung eines VMware HA-Clusters gewährleisten zu können, sollten Sie bestimmte empfohlene Vorgehensweisen einhalten. Bei der Planung und Implementierung eines Clusters sind Netzwerkkonfiguration und -redundanz von Bedeutung.

Einstellen von Alarmen für die Überwachung von Clusteränderungen

Wenn von VMware HA oder der Fehlertoleranz Aktionen für den Erhalt der Verfügbarkeit eingeleitet werden, z. B. das Failover einer virtuellen Maschine, kann es notwendig sein, dass Sie über diese Änderung informiert werden. Sie können in vCenter Server Alarme konfigurieren, die ausgelöst werden, wenn diese Aktionen durchgeführt werden, und Warnungen, z. B. E-Mails, an eine definierte Gruppe von Administratoren senden.

Überwachen der Clustergültigkeit

Ein Cluster ist gültig, wenn er nicht gegen die Richtlinie für die Zugangssteuerung verstößt.

Ein für VMware HA aktivierter Cluster wird rot gekennzeichnet, wenn die Anzahl an eingeschalteten virtuellen Maschinen die Failover-Anforderungen übersteigt, d.h. die aktuelle Failover-Kapazität geringer als die konfigurierte Failover-Kapazität ist. Falls die Zugangssteuerung deaktiviert ist, werden Cluster nicht ungültig.

Auf der Übersichtsseite des Clusters im vSphere-Client wird eine Liste mit den Clusterkonfigurationsproblemen angezeigt. In der Liste wird erläutert, was dazu geführt hat, dass der Cluster ungültig wurde bzw. überbelegt (gelb) ist.

Das DRS-Verhalten wird nicht beeinträchtigt, wenn ein Cluster aufgrund eines VMware HA-Problems rot gekennzeichnet wird.

Prüfen des Betriebsstatus des Clusters

Es gibt Konfigurationsprobleme und andere Fehler, die bei Ihrem Cluster oder dessen Hosts auftreten können, die den ordnungsgemäßen Betrieb von VMware HA nachteilig beeinflussen. Sie können diese Fehler auf dem Bildschirm „Betriebsstatus des Clusters“ überwachen, auf das im vSphere-Client vom Abschnitt „VMware HA“ der Registerkarte **[Übersicht]** des Clusters aus zugegriffen wird. Sie sollten auf alle Probleme eingehen, die hier aufgeführt werden.

Optimale Vorgehensweisen für Netzwerke

Für die Konfiguration der Host-Netzwerkkarten und der Netzwerktopologie für VMware HA werden bestimmte Vorgehensweisen empfohlen. Zu den empfohlenen Vorgehensweisen gehören Empfehlungen für die ESX/ESXi-Hosts sowie für die Verkabelung, Switches, Router und Firewalls.

Netzwerkconfiguration und -wartung

Die folgenden Vorschläge zur Netzwerkwartung können dazu beitragen, dass nicht aufgrund verlorener VMware HA-Taktsignale fälschlicherweise Hostausfälle und Netzwerkisolation diagnostiziert werden.

- Wenn Sie Änderungen an den Netzwerken vornehmen, zu denen Ihre ESX/ESXi-Host-Cluster gehören, wird empfohlen, die Funktion „Hostüberwachung“ anzuhalten. Das Ändern Ihrer Netzwerkhardware oder der Netzwerkeinstellungen kann die Taktsignale unterbrechen, die VMware HA verwendet, um Hostausfälle zu erkennen, und dies kann zu ungewünschten Failover-Versuchen für virtuelle Maschinen führen.
- Wenn Sie die Netzwerkconfiguration auf den ESX/ESXi-Hosts selbst ändern, beispielsweise, indem Sie Portgruppen hinzufügen oder vSwitches entfernen, wird empfohlen, dass Sie nicht nur die Hostüberwachung anhalten, sondern zusätzlich den Host in den Wartungsmodus versetzen.

HINWEIS Weil das Netzwerk eine kritische Komponente von VMware HA ist, sollte der VMware HA-Administrator über alle Wartungsarbeiten am Netzwerk vorab informiert werden.

Für VMware HA-Kommunikation verwendete Netzwerke

Um die Netzwerkvorgänge identifizieren zu können, die die Funktion von VMware HA unterbrechen, sollten Sie wissen, welche Verwaltungsnetzwerke für die Taktsignale und andere VMware HA-Kommunikation verwendet werden.

- Auf ESX-Hosts im Cluster verwendet die VMware HA-Kommunikation alle Netzwerke, die als Servicekonsolennetzwerke ausgewählt sind. VMkernel-Netzwerke werden von diesen Hosts nicht für die VMware HA-Kommunikation verwendet.
- Auf ESXi-Hosts im Cluster verwendet die VMware HA-Kommunikation standardmäßig VMkernel-Netzwerke, allerdings nicht solche, die für die Verwendung mit VMotion vorgesehen sind. Falls nur ein VMkernel-Netzwerk vorhanden ist, nutzt VMware HA dieses bei Bedarf gemeinsam mit VMotion. Bei ESXi 4.0 und später müssen Sie das Kontrollkästchen „Verwaltungsnetzwerk“ aktivieren, damit VMware HA dieses Netzwerk verwendet.

Hinweise für clusterweite Netzwerke

Damit VMware HA funktioniert, müssen alle Hosts im Cluster über kompatible Netzwerke verfügen. Der erste Knoten, der einem Cluster hinzugefügt wird, gibt die Netzwerke vor, über die alle nachfolgenden Hosts im Cluster verfügen müssen. Netzwerke werden als kompatibel betrachtet, wenn die Kombination aus IP-Adresse und Subnetzmaske ein Netzwerk ergibt, das dem Netzwerk eines anderen Hosts entspricht. Falls Sie versuchen, einen Host mit nicht genügend oder zu vielen Verwaltungsnetzwerken hinzuzufügen oder der hinzuzufügende Host über nicht kompatible Netzwerke verfügt, schlägt die Konfiguration fehl und die Inkompatibilität wird in den Aufgabedetails angezeigt.

Falls beispielsweise der Host, den Sie dem Cluster als Erstes hinzufügen, zwei Netzwerke, 10.10.135.0/255.255.255.0 und 10.17.142.0/255.255.255.0, hat, die für die VMware HA-Kommunikation verwendet werden, müssen alle nachfolgend hinzugefügten Hosts dieselben Netzwerke konfiguriert haben und für die VMware HA-Kommunikation einsetzen.

Netzwerkisolierungsadressen

Eine Netzwerkisolierungsadresse ist eine IP-Adresse, die angepingt wird, um festzustellen, ob ein Host vom Netzwerk isoliert ist. Diese Adresse wird nur dann angepingt, wenn ein Host keine Taktsignale mehr von den anderen Hosts im Cluster empfängt. Falls ein Host seine Netzwerkisolierungsadresse anpingen kann, ist der Host nicht netzwerkisoliert, sondern die anderen Hosts im Cluster sind ausgefallen. Falls der Host jedoch seine Isolierungsadresse nicht anpingen kann, ist es wahrscheinlich, dass der Host vom Netzwerk isoliert und keine Failover-Maßnahme ergriffen wurde.

Standardmäßig ist die Netzwerkisolierungsadresse das Standard-Gateway für den Host. Ungeachtet der Anzahl der definierten Verwaltungsnetzwerke ist nur ein Standard-Gateway angegeben. Daher sollten Sie das erweiterte Attribut „`das.isolationaddress[...]`“ verwenden, um Isolierungsadressen für weitere Netzwerke hinzuzufügen. Weitere Informationen hierzu finden Sie unter „[VMware HA - erweiterte Attribute](#)“, auf Seite 27.

Bei Angabe einer zusätzlichen Isolierungsadresse wird empfohlen, die Einstellung für das erweiterte Attribut `das.failedetectiontime` auf 20000 Millisekunden (20 Sekunden) oder mehr zu erhöhen. Ein Knoten, der vom Netzwerk isoliert ist, benötigt Zeit, um die VMFS-Sperren seiner virtuellen Maschine zu lösen, falls als Hostisolierungsreaktion ein Failover der virtuellen Maschinen durchgeführt wird (sie nicht eingeschaltet gelassen werden). Dies muss geschehen, bevor die anderen Knoten feststellen, dass dieser Knoten ausgefallen ist, damit sie die virtuellen Maschinen einschalten können, ohne die Fehlermeldung zu erhalten, dass die virtuellen Maschinen noch vom isolierten Knoten gesperrt ist.

Weitere Informationen zu den erweiterten Attributen von VMware HA finden Sie unter „[Anpassen des VMware-HA-Verhaltens](#)“, auf Seite 26.

Andere Netzwerkhinweise

Switches konfigurieren. Falls die physischen Netzwerkschwitches, die Ihre Server miteinander verbinden, die Einstellung „PortFast“ (oder eine entsprechende Einstellung) unterstützen, aktivieren Sie sie. Mit dieser Einstellung wird ein Host daran gehindert, fälschlicherweise festzustellen, dass bei der Ausführung eines umfangreichen Baum-Algorithmus ein Netzwerk isoliert ist.

Host-Firewalls. Auf ESX/ESXi-Hosts benötigt VMware HA die folgenden Firewallports und öffnet sie automatisch.

- Eingehender Port: TCP/UDP 8042-8045
- Ausgehender Port: TCP/UDP 2050-2250

Portgruppenname und Netzwerkbezeichnung. Verwenden Sie für öffentliche Netzwerke konsistente Portgruppennamen und Netzwerkbezeichnungen in VLANs. Portgruppennamen werden für die Neukonfiguration des Zugriffs auf das Netzwerk durch virtuelle Maschinen verwendet. Wenn Sie keine einheitlichen Namen zwischen dem ursprünglichen Server und dem Failover-Server verwenden, wird die Verbindung zwischen virtuellen Maschinen und Netzwerken nach einem Failover getrennt. Netzwerkbezeichnungen werden von virtuellen Maschinen verwendet, um die Netzwerkkonnektivität beim Neustart wiederherzustellen.

Netzwerkpfadredundanz

Redundanz des Netzwerkpfads zwischen Clusterknoten ist für die Zuverlässigkeit von VMware HA erforderlich. Ein einzelnes Verwaltungsnetzwerk wird zu einer einzelnen Fehlerstelle und kann zu Failovers führen, wenn nur das Netzwerk ausgefallen ist.

Wenn Sie nur über ein Verwaltungsnetzwerk verfügen, kann jeder Fehler zwischen dem Host und dem Cluster eine nicht notwendige (oder fehlerhafte) Failover-Situation herbeiführen. Zu den möglichen Ausfallursachen gehören Fehler in der Netzwerkkarte oder im Netzwerkkabel, das Entfernen des Netzwerkkabels und das Zurücksetzen des Switches. Berücksichtigen Sie diese möglichen Fehlerquellen zwischen Hosts und versuchen Sie, solche Fehler zu vermeiden, in der Regel durch Schaffung von Netzwerkredundanz.

Sie können die Netzwerkredundanz auf Netzwerkkartenebene mit NIC-Gruppierung oder auf Verwaltungsebene implementieren. Für die meisten Implementierungen reicht die durch die NIC-Gruppierung bereitgestellte Redundanz aus. Falls erforderlich, können Sie die Verwaltungsnetzwerkredundanz nutzen oder hinzufügen. Die Nutzung eines redundanten Verwaltungsnetzwerks ermöglicht eine zuverlässige Fehlererkennung und verhindert, dass Isolierungssituationen auftreten, da Taktsignale über mehrere Netzwerke gesendet werden können.

Konfigurieren Sie so wenig Hardwaresegmente wie möglich zwischen den Servern in einem Cluster. Dies dient dem Zweck, die Anzahl der einzelnen Ausfallstellen so gering wie möglich zu halten. Außerdem muss bei Weiterleitungen mit zu vielen Hops mit Verzögerungen von Netzwerkpaket für Taktsignale und potentiellen Fehlerstellen gerechnet werden.

Netzwerkredundanz mit NIC-Gruppierung

Durch die Verwendung einer Gruppe mit zwei Netzwerkkarten, die mit separaten physischen Switches verbunden sind, wird die Zuverlässigkeit eines Verwaltungsnetzwerks verbessert. Da über zwei Netzwerkkarten (und zwei separate Switches) verbundene Server über zwei unabhängige Pfade für das Senden und Empfangen von Taktsignalen verfügen, ist der Cluster belastbarer. Bei der Konfiguration einer Gruppe von Netzwerkkarten für das Verwaltungsnetzwerk sollten die virtuellen Netzwerkkarten beim Konfigurieren des vSwitches auf „Aktiv“ oder „Standby“ gesetzt werden. Folgende Parametereinstellungen für die virtuellen Netzwerkkarten werden empfohlen:

- Standardlastenausgleich = Anhand der Quelle der Port-ID routen (Route based on originating port ID)
- Failback = Nein (No)

Nach Hinzufügen einer Netzwerkkarte zu einem Host im VMware HA-Cluster müssen Sie VMware HA auf diesem Host neu konfigurieren.

Netzwerkredundanz durch Einsatz eines sekundären Netzwerks

Alternativ zur NIC-Gruppierung für die Bereitstellung redundanter Taktsignale können Sie auch eine sekundäre Verwaltungsnetzwerkverbindung erstellen, die an einen separaten Switch angeschlossen wird. Die primäre Verwaltungsnetzwerkverbindung dient Netzwerk- und Verwaltungszwecken. Sobald die sekundäre Verwaltungsnetzwerkverbindung erstellt wurde, sendet VMware HA Taktsignale sowohl über die primäre als auch über die sekundäre Verwaltungsnetzwerkverbindung. Sollte ein Pfad ausfallen, kann VMware HA über den anderen Pfad noch immer Taktsignale senden und empfangen.

Aktivieren der Fehlertoleranz für virtuelle Maschinen

3

Sie können die VMware-Fehlertoleranz für Ihre virtuellen Maschinen aktivieren, um die Business Continuity mit einer höheren Verfügbarkeit und einem besseren Datenschutz als bei VMware HA sicherzustellen.

Die Fehlertoleranz basiert auf der ESX/ESXi-Hostplattform (mithilfe der vLockstep-Technologie von VMware) und sie bietet eine unterbrechungsfreie Verfügbarkeit, indem identische virtuelle Maschinen in einem virtuellen Gleichschritt auf separaten Hosts ausgeführt werden.

Um mit der Fehlertoleranz optimale Ergebnisse zu erzielen, sollten Sie mit ihrer Funktionsweise, dem Vorgang zu ihrer Aktivierung für Ihren Cluster und Ihre virtuellen Maschinen, den Best Practices für ihre Verwendung und den Tipps zur Fehlerbehebung vertraut sein.

Dieses Kapitel behandelt die folgenden Themen:

- [„Wie die Fehlertoleranz funktioniert“](#), auf Seite 33
- [„Verwendung der Fehlertoleranz mit DRS“](#), auf Seite 35
- [„Beispiele für die Nutzen der Fehlertoleranz“](#), auf Seite 35
- [„Fehlertoleranz-Checkliste“](#), auf Seite 36
- [„Fehlertoleranzinteroperabilität“](#), auf Seite 37
- [„Vorbereiten Ihrer Cluster und Hosts für Fehlertoleranz“](#), auf Seite 39
- [„Aktivieren der Fehlertoleranz für virtuelle Maschinen“](#), auf Seite 43
- [„Anzeigen der Information zu fehlertoleranten virtuellen Maschinen“](#), auf Seite 45
- [„Best Practices für die Fehlertoleranz“](#), auf Seite 47
- [„VMware-Fehlertoleranz - Konfigurationsempfehlungen“](#), auf Seite 50
- [„Beheben von Problemen bei der Fehlertoleranz“](#), auf Seite 50

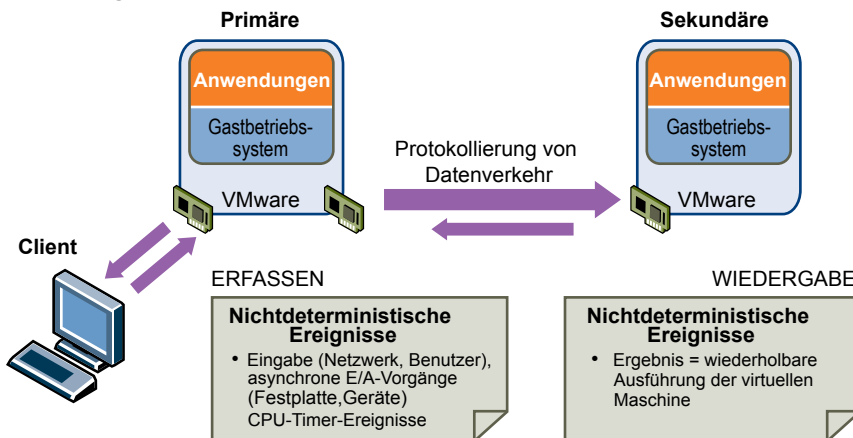
Wie die Fehlertoleranz funktioniert

Die VMware-Fehlertoleranz bietet unterbrechungsfreie Verfügbarkeit für virtuelle Maschinen, indem sie eine sekundäre virtuelle Maschine erstellt und verwaltet, die mit der primären virtuellen Maschine identisch ist und sie in einer Failover-Situation jederzeit ersetzen kann.

Sie können die Fehlertoleranz für die meisten unternehmenskritischen virtuellen Maschinen aktivieren. Es wird eine identische virtuelle Maschine, die als sekundäre virtuelle Maschine bezeichnet wird, erstellt und in virtuellem Gleichschritt mit der primären virtuellen Maschine ausgeführt. VMware vLockstep erfasst alle Eingaben und Ereignisse, die auf der primären virtuellen Maschine ausgeführt werden, und sendet sie an die sekundäre virtuelle Maschine, die auf einem anderen Host ausgeführt wird. Mithilfe dieser Informationen ist

die Ausführung der sekundären und der primären virtuellen Maschine identisch. Da die sekundäre virtuelle Maschine sich in einem virtuellen Gleichschritt mit der primären virtuellen Maschine befindet, kann sie die Ausführung zu einem beliebigen Zeitpunkt ohne Unterbrechung übernehmen. Damit bietet sie fehlertoleranten Schutz.

Abbildung 3-1. Primäre virtuelle Maschine und sekundäre virtuelle Maschine in einem Fehlertoleranzpaar



Die primären und sekundären virtuellen Maschinen tauschen kontinuierlich Taktsignale aus. Dieser Austausch ermöglicht den beiden virtuellen Maschinen das gegenseitige Überwachen ihres Zustands, um sicherzustellen, dass die Fehlertoleranz aufrechterhalten wird. Ein transparentes Failover tritt auf, wenn bei einem Ausfall des Hosts, der die primäre virtuelle Maschine ausführt, sofort die sekundäre virtuelle Maschine aktiviert wird, um die primäre virtuelle Maschine zu ersetzen. Eine neue sekundäre virtuelle Maschine wird gestartet und die Redundanz der Fehlertoleranz wird innerhalb weniger Sekunden wiederhergestellt. Wenn der Host, auf dem die sekundäre virtuelle Maschine läuft, ausfällt, wird diese ebenfalls sofort ersetzt. In beiden Fällen erleben Benutzer keine oder nur eine geringe Unterbrechung des laufenden Betriebs und keinen Datenverlust.

Eine fehlertolerante virtuelle Maschine und ihre sekundäre Kopie dürfen nicht auf demselben Host ausgeführt werden. Diese Einschränkung stellt sicher, dass ein Hostausfall nicht zum Verlust beider virtuellen Maschinen führen kann. Sie können VM-Host-Affinitätsregeln auch dazu verwenden, um festzulegen, auf welchen Hosts angegebene virtuelle Maschinen ausgeführt werden können. Achten Sie beim Verwenden dieser Regeln darauf, dass für alle primären virtuellen Maschinen, die von einer solchen Regel betroffen sind, auch die jeweils zugewiesene sekundäre virtuelle Maschine von dieser Regel betroffen sind. Weitere Informationen zu Affinitätsregeln finden Sie im *Handbuch zur Ressourcenverwaltung*.

Mithilfe der Fehlertoleranz wird verhindert, dass nach einem Ausfall in Folge der Wiederherstellung zwei aktive Kopien einer virtuellen Maschine vorhanden sind. Die atomische Dateisperre wird zur Koordinierung des Failovers verwendet, sodass nur eine Seite weiter als primäre virtuelle Maschine ausgeführt und eine neue sekundäre virtuelle Maschine automatisch erzeugt wird.

HINWEIS Die Anti-Affinitätsprüfung wird durchgeführt, wenn die primäre virtuelle Maschine eingeschaltet wird. Deshalb können sich die primären und sekundären virtuellen Maschine auf demselben Host befinden, wenn sie beide ausgeschaltet sind. Dies ist normal. Beim Einschalten der primären virtuellen Maschine wird die sekundäre virtuelle Maschine auf einem anderen Host gestartet.

Verwendung der Fehlertoleranz mit DRS

Sie können VMware-Fehlertoleranz zusammen mit VMware Distributed Resource Scheduler (DRS) verwenden, wenn Enhanced VMotion Compatibility (EVC) aktiviert ist. Dieser Vorgang sorgt dafür, dass fehlertolerante virtuelle Maschinen von einer besseren anfänglichen Platzierung profitieren und in die Lastausgleichsberechnungen des Clusters aufgenommen werden.

Wenn EVC für einen Cluster aktiviert ist, schlägt DRS Empfehlungen für die anfängliche Platzierung der fehlertoleranten virtuellen Maschinen vor, verschiebt diese während des Cluster-Lastausgleichs und sorgt dafür, dass Sie primären VMs eine DRS-Automatisierungsebene zuweisen können (die sekundäre virtuelle Maschine nimmt immer die gleiche Einstellung wie ihre zugewiesene primäre virtuelle Maschine an). Sie finden weitere Informationen zu EVC im *VMware vSphere Datacenter-Administratorhandbuch*.

DRS platziert nicht mehr als eine feste Anzahl von primären oder sekundären virtuellen Maschinen auf einem Host während der anfänglichen Platzierung oder des Lastausgleichs. Dieser Grenzwert wird durch die erweiterte Option „das.maxftvmsperhost“ gesteuert. Der Standardwert für diese Option ist 4. Wenn Sie diese Option jedoch auf 0 festlegen, ignoriert DRS diese Einschränkung.

Wenn VMware-Fehlertoleranz für virtuelle Maschinen in einem Cluster verwendet wird, bei dem EVC deaktiviert ist, erhalten die fehlertoleranten virtuellen Maschinen die DRS-Automatisierungsebenen „Deaktiviert“. In einem solchen Cluster wird jede primäre virtuelle Maschine nur auf ihrem registrierten Host eingeschaltet, die sekundäre virtuelle Maschine wird automatisch platziert und keine der beiden fehlertoleranten virtuellen Maschinen wird zwecks Lastausgleichs verschoben.

Wenn Sie Affinitätsregeln mit einem Paar von fehlertoleranten virtuellen Maschinen verwenden, gilt eine VM-VM-Affinitätsregel nur für die primäre virtuelle Maschine, wobei eine VM-Host-Affinitätsregel sowohl für die primäre als auch für deren sekundäre virtuelle Maschine gilt.

Beispiele für die Nutzen der Fehlertoleranz

Sie profitieren in mehreren typischen Situationen von der Verwendung der VMware-Fehlertoleranz.

Die Fehlertoleranz bietet einen höheren Level an Business Continuity als VMware HA. Wenn eine sekundäre virtuelle Maschine aufgerufen wird, um die primäre virtuelle Maschine zu ersetzen, übernimmt sie sofort deren Rolle und der gesamte Zustand der primären virtuellen Maschine bleibt erhalten. Gestartete Anwendungen und im Arbeitsspeicher gespeicherte Daten müssen weder neu geladen noch erneut eingegeben werden. Dies unterscheidet sich von einem VMware HA-Failover, das alle ausgefallenen virtuellen Maschinen neu startet.

Diese höhere Kontinuität und der zusätzliche Schutz von Zustandsinformationen und Daten wirken auf die Szenarien, in denen Sie möglicherweise die Fehlertoleranz bereitstellen möchten.

- Anwendungen, die immer bereit sein müssen vor allem diejenigen, die lang anhaltende Clientverbindungen benötigen, die Benutzer auch im Fall eines Hardwarefehlers aufrechterhalten möchten.
- Benutzerdefinierte Anwendungen, die keine Möglichkeit zur Clusterbildung haben.
- Fälle, in denen benutzerdefinierte Clusterlösungen High Availability bieten können, aber zu kompliziert sind, um konfiguriert und gewartet zu werden.

Fehlertoleranz bei Bedarf

Ein weiterer bedeutender Verwendungszweck für den Schutz einer virtuellen Maschine mithilfe der Fehlertoleranz kann als „Fehlertoleranz bei Bedarf“ bezeichnet werden. In diesem Fall wird eine virtuelle Maschine im normalen Betrieb durch VMware HA ausreichend geschützt. In bestimmten, kritischen Phasen erwägen Sie beispielsweise, den Schutz der virtuellen Maschine zu erhöhen. Beispielsweise erstellen Sie einen Bericht zum Quartalsende. Wenn Sie dabei unterbrochen werden, kann die Verfügbarkeit von unternehmenskritischen Informationen verzögert werden. Sie können diese virtuelle Maschine mithilfe der VMware-Fehlerto-

leranz schützen, bevor Sie diesen Bericht anfertigen, und die Fehlertoleranz danach wieder ausschalten oder deaktivieren. Sie können die Fehlertoleranz bei Bedarf dazu verwenden, die virtuelle Maschine in einer kritischen Phase zu schützen und danach die Ressourcen für den unkritischen Betrieb in den Normalzustand zurückzusetzen.

Fehlertoleranz-Checkliste

In der folgenden Checkliste sind die Cluster-, Host- und VM-Anforderungen aufgeführt, die Ihnen bekannt sein müssen, bevor Sie die VMware-Fehlertoleranz verwenden.

Überprüfen Sie diese Liste, bevor Sie die Fehlertoleranz einrichten. Sie können auch das VMware SiteSurvey-Dienstprogramm verwenden (herunterzuladen unter http://www.vmware.com/download/shared_utilities.html), um sich einen besseren Überblick über die Konfigurationsprobleme zu verschaffen, die im Zusammenhang mit dem Cluster, dem Host und den virtuellen Maschinen, die für die VMware-Fehlertoleranz verwendet werden, stehen.

Clusteranforderungen für die Fehlertoleranz

Die folgenden Clusteranforderungen müssen erfüllt sein, bevor Sie die Fehlertoleranz einsetzen können.

- Aktivieren der Hostzertifikatsüberprüfung. Weitere Informationen hierzu finden Sie unter „[Aktivieren der Hostzertifikatsüberprüfung](#)“, auf Seite 39.
- Mindestens zwei von der Fehlertoleranz zertifizierte Hosts, führen die gleiche Version der Fehlertoleranz aus oder weisen die gleiche Host-Build-Nummer auf. Die Versionsnummer der Fehlertoleranz wird auf der Registerkarte **[Übersicht]** eines Hosts im vSphere-Client angezeigt.

HINWEIS Im Falle von Hosts vor ESX/ESXi 4.1 wird stattdessen die Host-Build-Nummer angezeigt. Wegen Patches können Host-Build-Nummern zwischen ESX- und ESXi-Installationen variieren. Um sicherzustellen, dass Ihre Hosts FT-kompatibel sind, vermischen Sie keine ESX- und ESXi-Hosts in einem FT-Paar.

- ESX/ESXi-Hosts haben Zugriff auf dieselben VM-Datenspeicher und -Netzwerke. Weitere Informationen hierzu finden Sie unter „[Best Practices für die Fehlertoleranz](#)“, auf Seite 47.
- Fehlertoleranz-Protokollierung und VMotion-Netzwerke sind konfiguriert. Weitere Informationen hierzu finden Sie unter „[Konfigurieren von Netzwerken für Hostmaschinen](#)“, auf Seite 40.
- VMware HA-Cluster sind erstellt und aktiviert. Weitere Informationen hierzu finden Sie unter „[Erstellen eines VMware HA-Clusters](#)“, auf Seite 21. VMware HA muss aktiviert sein, bevor Sie fehlertolerante virtuelle Maschinen einschalten oder einem Cluster einen Host hinzufügen, der bereits fehlertolerante virtuelle Maschinen unterstützt.

Hostanforderungen für die Fehlertoleranz

Die folgenden Hostanforderungen müssen erfüllt sein, bevor Sie die Fehlertoleranz einsetzen können.

- Hosts müssen Prozessoren aus der FT-kompatiblen Prozessorgruppe besitzen. Es wird zudem dringend empfohlen, dass die Prozessoren der Hosts untereinander kompatibel sind. Weitere Informationen zu den unterstützten Prozessoren finden Sie in dem VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1008027>.
- Hosts müssen für die VMware-Fehlertoleranz lizenziert sein.
- Hosts müssen für die VMware-Fehlertoleranz zertifiziert sein. Rufen Sie die Seite <http://www.vmware.com/resources/compatibility/search.php> auf und wählen Sie **[Search by Fault Tolerant Compatible Sets]**, um zu ermitteln, ob Ihre Hosts zertifiziert sind.
- Bei der Konfiguration für jeden Host muss im BIOS die Hardwarevirtualisierung (HV) aktiviert sein.

Sie können auch Profilübereinstimmungsprüfungen ausführen, wie unter „[Erstellen von VMware HA-Clustern und Überprüfen der Übereinstimmung](#)“, auf Seite 43 beschrieben sind, um die Kompatibilität der Hosts im Cluster zum Unterstützen der Fehlertoleranz zu bestätigen.

HINWEIS Wenn ein Host VMware-Fehlertoleranz nicht unterstützt, können Sie die Gründe dafür im vSphere-Client in der Registerkarte **[Zusammenfassung]** des Hosts anzeigen. Wenn Sie auf das blau beschriftete Symbol neben dem Feld **[Host für die Fehlertoleranz konfiguriert]** klicken, wird eine Liste der Fehlertoleranzanforderungen angezeigt, die der Host nicht erfüllt.

VM-Anforderungen für die Fehlertoleranz

Die folgenden VM-Anforderungen müssen erfüllt sein, bevor Sie die Fehlertoleranz einsetzen können.

- Es dürfen keine nicht unterstützten Geräte mit den virtuellen Maschinen verbunden sein. Weitere Informationen hierzu finden Sie unter „[Fehlertoleranzinteroperabilität](#)“, auf Seite 37.
- Virtuelle Maschinen müssen in virtuellen RDM- oder in VMDK-Dateien gespeichert sein, die „Thick-Provisioned“ sind. Wenn eine virtuelle Maschine in einer schnell bereitgestellten VMDK-Datei gespeichert ist und ein Versuch zum Aktivieren der Fehlertoleranz unternommen wird, wird eine Meldung angezeigt, die angibt, dass die VMDK-Datei konvertiert werden muss. Sie müssen die virtuelle Maschine ausschalten, um diese Konvertierung auszuführen.
- Nicht kompatible Funktionen dürfen nicht mit den fehlertoleranten virtuellen Maschinen ausgeführt werden. Weitere Informationen hierzu finden Sie unter „[Fehlertoleranzinteroperabilität](#)“, auf Seite 37.
- Die Dateien der virtuellen Maschine müssen auf einem gemeinsam genutzten Speicher gespeichert sein. Zu den akzeptablen gemeinsam genutzten Speicherlösungen gehören Fibre-Channel, iSCSI (Hardware und Software), NFS und NAS.
- Nur virtuelle Maschinen mit einer einzelnen vCPU sind mit der Fehlertoleranz kompatibel.
- Virtuelle Maschinen müssen auf einem der unterstützten Gastbetriebssysteme ausgeführt werden. Weitere Informationen finden Sie in dem VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1008027>.

Fehlertoleranzinteroperabilität

Bevor Sie die VMware-Fehlertoleranz konfigurieren, sollten Sie die Funktionen und Produkte kennen, mit denen VMware-Fehlertoleranz nicht zusammenarbeiten kann.

vSphere-Funktionen, die für fehlertolerante VMs nicht unterstützt werden

Die folgenden vSphere-Funktionen werden nicht für fehlertolerante virtuelle Maschinen unterstützt.

- Snapshots. Snapshots müssen entfernt oder zugeordnet werden, bevor auf einer virtuellen Maschine die Fehlertoleranz aktiviert werden kann. Zudem ist es nicht möglich, Snapshots von virtuellen Maschinen zu erstellen, auf denen die Fehlertoleranz aktiviert ist.
- Storage VMotion. Sie können Storage VMotion nicht für virtuelle Maschinen mit aktivierter Fehlertoleranz verwenden. Wenn Sie den Speicher migrieren möchten, sollten Sie die Fehlertoleranz vorübergehend deaktivieren und die Storage VMotion-Aktion durchführen. Danach können Sie die Fehlertoleranz wieder aktivieren.

- Verknüpfte Klone. Sie können die Fehlertoleranz nicht auf einer virtuellen Maschine aktivieren, bei der es sich um einen verknüpften Klon handelt. Zudem können Sie keinen verknüpften Klon von einer virtuellen Maschine erstellen, für die die Fehlertoleranz aktiviert ist.
- VMware Consolidated Backup (VCB). Sie können keine virtuelle Maschine, für die die Fehlertoleranz aktiviert ist, mithilfe von VCB, vStorage API for Data Protection, VMware Data Recovery oder ähnlichen Sicherungsprodukten sichern, die die Verwendung eines VM-Snapshots voraussetzen, so wie es von ESX/ESXi durchgeführt wird. Sie müssen zum Sichern einer fehlertoleranten virtuellen Maschine auf diese Weise zunächst die Fehlertoleranz deaktivieren. Reaktivieren Sie anschließend die Fehlertoleranz, nachdem die Sicherung durchgeführt wurde. Speicher-Array-basierte Snapshots haben keine Auswirkung auf die Fehlertoleranz.

Funktionen und Geräte, die mit der Fehlertoleranz nicht kompatibel sind

Damit eine virtuelle Maschine mit der Fehlertoleranz kompatibel ist, darf diese die folgenden Funktionen und Geräte nicht verwenden.

Tabelle 3-1. Funktionen und Geräte, die mit Fehlertoleranz und fehlerbehebenden Aktionen nicht kompatibel sind

Nicht kompatible Funktion bzw. nicht kompatibles Gerät	Fehlerbehebende Aktion
Symmetrische Multiprozessor-VMs (SMP). Nur virtuelle Maschinen mit einer einzelnen vCPU sind mit der Fehlertoleranz kompatibel.	Konfigurieren Sie die virtuelle Maschine als eine einzelne vCPU neu. Die Leistung vieler Arbeitslasten ist bei der Konfiguration als eine einzelne vCPU gut.
Physische Raw-Festplattenzuordnung (RDM).	Konfigurieren Sie virtuelle Maschinen mit physischen, RDM-gestützten virtuellen Geräten neu, sodass diese stattdessen virtuelle RDMs verwenden.
CD-ROM- oder virtuelle Diskettengeräte, die von einem physischen oder Remotegerät gestützt sind.	Entfernen Sie das CD-ROM- bzw. virtuelle Diskettengerät oder konfigurieren Sie das Backing mit einem auf gemeinsam genutzten Speicher installierten ISO neu.
Paravirtualisierte Gastbetriebssysteme.	Wird die Paravirtualisierung nicht benötigt, konfigurieren Sie die virtuelle Maschine ohne ein VMI ROM neu.
USB- und Soundgeräte.	Entfernen Sie diese Geräte von der virtuellen Maschine.
N_Port-ID-Virtualisierung (NPIV).	Deaktivieren Sie die NPIV-Konfiguration der virtuellen Maschine.
NIC-Passthrough.	Diese Funktion wird von der Fehlertoleranz nicht unterstützt und muss daher ausgeschaltet werden.
vlance-Netzwerktreiber.	Die Fehlertoleranz unterstützt keine virtuellen Maschinen, die mit virtuellen vlance-Netzwerkkarten konfiguriert sind. vmxnet2, vmxnet3 und e1000 werden jedoch voll unterstützt.
Virtuelle Festplatten, die auf Thin-Provisioning-Speicher bzw. auf Thick-Provisioning-Festplatten ohne aktivierte Clusterfunktionen gestützt sind.	Wenn Sie die Fehlertoleranz einschalten, wird standardmäßig in das entsprechende Festplattenformat konvertiert. Sie müssen die virtuelle Maschine ausschalten, um diese Konvertierung auszulösen.

Tabelle 3-1. Funktionen und Geräte, die mit Fehlertoleranz und fehlerbehebenden Aktionen nicht kompatibel sind (Fortsetzung)

Nicht kompatible Funktion bzw. nicht kompatibles Gerät	Fehlerbehebende Aktion
Geräte im laufenden Betrieb wechseln.	Die Funktion zum Wechseln von Geräten im laufenden Betrieb ist für fehlertolerante virtuelle Maschinen deaktiviert. Wenn Geräte im laufenden Betrieb gewechselt (d. h. entweder hinzugefügt oder entfernt) werden sollen, müssen Sie die Fehlertoleranz vorübergehend ausschalten, den Wechsel durchführen und die Fehlertoleranz anschließend wieder einschalten. HINWEIS Beim Verwenden der Fehlertoleranz ist das Ändern der Einstellungen einer virtuellen Netzwerkkarte während der Ausführung einer virtuellen Maschine ein so genannter „hot-plug“-Vorgang, da die Netzwerkkarte entfernt und neu eingesetzt werden muss. Wenn Sie beispielsweise im Falle einer virtuellen Netzwerkkarte für eine laufende virtuelle Maschine das Netzwerk ändern, mit dem die virtuelle Netzwerkkarte verbunden ist, muss zuerst die Fehlertoleranz ausgeschaltet werden.
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI).	EPT/RVI ist automatisch für virtuelle Maschinen mit eingeschalteter Fehlertoleranz deaktiviert.
Serielle oder parallele Schnittstellen	Entfernen Sie diese Geräte von der virtuellen Maschine.
IPv6	Verwenden Sie mit der Fehlertoleranz IPv4-Adressen.

Vorbereiten Ihrer Cluster und Hosts für Fehlertoleranz

Zum Aktivieren der VMware-Fehlertoleranz für Ihren Cluster müssen die Voraussetzungen der Funktion erfüllt sein. Anschließend müssen Sie bestimmte Konfigurationsschritte auf Ihren Hosts ausführen. Nachdem Sie diese Schritte ausgeführt haben und Ihr Cluster erstellt wurde, können Sie auch überprüfen, ob Ihre Konfiguration die Anforderungen für das Aktivieren der Fehlertoleranz erfüllt.

Sie sollten die folgenden Aufgaben ausführen, bevor Sie versuchen, die Fehlertoleranz für Ihren Cluster zu aktivieren:

- Aktivieren der Hostzertifikatsüberprüfung (falls Sie ein Upgrade von einer vorherigen Version von vCenter Server durchführen).
- Konfigurieren des Netzwerks für die einzelnen Hosts.
- Erstellen des VMware HA-Clusters, Hinzufügen der Hosts und Prüfen der Übereinstimmung.

Nachdem Sie Ihren Cluster und Ihre Hosts für die Fehlertoleranz vorbereitet haben, können Sie sie für Ihre virtuellen Maschinen einschalten. Siehe [„Einschalten der Fehlertoleranz für virtuelle Maschinen“](#), auf Seite 45.

Aktivieren der Hostzertifikatsüberprüfung

Sie können ESX/ESXi-Hosts unter Verwendung der Hostzertifikatsüberprüfung für die gegenseitige Identitätsüberprüfung konfigurieren. Dadurch tragen Sie zur Herstellung einer sichereren Umgebung bei. Die Hostzertifikatsüberprüfung ist für ESX/ESXi-Hosts erforderlich, auf denen sich fehlertolerante virtuelle Maschinen befinden.

Wenn Sie VMware vCenter Server Version 4.1 installiert haben, wird die Hostzertifikatsüberprüfung automatisch aktiviert. Wenn Sie ein Upgrade von einer Vorgängerversion durchgeführt haben, müssen Sie den Vorgang manuell durchführen. Bei diesem Vorgang wird die Liste der Hosts mit den Zertifikaten für die Verifizierung angezeigt. Sie können das Host-Zertifikat prüfen, bevor Sie die Aktivierung der Zertifikatsüberprüfung übernehmen. Hosts, die in diesem Schritt nicht verifiziert wurden, müssen manuell verifiziert und erneut verbunden werden.

Vorgehensweise

- 1 Verbinden Sie den vSphere-Client mit vCenter Server.
- 2 Wählen Sie **[Verwaltung]** und dann **[vCenter Server-Einstellungen]** aus.
Das Fenster **[vCenter Server-Einstellungen]** wird angezeigt.
- 3 Klicken Sie auf **[SSL-Einstellungen]** im linken Fenster.
- 4 Wählen Sie das Kontrollkästchen **[vCenter benötigt verifizierte Host-SSL-Zertifikate]**.
- 5 Klicken Sie auf **[OK]**.

Konfigurieren von Netzwerken für Hostmaschinen

Auf jedem Host, den Sie zu einem VMware HA-Cluster hinzufügen möchten, müssen Sie zwei verschiedene Netzwerk-Switches konfigurieren, damit der Host auch die VMware-Fehlertoleranz unterstützen kann.

Sie müssen diesen Vorgang zweimal durchführen, um die Fehlertoleranz für einen Host zu aktivieren, je einmal pro Portgruppenoption. Dadurch wird sichergestellt, dass für die Protokollierung der Fehlertoleranz genügend Bandbreite zur Verfügung steht. Wählen Sie eine Option, schließen Sie den Vorgang ab, führen Sie den Vorgang dann erneut durch und wählen Sie die andere Portgruppenoption.

Voraussetzungen

Mehrere Gigabit-Netzwerkkarten sind erforderlich. Sie benötigen für jeden Host, der Fehlertoleranz unterstützt, mindestens zwei physische Gigabit-Netzwerkkarten. Sie benötigen beispielsweise eine für die Fehlertoleranzprotokollierung und eine für VMotion. Dennoch werden mindestens drei Netzwerkkarten empfohlen, um die Verfügbarkeit sicherzustellen. Die VMotion-Netzwerkkarte und die Netzwerkkarte mit Fehlertoleranzprotokollierung müssen sich in unterschiedlichen Subnetzen befinden.

Vorgehensweise

- 1 Verbinden Sie den vSphere-Client mit vCenter Server.
- 2 Wählen Sie in der vCenter Server-Bestandsliste den Host aus und klicken Sie auf die Registerkarte **[Konfiguration]**.
- 3 Wählen Sie **[Netzwerk]** unter **[Hardware]** aus und klicken Sie auf den Link **[Netzwerk hinzufügen]**.
Der Assistent zum Hinzufügen von Netzwerk wird angezeigt.
- 4 Wählen Sie **[VMkernel]** unter **[Verbindungstypen]** aus und klicken Sie auf **[Weiter]**.
- 5 Wählen Sie **[Einen virtuellen Switch erstellen]** aus und klicken Sie auf **[Weiter]**.
- 6 Geben Sie eine Bezeichnung für den Switch an.
- 7 Wählen Sie entweder **[Diese Portgruppe für VMotion verwenden]** oder **[Diese Portgruppe für die Fehlertoleranzprotokollierung verwenden]** und klicken Sie auf **[Weiter]**.
- 8 Geben Sie eine IP-Adresse und Subnetzmaske ein und klicken Sie anschließend auf **[Weiter]**.
- 9 Klicken Sie auf **[Beenden]**.

Nachdem Sie sowohl einen virtuellen VMotion- als auch einen virtuellen Fehlertoleranz-Protokollierungs-Switch erstellt haben, können Sie nach Bedarf weitere virtuelle Switches erstellen. Anschließend sollten Sie den Host zum Cluster hinzufügen und die Schritte zum Einschalten der Fehlertoleranz ausführen.

Weiter

Zeigen Sie die Registerkarte „Übersicht“ im vSphere-Client an, um zu bestätigen, dass Sie VMotion und die Fehlertoleranz erfolgreich auf dem Host installiert haben. [] In den Feldern **[VMotion aktiviert]** und **[Host für die Fehlertoleranz konfiguriert]** im Fenster „Allgemein“ muss „Ja“ angezeigt werden..

HINWEIS Wenn Sie das Netzwerk für die Unterstützung der Fehlertoleranz konfigurieren, daraufhin jedoch den Port für die Fehlertoleranzprotokollierung deaktivieren, bleiben die Paare von fehlertoleranten virtuellen Maschinen, die bereits eingeschaltet sind, immer noch eingeschaltet. Wenn dann jedoch ein Failover auftritt, wird keine neue sekundäre virtuelle Maschine gestartet, nachdem die primäre virtuelle Maschine durch ihre sekundäre virtuelle Maschine ersetzt wurde. Dadurch wird die neue primäre virtuelle Maschine mit dem Status „Nicht geschützt“ ausgeführt.

Fehlertoleranz - Beispiel einer Hostnetzwerkconfiguration

In diesem Beispiel wird die Host-Netzwerkconfiguration für Fehlertoleranz in einer Standardbereitstellung mit 4-GB-Netzwerkkarten beschrieben. Diese ist eine mögliche Bereitstellung, die ausreichenden Service für alle Datenverkehrstypen, die in diesem Beispiel erwähnt sind, gewährleistet und als „Best Practice“-Konfiguration gelten kann.

Die Fehlertoleranz sorgt für eine durchgehende Betriebszeit während des Ausfalls eines physischen Hosts aufgrund eines Stromausfalls, einer Systempanik oder ähnlicher Ursachen. Netzwerk- oder Speicherpfadausfälle oder andere physische Serverkomponenten, die auf den betrieblichen Status des Hosts keine Auswirkung haben, dürfen kein Fehlertoleranz-Failover auf die sekundäre virtuelle Maschine initiieren. Kunden wird deshalb dringend empfohlen, die entsprechende Redundanz (z. B. NIC-Gruppierung) zu verwenden, um die Chancen, die VM-Konnektivität mit Infrastrukturkomponenten (Netzwerken oder Speicher-Arrays) zu verlieren, zu reduzieren.

NIC-Gruppierungsrichtlinien werden auf den vSwitch-Portgruppen (bzw. verteilte virtuelle Portgruppen für vDS) konfiguriert und steuern, wie der vSwitch den Datenverkehr handhabt und ihn von den virtuellen Maschinen, VMkernel-Ports und Servicekonsolen-Ports über die physischen Netzwerkkarten (vnmics) verteilt. Eine eindeutige Portgruppe wird in der Regel für jeden Datenverkehrstyp verwendet, wobei jeder Datenverkehrstyp einem anderen VLAN zugewiesen wird.

Host-Netzwerkconfiguration - Richtlinien

Anhand der folgenden Richtlinien können Sie das Netzwerk Ihres Hosts konfigurieren, um die Fehlertoleranz mit verschiedenen Kombinationen von Datenverkehrstypen (z. B. NFS) und mehreren physischen Netzwerkkarten zu unterstützen.

- Verteilen Sie jede Netzwerkkartengruppe über zwei physische Switches, um die L2-Domänenkontinuität für jedes VLAN zwischen den zwei physischen Switches zu gewährleisten.
- Verwenden Sie deterministische Gruppierungsrichtlinien, um sicherzugehen, dass bestimmte Datenverkehrstypen eine Affinität mit einer bestimmten Netzwerkkarte (Aktiv/Standby) bzw. mit mehreren Netzwerkkarten (z. B. ID des virtuellen Quell-Ports) haben.
- Paaren Sie Datenverkehrstypen dort, wo Aktiv/Standby-Richtlinien verwendet werden, um in einer Failoversituation die Auswirkungen zu minimieren, wenn beide Datenverkehrstypen eine vnic teilen.
- Konfigurieren Sie dort, wo Aktiv/Standby-Richtlinien verwendet werden, alle aktiven Adapter eines bestimmten Datenverkehrstyps (z. B. Fehlertoleranzprotokollierung) für denselben physischen Switch. Dies minimiert die Anzahl der Netzwerk-Hops und reduziert die Chancen, dass die Switch-zu-Switch-Links überbucht werden.

Konfigurationsbeispiel mit 4-GB-Netzwerkkarten

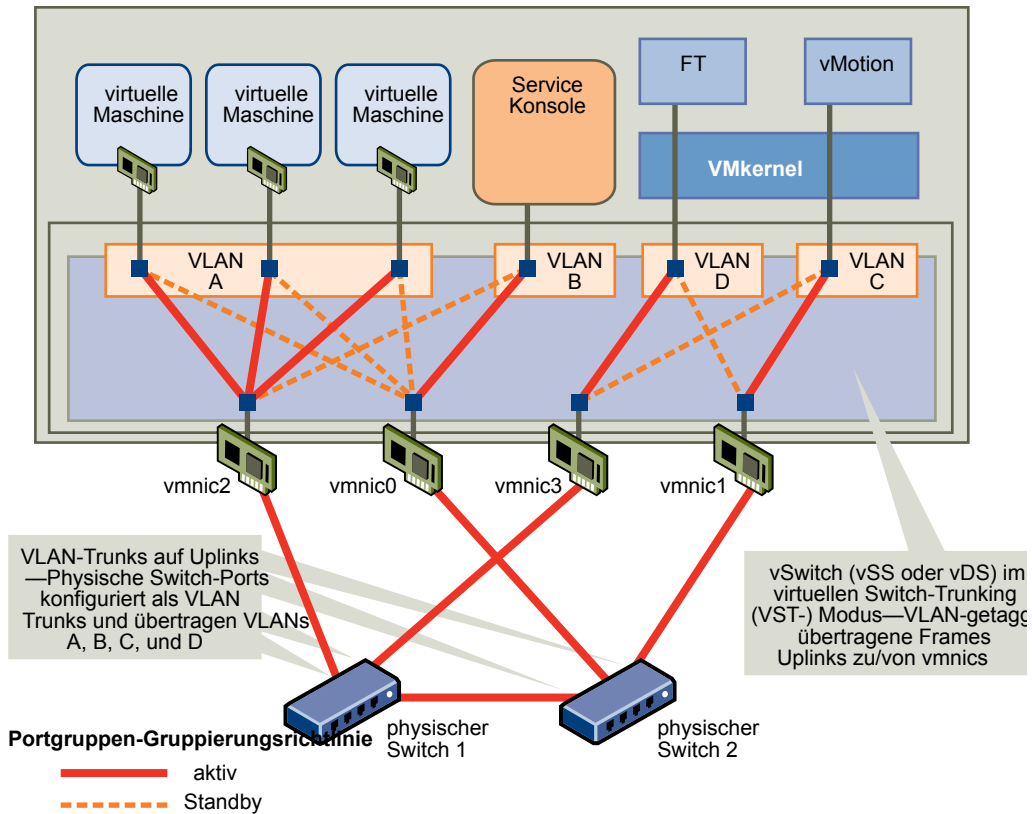
Abbildung 3-2 wird die Netzwerkconfiguration für einen einzelnen ESX/ESXi-Host mit 4-Gigabit-Netzwerkkarten dargestellt, die Fehlertoleranz unterstützen. Andere Hosts im fehlertoleranten Cluster würden ähnlich konfiguriert.

In diesem Beispiel werden vier Portgruppen verwendet, die folgendermaßen konfiguriert sind:

- VLAN A: VM-Netzwerk-Portgruppe - Aktiv auf vmnic2 (zu physischem Switch 1); Standby auf vmnic0 (zu physischem Switch 2.)
- VLAN B: Servicekonsolen-Portgruppe - Aktiv auf vmnic0 (zu physischem Switch 2); Standby auf vmnic1 (zu physischem Switch 1.)
- VLAN C: VMotion-Portgruppe - Aktiv auf vmnic1 (zu physischem Switch 2); Standby auf vmnic3 (zu physischem Switch 1.)
- VLAN D: Fehlertoleranzprotokollierung-Portgruppe - Aktiv auf vmnic3 (zu physischem Switch 1); Standby auf vmnic2 (zu physischem Switch 2.)

VMotion und die Fehlertoleranzprotokollierung können denselben VLAN gemeinsam nutzen (konfigurieren Sie hierfür dieselbe VLAN-Nummer für beide Portgruppen), aber sie benötigen ihre eigenen eindeutigen IP-Adressen, die sich in unterschiedlichen IP-Subnetzen befinden müssen. Separate VLANs werden möglicherweise bevorzugt, wenn auf dem physischen Netzwerk mit VLAN-basierendem QoS (Quality of Service) QoS-Einschränkungen gelten. QoS ist besonders in Situationen konkurrierender Datenströme nützlich, beispielsweise wenn mehrere physische Switch-Hops verwendet werden oder ein Failover erfolgt und mehrere Datenverkehrstypen um Netzwerkressourcen in Wettstreit treten.

Abbildung 3-2. Fehlertoleranz - Beispiel einer Netzwerkkonfiguration



Erstellen von VMware HA-Clustern und Überprüfen der Übereinstimmung

Die VMware-Fehlertoleranz wird im Kontext eines VMware HA-Clusters verwendet. Erstellen Sie den VMware HA-Cluster und fügen Sie ihm die Hosts hinzu, nachdem Sie Netzwerke auf jedem Host konfiguriert haben. Sie können überprüfen, ob der Cluster richtig konfiguriert ist und den Anforderungen für die erfolgreiche Aktivierung der Fehlertoleranz entspricht.

Vorgehensweise

- 1 Verbinden Sie den vSphere-Client mit vCenter Server.
- 2 Wählen Sie den Cluster in der vCenter Server-Bestandsliste aus und klicken Sie auf die Registerkarte **[Profil-Übereinstimmung]**.
- 3 Klicken Sie auf **[Jetzt auf Übereinstimmung prüfen]**, um die Übereinstimmung zu überprüfen.
Klicken Sie auf **[Beschreibung]**, um die ausgeführten Tests anzuzeigen.

Die Ergebnisse der Überprüfung werden am unteren Rand des Bildschirms angezeigt. Ein Host erhält entweder den Status „Übereinstimmung“ oder „Nicht übereinstimmend“.

HINWEIS Detaillierte Informationen zum Erstellen eines VMware HA-Clusters finden Sie unter [Kapitel 2, „Erstellen und Verwenden von VMware HA-Clustern“](#), auf Seite 11.

Aktivieren der Fehlertoleranz für virtuelle Maschinen

Nachdem Sie alle erforderlichen Schritte zum Aktivieren der VMware-Fehlertoleranz für Ihren Cluster ausgeführt haben, können Sie die Funktion nutzen, indem Sie sie für individuelle virtuelle Maschinen aktivieren.

Die Option zum Einschalten der Fehlertoleranz ist nicht verfügbar (abgeblendet), wenn eine der folgenden Bedingungen zutrifft:

- Die virtuelle Maschine wird auf einem Host ausgeführt, der für die Funktion nicht lizenziert ist.
- Die virtuelle Maschine wird auf einem Host ausgeführt, der im Wartungsmodus oder im Standby-Modus ist.
- Die virtuelle Maschine ist nicht verbunden oder verwaist (auf ihre VMX-Datei kann nicht zugegriffen werden).
- Der Benutzer hat keine Berechtigung, die Funktion zu aktivieren.

Wenn die Option zum Einschalten der Fehlertoleranz verfügbar ist, muss diese Aufgabe trotzdem validiert werden und kann fehlschlagen, wenn bestimmte Anforderungen nicht erfüllt werden.

Validierungsprüfungen für das Einschalten der Fehlertoleranz

Bevor die Fehlertoleranz eingeschaltet werden kann, werden auf einer virtuellen Maschine mehrere Validierungsprüfungen durchgeführt.

- Die SSL-Zertifikatsüberprüfung muss in den vCenter Server-Einstellungen aktiviert sein.
- Der Host muss sich in einem VMware HA-Cluster oder einem gemischten VMware HA- und DRS-Cluster befinden.
- Auf dem Host muss ESX/ESXi 4.0 oder höher installiert sein.
- Die virtuelle Maschine darf nicht über mehrere vCPUs verfügen.
- Die virtuelle Maschine darf nicht über Snapshots verfügen.

- Die virtuelle Maschine darf keine Vorlage sein.
- VMware HA darf auf der virtuellen Maschine nicht deaktiviert sein.

Für eingeschaltete virtuellen Maschinen (oder solche, die gerade eingeschaltet werden) werden mehrere zusätzliche Validierungsprüfungen durchgeführt.

- Das jeweilige BIOS der Hosts, auf denen sich die fehlertoleranten virtuellen Maschinen befinden, muss über eine aktivierte Hardwarevirtualisierung (HV) verfügen.
- Der Host, der die primäre virtuelle Maschine unterstützt, muss über einen Prozessor verfügen, der die Fehlertoleranz unterstützt.
- Der Host, der die sekundäre virtuelle Maschine unterstützt, muss über einen Prozessor verfügen, der die Fehlertoleranz unterstützt und zur selben CPU-Familie bzw. zum selben CPU-Modell gehört wie der Host, der die primäre virtuelle Maschine unterstützt.
- Ihre Hardware sollte als kompatibel mit Fehlertoleranz zertifiziert sein. Um dies zu bestätigen, schlagen Sie dies im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php> nach und wählen Sie den Abschnitt **[Search by Fault Tolerant Compatible Sets]**.
- Die Kombination des Gastbetriebssystems und des Prozessors muss von der Fehlertoleranz unterstützt werden (z. B. wird die Kombination von 32-Bit Solaris mit AMD-Prozessoren derzeit nicht unterstützt). Weitere Informationen über unterstützte Kombinationen von Prozessoren und Gastbetriebssystemen finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1008027>.
- Die Konfiguration der virtuellen Maschine muss für die Verwendung mit der Fehlertoleranz gültig sein (beispielsweise darf sie keine nicht unterstützten Geräte enthalten).

Wenn Ihr Versuch, die Fehlertoleranz für einer virtuellen Maschine einzuschalten, die Validierungsprüfungen besteht, wird die sekundäre virtuelle Maschine erstellt. Die Platzierung und der sofortige Status der sekundären virtuellen Maschine ist davon abhängig, ob die primäre virtuelle Maschine eingeschaltet oder ausgeschaltet war, als Sie die Fehlertoleranz eingeschaltet haben.

Wenn die primäre virtuelle Maschine eingeschaltet ist:

- Der gesamte Status der primären virtuellen Maschine wird kopiert und die sekundäre virtuelle Maschine wird erstellt, auf einem separaten, kompatiblen Host abgelegt und eingeschaltet, wenn sie die Zugangssteuerung passiert hat.
- Der im vSphere-Client auf der Registerkarte **[Übersicht]** für die virtuelle Maschine angezeigte Fehlertoleranzstatus lautet **[Geschützt]**.

Wenn die primäre virtuelle Maschine ausgeschaltet ist:

- Die sekundäre virtuelle Maschine wird sofort erstellt und bei einem Host im Cluster registriert (sie wird möglicherweise auf einen besser geeigneten Host verschoben, wenn sie eingeschaltet wird).
- Die sekundäre virtuelle Maschine wird nicht eingeschaltet, bevor die primäre virtuelle Maschine eingeschaltet wurde.
- Der im vSphere-Client auf der Registerkarte **[Übersicht]** für die virtuelle Maschine angezeigte Fehlertoleranzstatus lautet **[Nicht Geschützt, VM wird nicht ausgeführt]**.
- Wenn Sie versuchen, die primäre virtuelle Maschine einzuschalten, nachdem die Fehlertoleranz eingeschaltet wurde, werden die oben aufgeführten zusätzlichen Validierungsprüfungen durchgeführt. Die virtuelle Maschine darf nicht die Paravirtualisierung (VMI) verwenden, da sie sonst nicht ordnungsgemäß eingeschaltet wird.

Nachdem diese Prüfungen bestanden wurden, werden die primäre und sekundäre virtuelle Maschine eingeschaltet und auf separaten, kompatiblen Hosts platziert. Der im vSphere-Client auf der Registerkarte **[Übersicht]** für die virtuelle Maschine angezeigte Fehlertoleranzstatus lautet **[Geschützt]**.

Einschalten der Fehlertoleranz für virtuelle Maschinen

Sie können die VMware-Fehlertoleranz über den vSphere-Client einschalten.

Wenn die Fehlertoleranz eingeschaltet wird, setzt vCenter Server den Grenzwert der virtuellen Maschine für den Arbeitsspeicher zurück und legt die Arbeitsspeicherreservierung auf die Arbeitsspeichergröße der virtuellen Maschine fest. Sie können die Arbeitsspeicherreservierung, -größe, -anteile oder den Arbeitsspeichergrenzwert nicht ändern, solange die Fehlertoleranz eingeschaltet ist. Wenn die Fehlertoleranz ausgeschaltet wird, werden geänderte Parameter nicht auf ihre ursprünglichen Werte zurückgesetzt.

Verbinden Sie den vSphere-Client unter Verwendung eines Kontos mit Clusteradministratorberechtigungen mit vCenter Server.

Vorgehensweise

- 1 Wählen Sie die Ansicht „Hosts & Cluster“ aus.
- 2 Klicken Sie mit der rechten Maustaste auf eine einzelne virtuelle Maschine und wählen Sie **[Fehlertoleranz] > [Fehlertoleranz einschalten]**.

Wenn Sie mehr als eine virtuelle Maschine auswählen, wird das Menü **[Fehlertoleranz]** deaktiviert. Sie müssen die Fehlertoleranz jeweils für eine virtuelle Maschine einschalten.

Die angegebene virtuelle Maschine wird als primäre virtuelle Maschine festgelegt und eine sekundäre virtuelle Maschine wird auf einem anderen Host eingerichtet. Die primäre virtuelle Maschine ist jetzt fehlertolerant.

Anzeigen der Information zu fehlertoleranten virtuellen Maschinen

Sie können fehlertolerante virtuelle Maschinen mithilfe des vSphere-Clients in der Bestandsliste von vCenter Server anzeigen.

HINWEIS Sie können die Fehlertoleranz von der sekundären virtuellen Maschine aus nicht deaktivieren.

Die Registerkarte **[Übersicht]** für die primäre virtuelle Maschine enthält den Abschnitt (bzw. das Fenster) „VMware-Fehlertoleranz“ mit Informationen über die virtuelle Maschine.

Fehlertoleranzstatus

Zeigt den Fehlertoleranzstatus der virtuellen Maschine an.

- **Geschützt.** Zeigt an, dass die primäre und die sekundäre virtuelle Maschine eingeschaltet sind und ordnungsgemäß ausgeführt werden.
- **Nicht geschützt.** Zeigt an, dass die sekundäre virtuelle Maschine nicht ausgeführt wird. Mögliche Ursachen hierfür sind in der Tabelle aufgeführt.

Tabelle 3-2. Ursachen für den Status „Nicht geschützt“ der primären virtuellen Maschine

Ursache für den Status „Nicht geschützt“	Beschreibung
Starten	Die Fehlertoleranz ist dabei, die sekundäre virtuelle Maschine zu starten. Diese Meldung wird nur für kurze Zeit angezeigt.
Sekundäre VM erforderlich	Die primäre virtuelle Maschine wird ohne eine sekundäre virtuelle Maschine ausgeführt und ist somit aktuell nicht geschützt. Dies geschieht in der Regel dann, wenn kein kompatibler Host für die sekundäre virtuelle Maschine im Cluster verfügbar ist. Beheben Sie dies, indem Sie einen kompatiblen Host bereitstellen. Falls ein kompatibler Host im Cluster online ist, sind möglicherweise weitere Nachforschungen erforderlich. Unter bestimmten Umständen kann dieses Problem durch das Deaktivieren und erneute Aktivieren der Fehlertoleranz behoben werden.
Deaktiviert	Fehlertoleranz ist aktuell deaktiviert (es wird keine sekundäre virtuelle Maschine ausgeführt). Dies tritt ein, wenn die Fehlertoleranz durch den Benutzer deaktiviert wird oder wenn vCenter Server die Fehlertoleranz deaktiviert, nachdem die sekundäre virtuelle Maschine nicht eingeschaltet werden konnte.
VM wird nicht ausgeführt	Die Fehlertoleranz ist aktiviert, aber die virtuelle Maschine ist ausgeschaltet. Schalten Sie die virtuelle Maschine ein, um den Status „Geschützt“ zu erhalten.

Sekundärer Speicherort

Zeigt den ESX/ESXi-Host an, auf dem die sekundäre virtuelle Maschine gehostet wird.

Gesamtmenge an sekundärer CPU

Zeigt die CPU-Nutzung der sekundären virtuellen Maschine in MHz an.

Gesamtmenge an sekundärem Arbeitsspeicher

Zeigt die Arbeitsspeichernutzung der sekundären virtuellen Maschine in MB an.

vLockstep-Intervall	Das Zeitintervall (in Sekunden), das die sekundäre virtuelle Maschine benötigt, um den aktuellen Ausführungsstatus der primären virtuellen Maschine wieder herzustellen. In der Regel beträgt dieses Intervall weniger als eine halbe Sekunde. Unabhängig von dem Wert für das vLockstep-Intervall geht während eines Failovers kein Status verloren.
Protokollbandbreite	Zeigt die Menge an Netzwerkkapazität an, die für das Senden von Protokollinformationen über die VMware-Fehlertoleranz vom Host, auf dem die primäre virtuelle Maschine läuft, an den Host, auf dem die sekundäre virtuelle Maschine läuft, benötigt wird.

Für jeden Host, der so konfiguriert ist, dass er Fehlertoleranz unterstützt, können Sie Informationen zu dessen fehlertoleranten virtuellen Maschinen anzeigen, indem Sie im vSphere Client auf die Registerkarte **[Zusammenfassung]** des Hosts zugreifen. Der Abschnitt **[Fehlertoleranz]** dieses Bildschirms zeigt die Gesamtzahl primärer und sekundärer virtueller Maschinen an, die sich auf dem Host befinden, sowie die Anzahl der eingeschalteten virtuellen Maschinen. Falls der Host ESX/ESXi 4.1 oder höher ist, zeigt dieser Abschnitt auch die Version von Fehlertoleranz an, die auf dem Host ausgeführt wird. Anderenfalls wird die Build-Nummer des Hosts aufgelistet. Damit zwei Hosts kompatibel sind, müssen ihre FT-Versionennummern oder die Build-Nummern der Hosts übereinstimmen.

Best Practices für die Fehlertoleranz

Um optimale Fehlertoleranzergebnisse erzielen zu können, sollten Sie bestimmte empfohlene Vorgehensweisen einhalten.

Zusätzlich zu den folgenden Abschnitten können Sie das White Paper unter <http://www.vmware.com/resources/techresources/10040> für weitere Informationen zu den empfohlenen Vorgehensweisen für die Fehlertoleranz aufrufen.

Hostkonfiguration

Befolgen Sie beim Konfigurieren Ihrer Hosts die folgenden Best Practices.

- Hosts, auf denen die primären und sekundären virtuellen Maschinen ausgeführt werden, sollten mit annähernd denselben Prozessorfrequenzen arbeiten, anderenfalls könnte es sein, dass die sekundären virtuellen Maschinen häufiger neu gestartet werden. Plattform-Energieverwaltungsfunktionen, die sich nicht abhängig von der Arbeitslast anpassen (z. B. die Energiebeschränkung und erzwungene Niedrigfrequenzmodi zum Einsparen von Energie), können große Abweichungen der Prozessorfrequenzen verursachen. Falls sekundäre virtuelle Maschinen regelmäßig neu gestartet werden, deaktivieren Sie alle Energieverwaltungsmodi auf den Hosts, die fehlertolerante virtuelle Maschinen ausführen, oder stellen Sie sicher, dass alle Hosts im selben Energieverwaltungsmodus laufen.
- Wenden Sie dieselbe Erweiterungskonfiguration des Befehlssatzes (aktiviert oder deaktiviert) auf alle Hosts an. Der Vorgang zum Aktivieren oder Deaktivieren von Befehlssätzen ist je nach BIOS unterschiedlich. Einzelheiten zum Konfigurieren von Befehlssätzen finden Sie in der Dokumentation zu den BIOSes Ihrer Hosts.

Homogene Cluster

Die VMware-Fehlertoleranz kann in Clustern mit uneinheitlichen Hosts arbeiten, am besten funktioniert sie jedoch in Clustern mit kompatiblen Knoten. Wenn Sie Ihren Cluster erstellen, sollten alle Hosts über Folgendes verfügen:

- Prozessoren aus derselben kompatiblen Prozessorgruppe.
- Gemeinsamen Zugriff auf Datenspeicher, die von den virtuellen Maschinen verwendet werden.
- Dieselbe Netzwerkkonfiguration für virtuelle Maschinen.

- Dieselbe ESX/ESXi-Version.
- Dieselbe Versionsnummer der Fehlertoleranz (oder Host-Build-Nummer für Hosts vor Version ESX/ESXi 4.1).
- Die gleichen BIOS-Einstellungen (Energieverwaltung und Hyper-Threading) für alle Hosts.

Führen Sie **[Übereinstimmung prüfen]** aus, um Inkompatibilitäten zu identifizieren und zu beheben.

Leistung

Verwenden Sie zur Erhöhung der für den Protokollierungsdatenverkehr zwischen primären und sekundären virtuellen Maschinen verfügbaren Bandbreite eine 10 Gbit-Netzwerkkarte anstelle einer 1 Gbit-Netzwerkkarte und aktivieren Sie die Verwendung von Jumbo-Frames.

Speichern von ISOs auf gemeinsam genutztem Speicher für einen unterbrechungsfreien Zugriff

ISOs, auf die durch virtuelle Maschinen mit aktivierter Fehlertoleranz zugegriffen wird, sollten auf gemeinsam genutztem Speicher gespeichert werden, auf den beide Instanzen der fehlertoleranten virtuellen Maschine zugreifen können. Wenn diese Konfiguration verwendet wird, setzt die CD-ROM in der virtuellen Maschine auch bei einem Failover den normalen Betrieb fort.

Für virtuelle Maschinen mit aktivierter Fehlertoleranz können Sie ISO-Images verwenden, auf die nur die primäre virtuelle Maschine zugreifen kann. In diesem Fall kann die primäre virtuelle Maschine auf den ISO zugreifen, bei einem Failover meldet die CD-ROM jedoch Fehler, als ob kein Medium vorhanden wäre. Diese Situation kann akzeptabel sein, wenn die CD-ROM für einen vorübergehenden, unkritischen Vorgang, z. B. eine Installation, verwendet wird.

Failover von virtuellen Maschinen

Für eine primäre oder sekundäre virtuelle Maschine kann ein Failover durchgeführt werden, auch wenn deren ESX/ESXi-Host nicht abgestürzt ist. In solchen Fällen wird die Ausführung der virtuellen Maschine nicht unterbrochen, aber die Redundanz geht vorübergehend verloren. Um diese Art Failover zu vermeiden, sollten Sie sich mit einigen Situationen vertraut machen, wo dies eintreten kann, und die notwendigen Schritte ergreifen, um dies zu verhindern.

Teilweiser Hardwareausfall aufgrund von Speicherproblemen

Dieses Problem kann auftreten, wenn ein Host langsamen oder keinen Zugriff auf Speicher hat. Wenn dies auftritt, sind viele Speicherfehler im VMkernel-Protokoll aufgelistet. Zum Beheben dieses Problems müssen Sie Ihre speicherbezogenen Probleme beheben.

Teilweiser Hardwareausfall aufgrund von Netzwerkproblemen

Wenn die protokollierende Netzwerkkarte nicht funktioniert oder Verbindungen mit anderen Hosts über diese Netzwerkkarte ausfallen, kann dies ein Failover einer fehlertoleranten virtuellen Maschine auslösen, damit die Redundanz wiederhergestellt werden kann. Um dieses Problem zu vermeiden, sollten sich VMotion und die Fehlertoleranzprotokollierung auf unterschiedlichen Netzwerkkarten befinden. Führen Sie zudem die VMotion-Migrationen nur durch, wenn die virtuellen Maschinen weniger ausgelastet sind.

Ungenügende Bandbreite der protokollierenden Netzwerkkarte im Netzwerk

Dies kann auftreten, weil sich zu viele fehlertolerante virtuelle Maschinen auf einem Host befinden. Verteilen Sie die Paare der fehlertoleranten virtuellen Maschinen über mehrere Hosts, um dieses Problem zu beheben.

VMotion-Fehler aufgrund der Auslastung von virtuellen Maschinen

Wenn die Migration einer fehlertoleranten virtuellen Maschine mit VMotion fehlschlägt, muss für die virtuelle Maschine ein Failover durchgeführt werden. In der Regel tritt diese Art von Fehler auf, wenn die virtuelle Maschine noch zu ausgelastet ist, um einen Abschluss der Migration mit nur minimaler Unterbrechung des Vorgangs durchzuführen. Führen Sie VMotion-Migrationen nur durch, wenn die virtuellen Maschinen weniger ausgelastet sind, um dieses Problem zu vermeiden.

Zu viele Aktivitäten auf einem VMFS-Volume können zum Failover von virtuellen Maschinen führen

Wenn auf einem einzelnen VMFS-Volume mehrere Dateisystemsperrvorgänge, Einschalt- und Ausschaltvorgänge von virtuellen Maschinen oder VMotion-Migrationen gleichzeitig stattfinden, kann bei fehlertoleranten virtuellen Maschinen ein Failover ausgelöst werden. Ein Symptom, dass dies möglicherweise der Fall ist, ist der Empfang von mehreren Warnungen über SCSI-Reservierungen im VMkernel-Protokoll. Reduzieren Sie die Anzahl der Dateisystemvorgänge oder stellen Sie sicher, dass die fehlertolerante virtuelle Maschine sich auf einem VMFS-Volume befindet, das wenige andere virtuelle Maschinen enthält, die öfters eingeschaltet, ausgeschaltet oder unter Verwendung von VMotion migriert werden.

Die sekundäre virtuelle Maschine kann aufgrund von unzureichendem Speicherplatz nicht gestartet werden

Prüfen Sie, ob auf den `/(root)-` oder `/vmfs/Datenquelle-`Dateisystemen genügend freier Speicherplatz zur Verfügung steht. Auf diesen Dateisystemen kann der Speicherplatz aus mehreren Gründen knapp werden, was dazu führt, dass keine neue sekundäre virtuelle Maschine gestartet werden kann.

Upgrade von für die Fehlertoleranz verwendeten Hosts

Wenn Sie ein Upgrade für Hosts durchführen, die fehlertolerante virtuelle Maschinen enthalten, müssen Sie sicherzustellen, dass die primären und sekundären virtuellen Maschinen auf Hosts mit derselben Versionsnummer für die Fehlertoleranz oder derselben Host-Build-Nummer (für Hosts vor ESX/ESXi 4.1) ausgeführt werden.

Voraussetzungen

Stellen Sie sicher, dass Sie über Administratorberechtigungen für den Cluster verfügen.

Stellen Sie sicher, dass Sie über Gruppen von vier oder mehr ESX/ESXi-Hosts verfügen, die fehlertolerante virtuelle Maschinen hosten, die eingeschaltet sind. Falls sie ausgeschaltet sind, können die primären und sekundären virtuellen Maschinen auf Hosts mit unterschiedlichen Versionen verlagert werden.

HINWEIS Die folgenden Upgrade-Anweisungen gelten für Cluster mit mindestens vier Knoten. Bei kleineren Clustern können Sie dieselben Schritte ausführen, der nicht geschützte Zeitraum ist jedoch etwas länger.

Vorgehensweise

- 1 Migrieren Sie die fehlertoleranten virtuellen Maschinen unter Verwendung von VMotion von zwei Hosts weg.
- 2 Führen Sie ein Upgrade der zwei Hosts, deren fehlertoleranten virtuellen Maschinen entfernt wurden, auf dieselbe ESX/ESXi-Version durch.
- 3 Schalten Sie die Fehlertoleranz auf der primären virtuellen Maschine aus.
- 4 Verschieben Sie die deaktivierte primäre virtuelle Maschine unter Verwendung von VMotion auf einen der aktualisierten Hosts.
- 5 Schalten Sie die Fehlertoleranz auf der verschobenen primären virtuellen Maschine ein.

- 6 Wiederholen Sie [Schritt 1](#) bis [Schritt 5](#) für alle fehlertoleranten virtuellen Maschinen, die auf den aktualisierten Hosts untergebracht werden können.
 - 7 Verteilen Sie die fehlertoleranten virtuellen Maschinen unter Verwendung von VMotion.
- Es wird ein Upgrade aller ESX/ESXi-Hosts in einem Cluster durchgeführt.

VMware-Fehlertoleranz - Konfigurationsempfehlungen

Es wird empfohlen, beim Konfigurieren der Fehlertoleranz bestimmte Richtlinien zu beachten.

- Neben nicht-fehlertoleranten virtuellen Maschinen sollten auf einem einzelnen Host nicht mehr als vier fehlertolerante virtuelle Maschinen (primäre oder sekundäre Maschinen) vorhanden sein. Die Anzahl an fehlertoleranten virtuellen Maschinen, die Sie bedenkenlos auf jedem Host ausführen können, hängt von den Größen und den Arbeitslasten des ESX/ESXi-Hosts und der virtuellen Maschinen ab. Diese Werte können variieren.
- Falls Sie NFS für den Zugriff auf gemeinsam genutzten Speicher verwenden, sollten Sie dedizierte NAS-Hardware mit mindestens einer 1 Gbit Netzwerkkarte verwenden, um die für das ordnungsgemäße Funktionieren der Fehlertoleranz erforderliche Netzwerkleistung zu erzielen.
- Stellen Sie sicher, dass ein Ressourcenpool, der fehlertolerante virtuelle Maschinen enthält, eine größere Arbeitsspeichermenge als die für die virtuellen Maschinen erforderliche Menge besitzt. Die Arbeitsspeicherreservierung einer fehlertoleranten virtuellen Maschine wird auf die Arbeitsspeichergröße der virtuellen Maschine festgelegt, wenn die Fehlertoleranz eingeschaltet wird. Ohne diesen Überschuss im Ressourcenpool ist es möglich, dass kein Arbeitsspeicher mehr zur Verfügung steht, der als Overhead-Arbeitsspeicher genutzt werden kann.
- Verwenden Sie maximal 16 virtuelle Festplatten pro fehlertoleranter virtueller Maschine.
- Um Redundanz und maximalen Fehlertoleranzschutz zu gewährleisten, sollten sich mindestens drei Hosts im Cluster befinden. Auf diese Weise wird in einer Failover-Situation ein Host bereitgestellt, der die neu erstellte sekundäre virtuelle Maschine aufnehmen kann.

Beheben von Problemen bei der Fehlertoleranz

Sie sollten sich mit gewissen Themen zur Fehlerbehebung vertraut machen, um ein hohes Maß an Leistung und Beständigkeit für Ihre fehlertoleranten virtuellen Maschinen aufrechtzuerhalten und die Failover-Häufigkeit zu minimieren.

Die hier behandelten Themen zur Fehlerbehebung befassen sich hauptsächlich mit den Problemen, die auftreten können, wenn Sie die VMware-Fehlertoleranzfunktion auf Ihren virtuellen Maschinen verwenden. Außerdem werden Problemlösungen beschrieben.

Darüber hinaus können Sie auf die Informationen im Anhang *Fehlertoleranz-Fehlermeldungen* zugreifen, um zusätzliche Hilfe bei der Fehlerbehebung von Fehlertoleranzproblemen zu erhalten. Der Anhang enthält eine Liste von Fehlermeldungen, die möglicherweise ausgegeben werden, wenn Sie versuchen, diese Funktion zu verwenden, sowie ggf. Hinweise zum Beheben des jeweiligen Fehlers.

Die Hardwarevirtualisierung muss aktiviert sein

Sie müssen die Hardwarevirtualisierung (HV) aktivieren, bevor Sie die VMware-Fehlertoleranz verwenden können.

Problem

Beim Versuch, eine virtuelle Maschine mit aktivierter VMware-Fehlertoleranz einzuschalten, wird möglicherweise eine Fehlermeldung angezeigt, wenn Sie HV nicht aktiviert haben.

Ursache

Dieser Fehler ist oft darauf zurückzuführen, dass auf dem ESX/ESXi-Server, auf dem Sie versuchen, die virtuelle Maschine einzuschalten, die Hardwarevirtualisierung nicht verfügbar ist. HV ist nicht verfügbar, weil sie nicht von der ESX/ESXi-Serverhardware unterstützt wird oder im BIOS nicht aktiviert ist.

Lösung

Wenn HV von der ESX/ESXi-Serverhardware unterstützt wird, HV jedoch nicht aktiviert ist, aktivieren Sie HV im BIOS auf dem Server. Der Vorgang zum Aktivieren der HV ist je nach BIOS unterschiedlich. Einzelheiten zum Aktivieren der HV finden Sie in der Dokumentation zu den BIOSes Ihrer Hosts.

Wenn HV nicht von der ESX/ESXi-Serverhardware unterstützt wird, verwenden Sie Hardware, die Prozessoren nutzt, welche die Fehlertoleranz unterstützen.

Kompatible Hosts müssen für die sekundäre virtuelle Maschine verfügbar sein

Wenn Sie eine virtuelle Maschine mit aktivierter Fehlertoleranz einschalten und keine kompatiblen Hosts für deren sekundäre virtuelle Maschine zur Verfügung stehen, erhalten Sie möglicherweise eine Fehlermeldung.

Problem

Im Fenster „Kürzlich bearbeitete Aufgaben“ wird möglicherweise folgende Fehlermeldung angezeigt:

Sekundäre VM konnte nicht eingeschaltet werden, da es keine kompatiblen Hosts gibt, die sie aufnehmen können.

Ursache

Dies kann aus mehreren Gründen auftreten, z. B. weil es keine weiteren Hosts im Cluster gibt, weil es keine anderen Hosts mit aktivierter HV gibt, weil die Datenspeicher unzugänglich sind oder weil sich die Hosts im Wartungsmodus befinden.

Lösung

Falls die Anzahl der Hosts nicht ausreicht, fügen Sie mehr Hosts zum Cluster hinzu. Wenn es Hosts im Cluster gibt, stellen Sie sicher, dass sie HV unterstützen und HV aktiviert ist. Der Vorgang zum Aktivieren der HV ist je nach BIOS unterschiedlich. Einzelheiten zum Aktivieren der HV finden Sie in der Dokumentation zu den BIOS Ihrer Hosts. Vergewissern Sie sich, dass die Hosts über ausreichend Kapazität verfügen und sie sich nicht im Wartungsmodus befinden.

Sekundäre VM auf einem überlasteten Host beeinträchtigt die Leistung der primären VM

Falls es den Anschein hat, dass eine primäre virtuelle Maschine nur langsam läuft, obwohl deren Host nur mäßig belastet und dessen CPU im Leerlauf ist, überprüfen Sie, ob der Host, auf dem die sekundäre virtuelle Maschine läuft, stark ausgelastet ist.

Problem

Wenn sich eine sekundäre virtuelle Maschine auf einem Host befindet, der stark ausgelastet ist, kann sich dies auf die Leistung der primären virtuellen Maschine auswirken.

Ein Hinweis auf dieses Problem besteht darin, dass die vLockstep-Intervallanzeige im Fenster „Fehlertoleranz“ der primären virtuellen Maschine gelb oder rot aufleuchtet. Dies bedeutet, dass die sekundäre virtuelle Maschine mehrere Sekunden hinter der primären virtuellen Maschine läuft. In solchen Fällen sorgt die Fehlertoleranz dafür, dass die primäre virtuelle Maschine langsamer ausgeführt wird. Wenn die vLockstep-Intervallanzeige für längere Zeit gelb oder rot aufleuchtet, weist dies deutlich darauf hin, dass die sekundäre virtuelle Maschine nicht genügend CPU-Ressourcen erhält, um mit der primären virtuellen Maschine mithalten zu können.

Ursache

Eine sekundäre virtuelle Maschine, die auf einem Host ausgeführt wird, deren CPU-Ressourcen überlastet sind, erhält möglicherweise nicht die gleiche Menge an CPU-Ressourcen als die primäre virtuelle Maschine. Ist dies der Fall, muss die primäre virtuelle Maschine langsamer ausgeführt werden, um der sekundären virtuellen Maschine zu ermöglichen, Schritt zu halten. Dies führt dazu, dass deren Ausführungsgeschwindigkeit effektiv auf die langsamere Geschwindigkeit der sekundären VM gedrosselt wird.

Lösung

Legen Sie zum Beheben des Problems eine explizite CPU-Reservierung für die primäre virtuelle Maschine mit einem MHz-Wert fest, der zum Ausführen der Arbeitslast bei dem gewünschten Leistungsniveau ausreicht. Diese Reservierung wird sowohl bei der primären als auch bei der sekundären virtuellen Maschine angewendet, um sicherzustellen, dass beide Maschinen mit der angegebenen Geschwindigkeit ausgeführt werden können. Die Leistungsdiagramme der virtuellen Maschinen (bevor die Fehlertoleranz aktiviert wird) zeigen auf, wieviele CPU-Ressourcen unter normalen Bedingungen verbraucht werden, und können somit als Hilfe beim Einstellen dieser Reservierung dienen.

Virtuelle Maschinen mit viel Arbeitsspeicher können die Verwendung der Fehlertoleranz verhindern

Sie können die Fehlertoleranz nur auf virtuellen Maschinen aktivieren, die nicht über mehr als 64 GB Arbeitsspeicher verfügen.

Problem

Das Aktivieren der Fehlertoleranz auf einer virtuellen Maschine mit mehr als 64 GB Arbeitsspeicher kann fehlschlagen. Das Migrieren einer ausgeführten fehlertoleranten virtuellen Maschine mithilfe von VMotion kann auch dann fehlschlagen, wenn die VM über mehr als 15 GB an Arbeitsspeicher verfügt oder wenn sich der Speicher schneller ändert als VMotion die Daten über das Netzwerk kopieren kann.

Ursache

Dies tritt auf, wenn aufgrund der Größe des Hauptspeichers der virtuellen Maschine es nicht ausreichend Bandbreite gibt, um innerhalb des Standardzeitfensters (8 Sekunden) den VMotion-Wechselvorgang abzuschließen.

Lösung

Zum Beheben des Problems schalten Sie vor dem Aktivieren der Fehlertoleranz die virtuelle Maschine aus und erweitern Sie das Zeitfenster, indem Sie zur vmx-Datei der virtuellen Maschine die folgende Zeile hinzufügen:

```
ft.maxSwitchoverSeconds = "30"
```

wobei 30 die Angabe für das Zeitfenster in Sekunden ist. Aktivieren Sie die Fehlertoleranz und schalten Sie die virtuelle Maschine wieder ein. Diese Lösung sollte funktionieren, es sei denn, es herrscht eine sehr hohe Netzwerkaktivität.

HINWEIS Die Erhöhung des Zeitfensters auf 30 Sekunden kann dazu führen, dass die fehlertolerante virtuelle Maschine bis zu 30 Sekunden nicht mehr reagiert, wenn nach einem Failover die Fehlertoleranz aktiviert oder eine neue sekundäre virtuelle Maschine erstellt wird.

Übermäßige CPU-Nutzung von sekundären virtuellen Maschinen

In manchen Fällen ist der CPU-Bedarf der sekundären virtuellen Maschine höher als der CPU-Bedarf der entsprechenden primären virtuellen Maschine.

Problem

Wenn die primäre virtuelle Maschine im Leerlauf ist, erscheint der relative Unterschied zwischen der CPU-Nutzung der primären und der sekundären virtuellen Maschine groß.

Ursache

Die Wiedergabe von Ereignissen (z. B. Timer-Interrupts) auf der sekundären virtuellen Maschine kann etwas CPU-intensiver sein als deren Aufzeichnung auf der primären virtuellen Maschine. Dieser zusätzliche Overhead ist gering.

Lösung

Nicht erforderlich. Eine Überprüfung der tatsächlichen CPU-Nutzung zeigt, dass sehr wenig CPU-Ressourcen von der primären oder der sekundären virtuellen Maschine verbraucht werden.

Anhang: Fehlertoleranz-Fehlermeldungen

Wenn Sie die VMware-Fehlertoleranz (FT) verwenden, treten möglicherweise Fehlermeldungen auf. Einige dieser Fehlermeldungen werden in den folgenden Tabellen aufgeführt. Für jede Fehlermeldung gibt es eine Beschreibung und Informationen zum Beheben des Fehlers, sofern zutreffend. Zusätzlich zur Registerkarte **[Aufgaben & Ereignisse]** werden die Fehlertoleranzfehler auf der Registerkarte **[Übersicht]** der virtuellen Maschine angezeigt.

Fehlertoleranz-Konfigurationsfehlermeldungen

In der folgenden Tabelle werden einige der Fehlermeldungen aufgeführt, die auftreten können, falls Ihr Host oder Cluster für die Unterstützung der Fehlertoleranz nicht entsprechend konfiguriert ist. Weitere Informationen über die Konfigurationsanforderungen für die Fehlertoleranz finden Sie unter „[Fehlertoleranz-Checkliste](#)“, auf Seite 36.

Tabelle A-1. Konfigurationsfehler

Fehlermeldung	Beschreibung und Lösung
Host-CPU ist nicht kompatibel mit den Anforderungen der virtuellen Maschine. Nichtübereinstimmung bei diesen Funktionen: CPU stimmt nicht überein	FT erfordert, dass die Hosts für die primäre und sekundäre virtuelle Maschine die gleiche CPU verwenden. Aktivieren Sie FT auf einer virtuellen Maschine, die auf einem Host mit einem entsprechenden CPU-Modell, einer CPU aus der entsprechenden Familie und einem entsprechenden Stepping innerhalb des Clusters registriert ist. Wenn solche Hosts nicht existieren, müssen Sie einen hinzufügen. Dieser Fehler tritt ebenfalls auf, wenn Sie versuchen, eine fehlertolerante virtuelle Maschine auf einen anderen Host zu migrieren.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Fehlertoleranz nicht unterstützt von Hosthardware	FT wird nur auf bestimmten Prozessoren und BIOS-Einstellungen mit aktivierter Hardwarevirtualisierung (HV) unterstützt. Verwenden Sie Hosts mit unterstützten CPU-Modellen und BIOS-Einstellungen, um dieses Problem zu beheben.
ROM der virtuellen Maschine wird nicht unterstützt	Die virtuelle Maschine führt VMI-Kernel aus und ist paravirtualisiert. VMI wird nicht von der Fehlertoleranz unterstützt und sollte für die virtuelle Maschine deaktiviert werden.
Der Host {hostName} hat einige Fehlertoleranzprobleme mit der virtuellen Maschine {vmName}. In der Liste der Fehlermeldungen finden Sie weitere Details	Zur Behebung dieses Problems wählen Sie im vSphere-Client den fehlgeschlagenen FT-Vorgang entweder im Fenster „Kürzlich bearbeitete Aufgaben“ oder auf der Registerkarte [Aufgaben & Ereignisse] aus und klicken Sie auf den Link [Details anzeigen] , der in der Spalte „Details“ angezeigt wird.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Flag Hostzertifikate prüfen nicht gesetzt für vCenter Server	Die Option "Hostzertifikate prüfen" ist in den SSL-Einstellungen von vCenter Server nicht ausgewählt. Sie müssen diese Option auswählen. Siehe „ Aktivieren der Hostzertifikatsüberprüfung “, auf Seite 39.

Tabelle A-1. Konfigurationsfehler (Fortsetzung)

Fehlermeldung	Beschreibung und Lösung
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: HA ist auf der virtuellen Maschine nicht aktiviert.	Diese virtuelle Maschine befindet sich auf einem Host, der sich in keinem VMware HA-Cluster befindet oder dessen VMware HA deaktiviert wurde. Fehlertoleranz erfordert VMware HA.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Host ist inaktiv	Sie müssen FT auf einem aktiven Host aktivieren. Ein inaktiver Host ist ein Host, der getrennt wurde bzw. sich im Wartungsmodus oder im Standby-Modus befindet.
Die Fehlertoleranz wurde auf dem Host {hostName} nicht lizenziert.	Die Fehlertoleranz ist nicht in allen Editionen von VMware vSphere lizenziert. Prüfen Sie Ihre Edition und aktualisieren Sie sie auf eine Edition, die die Fehlertoleranz enthält.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Keine VMotion-Lizenz oder keine virtuelle Netzwerkkarte für VMotion konfiguriert	Stellen Sie sicher, dass Sie das Netzwerk auf dem Host richtig konfiguriert haben. Siehe „ Konfigurieren von Netzwerken für Hostmaschinen “, auf Seite 40. Wenn dies der Fall ist, müssen Sie möglicherweise eine VMotion-Lizenz erwerben.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Keine virtuelle Netzwerkkarte konfiguriert für die Fehlertoleranzprotokollierung	Eine Netzwerkkarte mit Fehlertoleranzprotokollierung wurde nicht konfiguriert. Weitere Anweisungen finden Sie im Abschnitt „ Konfigurieren von Netzwerken für Hostmaschinen “, auf Seite 40.
Der angegebene Host {hostName} unterstützt keine virtuellen Maschinen mit aktivierter Fehlertoleranz. Dieses VMware-Produkt unterstützt die Fehlertoleranz nicht	Das von Ihnen verwendete Produkt ist mit der Fehlertoleranz nicht kompatibel. Sie müssen die Fehlertoleranz ausschalten, um dieses Produkt zu verwenden. Diese Fehlermeldung tritt vor allem dann auf, wenn vCenter Server einen Host mit einer früheren Version von ESX/ESXi verwaltet oder wenn Sie VMware Server verwenden.
Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Fehlertoleranz nicht unterstützt von VMware Server 2.0	Aktualisieren Sie auf VMware ESX oder ESXi 4.1 oder höher.
Die Version des Builds oder der Fehlertoleranzfunktion auf dem Zielhost unterscheidet sich von der Version des aktuellen Builds oder der aktuellen Fehlertoleranzfunktion: {build}.	Die Fehlertoleranzversionen auf den aktuellen und den Zielhosts müssen übereinstimmen. Wählen Sie einen kompatiblen Host aus oder aktualisieren Sie inkompatible Hosts.

Konfigurationsfehler virtueller Maschinen

Es gibt mehrere Konfigurationsprobleme virtueller Maschinen, die Fehlermeldungen mit sich bringen.

Zwei Fehlermeldungen, die Sie möglicherweise sehen werden, wenn die Konfiguration der virtuellen Maschinen die Fehlertoleranz nicht unterstützt.

- Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Die aktuelle Konfiguration der virtuellen Maschine unterstützt die Fehlertoleranz nicht
- Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Die Aufzeichnungs- und Wiedergabefunktionalität wird von der VM nicht unterstützt

Die Fehlertoleranz läuft nur auf einer virtuellen Maschine mit einer einzelnen vCPU. Möglicherweise treten die folgenden Fehler beim Versuch auf, auf einer virtuellen Maschine mit mehreren vCPUs die Fehlertoleranz einzuschalten:

- Die virtuelle Maschine hat {numCpu} virtuelle CPUs. Dies wird nicht unterstützt: Fehlertoleranz
- Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Virtuelle Maschine mit mehreren virtuellen CPUs

Es gibt vSphere-Funktionen, mit denen die Fehlertoleranz nicht zusammen betrieben werden kann. Wenn Sie versuchen, mithilfe einer vSphere-Funktion, die von der Fehlertoleranz nicht unterstützt wird, die Fehlertoleranz auf einer virtuellen Maschine einzuschalten, sehen Sie möglicherweise eine der folgenden Fehlermeldungen. Sie müssen zum Verwenden der Fehlertoleranz die vSphere-Funktion auf der fehlerhaften virtuellen Maschine deaktivieren oder die Fehlertoleranz auf einer virtuellen Maschine aktivieren, ohne diese Funktionen zu benutzen.

- Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Die virtuelle Maschine hat einen oder mehrere Snapshots
- Bei der Fehlertoleranzkonfiguration des Elements {entityName} ist ein Problem aufgetreten: Vorlagen-VM

Die folgenden Fehlermeldungen können auftreten, wenn Ihre virtuelle Maschine über ein nicht unterstütztes Gerät verfügt. Entfernen Sie zum Aktivieren der Fehlertoleranz auf dieser virtuellen Maschine die nicht unterstützten Geräte und schalten Sie anschließend die Fehlertoleranz ein.

- Das Datei-Backing ({backingFilename}) für Gerät „Virtuelle Festplatte“ wird für die Fehlertoleranz nicht unterstützt
- Das Datei-Backing ({backingFilename}) für Gerät „Virtuelle Diskette“ wird für die Fehlertoleranz nicht unterstützt
- Das Datei-Backing ({backingFilename}) für Gerät „Virtuelle CDRom“ wird für die Fehlertoleranz nicht unterstützt
- Das Datei-Backing ({backingFilename}) für Gerät „Virtuelle serielle Schnittstelle“ wird für die Fehlertoleranz nicht unterstützt
- Das Datei-Backing ({backingFilename}) für Gerät „Virtuelle parallele Schnittstelle“ wird für die Fehlertoleranz nicht unterstützt

In der folgenden Tabelle werden weitere VM-Konfigurationsfehler aufgeführt. Weitere Informationen hierzu finden Sie unter [„Fehlertoleranzinteroperabilität“](#), auf Seite 37.

Tabelle A-2. Weitere VM-Konfigurationsprobleme

Fehlermeldung	Beschreibung und Lösung
Der angegebene Host ist nicht kompatibel mit der sekundären Fehlertoleranz-VM.	Informationen über mögliche Ursachen dieses Fehlers finden Sie unter „Beheben von Problemen bei der Fehlertoleranz“ , auf Seite 50.
Es sind keine kompatiblen Hosts für die sekundäre VM {vm.name} verfügbar	Informationen über mögliche Ursachen dieses Fehlers finden Sie unter „Beheben von Problemen bei der Fehlertoleranz“ , auf Seite 50.
{device} der Festplatte der virtuellen Maschine verwendet den Festplattenmodus '{mode}', der nicht unterstützt wird.	Bei der virtuellen Maschine ist mindestens eine Festplatte für die Verwendung des unabhängigen Modus konfiguriert. Bearbeiten Sie die Einstellung der virtuellen Maschine, wählen Sie jede Festplatte aus und heben Sie die Aktivierung des unabhängigen Modus auf. Stellen Sie zusammen mit Ihrem Systemadministrator sicher, dass diese Lösung für Ihre Umgebung akzeptabel ist.

Tabelle A-2. Weitere VM-Konfigurationsprobleme (Fortsetzung)

Fehlermeldung	Beschreibung und Lösung
Die nicht verwendeten Festplattenblöcke der Festplatten der virtuellen Maschine wurden auf dem Dateisystem nicht bereinigt. Dies ist erforderlich, damit Funktionen wie die Fehlertoleranz unterstützt werden können	Sie haben versucht, die FT auf einer eingeschalteten virtuellen Maschine zu aktivieren, die über Thick-Format-Festplatten mit der Lazy-Zeroed-Eigenschaft verfügt. FT kann auf einer solchen virtuellen Maschine nicht aktiviert werden, solange sie eingeschaltet ist. Schalten Sie die virtuelle Maschine aus, aktivieren Sie die Fehlertoleranz und schalten Sie die virtuelle Maschine wieder ein. Dies ändert das Festplattenformat der virtuellen Maschine, wenn sie wieder eingeschaltet wird. Das Einschalten der FT kann einige Zeit in Anspruch nehmen, wenn die virtuelle Festplatte groß ist.
Die Festplattenblöcke der Festplatten der virtuellen Maschine wurden auf dem Dateisystem nicht vollständig bereitgestellt. Dies ist erforderlich, damit Funktionen wie die Fehlertoleranz unterstützt werden können	Sie haben versucht, die Fehlertoleranz auf einer eingeschalteten virtuellen Maschine mit Thin-bereitgestellten Festplatten zu aktivieren. FT kann auf einer solchen virtuellen Maschine nicht aktiviert werden, solange sie eingeschaltet ist. Schalten Sie die virtuelle Maschine aus, aktivieren Sie die Fehlertoleranz und schalten Sie die virtuelle Maschine wieder ein. Dies ändert das Festplattenformat der virtuellen Maschine, wenn sie wieder eingeschaltet wird. Das Einschalten der FT kann einige Zeit in Anspruch nehmen, wenn die virtuelle Festplatte groß ist.

Betriebsfehler

In der folgenden Tabelle sind Fehlermeldungen aufgelistet, die bei der Verwendung von fehlertoleranten virtuellen Maschinen auftreten können.

Tabelle A-3. Betriebsfehler

Fehlermeldung	Beschreibung und Lösung
Es wurde kein geeigneter Host gefunden zum Ablegen der sekundären Fehlertoleranz für die VM {vmName}	Die Fehlertoleranz erfordert, dass die Hosts für die primären und sekundären virtuellen Maschinen das gleiche CPU-Modell bzw. die gleiche CPU-Familie verwenden und die gleiche Versionsnummer oder Host-Build-Nummer sowie das gleiche Patch-Level für die Fehlertoleranz aufweisen. Aktivieren Sie die FT auf einer virtuellen Maschine, die auf einem Host mit einem entsprechenden CPU-Modell oder mit einer CPU aus der entsprechenden Familie innerhalb des Clusters registriert ist. Wenn solche Hosts nicht existieren, müssen Sie einen hinzufügen.
Die sekundäre fehlertolerante VM wurde nicht eingeschaltet, da die primäre fehlertolerante VM nicht eingeschaltet werden konnte.	vCenter Server wird den Grund melden, weshalb die primäre VM nicht eingeschaltet werden konnte. Beheben Sie die Probleme und wiederholen Sie den Vorgang.
Das Einschalten der sekundären Fehlertoleranz für {vmName} konnte nicht in {timeout} Sekunden abgeschlossen werden	Versuchen Sie, die sekundäre virtuelle Maschine erneut einzuschalten. Die Zeitüberschreitung kann aufgrund von Netzwerk- oder anderen flüchtigen Problemen auftreten.
vCenter hat die Fehlertoleranz auf der VM '{vmName}' deaktiviert, weil die sekundäre VM nicht eingeschaltet werden konnte.	Weitere Informationen zum Diagnostizieren, warum die sekundäre virtuelle Maschine nicht eingeschaltet werden konnte, finden Sie unter „ Beheben von Problemen bei der Fehlertoleranz “, auf Seite 50.

Tabelle A-3. Betriebsfehler (Fortsetzung)

Fehlermeldung	Beschreibung und Lösung
Primäre und sekundäre VM werden neu synchronisiert	Die Fehlertoleranz hat einen Unterschied zwischen der primären und sekundären virtuellen Maschine ermittelt. Die Ursache hierfür sind vorübergehende Ereignisse, die aufgrund von Hardware- oder Softwareunterschieden zwischen den beiden Hosts auftreten können. Die Fehlertoleranz hat automatisch eine neue sekundäre virtuelle Maschine gestartet und es ist keine Aktion erforderlich. Falls diese Meldung oft angezeigt wird, wenden Sie sich an den Support, um herauszufinden, ob es sich um ein Problem handelt.
Bei der Fehlertoleranzkonfiguration des Elements {entity-Name} ist ein Problem aufgetreten: Keine Konfigurationsinformationen für die virtuelle Maschine	vCenter Server verfügt über keine Informationen zur Konfiguration der virtuellen Maschine. Ermitteln Sie, ob sie falsch konfiguriert ist. Versuchen Sie, die virtuelle Maschine aus der Bestandsliste zu entfernen und registrieren Sie sie erneut.
Das DRS-Verhalten für die fehlertolerante sekundäre virtuelle Maschine {vmName} kann nicht geändert werden.	Sie können das DRS-Verhalten auf fehlertoleranten sekundären virtuellen Maschinen nicht ändern. Diese Konfiguration wird von der primären virtuellen Maschine geerbt.
Virtuelle Maschinen desselben Fehlertoleranz-Paars dürfen sich nicht auf demselben Host befinden	Sie haben versucht, eine sekundäre virtuelle Maschine unter Verwendung von VMotion auf einen Host zu verschieben, auf dem sich eine primäre virtuelle Maschine befindet. Eine primäre virtuelle Maschine und ihre sekundäre virtuelle Maschine können nicht auf demselben Host gespeichert werden. Wählen Sie einen anderen Zielhost für die sekundäre virtuelle Maschine.
Ein Host mit virtuellen Maschinen, auf denen die Fehlertoleranz aktiviert ist, kann nicht zu einem nicht-HA-fähigen Cluster hinzugefügt werden	FT erfordert, dass der Cluster für VMware HA aktiviert ist. Bearbeiten Sie Ihre Clustereinstellungen und schalten Sie VMware HA ein.
Ein Host mit virtuellen Maschinen, auf denen die Fehlertoleranz aktiviert ist, kann nicht zu einem eigenständigen Host hinzugefügt werden	Schalten Sie die Fehlertoleranz aus, bevor Sie den Host als eigenständigen Host zu vCenter Server hinzufügen. Um die Fehlertoleranz auszuschalten, fügen Sie den Host zu einem VMware HA-Cluster hinzu, klicken Sie mit der rechten Maustaste auf jede virtuelle Maschine auf dem Host und wählen Sie „Fehlertoleranz ausschalten“. Wenn FT deaktiviert wurde, kann der Host ein eigenständiger Host werden.
Die HA-Neustartpriorität für die fehlertolerante VM '{vmName}' konnte nicht auf 'Deaktiviert' gesetzt werden.	Diese Einstellung ist für fehlertolerante virtuelle Maschinen nicht zulässig. Sie sehen diesen Fehler nur dann, wenn Sie die Neustartpriorität einer fehlertoleranten virtuellen Maschine auf „Deaktiviert“ ändern.
Auf dem Host werden bereits die empfohlene Anzahl von {maxNumFtVms} fehlertoleranten virtuellen Maschinen ausgeführt	Wenn Sie mehr fehlertolerante VMs einschalten oder auf diesen Host migrieren möchten, können Sie eine der vorhandenen fehlertoleranten VMs auf einen anderen Host verschieben oder diese Einschränkung deaktivieren, indem Sie die erweiterte VMware HA-Option 'das.maxFtVmsPerHost' auf 0 setzen.

Betriebliche SDK-Fehler

In der folgenden Tabelle sind Fehlermeldungen aufgelistet, die bei der Verwendung des SDK zum Ausführen von Vorgängen auftreten können.

Tabelle A-4. Betriebliche SDK-Fehler

Fehlermeldung	Beschreibung und Lösung
Dieser Vorgang wird auf einer sekundären virtuellen Maschine eines Fehlertoleranzpaars nicht unterstützt.	Ein nicht unterstützter Vorgang wurde mithilfe der API direkt auf der sekundären virtuellen Maschine ausgeführt. Die Fehlertoleranz lässt keine direkte Interaktion mit der sekundären virtuellen Maschine zu (außer für das Verlagern oder das Migrieren auf einen anderen Host).
Bei der Fehlertoleranzkonfiguration des Elements {entity-Name} ist ein Problem aufgetreten: Sekundäre VM ist bereits vorhanden	Die primäre virtuelle Maschine verfügt bereits über eine sekundäre virtuelle Maschine. Versuchen Sie nicht, mehrere sekundäre virtuelle Maschinen für dieselbe primäre virtuelle Maschine zu erstellen.
Die sekundäre virtuelle Maschine mit der Instanz-UUID '{instanceUuid}' wurde bereits aktiviert.	Es wurde versucht, die FT für eine virtuelle Maschine zu aktivieren, auf der die FT bereits aktiviert war. In der Regel geht solch ein Vorgang von einem API aus.
Die sekundäre virtuelle Maschine mit der Instanz-UUID '{instanceUuid}' wurde bereits deaktiviert.	Es wurde versucht, die FT für eine sekundäre virtuelle Maschine zu deaktivieren, auf der die FT bereits deaktiviert war. In der Regel geht solch ein Vorgang von einem API aus.

HINWEIS Wenn Fehler in Bezug auf die CPU-Kompatibilität auftreten, finden Sie Informationen zu unterstützten Prozessoren und Gastbetriebssystemen im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/1008027>. Sie können auch das VMware SiteSurvey-Dienstprogramm verwenden (herunterzuladen unter http://www.vmware.com/download/shared_utilities.html), um sich einen besseren Überblick über die Konfigurationsprobleme zu verschaffen, die im Zusammenhang mit dem Cluster, dem Host und den virtuellen Maschinen, die für die VMware-Fehlertoleranz verwendet werden, stehen.

Index

A

- Affinitätsregeln **33, 35**
- Aktuelle Failover-Kapazität **14, 17**
- Aktueller Failover-Host **18**
- Ändern von Clustereinstellungen **21**
- Angeben eines Failover-Hosts **18**
- Anpassen von VMware HA **26**
- Anti-Affinitätsregeln **33**
- Anwendungsbeispiele, Fehlertoleranz **35**
- Anwendungsüberwachung **25**
- Ausfallzeit
 - Geplant **7**
 - Ungeplant **8**
- Ausfallzeiten minimieren **7**

B

- Beheben von Problemen bei der Fehlertoleranz **50**
- Best Practices
 - Fehlertoleranz **47**
 - VMware HA-Cluster **29**
 - VMware HA-Netzwerk **30**
- Betriebsstatus des Clusters **29**
- Business Continuity **7**

C

- Clustereinstellungen **21**
- Clustergültigkeit **29**

D

- das.failedetectioninterval **27**
- das.failedetectiontime **27, 30**
- das.iostatsinterval **25, 27**
- das.isolationsadresse **27, 30**
- das.isolationshutdowntimeout **23, 27**
- das.maxftvmsperhost **35**
- das.slotcpuminmhz **14, 27**
- das.slotmeminmb **14, 27**
- das.standardfailoverhost **27**
- das.usedefaultisolationaddress **27**
- das.vmcpcuminmhz **14, 17, 27**
- das.vmMemoryMinMB **27**
- Distributed Power Management (DPM) **11, 13**
- Distributed Resource Scheduler (DRS)
 - Deaktivieren **22**

- Fehlertoleranz-Fehler **55**
 - Mit VMware HA **11**
 - Und Fehlertoleranz **37**
 - Verwenden mit VMware-Fehlertoleranz **35**

DNS-Suche **20**

E

- E/A-Statistikintervall **25**
- Einschalten von VMware HA **22**
- Enhanced vMotion Compatibility **35**
- Ereignisse und Alarme, einstellen **29**
- Erstellen eines VMware HA-Clusters **21**
- erweiterte Attribute, VMware HA **26**
- Erweiterte Laufzeitinformationen **14**
- EVC **35**
- Extended Page Tables (EPT) **37**

F

- Failover-Host **18**
- Fehlermeldungen, Fehlertoleranz **55**
- Fehlertoleranz
 - aktivieren **39**
 - Anti-Affinitätsregeln **33**
 - Anwendungsbeispiele **35**
 - Best Practices **47**
 - Checkliste **36**
 - Deaktivieren **45**
 - Einschränkungen, einschalten **43**
 - Fehlerbehebung **50–53**
 - Fehlermeldungen **55**
 - Gesamtmenge an sekundärem Arbeitsspeicher **45**
 - Gesamtmenge an sekundärer CPU **45**
 - Interoperabilität **37**
 - Konfigurationsempfehlungen **50**
 - Netzwerkkonfiguration **40, 41**
 - Protokollbandbreite **45**
 - Protokollierung **40, 41, 48**
 - Sekundärer Speicherort **45**
 - Überblick **33**
 - Überprüfung der Richtlinieneinhaltung **43**
 - Unterbrechungsfreie Verfügbarkeit **9**
 - Validierungsprüfungen **43**
 - Version **36**
 - vLockstep-Intervall **45**

- Voraussetzungen **36**
- vSphere-Konfiguration **36**
- Fehlertoleranz bei Bedarf **35**
- Fehlertoleranzstatus
 - Deaktiviert **45**
 - Sekundäre VM erforderlich **45**
 - Starten **45**
 - VM wird nicht ausgeführt **45**
- Firewallports **30**
- ft.maxSwitchoverSeconds **52**

G

- Geplante Ausfallzeit **7**

H

- Hardwarevirtualisierung (HV) **36, 43, 50, 51**
- Hostisolierungsreaktionseinstellung **23**
- Hosts
 - Netzwerkisolierung **11**
 - Wartungsmodus **11**
- Hostüberwachung **23, 30**
- Hostzertifikatsüberprüfung **36, 39**

I

- Interoperabilität, Fehlertoleranz **37**
- IPv6 **37**
- iSCSI-SAN **36**
- ISO-Images **47**

K

- Konfigurieren von erweiterten VMware HA-Optionen **26**
- Konfigurierte Failover-Kapazität **14, 17**

L

- Lastausgleich **35**

M

- Maximale Rücksetzungen pro VM **25**

N

- N_Port-ID-Virtualisierung (NPIV) **37**
- Netzwerkbezeichnungen **30**
- Netzwerkisolierungsadresse **30**
- Netzwerkconfiguration, Fehlertoleranz **40, 41**
- NIC-Gruppierung **31, 41**

P

- Paravirtualisierung **37**
- Planen eines VMware HA-Clusters **11**
- PortFast **30**
- Portgruppennamen **30**
- Primäre Hosts in Clustern **11**

- Prozentsatz der reservierten Clusterressourcen **17**

R

- Rapid Virtualization Indexing (RVI) **37**
- RDM **36, 37**
- Ressourcenfragmentierung **19**

S

- Schulungssupport **5**
- Sekundäre Hosts in Clustern **11**
- Slotgrößenberechnung **14**
- Snapshots **37**
- Speicher
 - iSCSI **36**
 - NAS **36, 50**
 - NFS **36, 50**
- Standard-Gateway **30**
- Starten und Herunterfahren von virtuellen Maschinen **21**
- Steckplatz **14**
- Storage vMotion **7, 37**
- Symmetrischer Multiprozessor (SMP) **37**

T

- Technischer Support **5**
- Tolerieren, Hostausfälle **14**
- Transparentes Failover **9, 33**

U

- Überlasteter Host **51**
- Überprüfung der Richtlinieneinhaltung, Fehlertoleranz **43**
- Überwachen von VMware HA **29**
- Überwachungsempfindlichkeit **25**
- Ungeplante Ausfallzeiten **8**
- Upgrade von Hosts mit fehlertoleranten virtuellen Maschinen **49**

V

- Validierungsprüfungen **43**
- Verwaltungsnetzwerk **20, 30**
- VLAN **41**
- VM-Außerkräftsetzungen **23, 28**
- VM-Neustartpriorität, Einstellung **23**
- VM-Überwachung **25**
- VMDK **36**
- VMFS **11, 30, 48**
- VMware Consolidated Backup (VCB) **37**
- VMware HA
 - anhalten **23**
 - anpassen **26**
 - Checkliste **20**

- Clustereinstellungen **21**
 - Deaktivieren **22**
 - erweiterte Attribute **26**
 - überwachen **29**
 - Vorteile **8**
 - Wiederherstellung nach Ausfällen **8**
 - VMware HA anhalten **23**
 - VMware HA-Cluster
 - Best Practices **29**
 - erstellen **21, 43**
 - Heterogenität **19**
 - planen **11**
 - Primäre Hosts **11**
 - Sekundäre Hosts **11**
 - Zugangssteuerung **13**
 - VMware HA-Netzwerk
 - Best Practices **30**
 - Pfadredundanz **31**
 - VMware Tools **25**
 - VMware vLockstep **9, 33**
 - Vom Cluster tolerierte Hostfehler **14**
 - Voraussetzungen, Fehlertoleranz **36**
- Z**
- Zugangssteuerung
 - Aktivieren **23**
 - Richtlinie **23**
 - Typen **13**
 - VMware HA **13**
 - Zugangssteuerungsrichtlinie
 - Angeben eines Failover-Hosts **18**
 - auswählen **19**
 - Prozentsatz der reservierten Clusterressourcen **17**
 - Vom Cluster tolerierte Hostfehler **14**

