Handbuch zur Verfügbarkeit in vSphere

Update 1
VMware vSphere 6.0
VMware ESXi 6.0
vCenter Server 6.0

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

DE-001810-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

Grundlegende Informationen zur Verfügbarkeit in vSphere 5

1 Business Continuity und Minimieren der Ausfallzeit 7
- Reduzieren geplanter Ausfallzeiten 7
- Verhindern ungeplanter Ausfallzeiten 8
- vSphere HA bietet eine schnelle Wiederherstellung nach Ausfällen 8
- vSphere Fault Tolerance bietet unterbrechungsfreie Verfügbarkeit 9

2 Erstellen und Verwenden von vSphere HA-Clustern 11
- Arbeitsweise von vSphere HA 11
- vSphere HA-Zugangssteuerung 21
- vSphere HA-Interoperabilität 28
- Erstellen und Konfigurieren eines vSphere HA-Clusters 32
- Empfohlene Vorgehensweisen für vSphere HA-Cluster 41

3 Aktivieren der Fault Tolerance für virtuelle Maschinen 47
- Wie Fault Tolerance funktionert 47
- Beispiele für die Nutzen der Fault Tolerance 48
- Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance 49
- Fault Tolerance-Interoperabilität 49
- Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance 52
- Verwenden von Fault Tolerance 54
- Best Practices für Fault Tolerance 59
- Legacy Fault Tolerance 61

Index 65

Grundlegende Informationen zur Verfügbarkeit in vSphere

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

Zielgruppe

Diese Informationen sind an alle gerichtet, die mithilfe von vSphere HA und Fault Tolerance Business Continuity bieten möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datencenteroperationen vertraut sind.

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.
- Reduzieren 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
- „vSphere HA bietet eine schnelle Wiederherstellung nach Ausfällen“, auf Seite 8
- „vSphere Fault Tolerance 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 vSphere 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 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 Datencenterinfrastruktur, 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 Verfügbarkeit 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 vSphere HA und Fault Tolerance ungeplante Ausfallzeiten minimieren oder eliminieren, indem sie schnelle Wiederherstellung nach Ausfällen bzw. unterbrechungsfreie Verfügbarkeit bieten.

vSphere HA bietet eine schnelle Wiederherstellung nach Ausfällen

vSphere HA nutzt mehrere ESXi-Hosts, die als Cluster konfiguriert sind, um eine schnelle Wiederherstellung nach Ausfällen und eine kosteneffektive hohe Verfügbarkeit für Anwendungen, die in virtuellen Maschinen ausgeführt werden, zu gewährleisten.

vSphere 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.
- Es schützt vor Problemen beim Zugriff auf Datenspeicher, indem die betroffenen virtuellen Maschinen auf anderen Hosts, die noch Zugriff auf ihre Datenspeicher haben, neu gestartet werden.
- Dadurch werden virtuelle Maschinen vor Netzwerkisolierung geschützt, indem sie neu gestartet werden, wenn ihr Host im Verwaltungs- oder Virtual SAN-Netzwerk isoliert wird. Dieser Schutz besteht selbst dann, wenn das Netzwerk partitioniert wurde.

Im Gegensatz zu anderen Clusterlösungen bietet vSphere 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 vSphere HA geschützt. Nachdem vSphere HA konfiguriert wurde, sind keine weiteren Aktionen erforderlich, um neue virtuelle Maschinen zu schützen. Sie werden automatisch geschützt.

- Sie können vSphere HA mit vSphere Distributed Resource Scheduler (DRS) kombinieren, um gegen Ausfälle geschützt zu sein und um Lastausgleich zwischen den Hosts innerhalb eines Clusters zu bieten.

vSphere HA bietet mehrere Vorteile gegenüber herkömmlichen Failover-Lösungen:

Minimalinstallation	Nachdem ein vSphere 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 vSphere HA müssen ausreichend Ressourcen vorhanden sein, um die Failover-Funktion für die gewünschte Anzahl an Hosts zu gewährleisten, die Sie mit vSphere HA schützen möchten. Allerdings verwaltet das vCenter Server-System Ressourcen und konfiguriert Cluster automatisch.
Erhöhte Anwendungsverfügbarkeit	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 den Neustart 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 vSphere HA die Wiederherstellung nach dem Ausfall.

vSphere Fault Tolerance bietet unterbrechungsfreie Verfügbarkeit

vSphere HA bietet einen Basisschutz für Ihre virtuelle Maschinen, indem es im Fall eines Hostausfalls virtuelle Maschinen neu startet. vSphere Fault Tolerance bietet ein höheres Maß an Verfügbarkeit, wodurch Benutzer jede beliebige virtuelle Maschine vor einem Hostausfall schützen können, ohne dass Daten, Transaktionen oder Verbindungen verloren gehen.

Fault Tolerance bietet unterbrechungsfreie Verfügbarkeit, indem es sicherstellt, dass die Statuszustände der primären und der sekundären virtuellen Maschine zu jedem Zeitpunkt der Instruktionsausführung der virtuellen Maschine identisch sind.

Wenn entweder der Host, auf dem die primäre virtuelle Maschine ausgeführt wird, oder der Host, auf dem die sekundäre virtuelle Maschine ausgeführt wird, ausfällt, erfolgt sofort ein transparentes Failover. Der funktionierende 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 vSphere HA-Clustern

2

vSphere HA-Cluster ermöglichen einer Sammlung von ESXi-Hosts das Zusammenarbeiten in einer Gruppe und bieten virtuellen Maschinen dadurch eine höhere Verfügbarkeit, als es einzelne ESXi-Hosts können. Wenn Sie planen, einen neuen vSphere HA-Cluster zu erstellen und zu verwenden, beeinflussen die ausgewählten Optionen, wie der Cluster auf Ausfälle von Hosts oder virtuellen Maschinen reagieren wird.

Vor dem Erstellen eines vSphere HA-Clusters sollten Sie wissen, wie vSphere HA Hostausfälle und -isolierung identifiziert und auf solche Situationen reagiert. Darüber hinaus sollten Sie wissen, wie die Zugangssteuerung funktioniert, damit Sie die für Ihre Failover-Anforderungen geeignete Richtlinie wählen können. Nach der Einrichtung eines Clusters können Sie mit erweiterten Optionen dessen Verhalten beeinflussen und seine Leistung optimieren, wenn Sie sich an die folgenden Best Practices halten.

Hinweis Möglicherweise erhalten Sie eine Fehlermeldung, wenn Sie versuchen, vSphere HA zu verwenden. Informationen zu Fehlermeldungen im Zusammenhang mit vSphere HA finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1033634.

Dieses Kapitel behandelt die folgenden Themen:

- „Arbeitsweise von vSphere HA“, auf Seite 11
- „vSphere HA-Zugangssteuerung“, auf Seite 21
- „vSphere HA-Interoperabilität“, auf Seite 28
- „Erstellen und Konfigurieren eines vSphere HA-Clusters“, auf Seite 32
- „Empfohlene Vorgehensweisen für vSphere HA-Cluster“, auf Seite 41

Arbeitsweise von vSphere HA

vSphere 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.

Wenn Sie einen vSphere HA-Cluster erstellen, wird automatisch ein einzelner Host als Master-Host ausgewählt. Der Master-Host kommuniziert mit vCenter Server und überwacht den Zustand aller geschützten virtuellen Maschinen und des Slave-Hosts. Es sind verschiedene Arten von Hostausfällen möglich. Der Master-Host muss den Ausfall erkennen und angemessen mit ihm umgehen. Der Master-Host muss zwischen einem ausgefallenen Host und einem Host unterscheiden, der sich in einer Netzwerkpartition befindet oder netzwerkisoliert ist. Der Master-Host verwendet Netzwerk- und Datenspeicher-Taktsignale, um die Art des Ausfalls zu ermitteln.

vSphere HA-Cluster (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:vSphereHAClusters)

Master- und Slave-Hosts

Wenn Sie einen Host zu einem vSphere HA-Cluster hinzufügen, wird ein Agent auf den Host hochgeladen und für die Kommunikation mit anderen Agenten im Cluster konfiguriert. Jeder Host im Cluster fungiert als Master- oder Slave-Host.

Wenn vSphere HA für einen Cluster aktiviert ist, nehmen alle aktiven Hosts (d. h. diejenigen Hosts, die sich nicht im Standby- oder Wartungsmodus befinden und nicht getrennt sind) an der Wahl des Master-Hosts für den Cluster teil. Der Host, der die meisten Datenspeicher mountet, hat einen Vorteil bei der Wahl. Es gibt in der Regel nur einen Master-Host pro Cluster. Alle anderen Hosts sind Slave-Hosts. Falls der Master-Host ausfällt, heruntergefahren, in Standby-Modus versetzt oder aus dem Cluster entfernt wird, findet eine Neuwahl statt.

Der Master-Host in einem Cluster hat zahlreiche Verpflichtungen:

- Überwachung des Zustands von Slave-Hosts. Falls ein Slave-Host ausfällt oder unerreichbar wird, identifiziert der Master-Host die virtuellen Maschinen, die neu gestartet werden müssen.
- Überwachung des Betriebszustands aller geschützten virtuellen Maschinen. Falls eine virtuelle Maschine ausfällt, sorgt der Master-Host dafür, dass sie neu gestartet wird. Mithilfe einer Engine für die lokale Platzierung bestimmt der Master-Host auch die Stelle, an der der Neustart erfolgen soll.
- Verwaltung der Listen der Cluster-Hosts und der geschützten virtuellen Maschinen.
- Dient als vCenter Server-Verwaltungsschnittstelle für den Cluster und meldet den Zustand des Clusters.

Die Slave-Hosts tragen in erster Linie zum Cluster bei, indem sie virtuelle Maschinen lokal ausführen, ihren Laufzeitstatus überwachen und Zustand-Updates an den Master-Host melden. Ein Master-Host kann auch virtuelle Maschinen ausführen und überwachen. Sowohl Slave-Hosts als auch Master-Hosts implementieren die VM- und Anwendungsüberwachungsfunktionen.

Eine der vom Master-Host ausgeführten Funktionen ist das orchestrierte Neustarten von virtuellen Maschinen. Eine virtuelle Maschine wird durch einen Master-Host geschützt, nachdem vCenter Server festgestellt hat, dass der Betriebszustand der virtuellen Maschine gdurch einen Benutzereingriff von „ausgeschaltet“ auf „eingeschaltet“ wechselt. Der Master-Host führt dauerhaft eine Liste der geschützten virtuellen Maschinen in den Datenspeichern des Clusters. Ein neu gewählter Master-Host benutzt die Informationen, um zu ermitteln, welche virtuellen Maschinen geschützt werden sollen.

Hinweis Wenn Sie einen Host von einem Cluster trennen, bleiben alle virtuellen Maschinen, die mit diesem Host registriert sind, von vSphere HA ungeschützt.

Arten des Hostausfalls und deren Erkennung

Der Master-Host eines vSphere HA-Clusters ist verantwortlich für das Erkennen des Ausfalls eines Slave-Hosts. Je nach Art des erkannten Ausfalls muss für die auf den Hosts ausgeführten virtuellen Maschinen möglicherweise ein Failover durchgeführt werden.

Es werden drei Typen von Hostausfällen in einem vSphere HA-Cluster erkannt:

- Fehler – Ein Host funktioniert nicht mehr.
- Isolierung – Ein Host wird netzwerkisoliert.
- Partition – Die Netzwerkkonnektivität zwischen dem Host und dem Master-Host wird unterbrochen.

Der Master-Host überwacht, ob die Slave-Hosts im Cluster noch aktiv sind. Die Kommunikation erfolgt über den Austausch von Taktsignalen im Sekundentakt. Wenn der Master-Host keine Taktsignale von einem Slave-Host empfängt, überprüft er, ob der Host noch aktiv ist, bevor er den Host als ausgefallen betrachtet. Beim Überprüfen, ob der Slave-Host noch aktiv ist, ermittelt der Master-Host, ob der Slave-Host Taktsignale mit einem der Datenspeicher austauscht. Siehe „Datenspeicher-Taktsignale“, auf Seite 19. Der Master-Host überprüft zudem, ob der Host auf ICMP-Pings reagiert, die an seine Management-IP-Adressen gesendet werden.

Wenn ein Master-Host nicht direkt mit dem Agenten auf einem Slave-Host kommunizieren kann, der Slave-Host nicht auf die ICMP-Pings reagiert und der Agent keine Taktsignale sendet, gilt der Slave-Host als ausgefallen. Die virtuellen Maschinen des Hosts werden auf alternativen Hosts neu gestartet. Wenn ein solcher Slave-Host Taktsignale mit einem Datenspeicher austauscht, unterstellt der Master-Host, dass sich der Slave-Host in einer Netzwerkpartition befindet oder netzwerkisoliert ist, und überwacht den Host und dessen virtuelle Maschinen weiterhin. Siehe „Netzwerkpartitionen“, auf Seite 19.

Eine Hostnetzwerkisolierung liegt vor, wenn ein Host noch ausgeführt wird, jedoch keinen Datenverkehr von den vSphere HA-Agenten im Verwaltungsnetzwerk beobachten kann. Wenn dieser Datenverkehr vom Host nicht mehr beobachtet wird, versucht der Host, die Cluster-Isolierungsadressen anzupingen. Falls dies ebenfalls fehlschlägt, deklariert er sich selbst als vom Netzwerk isoliert.

Der Master-Host überwacht die virtuellen Maschinen, die auf einem isolierten Host ausgeführt werden, und wenn er beobachtet, dass sie ausgeschaltet werden und der Master-Host für die virtuellen Maschinen verantwortlich ist, startet er sie neu.

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

Festlegen von Antworten auf Hostproblemen

Wenn ein Host ausfällt und seine virtuellen Maschinen neu gestartet werden müssen, können Sie mit der Einstellung für die VM-Neustartpriorität festlegen, in welcher Reihenfolge die virtuellen Maschinen neu gestartet werden. Mit der Einstellung für die Hostisolierungsreaktion können Sie auch konfigurieren, wie vSphere HA reagiert, wenn Hosts die Verwaltungsnetzwerkkonnektivität mit anderen Hosts verlieren. Beim Neustart einer virtuellen Maschine durch vSphere HA nach einem Fehler werden noch weitere Faktoren berücksichtigt.

Die folgenden Einstellungen gelten für alle virtuellen Maschinen im Cluster im Falle eines Hostausfalls oder einer Hostisolation.D Sie können zudem Ausnahmen für bestimmte virtuelle Maschinen konfigurieren. Siehe „Anpassen einer einzelnen virtuellen Maschine“, auf Seite 40.

VM-Neustartpriorität

Mithilfe der VM-Neustartpriorität legen Sie die relative Reihenfolge fest, in der den virtuellen Maschinen nach einem Hostausfall Ressourcen zugeordnet werden. Diese virtuellen Maschinen werden Hosts mit nicht reservierter Kapazität zugewiesen. Virtuelle Maschinen mit der höchsten Priorität kommen an erster Stelle, dann wird mit VMs mit geringerer Priorität fortgefahren, bis alle virtuellen Maschinen platziert sind oder keine Cluster-Kapazität mehr verfügbar ist, um die Reservierungen oder den Arbeitsspeicher-Overhead der virtuellen Maschinen zu erfüllen. Dann startet der Host die zugewiesenen virtuellen Maschinen in der Reihenfolge ihrer Priorität neu. Wenn nicht ausreichend Ressourcen vorhanden sind, wartet vSphere HA, bis weitere nicht reservierte Kapazität verfügbar wird, zum Beispiel, wenn ein Host wieder online ist, und versucht dann erneut, diese virtuellen Maschinen zu platzieren. Um die Möglichkeit einer solchen Situation zu verringern, sollten Sie die vSphere HA-Zugangssteuerung so konfigurieren, dass mehr Ressourcen für Ausfälle reserviert werden. Mit der Zugangssteuerung kann gesteuert werden, welche Cluster-Kapazität von virtuellen Maschinen reserviert wird und Reservierungen und den Arbeitsspeicher-Overhead anderer virtueller Maschinen bei einem Ausfall nicht bedienen kann.

Die Werte für diese Einstellung sind: „Deaktiviert“, „Niedrig“, „Mittel“ (Standardeinstellung) und „Hoch“. Die Einstellung „Deaktiviert“ wird von der VM/Anwendungsüberwachungsfunktion von vSphere HA ignoriert, da diese Funktion virtuelle Maschinen vor Ausfällen der Betriebssystem-Ebene und nicht vor Ausfällen virtueller Maschinen schützt. Wenn ein Fehler auf Betriebssystemebene auftritt, wird das Betriebssystem von vSphere HA neu gestartet und die virtuelle Maschine wird weiterhin auf demselben Host ausgeführt. Diese Einstellung kann für einzelne virtuelle Maschinen geändert werden.

Hinweis Das Zurücksetzen einer virtuellen Maschine führt zu einem harten Neustart des Gastbetriebssystems, aber nicht zu einem Ein-/Ausschalten der virtuellen Maschine.

Die Neustartprioritätseinstellungen für virtuelle Maschinen sind je nach Benutzererfordnissen unterschiedlich. Weisen Sie den virtuellen Maschinen, die die wichtigsten Dienste verrichten, eine höhere Neustartpriorität zu.

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.

Wenn ein Host ausfällt, versucht vSphere HA, die betroffenen virtuellen Maschinen, die eingeschaltet waren und deren Neustartpriorität auf „Deaktiviert“ eingestellt ist bzw. die ausgeschaltet waren, bei einem aktiven Host zu registrieren.

Hostisolierungsreaktion

Die Hostisolierungsreaktion legt fest, was geschieht, wenn die Verbindungen des Hosts in einem vSphere HA-Cluster zum Verwaltungsnetzwerk verloren gehen, dieser aber weiter ausgeführt wird. Mit der Isolierungsreaktion können Sie vSphere HA so konfigurieren, dass virtuelle Maschinen, die auf einem isolierten Host ausgeführt werden, ausgeschaltet und auf einem nicht isolierten Host neu gestartet werden. 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 nicht mit den Agenten, die auf anderen Hosts ausgeführt werden, kommunizieren und seine Isolierungsadressen nicht anpingen kann. Der Host führt dann seine Isolierungsreaktion aus. Die Reaktionen sind „VMs ausschalten und neu starten“ bzw. „VMs herunterfahren und neu starten“. Diese Eigenschaft kann für einzelne virtuelle Maschinen geändert werden.

Hinweis Wenn eine virtuelle Maschine eine Neustartprioritätseinstellung „Deaktiviert“ hat, wird keine Hostisolierungsreaktion vorgenommen.

Sie müssen zum Verwenden der Einstellung „VMs herunterfahren und neu starten“ 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 der erweiterten Option `das.isolationShutdownTimeout` angegeben ist, heruntergefahren werden, werden ausgeschaltet.

Nach dem Erstellen eines vSphere 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.

Es kann zu einer „Split-Brain"-Situation für die virtuelle Maschine kommen, wenn ein Host von einem Master-Host isoliert oder partitioniert wird und der Master-Host nicht über Taktsignal-Datenspeicher mit ihm kommunizieren kann. In dieser Situation kann der Master-Host nicht feststellen, ob der Host läuft, und erklärt ihn daher für ausgefallen. Der Master-Host versucht dann, die virtuellen Maschinen, die auf dem isolierten oder partitionierten Host ausgeführt werden, neu zu starten. Dieser Versuch ist erfolgreich, wenn die virtuellen Maschinen auf dem isolierten/partitionierten Host weiter ausgeführt werden und der Host den Zugriff auf die Datenspeicher der virtuellen Maschinen verlor, als er isoliert oder partitioniert wurde. Dann liegt ein „Split-Brain"-Zustand vor, weil zwei Instanzen der virtuellen Maschine vorhanden sind. Es ist jedoch nur eine Instanz in der Lage, die virtuellen Festplatten der virtuellen Maschine zu lesen oder darauf zu schreiben. Um diesen Split-Brain-Zustand zu verhindern, kann der VM-Komponentenschutz verwendet werden. Wenn Sie die aggressive Einstellung des VM-Komponentenschutzes aktivieren, wird der Zugriff auf Datenspeicher für eingeschaltete virtuelle Maschinen überwacht, und virtuelle Maschinen, die den Zugriff auf ihre Datenspeicher verlieren, werden heruntergefahren.

Um dieses Problem zu beheben, generiert ESXi eine Frage auf der virtuellen Maschine, die die Festplattensperren verloren hat, für den Fall, dass der Host die Isolation verlässt und feststellt, dass er die Festplattensperren nicht mehr wiederherstellen kann. vSphere HA beantwortet diese Frage automatisch und ermöglicht der Instanz der virtuellen Maschine, die die Festplattensperren verloren hat, sich auszuschalten. Übrig bleibt die Instanz, die über Festplattensperren verfügt.

Berücksichtigte Faktoren für den Neustart von virtuellen Maschinen

Nach einem Ausfall versucht der Master-Host des Clusters, die betroffenen virtuellen Maschinen neu zu starten, indem ein Host identifiziert wird, der sie einschalten kann. Bei der Auswahl eines derartigen Hosts berücksichtigt der Master-Host eine Reihe von Faktoren.

Zugriffsfähigkeit auf Dateien
Bevor eine virtuelle Maschine gestartet werden kann, muss auf ihre Dateien von einem der aktiven Cluster-Hosts, mit dem der Master über das Netzwerk kommunizieren kann, zugegriffen werden können.

Virtuelle Maschine und Hostkompatibilität
Wenn Hosts vorhanden sind, auf die zugegriffen werden kann, muss die virtuelle Maschine mit mindestens einem der Hosts kompatibel sein. Zur für eine virtuelle Maschine festgelegten Kompatibilität zählt die Wirkung aller erforderlichen VM-Host-Affinitätsregeln. Wenn z. B. eine Regel nur die Ausführung der virtuellen Maschine auf zwei Hosts zulässt, wird sie für die Platzierung auf diesen beiden Hosts berücksichtigt.

Ressourcenreservierungen
Mindestens einer der Hosts, auf denen die virtuelle Maschine ausgeführt werden kann, muss über ausreichend nicht reservierte Kapazität verfügen, um den Arbeitsspeicher-Overhead der virtuellen Maschine und etwaige Ressourcenreservierungen zu erfüllen. Es kommen vier Reservierungstypen in Betracht: CPU, Arbeitsspeicher, vNIC und virtueller Flash. Zudem müssen genügend Netzwerkports verfügbar sein, um die virtuelle Maschine einzuschalten.

Hostgrenzwerte
Zusätzlich zu den Ressourcenreservierungen kann eine virtuelle Maschine nur auf einem Host platziert werden, wenn dadurch nicht die maximale Anzahl zulässiger virtueller Maschinen oder die Anzahl der verwendeten vCPUs überschritten wird.

Funktionsbeschränkungen
Wenn die erweiterte Option festgelegt wird, in der vSphere HA Anti-Affinitätsregeln von VM zu VM durchsetzen muss, dann wird diese Regel durch vSphere HA nicht verletzt. Zudem verletzt vSphere HA keine pro Host konfigurierten Limits für fehlertolerante virtuelle Maschinen.

Wenn kein Host die obigen Bedingungen erfüllt, gibt der Master-Host ein Ereignis aus, das besagt, dass nicht genügend Ressourcen vorhanden sind, damit vSphere HA die VM starten kann, und versucht es erneut, nachdem sich die Clusterbedingungen geändert haben. Wenn zum Beispiel die virtuelle Maschine nicht zugänglich ist, versucht der Master-Host es erneut, nachdem sich die Dateizugänglichkeit geändert hat.

Limits für Neustartversuche der virtuellen Maschinen

Wenn der Master-Agent von vSphere HA versucht, eine VM neu zu starten (was deren Registrierung und Einschaltung umfasst) und der Versuch fehlschlägt, wird der Neustart nach einer Verzögerung erneut versucht. vSphere HA unternimmt eine maximale Anzahl Versuche (standardmäßig 6), die VM neu zu starten. Bei diesem Höchstwert zählen jedoch nicht alle Neustartfehler.

So besteht z. B. der wahrscheinlichste Grund für einen fehlgeschlagenen Neustart darin, dass die VM entweder auf einem anderen Host noch ausgeführt wird, oder dass vSphere HA zu früh versucht hat, die VM nach einem Ausfall neu zu starten. In dieser Situation verzögert der Master-Agent den erneuten Versuch um das Doppelte der Verzögerung nach dem letzten Versuch (mindestens 1 und höchstens 30 Minuten). Wenn also die Verzögerung auf 1 Minute festgelegt ist, wird ein erster Versuch bei T=0 gemacht. Weitere Versuche finden bei T=1 (1 Minute), T=3 (3 Minuten), T=7 (7 Minuten), T=15 (15 Minuten) und T=30 (30 Minuten) statt. Jeder dieser Versuche zählt für das Limit, und standardmäßig finden nur sechs Versuche statt.

Weitere Neustartfehler führen zu zählbaren erneuten Versuchen, aber mit einem anderen Verzögerungsintervall. Ein Beispiel dafür ist ein Szenario, in dem der für den Neustart der virtuellen Maschine ausgewählte Host den Zugriff auf einen der Datenspeicher der VM verliert, nachdem die Auswahl durch den Master-Agent getroffen wurde. In diesem Fall wird nach einer Standardverzögerung von 2 Minuten ein erneuter Versuch gestartet. Dieser Versuch zählt ebenfalls für das Limit.

Schließlich gibt es noch Versuche, die nicht zählen. Das ist beispielsweise der Fall, wenn der Host, auf dem die virtuelle Maschine neu gestartet werden sollte, ausfällt, bevor der Master-Agent die Neustartanforderung ausgibt. Der Versuch wird nach 2 Minuten wiederholt, aber dieser Fehler zählt nicht bei der maximalen Anzahl der Versuche.

Benachrichtigungen über Neustart der virtuellen Maschine

vSphere HA generiert ein Clusterereignis, wenn ein Failover-Vorgang für virtuelle Maschinen im Cluster läuft. Durch das Ereignis wird auch ein Konfigurationsproblem auf der Registerkarte **Cluster-Übersicht** angezeigt. Dort wird die Anzahl der virtuellen Maschinen angegeben, die neu gestartet werden. Es gibt vier verschiedene Kategorien für diese VMs.

- VMs, die platziert werden: vSphere HA versucht derzeit, diese VMs neu zu starten
- VMs, für die auf einen neuen Versuch gewartet wird: Ein vorheriger Neustartversuch ist fehlgeschlagen, und vSphere HA wartet, bis ein Zeitintervall abgelaufen ist, bevor ein weiterer Versuch unternommen wird.
- VMs, die zusätzliche Ressourcen benötigen: Es sind nicht ausreichend Ressourcen für den Neustart dieser VMs vorhanden. vSphere HA wiederholt den Versuch, wenn neue Ressourcen verfügbar werden, z. B. wenn ein Host wieder online ist.
- Virtual SAN-VMs, auf die kein Zugriff möglich ist: vSphere HA kann diese Virtual SAN-VMs nicht neu starten, weil kein Zugriff darauf möglich ist. Der Versuch wird wiederholt, sobald sich die Zugriffsfähigkeit ändert.

Die Anzahl der virtuellen Maschinen wird dynamisch aktualisiert, sobald eine Änderung an der Anzahl der VMs beobachtet wird, für die ein Neustartvorgang läuft. Das Konfigurationsproblem wird gelöscht, wenn vSphere HA alle VMs neu gestartet oder die Versuche eingestellt hat.

In vSphere 5.5 oder früher wird ein Ereignis pro VM ausgegeben, wenn ein erfolgloser Versuch zum Neustarten der virtuellen Maschine unternommen wurde. Dieses Ereignis ist in vSphere 6.x standardmäßig deaktiviert. Es kann aktiviert werden, indem die erweiterte vSphere HA-Option `das.config.fdm.reportfailoverfailevent` auf „1“ festgelegt wird.

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 vSphere 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 Gastbetriebssystems 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 vermeiden, 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 die erweiterte Option `das.iostatsInterval` 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

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

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

Hinweis Die Statistik der Rücksetzungen wird gelöscht, wenn eine virtuelle Maschine aus- und wieder angeschaltet wird, oder wenn Sie mittels vMotion zu einem anderen Host migriert wird. Das hat zur Folge, dass das Gastbetriebssystem erneut startet, was jedoch nicht dasselbe wie ein 'Neustart' ist, bei dem der Betriebszustand sich ändert.

Wenn bei einer virtuellen Maschine ein Fehler beim Zugriff auf den Datenspeicher auftritt (entweder „keine Pfade verfügbar“ oder „dauerhafter Geräteverlust“), wird sie vom VM-Überwachungsdienst erst dann zurückgesetzt, nachdem der Fehler behoben wurde.

VM Component Protection

Wenn der VM Component Protection (VMCP) aktiviert ist, kann vSphere HA Ausfälle beim Zugriff auf Datenspeicher feststellen und automatische Wiederherstellung für die betroffenen virtuellen Maschinen bereitstellen.

Der VM-Komponentenschutz bietet Schutz gegen Fehler beim Datenspeicherzugriff, von denen eine virtuelle Maschine auf einem Host in einem vSphere HA-Cluster betroffen sein kann. Wenn ein Datenspeicherzugriffsfehler eintritt, kann der betroffene Host nicht mehr auf den Speicherpfad für einen bestimmten Datenspeicher zugreifen. Sie können festlegen, wie vSphere HA auf einen derartigen Fehler reagiert. Die Möglichkeiten reichen von der Erstellung von Ereignisalarmen bis zu Neustarts der virtuellen Maschinen auf anderen Hosts.

Hinweis Bei Verwendung der VM Component Protection-Funktion müssen Ihre ESXi-Hosts mindestens Version 6.0 aufweisen.

Fehlertypen

Es gibt zwei Typen von Datenspeicherzugriffsfehlern:

PDL PDL (Permanent Device Loss, dauerhafter Geräteausfall) ist ein nicht wiederherstellbarer Zugriffsverlust, der eintritt, wenn ein Speichergerät meldet, dass der Host nicht mehr auf den Datenspeicher zugreifen kann. Dieser Zustand kann ohne Ausschalten der virtuellen Maschinen nicht rückgängig gemacht werden.

APD APD (All Paths Down, keine Pfade verfügbar) steht für einen vorübergehenden oder unbekannten Zugriffsverlust oder eine andere nicht identifizierte Verzögerung bei der I/O-Verarbeitung. Dieser Zugriffsfehlertyp ist wiederherstellbar.

Konfigurieren des VM-Komponentenschutzes

VM Component Protection wird im vSphere Web Client konfiguriert. Navigieren Sie zur Registerkarte **Konfigurieren** und klicken Sie auf **vSphere Availability** und **Bearbeiten**. Unter **Fehler und Reaktionen** können Sie **Datenspeicher mit PDL** oder **Datenspeicher mit APD** auswählen. Die auswählbaren Speicherschutzstufen und die verfügbaren Problembehebungsaktionen für virtuelle Maschinen sind je nach Typ des Datenbankzugriffsfehlers unterschiedlich.

PDL-Fehler Unter **Datenspeicher mit PDL** können Sie **Ereignisse ausgeben** oder **VMs ausschalten und neu starten** auswählen.

APD-Fehler In diesem Fall ist die Reaktion auf APD-Ereignisse komplexer und daher auch die Konfiguration aufwendiger. Sie können **Ereignisse ausgeben**, **VMs ausschalten und neu starten – konservative Neustartrichtlinie** oder **VMs ausschalten und neu starten – aggressive Neustartrichtlinie** auswählen.

Hinweis Wenn die Einstellungen für Hostüberwachung oder VM-Neustartpriorität deaktiviert werdenn, kann der VM-Komponentenschutz die virtuellen Maschinen nicht neu starten. Davon unabhängig können aber die Speicher überwacht und Ereignisse ausgegeben werden.

Netzwerkpartitionen

Wenn bei einem vSphere HA-Cluster das Verwaltungsnetzwerk ausfällt, kann möglicherweise ein Teil der Hosts des Clusters nicht über das Verwaltungsnetzwerk mit anderen Hosts kommunizieren. Ein Cluster kann mehrere Partitionen enthalten.

Ein partitionierter Cluster vermindert den Schutz von virtuellen Maschinen und bietet eine geringere Clusterverwaltungsfunktionalität. Korrigieren Sie den partitionierten Cluster so bald wie möglich.

- Schutz von virtuellen Maschinen. vCenter Server lässt zu, dass eine virtuelle Maschine eingeschaltet wird, sie kann allerdings nur dann geschützt werden, wenn sie in derselben Partition wie der Master-Host ausgeführt wird, der für sie verantwortlich ist. Der Master-Host muss mit vCenter Server kommunizieren. Ein Master-Host ist verantwortlich für eine virtuelle Maschine, wenn er eine vom System definierte Datei auf dem Datenspeicher exklusiv gesperrt hat, auf dem sich die Konfigurationsdatei der virtuellen Maschine befindet.
- Clusterverwaltung. vCenter Server kann mit dem Master-Host kommunizieren, aber nur mit einer Teilmenge der Slave-Hosts. Folglich werden Änderungen an der Konfiguration, die vSphere HA betreffen, möglicherweise erst wirksam, nachdem die Partition behoben wurde. Dieser Fehler könnte dazu führen, dass eine der Partitionen unter der alten Konfiguration betrieben wird, während eine andere Partition die neuen Einstellungen nutzt.

Datenspeicher-Taktsignale

Wenn der Master-Host in einem vSphere HA-Cluster nicht über das Verwaltungsnetzwerk mit einem Slave-Host kommunizieren kann, verwendet der Master-Host Datenspeicher-Taktsignale, um festzustellen, ob der Slave-Host ausgefallen ist, sich in einer Netzwerkpartition befindet oder netzwerkisoliert ist. Wenn der Datenspeicher des Slave-Hosts keine Taktsignale mehr sendet, wird er als ausgefallen betrachtet und seine virtuellen Maschinen werden an anderer Stelle neu gestartet.

vCenter Server wählt eine bevorzugte Gruppe von Datenspeichern für Taktsignale aus. Diese Auswahl wird getroffen, um die Anzahl der Hosts, die Zugriff auf die Taktsignale eines Datenspeichers haben, zu maximieren und die Wahrscheinlichkeit, dass die Datenspeicher von denselben LUNs oder NFS-Servern gestützt werden, zu minimieren.

Sie können die erweiterte Option `das.heartbeatdsperhost` verwenden, um die Anzahl der Taktsignal-Datenspeicher zu ändern, die für jeden Host von vCenter Server ausgewählt wurden. Der Standardwert beträgt zwei und der Maximalwert fünf.

vSphere HA erstellt ein Verzeichnis im Stammverzeichnis eines jeden Datenspeichers, das für Datenspeicher-Taktsignale und zum Aufrechterhalten der Gruppe von geschützten virtuellen Maschinen verwendet wird. Der Name des Verzeichnisses lautet `.vSphere-HA`. Löschen oder ändern Sie die Dateien in diesem Verzeichnis nicht, da dies den betrieblichen Ablauf beeinträchtigen kann. Da ein Datenspeicher von mehr als einem Cluster verwendet werden kann, werden Unterverzeichnisse für jeden Cluster erstellt. Der Root-Benutzer ist Eigentümer dieser Verzeichnisse und Dateien. Lese- und Schreibzugriffe auf sie sind dem Root-Benutzer vorbehalten. Der von vSphere HA verwendete Festplattenspeicher hängt von mehreren Faktoren ab, z. B. der verwendeten VMFS-Version und der Anzahl der Hosts, die den Datenspeicher zum Senden von Taktsignalen verwenden. Im Falle von vmfs3 beträgt die Maximalnutzung etwa 2 GB und die übliche Nutzung etwa 3 MB. Bei vmfs5 betragen die Maximal- und die typische Nutzung ungefähr 3 MB. Die Nutzung der Datenspeicher durch vSphere HA geht mit einem vernachlässigbaren Overhead und ohne Auswirkungen auf die Leistung anderer Datenspeichervorgänge einher.

vSphere HA beschränkt die Anzahl an virtuellen Maschinen, die Konfigurationsdateien in einem einzelnen Datenspeicher haben können. Aktualisierte Grenzwerte finden Sie unter *Maximalwerte für die Konfiguration*. Wenn Sie mehr als diese Anzahl an virtuellen Maschinen in einem Datenspeicher platzieren und diese einschalten, schützt vSphere HA nur eine durch den Grenzwert beschränkte Anzahl an virtuellen Maschinen.

Hinweis Ein Datenspeicher für Virtual SAN kann nicht für Datenspeicher-Taktsignale verwendet werden. Wenn deshalb kein anderer gemeinsam genutzter Speicher verfügbar ist, auf den alle Hosts im Cluster Zugriff haben, können keine Taktsignal-Datenspeicher in Verwendung sein. Wenn allerdings Speicher vorhanden ist, der über einen alternativen Netzwerkpfad erreichbar ist, der unabhängig vom Netzwerk des Virtual SAN ist, können Sie damit einen Taktsignal-Datenspeicher einrichten.

vSphere HA-Sicherheit

vSphere HA wurde um mehrere Sicherheitsfunktionen erweitert.

Auswahl der geöffneten Firewallports

vSphere HA verwendet TCP- und UDP-Port 8182 für die Kommunikation zwischen Agenten. Die Firewallports werden automatisch geöffnet und geschlossen, um sicherzustellen, dass sie nur dann geöffnet sind, wenn dies erforderlich ist.

Schutz von Konfigurationsdateien mithilfe von Dateisystemberechtigungen

vSphere HA speichert Informationen zur Konfiguration auf dem lokalen Speicher oder auf einer Ramdisk, falls kein lokaler Datenspeicher zur Verfügung steht. Diese Dateien sind durch Dateisystemberechtigungen geschützt und nur dem Root-Benutzer zugänglich. Hosts ohne lokalen Speicher werden nur dann unterstützt, wenn sie durch Auto Deploy verwaltet werden.

Detaillierte Protokollierung

Der Speicherort, an den vSphere HA Protokolldateien ablegt, hängt von der Hostversion ab.

- Bei ESXi 5.x-Hosts schreibt vSphere HA standardmäßig nur in syslog. Die Protokolle werden an dem Speicherort abgelegt, der für syslog konfiguriert wurde. Den Namen der Protokolldateien für vSphere HA wird `fdm` (fault domain manager) vorangestellt. Dies ist ein Dienst von vSphere HA.
- Bei älteren ESXi 4.x-Hosts schreibt vSphere HA in `/var/log/vmware/fdm` auf der lokalen Festplatte sowie in syslog, falls dies konfiguriert wurde.
- Bei älteren ESX 4.x-Hosts schreibt vSphere HA in `/var/log/vmware/fdm`.

Sichere vSphere HA-Anmeldungen

vSphere HA meldet sich bei vSphere HA-Agenten mit dem Benutzerkonto **vpxuser** an, das von vCenter Server erstellt wurde. Dieses Konto ist dasselbe Konto, das von vCenter Server zum Verwalten des Hosts verwendet wird. vCenter Server erstellt ein Zufallskennwort für dieses Konto und ändert es regelmäßig. Der Zeitraum wird durch die vCenter Server-Einstellung `VirtualCenterVimPasswordExpirationInDays` festgelegt. Benutzer mit administrativen Rechten auf den Root-Ordner des Hosts können sich ebenfalls beim Agenten anmelden.

Sichere Kommunikation

Die gesamte Kommunikation zwischen vCenter Server und dem vSphere HA-Agenten wird über SSL abgewickelt. Die Kommunikation zwischen Agenten wird ebenfalls über SSL abgewickelt. Ausgenommen davon sind Wahlmeldungen, für die UDP verwendet wird. Wahlmeldungen werden über SSL verifiziert, damit ein bösartiger Agent nur den Host, auf dem der Agent ausgeführt wird, daran hindern kann, dass er als Master-Host ausgewählt wird. In diesem Fall wird ein Konfigurationsproblem für den Cluster ausgestellt, damit der Benutzer über das Problem Bescheid weiß.

Verifizierung des Host-SSL-Zertifikats erforderlich

vSphere HA erfordert, dass jeder Host über ein verifiziertes SSL-Zertifikat verfügt. Jeder Host generiert beim erstmaligen Starten ein selbstsigniertes Zertifikat. Dieses Zertifikat kann anschließend neu generiert oder durch ein von einer Zertifizierungsstelle ausgestelltes Zertifikat ersetzt werden. Falls das Zertifikat ersetzt wird, muss vSphere HA auf dem Host neu konfiguriert werden. Falls ein Host die Verbindung zu vCenter Server verliert, nachdem sein Zertifikat aktualisiert und der ESXi- oder ESX-Host-Agent neu gestartet wurde, wird vSphere HA automatisch neu konfiguriert, wenn der Host eine neue Verbindung zu vCenter Server herstellt. Falls die Verbindung nicht getrennt wird, weil die Verifizierung des Host-SSL-Zertifikats durch vCenter Server zu diesem Zeitpunkt deaktiviert ist, verifizieren Sie das neue Zertifikat und konfigurieren Sie vSphere HA auf dem Host neu.

vSphere 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.

vSphere 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 vSphere HA-Zugangssteuerung deaktiviert werden. Es gibt ohne diese jedoch keine Garantie dafür, dass nach einem Hostausfall die erwartete Anzahl an virtuellen Maschinen neu gestartet werden kann. Deaktivieren Sie die Zugangssteuerung nicht dauerhaft. 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 Distributed Power Management (DPM) zu testen.
- Wenn ein automatisierter Vorgang Aktionen ausführen muss, die vorübergehend gegen die Failover-Einschränkungen verstoßen (z. B. als Teil eines von vSphere Update Manager durchgeführten Upgrades oder Patches von ESXi-Hosts).
- Wenn Sie Test- oder Wartungsvorgänge durchführen müssen.

Die Zugangssteuerung reserviert Kapazität, aber bei einem Fehler nutzt vSphere HA die gesamte verfügbare Kapazität für den Neustart der virtuellen Maschine. Beispiel: vSphere HA platziert mehr virtuelle Maschinen auf einem Host, als die Zugangssteuerung für vom Benutzer initiierte Einschaltvorgänge zulässt.

Hinweis Wenn die vSphere HA-Zugangssteuerung deaktiviert ist, stellt vSphere HA sicher, dass es mindestens zwei eingeschaltete Hosts im Cluster gibt, selbst wenn DPM aktiviert ist und alle virtuellen Maschinen auf einen einzelnen Host konsolidieren kann. Dadurch wird sichergestellt, dass Failover möglich ist.

Zugangssteuerung mit der Richtlinie „Vom Cluster tolerierte Hostfehler“

Sie können vSphere HA für das Tolerieren einer angegebenen Anzahl an Hostausfällen konfigurieren. vSphere 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 vSphere HA die Zugangssteuerung folgendermaßen aus:

1 Berechnet die Steckplatzgröße.

   Ein Steckplatz 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 Steckplätze 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 Steckplätze 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 Sie können im Zugangssteuerungsabschnitt der vSphere-HA-Einstellungen im vSphere Web Client eine spezifische Steckplatzgröße für die CPU und den Arbeitsspeicher festlegen.

Steckplatzgrößenberechnung

vSphere HA-Steckplatzgröße und -Zugangssteuerung (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_slot_admission_control)

Die Steckplatzgröße besteht aus zwei Komponenten: CPU und Arbeitsspeicher.

- vSphere HA berechnet die CPU-Komponente, indem es die CPU-Reservierung von jeder eingeschalteten virtuellen Maschine abruft und den größten Wert auswählt. Wenn Sie keinen Wert für die CPU-Reservierung einer virtuellen Maschine angegeben haben, wird ein Standardwert von 32 MHz zugewiesen. Sie können diesen Wert anhand der erweiterten Option `das.vmcpuminmhz` ändern.
- vSphere HA berechnet die Arbeitsspeicherkomponente, indem es die Arbeitsspeicherreservierung (zuzüglich Arbeitsspeicher-Overhead) von jeder eingeschalteten virtuellen Maschine abruft 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 Steckplatzgröße. Um dies zu vermeiden, können Sie eine Obergrenze für die CPU- oder Arbeitsspeicherkomponente der Steckplatzgröße festlegen, indem Sie die erweiterte Option `das.slotcpuinmhz` bzw.`das.slotmeminmb` verwenden. Siehe „Erweiterte vSphere HA-Optionen“, auf Seite 38.

Sie können auch das Risiko der Ressourcenfragmentierung in Ihrem Cluster ermitteln, indem Sie die Anzahl der virtuellen Maschinen anzeigen, die mehrere Steckplätze benötigen. Dies kann im Zugangssteuerungsabschnitt der vSphere HA-Einstellungen im vSphere Web Client berechnet werden. Virtuelle Maschinen erfordern möglicherweise mehrere Steckplätze, wenn Sie eine feste Steckplatzgröße oder eine maximale Steckplatzgröße mit erweiterten Optionen festgelegt haben.

Verwenden von Steckplätzen zum Berechnen der aktuellen Failover-Kapazität

Wenn die Steckplatzgröße berechnet wurde, ermittelt vSphere 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 Ressourcendaten für einen Host, der von vSphere HA verwendet wird, finden Sie auf der Registerkarte **Übersicht** für den Host auf dem vSphere Web Client. Wenn alle Hosts im Cluster gleich sind, können diese Daten durch Dividieren der Gesamtzahlen für die Cluster-Ebene durch die Anzahl der Hosts ermittelt werden. Die für die Virtualisierung verwendeten Ressourcen sind nicht enthalten. Nur Hosts, die verbunden und nicht im Wartungsmodus sind sowie keine vSphere HA-Fehler aufweisen, werden berücksichtigt.

Die maximale Anzahl an Steckplätzen, die jeder Host unterstützen kann, wird daraufhin ermittelt. Dazu wird die CPU-Ressourcenmenge des Hosts durch die CPU-Komponente der Steckplatzgröße 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 Steckplätzen 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 Steckplätze 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 der Bereich **Erweiterte Laufzeitinformationen** im Abschnitt „vSphere HA“ der Registerkarte **Überwachen** des Clusters im vSphere Web Client angezeigt. In diesem Fenster werden die folgenden Informationen zum Cluster angezeigt:

- Slotgröße.
- Gesamtzahl der Steckplätze im Cluster. Die Summe der Steckplätze, die von den guten Hosts im Cluster unterstützt werden.
- Verwendete Steckplätze. Die Anzahl an Steckplätzen, 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 Steckplatzgröße festgelegt haben. Dies liegt daran, dass einige virtuelle Maschinen mehrere Steckplätze einnehmen können.

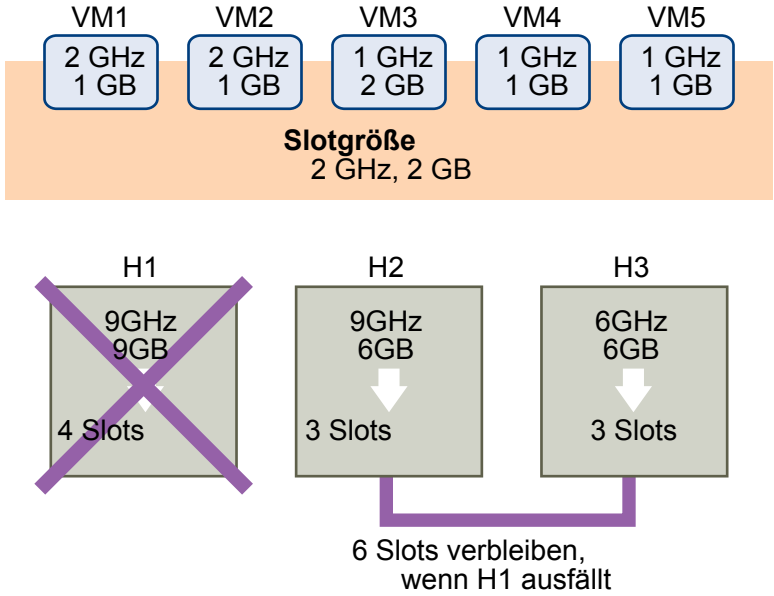
- Verfügbare Steckplätze. Die Anzahl der verfügbaren Steckplätze zum Einschalten zusätzlicher virtueller Maschinen im Cluster. vSphere HA reserviert die erforderliche Anzahl von Steckplätzen für das Failover. Die verbleibenden Steckplätze stehen für das Einschalten neuer virtueller Maschinen zur Verfügung.
- Failover-Steckplätze. Die Gesamtzahl der Steckplätze, wobei die verwendeten Steckplätze und die verfügbaren Steckplätze nicht mitgerechnet sind.
- Die Gesamtzahl eingeschalteter virtueller Maschinen im Cluster.
- Gesamtzahl an Hosts im Cluster.
- Gesamtzahl der guten Hosts im Cluster. Die Anzahl an Hosts, die verbunden und nicht im Wartungsmodus sind sowie keine vSphere HA-Fehler aufweisen.

Beispiel: Zugangssteuerung, die die Richtlinie „Vom Cluster tolerierte Hostfehler“ verwendet

Die Art, wie die Steckplatzgröße 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 Steckplatzgröße 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 Steckplatzgröße auf 2 GHz für die CPU und 2 GB für den Arbeitsspeicher festgelegt.

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

   H1 unterstützt vier Steckplätze. H2 unterstützt drei (der kleinere Wert von 9 GHz/2 GHz und 6 GB/2 GB) und H3 unterstützt ebenfalls drei Steckplätze.

3 Die aktuelle Failover-Kapazität wird berechnet.

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

Der Cluster verfügt über einen verfügbaren Steckplatz (die sechs Steckplätze auf H2 und H3 minus den fünf verwendeten Steckplätzen).

Zugangssteuerung mit der Richtlinie „Prozentsatz der reservierten Clusterressourcen“

Sie können vSphere HA konfigurieren, die Zugangssteuerung durchzuführen, indem Sie einen bestimmten Prozentsatz der Cluster-CPU- und Arbeitsspeicherressourcen für das Wiederherstellen nach einem Hostausfall reservieren.

Anhand der Zugangssteuerungsrichtlinie „Prozentsatz der reservierten Clusterressourcen“ stellt vSphere HA sicher, dass ein bestimmter Prozentsatz der gesamten CPU- und Arbeitsspeicherressourcen für das Failover reserviert wird.

Mit der Richtlinie für die Reservierung von Clusterressourcen führt vSphere 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 geringer als die entsprechende, (vom Benutzer angegebene) konfigurierte Failover-Kapazität ist.

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

vSphere 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 32 MHz CPU angesetzt.

Hinweis Die Zugangssteuerungsrichtlinie „Prozentsatz der reservierten Clusterressourcen“ überprüft zudem, dass sich mindestens zwei vSphere HA-fähige Hosts im Cluster befinden (ausgenommen Hosts, die in den Wartungsmodus wechseln). Wenn es nur einen vSphere HA-fähigen Host gibt, ist selbst dann kein Vorgang zulässig, wenn der Prozentsatz an verfügbaren Ressourcen ausreichend ist. Der Grund für diese zusätzliche Überprüfung liegt darin, dass vSphere HA kein Failover durchführen kann, wenn sich nur ein einziger Host im Cluster befindet.

Berechnen der aktuellen Failover-Kapazität

Die gesamten Ressourcenanforderungen für die eingeschalteten virtuellen Maschinen setzen sich aus zwei Komponenten zusammen: CPU und Arbeitsspeicher. vSphere 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 32 MHz zugewiesen (dieser Wert kann kann durch Zuweisung der erweiterten Option `das.vmcpuminmhz` geändert werden).

- Die Arbeitsspeicherkomponente durch Addieren der Arbeitsspeicherreservierung (zzgl. Arbeitsspeicher-Overhead) einer jeden eingeschalteten virtuellen Maschine.

Die gesamten, für virtuelle 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 vSphere HA-Fehler aufweisen, werden berücksichtigt.

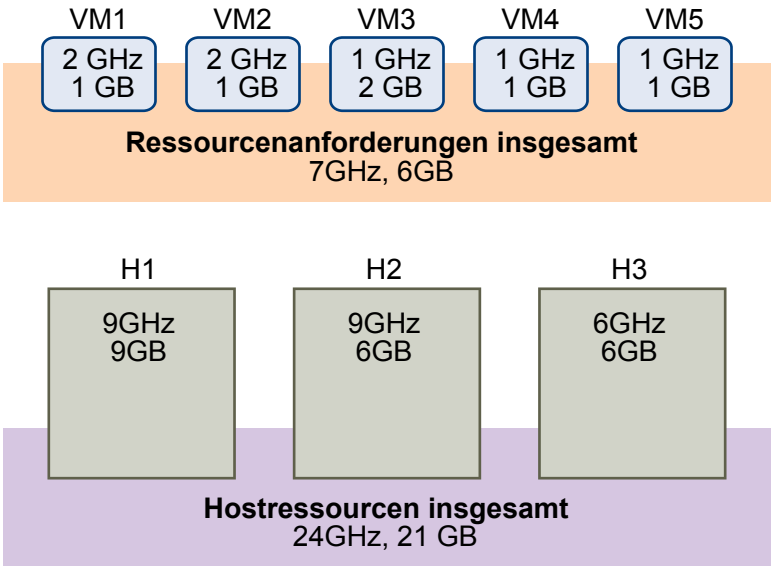
Die aktuelle CPU-Failover-Kapazität wird durch Subtrahieren der gesamten CPU-Ressourcenanforderungen von den gesamten Host-CPU-Ressourcen und Dividieren des Ergebnisses durch die gesamten Host-CPU-Ressourcen berechnet. Die aktuelle Arbeitsspeicher-Failover-Kapazität wird in gleicher Weise berechnet.

Beispiel: 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 für CPU und Arbeitsspeicher 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 GHz - 7 GHz)/24 GHz). Auf die gleiche Weise beläuft sich die aktuelle Arbeitsspeicher-Failover-Kapazität auf 71 % ((21 GB - 6 GB)/21 GB).

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

Zugangssteuerungsrichtlinie „Failover-Hosts angeben“

Sie können vSphere HA für das Auswählen bestimmter Hosts als Failover-Hosts konfigurieren.

Wenn ein Host ausfällt, versucht vSphere HA unter Verwendung der Zugangssteuerungsrichtlinie „Failover-Hosts angeben“, seine virtuellen Maschinen auf einem der angegebenen Failover-Hosts neu zu starten. Wenn dies nicht möglich ist, z. B. weil die Failover-Hosts ausgefallen sind oder nicht über genügend Ressourcen verfügen, versucht vSphere 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 einem Failover-Host verfügbar bleibt. Außerdem verwendet DRS keinen Failover-Host für den Lastausgleich.

Hinweis Wenn Sie die Zugangssteuerungsrichtlinie „Failover-Hosts angeben“ verwenden und dabei mehrere Failover-Hosts auswählen, versucht DRS nicht, die VM-VM-Affinitätsregeln für virtuelle Maschinen zu erzwingen, die auf Failover-Hosts laufen.

Im vSphere-Client werden die aktuellen Failover-Hosts im Abschnitt „vSphere HA“ der Registerkarte **Übersicht** des Clusters angezeigt. Das Statussymbol neben jedem Host kann grün, gelb oder rot sein.

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

Auswählen einer Richtlinie für die Zugangssteuerung

Wählen Sie eine vSphere 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. Diese Steckplätze befinden sich jedoch auf mehreren Hosts und können nicht verwendet werden, da eine virtuelle Maschine nicht gleichzeitig auf mehreren ESXi-Hosts ausgeführt werden kann. Die Standardkonfiguration der Richtlinie „Vom Cluster tolerierte Hostfehler“ vermeidet die Ressourcenfragmentierung, indem sie einen Steckplatz 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 Hosts für das Failover reserviert werden.

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 als eine Anzahl an Hosts. Die Richtlinie „Prozentsatz der Clusterressourcen“ ermöglicht Ihnen das Auswählen von bis zu 100 % der Cluster-CPU oder Arbeitsspeicherressourcen für das Failover. Die Richtlinie „Failover-Host angeben“ ermöglicht Ihnen, eine Gruppe von Failover-Hosts anzugeben.

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 Steckplatzgröße 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 vSphere HA bezieht bei der Durchführung von Zugangssteuerungsberechnungen die Ressourcennutzung der sekundären VM von Fault Tolerance ein. Für die Richtlinie „Vom Cluster tolerierte Hostfehler“ wird einer sekundären virtuellen Maschine ein Steckplatz 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.

vSphere HA-Interoperabilität

vSphere HA kann mit zahlreichen anderen Funktionen interoperieren, darunter DRS und Virtual SAN.

Bevor Sie vSphere HA konfigurieren, sollten Sie sich über die Einschränkungen der Interoperabilität mit diesen weiteren Funktionen oder Produkten im Klaren sein.

Verwenden von vSphere HA mit Virtual SAN

Virtual SAN kann als gemeinsam genutzter Speicher für einen vSphere HA-Cluster verwendet werden. Wenn Virtual SAN aktiviert ist, werden die angegebenen lokalen Speicherfestplatten, die auf den Hosts verfügbar sind, zu einem einzigen Datenspeicher zusammengefasst, der von allen Hosts gemeinsam genutzt wird.

Für die Verwendung von vSphere HA mit Virtual SAN müssen Sie bestimmte Überlegungen und Einschränkungen für die Interoperabilität dieser beiden Funktionen beachten.

Weitere Informationen zum Virtual SAN finden Sie unter *VMware Virtual SAN*.

Anforderungen für ESXi-Hosts

Virtual SAN kann nur mit einem vSphere HA-Cluster verwendet werden, wenn die folgenden Bedingungen erfüllt sind:

- Für die ESXi-Hosts des Clusters ist mindestens Version 5.5 erforderlich.
- Der Cluster muss aus mindestens drei ESXi-Hosts bestehen.

Unterschiede beim Netzwerk

Virtual SAN weist ein eigenes Netzwerk auf. Wenn Virtual SAN und vSphere HA für denselben Cluster aktiviert sind, wird der HA-Datenverkehr zwischen den Agenten nicht über das Verwaltungsnetzwerk, sondern über dieses Speichernetzwerk übertragen. Das Verwaltungsnetzwerk wird von vSphere HA nur verwendet, wenn Virtual SAN deaktiviert ist. vCenter Server wählt das entsprechende Netzwerk aus, wenn vSphere HA auf einem Host konfiguriert ist.

Hinweis Virtual SAN kann nur aktiviert werden, wenn vSphere HA deaktiviert ist.

Wenn Sie die Netzwerkkonfiguration des Virtual SAN ändern, übernehmen die vSphere HA-Agenten nicht automatisch die neuen Netzwerkeinstellungen. Um Änderungen am Netzwerk des Virtual SAN vorzunehmen, müssen Sie deshalb die folgenden Schritte im vSphere Web Client ausführen:

1 Deaktivieren Sie die Hostüberwachung für den vSphere HA-Cluster.

2 Nehmen Sie die Änderungen am Netzwerk des Virtual SAN vor.

3 Klicken Sie mit der rechten Maustaste auf alle Hosts im Cluster und wählen Sie **Für vSphere HA neu konfigurieren** aus.

4 Aktivieren Sie erneut die Hostüberwachung für den vSphere HA-Cluster.

Tabelle 2-2 werden die Unterschiede beim vSphere HA-Netzwerk erläutert, wenn Virtual SAN verwendet bzw. nicht verwendet wird.

Tabelle 2-2. Unterschiede beim vSphere HA-Netzwerk

	Virtual SAN aktiviert	Virtual SAN deaktiviert
Von vSphere HA verwendetes Netzwerk	Speichernetzwerk für Virtual SAN	Verwaltungsnetzwerk
Taktsignal-Datenspeicher	Jeder für > 1 Host gemountete Datenspeicher, nicht jedoch Datenspeicher für Virtual SAN	Jeder für > 1 Host gemountete Datenspeicher
Als isoliert erklärter Host	Isolationsadressen können nicht angepingt werden, kein Zugriff auf das Speichernetzwerk für Virtual SAN	Isolationsadressen können nicht angepingt werden, kein Zugriff auf das Verwaltungsnetzwerk

Einstellungen für die Kapazitätsreservierung

Wenn Sie Kapazität für Ihren vSphere HA-Cluster mit einer Zugangssteuerungsrichtlinie reservieren, muss diese Einstellung mit der entsprechenden Einstellung für Virtual SAN koordiniert werden, die den Zugriff auf die Daten bei Fehlern sicherstellt. Insbesondere darf die Einstellung „Anzahl der zu tolerierenden Fehler“ im Regelsatz für Virtual SAN nicht niedriger als die durch die Einstellung für die vSphere HA-Zugangssteuerung reservierte Kapazität sein.

Wenn beispielsweise der Regelsatz für Virtual SAN nur zwei Fehler zulässt, muss die vSphere HA-Zugangssteuerungsrichtlinie Kapazität reservieren, die nur einem oder zwei Hostfehlern entspricht. Falls Sie die Richtlinie „Prozentsatz der reservierten Clusterressourcen“ für einen Cluster mit acht Hosts verwenden, dürfen Sie nicht mehr als 25 % der Clusterressourcen reservieren. Für denselben Cluster darf mit der Richtlinie „Vom Cluster tolerierte Hostfehler“ diese Einstellung nicht höher als zwei Hosts sein. Wenn weniger Kapazität durch vSphere HA reserviert wird, kann die Failover-Aktivität unvorhersehbar sein. Die Reservierung von zu viel Kapazität bedeutet dagegen, dass das Einschalten von virtuellen Maschinen und die vMotion-Migrationen zwischen Clustern übermäßig belastet werden.

Gemeinsame Verwendung von vSphere HA und DRS

Wenn Sie vSphere HA mit Distributed Resource Scheduler (DRS) verwenden, werden die Funktionen des automatischen Failovers und des Lastausgleichs kombiniert. Diese Kombination kann zu einem ausgeglicheneren Cluster führen, nachdem vSphere HA virtuelle Maschinen auf verschiedene Hosts verschoben hat.

Wenn vSphere HA ein Failover durchführt und virtuelle Maschinen auf anderen Hosts neu startet, ist die erste Priorität die unmittelbare Verfügbarkeit aller virtuellen Maschinen. Nach dem Neustart der virtuellen Maschinen sind jene Hosts, auf denen sie eingeschaltet wurden, möglicherweise stark ausgelastet, wohingegen andere Hosts vergleichsweise gering ausgelastet sind. vSphere HA ermittelt anhand der CPU- und der Arbeitsspeicherreservierung sowie des Arbeitsspeicher-Overheads der virtuellen Maschine, ob ein Host über genügend Kapazität zur Unterbringung der virtuellen Maschine verfügt.

In einem Cluster, in dem DRS und vSphere 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 vSphere 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 kann vSphere HA DRS verwenden, 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 die Failover durchführen kann.

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

Wenn Sie erforderliche VM-Host-Affinitätsregeln verwenden, beachten Sie, dass gegen diese Regeln nicht verstoßen werden darf. vSphere HA führt kein Failover durch, wenn dadurch gegen eine Regel verstoßen würde.

Weitere Informationen zu DRS finden Sie in der *Handbuch zur vSphere-Ressourcenverwaltung*-Dokumentation.

Affinitätsregeln für vSphere HA und DRS

Wenn Sie eine DRS-Affinitätsregel für den Cluster erstellen, können Sie angeben, wie vSphere HA diese Regel während eines Failover von virtuellen Maschinen anwendet.

Zum Festlegen des Failover-Verhaltens von vSphere HA können die folgenden beiden Regeltypen festgelegt werden:

- Mit VM-Anti-Affinitätsregeln wird erzwungen, dass bestimmte virtuelle Maschinen bei Failover-Aktionen nicht berücksichtigt werden.
- VM-Host-Affinitätsregeln platzieren bestimmte virtuelle Maschinen bei Failover-Aktionen auf einem bestimmten Host oder einem Mitglied einer definierten Gruppe von Hosts.

Wenn Sie eine DRS-Affinitätsregel bearbeiten, aktivieren Sie die Kontrollkästchen, die das gewünschte Failover-Verhalten für vSphere HA erzwingen.

- **vSphere HA muss während des Failovers die VM-Anti-Affinitätsregeln respektieren** – wenn VMs mit dieser Regel zusammen platziert werden, wird das Failover abgebrochen.
- **vSphere HA sollte während des Failovers die VM-zu-Host-Affinitätsregeln respektieren** – vSphere HA versucht, VMs mit dieser Regel auf den angegebenen Hosts zu platzieren, wenn sich dies irgendwie machen lässt.

Hinweis vSphere HA kann eine VM in einem DRS-deaktivierten Cluster neu starten und damit eine VM-Host-Affinitätsregelzuordnung außer Kraft setzen, wenn der Hostausfall kurz nach dem Festlegen der Regel eintritt (standardmäßig innerhalb von 5 Minuten).

Andere Probleme mit der vSphere HA-Interoperabilität

Wenn Sie vSphere HA verwenden möchten, müssen Sie die folgenden zusätzlichen Interoperabilitätsprobleme kennen.

VM Component Protection

Für den VM-Komponentenschutz gelten die folgenden Interoperabilitätsprobleme und -einschränkungen:

- VM-Komponentenschutz unterstützt vSphere Fault Tolerance nicht. Wenn der VM-Komponentenschutz auf einem Cluster aktiviert wird, der Fault Tolerance verwendet, erhalten die betroffenen virtuellen Maschinen mit Fault Tolerance automatisch Außerkraftsetzungen, die den VM-Komponentenschutz deaktivieren.
- Der VM-Komponentenschutz erkennt keine Zugriffsprobleme für Dateien, die sich auf Virtual SAN-Datenspeichern befinden, und reagiert auch nicht darauf. Wenn die Konfigurations- und VMDK-Dateien einer virtuellen Maschine sich nur auf Virtual SAN-Datenspeichern befinden, werden sie vom VM-Komponentenschutz nicht geschützt.
- Der VM-Komponentenschutz erkennt keine Zugriffsprobleme für Dateien, die sich auf VVOL-Datenspeichern befinden, und reagiert auch nicht darauf. Wenn die Konfigurations- und VMDK-Dateien einer virtuellen Maschine sich nur auf VVOL-Datenspeichern befinden, werden sie vom VM-Komponentenschutz nicht geschützt.
- Der VM-Komponentenschutz schützt nicht vor Zugriffsproblemen auf Raw-Gerätezuordnungen (RDMs).

IPv6

vSphere HA kann in IPv6-Netzwerkkonfigurationen verwendet werden, die vollständig unterstützt werden, wenn die folgenden Punkte beachtet werden:

- Der Cluster enthält nur Hosts der Version ESXi 6.0 oder höher.
- Das Verwaltungsnetzwerk für alle Hosts im Cluster muss mit der gleichen IP-Version konfiguriert sein, entweder IPv6 oder IPv4. vSphere HA-Cluster können nicht beide Typen der Netzwerkkonfiguration enthalten.
- Die von vSphere HA verwendeten Netzwerkisolierungsadressen müssen der IP-Version entsprechen, die der Cluster für sein Verwaltungsnetzwerk verwendet.
- IPv6 kann nicht in vSphere HA-Clustern verwendet werden, die auch Virtual SAN verwenden.

Zusätzlich zu den obigen Einschränkungen werden die folgenden IPv6-Adresstypen nicht zusammen mit der vSphere HA-Isolierungsadresse bzw. dem Verwaltungsnetzwerk unterstützt: verbindungslokal, ORCHID und verbindungslokal mit Zonenindizes. Daneben darf auch der Loopback-Adresstyp nicht für das Verwaltungsnetzwerk verwendet werden.

Hinweis Um eine vorhandene IPv4-Bereitstellung auf IPv6 zu aktualisieren, müssen Sie zunächst vSphere HA deaktivieren.

Erstellen und Konfigurieren eines vSphere HA-Clusters

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

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

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

Hinweis Die Funktion „Starten und Herunterfahren von virtuellen Maschinen“ (automatischer Start) ist für alle virtuellen Maschinen deaktiviert, die sich auf den in einem vSphere HA-Cluster verfügbaren Hosts befinden (oder dorthin verschoben werden). Der automatische Start wird bei Verwendung mit vSphere HA nicht unterstützt.

vSphere HA-Checkliste

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

Überprüfen Sie diese Liste, bevor Sie einen vSphere HA-Cluster einrichten. Weitere Informationen erhalten Sie in den entsprechenden Querverweisen.

- Alle Hosts müssen für vSphere HA lizenziert sein.
- Ein Cluster muss mindestens zwei Hosts enthalten.
- Alle Hosts müssen mit statischen IP-Adressen konfiguriert werden. Wenn Sie DHCP verwenden, müssen Sie sichergehen, dass nach jedem Neustart die Adresse eines jeden Hosts beibehalten wird.
- Alle Hosts müssen mindestens ein gemeinsames Verwaltungsnetzwerk haben. Es werden mindestens zwei gemeinsame Verwaltungsnetzwerke empfohlen. Verwenden Sie das VMkernel-Netzwerk mit aktiviertem Kontrollkästchen **Verwaltungsdatenverkehr**. Die Netzwerke müssen füreinander zugänglich sein, und vCenter Server und die Hosts müssen in den Verwaltungsnetzwerken füreinander zugänglich sein. Siehe „Best Practices für Netzwerke“, auf Seite 41.
- Alle Hosts müssen auf dieselben VM-Netzwerke und -Datenspeicher zugreifen können, um sicherzustellen, dass jede virtuelle Maschine auf jedem Host im Cluster ausgeführt werden kann. In gleicher Weise müssen sich virtuelle Maschinen auf gemeinsam genutztem, nicht lokalem Speicher befinden. Anderenfalls kann im Falle eines Hostsausfalls kein Failover erfolgen.

  Hinweis vSphere HA verwendet Datenspeicher-Taktsignale, um zwischen partitionierten, isolierten und ausgefallenen Hosts zu unterscheiden. Sind also einige Datenspeicher in Ihrer Umgebung zuverlässiger, konfigurieren Sie vSphere HA so, dass diese Priorität haben.

- VMware Tools muss installiert sein, damit die VM-Überwachung funktionieren kann. Siehe „VM- und Anwendungsüberwachung“, auf Seite 17.
- vSphere HA unterstützt sowohl IPv4 als auch IPv6. Überlegungen zur Verwendung von IPv6 finden Sie unter „Andere Probleme mit der vSphere HA-Interoperabilität“, auf Seite 31.

- Der VM-Komponentenschutz funktioniert nur, wenn für die Hosts die Zeitüberschreitungsfunktion „Keine Pfade verfügbar“ (All Paths Down, ADP) aktiviert ist.
- Damit der VM-Komponentenschutz verwendet werden kann, müssen die Cluster ESXi 6.0-Hosts oder höher enthalten.
- Nur vSphere HA-Cluster, die Hosts der Version ESXi 6.0 oder höher enthalten, können zum Aktivieren des VM-Komponentenschutzes verwendet werden. Cluster, die Hosts einer früheren Version enthalten, können den VM-Komponentenschutz nicht aktivieren, und diese Hosts können einem Cluster mit aktiviertem VM-Komponentenschutz nicht hinzugefügt werden.
- Wenn der Cluster Datenspeicher mit virtuellen Volumes (VVOL) verwendet, wird beim Aktivieren von vSphere HA von vCenter Server ein Konfigurations-VVOL auf jedem Datenspeicher erstellt. In diesen Containern speichert vSphere HA die Dateien, die zum Schutz von virtuellen Maschinen verwendet werden. vSphere HA funktioniert nicht richtig, wenn Sie diese Container löschen. Pro VVOL-Datenspeicher wird nur ein Container erstellt.

Erstellen eines vSphere HA-Clusters

Wenn Sie Ihren Cluster für vSphere HA aktivieren möchten, müssen Sie zuerst einen leeren Cluster erstellen. Nachdem Sie die Planung der Ressourcen und der Netzwerkarchitektur für Ihren Cluster abgeschlossen haben, fügen Sie mithilfe des vSphere Web Client Hosts zum Cluster hinzu und legen die Einstellungen für vSphere HA fest.

Ein vSphere HA-aktivierter Cluster ist eine Voraussetzung zur Verwendung von Fault Tolerance.

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 den gemeinsam genutzten Speicher haben, damit Sie die virtuellen Maschinen mithilfe verschiedener Hosts im Cluster einschalten können.
- Stellen Sie sicher, dass Hosts für den Zugriff auf das Netzwerk virtueller Maschinen konfiguriert sind.
- Stellen Sie sicher, dass Sie redundante Verwaltungsnetzwerkverbindungen für vSphere HA verwenden. Informationen zur Einrichtung von Netzwerkredundanz finden Sie unter „Best Practices für Netzwerke“, auf Seite 41.
- Stellen Sie sicher, dass Sie Hosts mit mindestens zwei Datenspeichern konfiguriert haben, um Redundanz für Datenspeicher-Taktsignale von vSphere HA bereitzustellen.
- Verbinden Sie den vSphere Web Client unter Verwendung eines Kontos mit Clusteradministratorberechtigungen mit vCenter Server.

Vorgehensweise

1. Navigieren Sie in vSphere Web Client zu dem Datencenter, in dem der Cluster untergebracht werden soll, und klicken Sie auf **Cluster erstellen**.
2. Führen Sie den Assistenten für Neue Cluster aus.

   Schalten Sie vSphere HA (oder DRS) nicht ein.
3. Klicken Sie auf **OK**, um den Assistenten zu schließen und einen leeren Cluster zu erstellen.
4. Fügen Sie basierend auf Ihrer Ressourcen- und Netzwerkarchitekturplanung mithilfe des vSphere Web Client Hosts zum Cluster hinzu.

5 Navigieren Sie zum Cluster und aktivieren Sie vSphere HA.

   a Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

   b Wählen Sie **vSphere HA** und klicken Sie auf **Bearbeiten**.

   c Wählen Sie **vSphere HA einschalten** aus.

6 Wählen Sie **Hostüberwachung** aus.

   Durch Aktivieren der Hostüberwachung ermöglichen Sie Hosts im Cluster das Austauschen von Netzwerktaktsignalen, damit vSphere HA Maßnahmen ergreifen kann, wenn Fehler auftreten. Die Hostüberwachung ist erforderlich, damit der vSphere Fault Tolerance-Wiederherstellungsprozess ordnungsgemäß ausgeführt wird.

7 Wählen Sie eine Einstellung für **Überwachung virtueller Maschinen**.

   Wählen Sie **Nur VM-Überwachung**, um individuelle virtuelle Maschinen neu zu starten, wenn ihr Taktsignal nicht innerhalb einer festgelegten Zeit empfangen wird. Sie können auch **VM- und Anwendungsüberwachung** auswählen, um die Anwendungsüberwachung zu aktivieren.

8 Klicken Sie auf **OK**.

Sie verfügen über einen vSphere HA-Cluster mit den angegebenen Hosts.

Weiter

Konfigurieren Sie dann die vSphere HA-Einstellungen gemäß den Anforderungen Ihres Clusters.

- Fehlerbedingungen und VM-Antwort
- Zugangssteuerung
- Datenspeicher für Taktsignal
- Erweiterte Optionen

Siehe „Konfigurieren der vSphere HA-Clustereinstellungen“, auf Seite 34.

Konfigurieren der vSphere HA-Clustereinstellungen

Wenn Sie einen vSphere HA-Cluster erstellen oder einen vorhandenen Cluster konfigurieren, müssen Sie die Einstellungen konfigurieren, die festlegen, wie die Funktion funktioniert.

Die folgenden vSphere HA-Einstellungen können Sie in vSphere Web Client konfigurieren:

Fehlerbedingungen und VM-Antwort	Hier geben Sie Einstellungen wie die VM-Neustartpriorität, die Hostisolierungsreaktion, die VM-Überwachungsempfindlichkeit und VM-Komponentenschutz an.
Zugangssteuerung	Aktivieren oder deaktivieren Sie die Zugangssteuerung für den vSphere HA-Cluster und wählen Sie eine Richtlinie dafür aus, wie diese erzwungen wird.
Datenspeicher für Taktsignal	Geben Sie die Voreinstellungen für die Datenspeicher an, die vSphere HA für Datenspeicher-Taktsignale verwendet.
Erweiterte Optionen	Passen Sie das Verhalten von vSphere HA an, indem Sie erweiterte Optionen festlegen.

Hinweis Sie können den Status der vSphere HA-Konfigurationsaufgaben auf jedem der Hosts in der Aufgabenkonsole des vSphere Web Client prüfen.

Konfigurieren der Reaktionen virtueller Maschinen

Auf der Seite „Fehlerbedingungen und VM-Antwort“ können Sie Einstellungen auswählen, die festlegen, wie vSphere HA auf Hostfehler und -isolierungen reagiert. Zu diesen Einstellungen gehören die VM-Neustartpriorität, die Hostisolierungsreaktion, Einstellungen für VM Component Protection und die VM-Überwachungsempfindlichkeit.

Die Seite „Antwort der virtuellen Maschine“ kann nur bearbeitet werden, wenn Sie vSphere HA aktiviert haben.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSphere HA-Cluster.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie unter „Einstellungen“ **vSphere HA** und klicken Sie auf **Bearbeiten**.

4 Erweitern Sie **Fehlerbedingungen und VM-Antwort**, um die Konfigurationsoptionen anzuzeigen.

Option	Beschreibung
VM-Neustartpriorität	Mithilfe der VM-Neustartpriorität legen Sie fest, in welcher Reihenfolge die virtuellen Maschinen nach einem Hostausfall neu gestartet werden. Virtuelle Maschinen mit einer höheren Priorität werden zuerst gestartet. Diese Priorität gilt nur bezogen auf den jeweiligen Host. Falls mehrere Hosts ausfallen, werden alle virtuellen Maschinen des ersten Hosts in der Reihenfolge der festgelegten Priorität migriert, anschließend werden alle virtuellen Maschinen des zweiten Hosts ebenfalls in der Reihenfolge der festgelegten Priorität migriert usw.
Reaktion bei Hostisolierung	Die Hostisolierungsreaktion legt fest, was geschieht, wenn die Netzwerkkonsolenverbindung eines Hosts innerhalb eines vSphere HA-Clusters unterbrochen wird, der Host aber weiterhin ausgeführt wird.
Reaktion bei Datenspeicher mit dauerhaftem Geräteausfall (PDL)	Diese Einstellung legt fest, wie VMCP im Fall eines PDL-Fehlers reagiert. Sie können zwischen den Optionen **Ereignisse ausgeben** oder **VMs ausschalten und neu starten** wählen.
Reaktion bei 'Keine Pfade verfügbar' (APD) im Datenspeicher	Diese Einstellung legt fest, wie VMCP im Fall eines ADP-Fehlers reagiert. Sie können zwischen den Optionen **Ereignisse ausgeben** oder **VMs ausschalten und neu starten** wählen (konservativ oder aggressiv).
Verzögerung für das VM-Failover für APD	Diese Einstellung ist die Anzahl der Minuten, die VMCP vor einer Aktion wartet.
Reaktion bei APD-Wiederherstellung nach APD-Zeitüberschreitung	Sie können wählen, ob VMCP eine VM in dieser Situation zurücksetzt oder nicht.
VM-Überwachungsempfindlichkeit	Legen Sie diese Option fest, indem Sie den Schieberegler zwischen **Niedrig** und **Hoch** verschieben. Sie können auch **Benutzerdefiniert** auswählen, um benutzerdefinierte Einstellungen bereitzustellen.

5 Klicken Sie auf **OK**.

Die Einstellungen für die Antwort der virtuellen Maschine werden wirksam.

Konfigurieren der Zugangssteuerung

Nachdem Sie einen Cluster erstellt haben, können Sie über die Zugangssteuerung angeben, ob virtuelle Maschinen gestartet werden können, wenn sie gegen Verfügbarkeitsbedingungen verstoßen. Der Cluster reserviert Ressourcen, um für alle ausgeführten virtuellen Maschinen auf der angegebenen Anzahl von Hosts ein Failover zu ermöglichen.

Die Seite „Zugangssteuerung“ erscheint nur, wenn Sie vSphere HA aktiviert haben.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSphere HA-Cluster.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie unter „Einstellungen“ **vSphere HA** und klicken Sie auf **Bearbeiten**.

4 Erweitern Sie **Zugangssteuerung**, um die Konfigurationsoptionen anzuzeigen.

5 Wählen Sie eine auf den Cluster anzuwendende Zugangssteuerungsrichtlinie.

Option	Beschreibung
Failover-Kapazität durch statische Anzahl an Hosts festlegen	Geben Sie an, wie viele Hosts maximal ausfallen dürfen, um noch wiederhergestellt werden zu können oder für die ein Failover garantiert werden kann. Sie müssen auch eine Richtlinie für Steckplatzgröße auswählen.
Legen Sie die Failover-Kapazität fest, indem Sie einen bestimmten Prozentsatz der Clusterressourcen reservieren.	Geben Sie einen Prozentsatz für die CPU- und Arbeitsspeicherressourcen des Clusters an, der zusätzlich reserviert werden soll, um Failover zu unterstützen.
Dedizierte Failover-Hosts verwenden	Wählen Sie Hosts für Failover-Aktionen aus. Failover können immer noch von anderen Hosts im Cluster übernommen werden, wenn ein Standard-Failover-Host nicht über genügend Ressourcen verfügt.
Failover-Kapazität nicht reservieren.	Diese Option ermöglicht Einschaltungen virtueller Maschinen, die gegen die Verfügbarkeitseinschränkungen verstoßen.

6 Klicken Sie auf **OK**.

Die Zugangssteuerung wird aktiviert und die von Ihnen gewählte Richtlinie wird wirksam.

Konfigurieren des Datenspeichers für Taktsignal

vSphere HA verwendet Datenspeicher-Taktsignale, um ausgefallene Hosts und Hosts, die sich auf einer Netzwerkpartition befinden, voneinander zu unterscheiden. Datenspeicher-Taktsignale ermöglichen vSphere HA, Hosts zu überwachen, wenn eine Verwaltungsnetzwerkpartition auftritt, und weiterhin auf Ausfälle zu reagieren.

Sie können die Datenspeicher angeben, die für Datenspeicher-Taktsignale verwendet werden sollen.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSphere HA-Cluster.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie unter „Einstellungen“ **vSphere HA** und klicken Sie auf **Bearbeiten**.

4 Erweitern Sie **Datenspeicher für Taktsignal**, um die Konfigurationsoptionen für die Datenspeicher-Taktsignale anzuzeigen.

5 Um vSphere HA anzuweisen, wie Datenspeicher auszuwählen und Ihre Voreinstellungen zu behandeln sind, wählen Sie aus den folgenden Optionen:

Tabelle 2-3.

Datenspeicher-Taktsignaloptionen
Datenspeicher automatisch auswählen, auf die über den Host zugegriffen werden kann
Datenspeicher nur aus der angegebenen Liste verwenden
Datenspeicher aus der angegebenen Liste verwenden und bei Bedarf automatisch ergänzen

6 Wählen Sie im Bereich **Verfügbare Taktsignal-Datenspeicher** die Datenspeicher aus, die Sie für Taktsignale verwenden möchten.

   Die aufgelisteten Datenspeicher werden von mehreren Hosts im vSphere HA-Cluster gemeinsam verwendet. Wenn ein Datenspeicher ausgewählt wird, werden im unteren Bereich alle Hosts im vSphere HA-Cluster angezeigt, die auf diesen zugreifen können.

7 Klicken Sie auf **OK**.

Festlegen erweiterter Optionen

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

Voraussetzungen

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

Hinweis Da sich diese Optionen auf die Funktionsweise von vSphere HA auswirken, sollten Sie sie mit Bedacht ändern.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSphere HA-Cluster.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie unter „Einstellungen“ **vSphere HA** und klicken Sie auf **Bearbeiten**.

4 Erweitern Sie **Erweiterte Optionen**.

5 Klicken Sie auf **Hinzufügen** und geben Sie den Namen der erweiterten Optionen in das Textfeld ein.

   Sie können den Wert der Option im Textfeld in der Spalte „Wert“ festlegen.

6 Wiederholen Sie Schritt 5 für jede neue Option, die Sie hinzufügen möchten, und klicken Sie auf **OK**.

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

Weiter

Nachdem Sie eine erweiterte vSphere HA-Option festgelegt haben, bleibt sie gültig, bis Sie einen der folgenden Schritte durchführen:

- Den Wert mit vSphere Web Client auf den Standardwert zurücksetzen
- Die Option manuell in der Datei „fdm.cfg“ auf allen Hosts im Cluster bearbeiten bzw. daraus löschen

Erweiterte vSphere HA-Optionen

Sie können erweiterte Optionen festlegen, die das Verhalten Ihres vSphere HA-Clusters beeinflussen.

Tabelle 2-4. Erweiterte vSphere HA-Optionen

Option	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 = 0-9. In der Regel sollten Sie eine Adresse pro Verwaltungsnetzwerk angeben. Die Angabe zu vieler Adressen führt dazu, dass die Isolationserkennung zu lange dauert.
`das.usedefaultisolationaddress`	Standardmäßig verwendet vSphere HA das Standard-Gateway des Konsolennetzwerks als Prüfadresse, um eine Isolierung festzustellen. Diese Option legt fest, ob dieser Standardwert verwendet wird (true|false).
`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.
`das.vmcpuminmhz`	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 32 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** Werte von weniger als 50 werden nicht empfohlen, da kleinere Werte dazu führen können, dass vSphere HA eine virtuelle Maschine unerwartet zurücksetzt.

Tabelle 2-4. Erweiterte vSphere HA-Optionen (Fortsetzung)

Option	Beschreibung
das.ignoreinsufficienthbdatastore	Deaktiviert Konfigurationsprobleme, die entstehen, wenn der Host nicht über genügend Taktsignal-Datenspeicher für vSphere HA verfügt. Der Standardwert ist FALSE.
das.heartbeatdsperhost	Ändert die Anzahl der erforderlichen Taktsignal-Datenspeicher. Gültige Werte sind 2 bis 5 und der Standardwert ist 2.
fdm.isolationpolicydelaysec	Die Anzahl der Sekunden, die das System (nachdem festgelegt wurde, dass ein Host isoliert wird) wartet, bevor die Isolierungsrichtlinie ausgeführt wird. Der Mindestwert ist 30. Wird ein niedrigerer Wert eingestellt, beträgt die Verzögerung 30 Sekunden.
das.respectvmvmantiaffinityrules	Ermittelt, ob vSphere HA VM-VM-Anti-Affinitätsregeln erzwingt. Der Standardwert ist „false“, wobei die Regeln nicht erzwungen werden. Der Wert kann auch auf „true“ festgelegt werden und die Regeln werden erzwungen (auch wenn vSphere DRS nicht aktiviert ist). In diesem Fall führt vSphere HA kein Failover einer virtuellen Maschine durch, wenn dies gegen eine Regel verstößt, gibt aber eine Ereignismeldung aus, dass nicht genügend Ressourcen vorhanden sind, um den Failover durchzuführen. Weitere Informationen zu Anti-Affinitätsregeln finden Sie unter *vSphere-Ressourcenverwaltung*.
das.maxresets	Die maximale Anzahl der Zurücksetzungsversuche, die vom VM-Komponentenschutz unternommen werden. Wenn ein Zurücksetzungsvorgang auf einer von einem APD betroffenen virtuellen Maschine fehlschlägt, versucht der VM-Komponentenschutz mehrere Male, den Versuch zu wiederholen.
das.maxterminates	Die maximale Anzahl der wiederholten Versuche, die vom VM-Komponentenschutz zur Beendigung der virtuellen Maschine unternommen werden.
das.terminateretryintervalsec	Wenn der VM-Komponentenschutz eine virtuelle Maschine nicht beenden kann, ist dies die Anzahl der Sekunden, die das System wartet, bevor der Beendigungsversuch wiederholt wird.
das.config.fdm.reportfailoverfailevent	Wenn „1“ festgelegt ist, wird die Generierung eines detaillierten Ereignisses pro VM aktiviert, wenn ein Versuch zum Neustarten der virtuellen Maschine durch vSphere HA fehlschlägt. Der Standardwert ist „0“. In Versionen vor vSphere 6.0 wird dieses Ereignis standardmäßig generiert.

Tabelle 2-4. Erweiterte vSphere HA-Optionen (Fortsetzung)

Option	Beschreibung
`vpxd.das.completemetadataupdateintervalsec`	Der Zeitraum (Sekunden), nachdem eine VM-Host-Affinitätsregel festgelegt wird, während der vSphere HA eine VM in einem DRS-deaktivierten Cluster neu starten und die Regel außer Kraft setzen kann. Der Standardwert beträgt 300 Sekunden.
`das.config.fdm.memreservationmb`	Standardmäßig werden vSphere HA-Agenten mit einem konfigurierten Arbeitsspeicherlimit von 250 MB ausgeführt. Es kann vorkommen, dass ein Host diese Reservierung nicht zulässt, wenn seine reservierbare Kapazität knapp wird. Anhand dieser erweiterten Option können Sie das Arbeitsspeicherlimit heruntersetzen, um dieses Problem zu vermeiden. Es können nur Ganzzahlen größer als 100 (dem Mindestwert) festgelegt werden. Andererseits sollten Sie zum Verhindern von Problemen bei Master-Agent-Wahlen in einem großen Cluster (mit 6000 bis 8000 VMs) diesen Grenzwert auf 325 MB anheben. **Hinweis** Wenn dieser Grenzwert geändert wird, müssen Sie für alle Hosts im Cluster die Aufgabe zum Neukonfigurieren von HA ausführen. Wenn dem Cluster ein neuer Host hinzugefügt wird oder ein vorhandener Host neu gestartet wird, sollte diese Aufgabe auf solchen Hosts durchgeführt werden, um diese Speichereinstellung zu aktualisieren.

Hinweis Wenn Sie den Wert einer der folgenden erweiterten Optionen ändern, müssen Sie vSphere HA deaktivieren und neu aktivieren, damit Ihre Änderungen wirksam werden.

- `das.isolationaddress[...]`
- `das.usedefaultisolationaddress`
- `das.isolationshutdowntimeout`

Anpassen einer einzelnen virtuellen Maschine

In einem vSphere HA-Cluster werden allen virtuellen Maschinen die Standard-Clustereinstellungen für VM-Neustartpriorität, Hostisolierungsreaktion, VM Component Protection und 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 Navigieren Sie im vSphere Web Client zum vSphere HA-Cluster.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie unter „Einstellungen“ die Option **VM-Außerkraftsetzungen** aus und klicken Sie auf **Hinzufügen**.

4 Wählen Sie mit der Schaltfläche **+** die virtuellen Maschinen aus, auf die die Außerkraftsetzungen angewendet werden sollen.

5 Klicken Sie auf **OK**.

6 (Optional) Sie können andere Einstellungen wie beispielsweise **Automatisierungsebene**, **VM-Neustartpriorität**, **Hostisolierungsreaktion**, VMCP-Einstellungen, **VM-Überwachung** oder **VM-Überwachungsempfindlichkeit** ändern.

Hinweis Sie können die Standardeinstellungen für den Cluster anzeigen, indem Sie zuerst **Relevante Clustereinstellungen** und anschließend **vSphere HA** erweitern.

7 Klicken Sie auf **OK**.

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

Empfohlene Vorgehensweisen für vSphere HA-Cluster

Um die optimale Leistung eines vSphere HA-Clusters gewährleisten zu können, sollten Sie bestimmte empfohlene Vorgehensweisen einhalten. In diesem Abschnitt werden einige der wichtigsten Best Practices für einen vSphere HA-Cluster behandelt.

Eine weitergehende Erörterung zu diesem Thema finden Sie in der Veröffentlichung *vSphere High Availability Deployment Best Practices*.

Best Practices für Netzwerke

Für die Konfiguration der Host-Netzwerkkarten und der Netzwerktopologie für vSphere HA sollten Sie die folgenden Best Practices berücksichtigen. Zu den empfohlenen Vorgehensweisen gehören Empfehlungen für die ESXi-Hosts sowie für die Verkabelung, Switches, Router und Firewalls.

Netzwerkkonfiguration und -wartung

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

- Wenn Sie Änderungen an den Netzwerken vornehmen, zu denen Ihre ESXi-Host-Cluster gehören, halten Sie die Funktion „Hostüberwachung“ an. Das Ändern Ihrer Netzwerkhardware oder der Netzwerkeinstellungen kann die Taktsignale unterbrechen, die vSphere HA verwendet, um Hostausfälle zu erkennen, und dies kann zu ungewünschten Failover-Versuchen für virtuelle Maschinen führen.
- Wenn Sie die Netzwerkkonfiguration auf den ESXi-Hosts ändern, beispielsweise durch Hinzufügen von Gruppen oder Entfernen von vSwitches, halten Sie die Hostüberwachung an. Nachdem Sie die Änderungen an der Netzwerkkonfiguration durchgeführt haben, müssen Sie vSphere HA auf allen Hosts im Cluster konfigurieren, womit bewirkt wird, dass die Netzwerkinformationen erneut untersucht werden. Danach reaktivieren Sie die Hostüberwachung.

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

Für vSphere HA-Kommunikation verwendete Netzwerke

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

- Auf Legacy-ESX-Hosts im Cluster verwendet die vSphere HA-Kommunikation alle Netzwerke, die als Servicekonsolennetzwerke ausgewählt sind. VMkernel-Netzwerke werden von diesen Hosts nicht für die vSphere HA-Kommunikation verwendet. Verwenden Sie die erweiterte Option `allowedNetworks`, um den vSphere HA-Datenverkehr auf bestimmte ESX-Konsolennetzwerke zu beschränken.

- Auf ESXi-Hosts im Cluster verwendet die vSphere HA-Kommunikation standardmäßig VMkernel-Netzwerke. Wenn Sie bei einem ESXi-Host ein anderes als das von vCenter Server verwendete Netzwerk für die Kommunikation mit dem Host für vSphere HA verwenden möchten, müssen Sie explizit das Kontrollkästchen **Verwaltungsdatenverkehr** aktivieren.

Um den Datenverkehr des vSphere HA-Agenten auf die von Ihnen angegebenen Netzwerke zu beschränken, konfigurieren Sie die Hosts so, dass von vSphere HA verwendete vmkNICs Subnetze nicht gemeinsam mit vmkNICs nutzen, die für andere Zwecke verwendet werden. vSphere HA-Agenten senden Pakete unter Verwendung einer pNIC, die einem vorhandenen Subnetz zugewiesen ist, wenn es auch mindestens eine vmkNIC gibt, die für den vSphere HA-Verwaltungsdatenverkehr konfiguriert ist. Um die Trennung des Netzwerkflusses sicherzustellen, müssen sich die von vSphere HA und anderen Funktionen verwendeten vmkNICs folglich auf unterschiedlichen Subnetzen befinden.

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, und die anderen Hosts im Cluster sind entweder ausgefallen oder netzwerkpartitioniert. 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 wird nur ein Standard-Gateway angegeben. Sie sollten die erweiterte Option `das.isolationaddress[...]` verwenden, um weitere Netzwerkisolierungsadressen hinzuzufügen. Siehe „Erweiterte vSphere HA-Optionen“, auf Seite 38.

Netzwerkpfadredundanz

Die Netzwerkpfadredundanz zwischen Clusterknoten ist für die Zuverlässigkeit von vSphere HA wichtig. Ein einzelnes Verwaltungsnetzwerk wird zu einer einzelnen Fehlerstelle und kann zu Failovern 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-Aktivität herbeiführen, wenn die Taktsignal-Datenspeicherkonnektivität während des Netzwerkausfalls nicht aufrechterhalten wird. 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.

Die erste Methode zum Implementieren der Netzwerkredundanz besteht auf der Netzwerkkartenebene durch 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 ursprünglichen ID des Ports routen (Route based on originating port ID)
- Failback = Nein (No)

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

Für die meisten Implementierungen reicht die durch die NIC-Gruppierung bereitgestellte Redundanz aus. Alternativ können Sie auch eine zweite Verwaltungsnetzwerkverbindung erstellen, die an einen separaten virtuellen Switch angeschlossen wird. Die Nutzung eines redundanten Verwaltungsnetzwerks ermöglicht eine zuverlässige Fehlererkennung und verhindert, dass Isolierungs- oder Partitionssituationen auftreten, da Taktsignale über mehrere Netzwerke gesendet werden können. Die ursprüngliche Verwaltungsnetzwerkverbindung dient Netzwerk- und Verwaltungszwecken. Sobald die zweite Verwaltungsnetzwerkverbindung erstellt wurde, sendet vSphere HA Taktsignale über beide Verwaltungsnetzwerkverbindungen. Sollte ein Pfad ausfallen, sendet und empfängt vSphere HA über den anderen Pfad noch immer Taktsignale.

Hinweis 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 Netzwerkpaketen für Taktsignale und potentiellen Fehlerstellen gerechnet werden.

Verwenden von IPv6-Netzwerkkonfigurationen

Nur eine IPv6-Adresse sollte einer bestimmten Netzwerkschnittstelle, die von Ihrem vSphere HA-Cluster verwendet wird, zugewiesen werden. Durch die Zuweisung mehrerer IP-Adressen erhöht sich die Anzahl der Taktsignalmeldungen, die vom Master-Host des Clusters gesendet werden, ohne dass dies einen entsprechenden Vorteil bietet.

Best Practices für die Interoperabilität

Für die ordnungsgemäße Interoperabilität zwischen vSphere HA und anderen Funktionen sollten Sie die folgenden Best Practices berücksichtigen.

Interoperabilität von vSphere HA und Storage vMotion in einem gemischten Cluster

Setzen Sie in Clustern, in denen ESXi 5.x-Hosts und Hosts der Version ESX/ESXi 4.1 oder früherer Versionen vorhanden sind und bei denen Storage vMotion oft genutzt wird oder Speicher-DRS aktiviert ist, vSphere HA nicht ein. vSphere HA könnte auf einen Hostausfall reagieren, indem es eine virtuelle Maschine auf einem Host mit einer ESXi-Version neu startet, die sich von der Version des Hosts unterscheidet, auf dem die virtuelle Maschine vor dem Ausfall ausgeführt wurde. Ein Problem kann auftreten, wenn zum Zeitpunkt des Ausfalls die virtuelle Maschine an einer Storage vMotion-Aktion auf einem ESXi 5.x-Host beteiligt war und vSphere HA die virtuelle Maschine auf einem Host mit einer Version vor ESXi 5.0 neu startet. Obwohl die virtuelle Maschine möglicherweise neu gestartet wird, könnten alle nachfolgenden Snapshot-Vorgänge den vdisk-Zustand beschädigen und die virtuelle Maschine in einem instabilen Zustand lassen.

Verwenden von Auto Deploy mit vSphere HA

Sie können vSphere HA und Auto Deploy zusammen verwenden, um die Verfügbarkeit von virtuellen Maschinen zu verbessern. Auto Deploy stellt Hosts bereit, wenn sie gestartet werden, und Sie können es auch so konfigurieren, dass während des Startvorgangs der vSphere HA-Agent auf solchen Hosts installiert wird. Weitere Informationen finden Sie in der Dokumentation zu Auto Deploy im Installations- und Einrichtungshandbuch für vSphere.

Durchführen eines Upgrades von Hosts in einem Cluster unter Verwendung vom Virtual SAN

Gehen Sie wie folgt vor, wenn Sie ein Upgrade der ESXi-Hosts in Ihrem vSphere HA-Cluster auf Version 5.5 oder höher vornehmen und außerdem Virtual SAN verwenden möchten.

1 Führen Sie ein Upgrade für alle Hosts durch.

2 Deaktivieren Sie vSphere HA.

3 Aktivieren Sie Virtual SAN.

4 Aktivieren Sie vSphere HA erneut.

Best Practices für die Zugangssteuerung

Für die Konfiguration und die Verwendung der Zugangssteuerung für vSphere HA sollten Sie die folgenden Best Practices berücksichtigen.

Die folgenden Empfehlungen sind Best Practices für die vSphere HA-Zugangssteuerung.

- Wählen Sie die Zugangssteuerungsrichtlinie „Prozentsatz der reservierten Clusterressourcen“ aus. Diese Richtlinie bietet die größte Flexibilität in Bezug auf die Größeneinteilung von Hosts und virtuellen Maschinen. Wählen Sie beim Konfigurieren dieser Richtlinie einen Prozentsatz für CPU und Arbeitsspeicher, der der Anzahl der Hostausfälle entspricht, die unterstützt werden sollen. Wenn Sie beispielsweise möchten, dass vSphere HA Ressourcen für zwei Hostausfälle reservieren soll und sich im Cluster zehn Hosts mit gleicher Kapazität befinden, geben Sie 20 % (2/10) an.
- Stellen Sie sicher, dass Sie alle Cluster-Hosts auf die gleiche Größe konfigurieren. Bei der Richtlinie „Vom Cluster tolerierte Hostfehler“ führt ein unausgewogener Cluster zu einer Überkapazität, die zum Behandeln von Ausfällen reserviert wird, da vSphere HA Kapazität für die größten Hosts reserviert. Bei der Richtlinie „Prozentsatz der Clusterressourcen“ erfordert ein unausgeglichener Cluster, dass Sie einen größeren Prozentsatz festlegen, als sonst erforderlich wäre, um ausreichend Kapazität für die antizipierte Anzahl von Hostausfällen zu reservieren.
- Wenn Sie planen, die Richtlinie „Vom Cluster tolerierte Hostfehler“ zu verwenden, versuchen Sie, ähnliche VM-Größenanforderungen für alle konfigurierten virtuellen Maschinen beizubehalten. Diese Richtlinie verwendet Steckplatzgrößen, um die Kapazität zu berechnen, die für jede virtuelle Maschine reserviert werden soll. Die Steckplatzgröße basiert auf dem größten reservierten Arbeitsspeicher und der CPU, die für eine virtuelle Maschine benötigt wird. Wenn Sie virtuelle Maschinen mit unterschiedlichen CPU- und Speichererfordernissen mischen, ergibt sich bei der Steckplatzgrößenberechnung ein Standardwert, der dem größtmöglichen Speicherbedarf entspricht, was die Konsolidierung eingrenzt.
- Wenn Sie planen, die Richtlinie „Failover-Hosts angeben“ zu verwenden, entscheiden Sie, wie viele Hostausfälle unterstützt werden sollen, und geben Sie dann diese Anzahl von Hosts als Failover-Hosts an. Wenn der Cluster ungleichmäßig ist, sollten die festgelegten Failover-Hosts wenigstens dieselbe Größe haben wie die Nicht-Failover-Hosts im Cluster. Auf diese Weise wird sichergestellt, dass die Kapazität im Falle eines Ausfalls ausreicht.

Best Practices für die Cluster-Überwachung

Für die Überwachung des Status und der Gültigkeit Ihres vSphere HA-Clusters sollten Sie die folgenden Best Practices berücksichtigen.

Einstellen von Alarmen für die Überwachung von Clusteränderungen

Wenn von vSphere HA oder Fault Tolerance Aktionen für den Erhalt der Verfügbarkeit eingeleitet werden, z. B. das Failover einer virtuellen Maschine, können Sie über diese Änderung informiert werden. Konfigurieren Sie Alarme in vCenter Server, die ausgelöst werden, wenn diese Aktionen stattfinden, und sorgen Sie dafür, dass Warnungen, z. B. E-Mails, an eine definierte Gruppe von Administratoren gesendet werden.

Mehrere Standard-vSphere HA-Alarme sind verfügbar.

- Unzureichende Failover-Ressourcen (ein Clusteralarm)
- Master nicht auffindbar (ein Clusteralarm)
- Failover läuft (ein Clusteralarm)
- HA-Status des Hosts (ein Hostalarm)
- VM-Überwachungsfehler (ein VM-Alarm)
- VM-Überwachungsaktion (ein VM-Alarm)

- Failover fehlgeschlagen (ein VM-Alarm)

Hinweis Die Standardalarme enthalten den Namen der Funktion, vSphere HA.

Überwachen der Clustergültigkeit

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

Ein für vSphere HA aktivierter Cluster wird ungültig, 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.

Wählen Sie im vSphere Web Client **vSphere HA** auf der Registerkarte **Monitor** des Clusters aus und wählen Sie anschließend **Konfigurationsprobleme**. Eine Liste der aktuellen vSphere HA-Probleme wird angezeigt.

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

Aktivieren der Fault Tolerance für virtuelle Maschinen 3

Sie können vSphere Fault Tolerance für Ihre virtuellen Maschinen nutzen, um Business Continuity mit höherer Verfügbarkeit und besserem Datenschutz als bei vSphere HA sicherzustellen.

Fault Tolerance basiert auf der ESXi-Hostplattform und stellt unterbrechungsfreie Verfügbarkeit bereit, indem identische virtuelle Maschinen auf getrennten Hosts ausgeführt werden.

Um mit Fault Tolerance optimale Ergebnisse zu erzielen, sollten Sie mit ihrer Funktionsweise, dem Vorgang zu ihrer Aktivierung für Ihren Cluster und Ihre virtuellen Maschinen und den Best Practices für ihre Nutzung vertraut sein.

Fault Tolerance-Schutz für virtuelle Maschinen (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_fault_tolerance_protection_vms)

Dieses Kapitel behandelt die folgenden Themen:

- „Wie Fault Tolerance funktionert“, auf Seite 47
- „Beispiele für die Nutzen der Fault Tolerance“, auf Seite 48
- „Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance“, auf Seite 49
- „Fault Tolerance-Interoperabilität“, auf Seite 49
- „Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance“, auf Seite 52
- „Verwenden von Fault Tolerance“, auf Seite 54
- „Best Practices für Fault Tolerance“, auf Seite 59
- „Legacy Fault Tolerance“, auf Seite 61

Wie Fault Tolerance funktionert

Sie können vSphere Fault Tolerance für die meisten unternehmenskritischen virtuellen Maschinen verwenden. Fault Tolerance bietet für eine virtuelle Maschine unterbrechungsfreie Verfügbarkeit, indem eine weitere VM erstellt und gepflegt wird, die mit der ersten identisch und ständig verfügbar ist, um sie im Fall einer Failover-Situation zu ersetzen.

Die geschützte virtuelle Maschine wird als primäre VM bezeichnet. Die duplizierte virtuelle Maschine, die sekundäre VM, wird auf einem anderen Host erstellt und ausgeführt. Die Ausführung der sekundären VM ist mit der primären VM identisch. Daher kann sie deren Funktion jederzeit ohne Unterbrechung übernehmen und bietet fehlertoleranten Schutz.

Die primäre und die sekundäre VM überwachen kontinuierlich gegenseitig ihren Status, um sicherzustellen, dass Fault Tolerance gewährleistet bleibt. 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 automatisch 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 VMs führen kann.

Hinweis 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 in der Dokumentation zu *Handbuch zur vSphere-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.

vSphere Fault Tolerance kann mit symmetrischen Multiprozessor-VMs (SMP) mit bis zu vier vCPUs eingerichtet werden. In früheren Versionen von vSphere wurde eine andere Technologie für Fault Tolerance verwendet (jetzt als Fault Tolerance-Legacy-Version bezeichnet). Dafür galten andere Voraussetzungen und Merkmale (darunter eine Einschränkung auf einzelne vCPUs für VMs mit der Fault Tolerance-Legacy-Version). Wenn Kompatibilität mit diesen früheren Voraussetzungen benötigt wird, können Sie die Fault Tolerance-Legacy-Version verwenden. Dafür muss jedoch auf jeder VM eine erweiterte Option eingerichtet werden. Weitere Informationen hierzu finden Sie unter „Legacy Fault Tolerance“, auf Seite 61.

Beispiele für die Nutzen der Fault Tolerance

Sie profitieren in mehreren typischen Situationen von der Verwendung von vSphere Fault Tolerance.

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

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

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

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

Tolerance schützen, bevor Sie diesen Bericht ausführen, und die Fault Tolerance danach wieder deaktivieren oder aussetzen. Sie können die Fehlertoleranz bei Bedarf dazu verwenden, die virtuelle Maschine in einer kritischen Phase zu schützen und danach die Ressourcen für den unkritischen Betrieb in den Normalzustand zurückversetzen.

Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance

Bevor Sie vSphere Fault Tolerance verwenden, sollten Sie sich einen Überblick über die Voraussetzungen, Einschränkungen und Lizenzierungen verschaffen, die für diese Funktion gelten.

Anforderungen

Die folgenden CPU- und Netzwerkvoraussetzungen gelten für Fault Tolerance.

CPUs, die auf Hostmaschinen für fehlertolerante VMs verwendet werden, müssen mit vSphere vMotion kompatibel sein bzw. mit Enhanced vMotion Compatibility erweitert werden. Zudem sind CPUs erforderlich, die Hardware MMU-Virtualisierung (Intel EPT oder AMD RVI) unterstützen. Die folgenden CPUs werden unterstützt.

- Intel Sandy Bridge oder höher. Avoton wird nicht unterstützt.
- AMD Bulldozer oder höher.

Verwenden Sie ein 10-GBit-Protokollierungsnetzwerk für FT und stellen Sie sicher, dass das Netzwerk eine niedrige Latenz aufweist. Ein dediziertes FT-Netzwerk wird dringend empfohlen.

Grenzwerte

In einem Cluster, der für die Verwendung von Fault Tolerance konfiguriert ist, werden zwei Einschränkungen unabhängig voneinander erzwungen.

das.maxftvmsperhost	Die maximale Anzahl der fehlertoleranten VMs auf einem Host im Cluster. Sowohl primäre als auch sekundäre VMs zählen für diese Anzahl mit. Der Standardwert ist 4.
das.maxftvcpusperhost	Die maximale Anzahl vCPUs, die über alle fehlertoleranten VMs auf einem Host aggregiert werden. Es zählen sowohl vCPUs von primären VMs als auch von sekundären VMs. Der Standardwert ist 8.

Lizenzierung

Die Anzahl der vCPUs, die von einer einzelnen fehlertoleranten VM unterstützt werden, ist durch die Lizenzierungsstufe beschränkt, die Sie für vSphere erworben haben. Fault Tolerance wird wie folgt unterstützt:

- vSphere Standard und Enterprise. Bis zu 2 vCPUs zulässig
- vSphere Enterprise Plus Bis zu 4 vCPUs zulässig

Hinweis Fault Tolerance und die Fault Tolerance-Legacy-Version werden in vSphere Essentials und vSphere Essentials Plus nicht unterstützt.

Fault Tolerance-Interoperabilität

vSphere Fault Tolerance weist mehrere Einschränkungen bezüglich der vSphere-Funktionen, -Geräte und anderen Funktionen auf, mit denen interoperiert werden kann.

Bevor Sie vSphere Fault Tolerance konfigurieren, sollten Sie die Funktionen und Produkte kennen, mit denen vSphere Fault Tolerance nicht zusammenarbeiten kann.

vSphere-Funktionen, die für Fault Tolerance nicht unterstützt werden

Beim Konfigurieren des Clusters sollten Sie beachten, dass nicht alle vSphere-Funktionen mit Fault Tolerance interoperieren können.

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

- Snapshots. Snapshots müssen entfernt oder zugeordnet werden, bevor auf einer virtuellen Maschine Fault Tolerance aktiviert werden kann. Zudem ist es nicht möglich, Snapshots von virtuellen Maschinen zu erstellen, auf denen Fault Tolerance aktiviert ist.

  Hinweis Snapshots nur von Festplatten, die für vStorage-APIs – Data Protection-Sicherungen (VADP) erstellt werden, werden für Fault Tolerance unterstützt. VADP wird jedoch von Legacy-FT nicht unterstützt.

- Storage vMotion. Sie können Storage vMotion nicht für virtuelle Maschinen mit aktivierter Fault Tolerance verwenden. Wenn Sie den Speicher migrieren möchten, sollten Sie Fault Tolerance vorübergehend deaktivieren und die Storage vMotion-Aktion durchführen. Danach können Sie Fault Tolerance wieder aktivieren.
- Verknüpfte Klone. Sie können Fault Tolerance nicht auf einer virtuellen Maschine verwenden, bei der es sich um einen verknüpften Klon handelt. Zudem können Sie keinen verknüpften Klon von einer virtuellen Maschine erstellen, für die Fault Tolerance aktiviert ist.
- VM-Komponentenschutz. Wenn der VM-Komponentenschutz für Ihren Cluster aktiviert ist, werden Außerkraftsetzungen für fehlertolerante virtuelle Maschinen erstellt, die diese Funktion deaktivieren.
- Datenspeicher für virtuelle Volumes (VVOL)
- Speicherbasierte Richtlinienverwaltung
- I/O-Filter

Funktionen und Geräte, die mit Fault Tolerance nicht kompatibel sind

Nicht alle Geräte, Funktionen oder Produkte von Drittanbietern können mit Fault Tolerance interoperieren.

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

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

Nicht kompatible Funktion bzw. nicht kompatibles Gerät	Fehlerbehebende Aktion
Physische Raw-Festplattenzuordnung (RDM).	Mit der Fault Tolerance-Legacy-Version können Sie virtuelle Maschinen mit physischen, RDM-gesicherten virtuellen Geräten neu konfigurieren, 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.
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 Fault Tolerance nicht unterstützt und muss daher ausgeschaltet werden.

Tabelle 3-1. Funktionen und Geräte, die mit Fault Tolerance 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 Fault Tolerance vorübergehend ausschalten, den Wechsel durchführen und Fault Tolerance anschließend wieder einschalten. **Hinweis** Beim Verwenden von Fault Tolerance 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 Fault Tolerance ausgeschaltet werden.
Serielle oder parallele Schnittstellen	Entfernen Sie diese Geräte von der virtuellen Maschine.
Videogeräte, bei denen 3D aktiviert ist.	Fault Tolerance unterstützt keine Videogeräte, bei denen 3D aktiviert ist.
Virtuelle EFI-Firmware	Stellen Sie sicher, dass die virtuelle Maschine für die Verwendung der BIOS-Firmware konfiguriert ist, bevor Sie das Gastbetriebssystem installieren.
Virtual Machine Communication Interface (VMCI)	Von Fault Tolerance nicht unterstützt.
2 TB+ VMDK	Mit 2 TB+ VMDK wird Fault Tolerance nicht unterstützt.

Verwendung der Fault Tolerance mit DRS

Sie können vSphere Fault Tolerance nur zusammen mit vSphere Distributed Resource Scheduler (DRS) verwenden, wenn Enhanced vMotion Compatibility (EVC) aktiviert ist. Mit diesem Prozess können virtuelle Maschinen mit Fault Tolerance von einer besseren anfänglichen Platzierung profitieren.

Wenn EVC für einen Cluster aktiviert ist, schlägt DRS Empfehlungen für die anfängliche Platzierung der fehlertoleranten virtuellen Maschinen vor 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).

Wenn vSphere Fault Tolerance für virtuelle Maschinen in einem Cluster verwendet wird, bei dem EVC deaktiviert ist, erhalten die fehlertoleranten virtuellen Maschinen die DRS-Automatisierungsebenen „Deaktiviert“. In einem derartigen Cluster wird jede primäre VM nur auf dem registrierten Host eingeschaltet, und die sekundäre VM wird automatisch platziert.

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. Wenn eine VM-VM-Affinitätsregel für eine primäre virtuelle Maschine festgelegt ist, versucht DRS, Verstöße nach einem Failover (d. h., nachdem die primäre virtuelle Maschine auf einen neuen Host verschoben wurde) zu beheben.

Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance

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

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

- Vergewissern Sie sich, dass Cluster, Hosts und virtuelle Maschinen die Voraussetzungen gemäß der Fault Tolerance-Checkliste erfüllen.
- Konfigurieren des Netzwerks für die einzelnen Hosts.
- Erstellen des vSphere HA-Clusters, Hinzufügen der Hosts und Prüfen der Übereinstimmung.

Nachdem Sie Ihren Cluster und Ihre Hosts für Fault Tolerance vorbereitet haben, können Sie sie für Ihre virtuellen Maschinen einschalten. Siehe „Fault Tolerance einschalten“, auf Seite 56.

Fault Tolerance-Checkliste

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

Überprüfen Sie diese Liste, bevor Sie Fault Tolerance einrichten.

Hinweis Das Failover von fehlertoleranten virtuellen Maschinen ist unabhängig von vCenter Server, allerdings müssen Sie vCenter Server verwenden, um Fault Tolerance-Cluster einzurichten.

Clusteranforderungen für Fault Tolerance

Die folgenden Clusteranforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Fehlertoleranz-Protokollierung und vMotion-Netzwerke sind konfiguriert. Siehe „Konfigurieren von Netzwerken für Hostmaschinen“, auf Seite 53.
- vSphere HA-Cluster wurden erstellt und aktiviert. Weitere Informationen hierzu finden Sie unter „Erstellen und Konfigurieren eines vSphere HA-Clusters“, auf Seite 32. vSphere HA muss aktiviert sein, bevor Sie fehlertolerante virtuelle Maschinen einschalten oder einem Cluster einen Host hinzufügen können, der bereits fehlertolerante virtuelle Maschinen unterstützt.

Hostanforderungen für Fault Tolerance

Die folgenden Hostanforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Hosts müssen unterstützte Prozessoren verwenden.
- Hosts müssen für Fault Tolerance lizenziert sein.
- Hosts müssen für Fault Tolerance zertifiziert sein. Rufen Sie die Seite http://www.vmware.com/resources/compatibility/search.php auf und wählen Sie **Search by Fault Tolerant Compatible Sets**, um zu ermitteln, ob Ihre Hosts zertifiziert sind.
- Bei der Konfiguration für jeden Host muss im BIOS die Hardwarevirtualisierung (HV) aktiviert sein.

Hinweis VMware empfiehlt, dass für die Hosts, die Sie zur Unterstützung von Fault Tolerance-VMs verwenden, die BIOS-Einstellungen zur Energieverwaltung auf maximale Leistung bzw. auf vom Betriebssystem verwaltete Leistung festgelegt sind.

Sie können auch Profilübereinstimmungsprüfungen ausführen, wie unter „Erstellen eines Clusters und Überprüfen der Übereinstimmung“, auf Seite 54 beschrieben sind, um die Kompatibilität der Hosts im Cluster zum Unterstützen von Fault Tolerance zu bestätigen.

VM-Anforderungen für Fault Tolerance

Die folgenden VM-Anforderungen müssen erfüllt sein, bevor Sie Fault Tolerance einsetzen können.

- Es dürfen keine nicht unterstützten Geräte mit den virtuellen Maschinen verbunden sein. Siehe „Fault Tolerance-Interoperabilität“, auf Seite 49.
- Nicht kompatible Funktionen dürfen nicht mit den fehlertoleranten virtuellen Maschinen ausgeführt werden. Siehe „Fault Tolerance-Interoperabilität“, auf Seite 49.
- Die Dateien der virtuellen Maschine müssen auf einem gemeinsam genutzten Speicher gespeichert sein. Zu den akzeptablen gemeinsam genutzten Speicherlösungen gehören Fibre-Channel, iSCSI (Hardware und Software), NFS und NAS.

Weitere Konfigurationsempfehlungen

Beim Konfigurieren von Fault Tolerance sollten Sie zudem die folgenden Richtlinien beachten.

- Falls Sie NFS für den Zugriff auf gemeinsam genutzten Speicher verwenden, sollten Sie dedizierte NAS-Hardware mit mindestens einer 1 Gbit Netzwerkkarte verwenden, um die für das ordnungsgemäße Funktionieren von Fault Tolerance erforderliche Netzwerkleistung zu erzielen.
- Die Arbeitsspeicherreservierung einer fehlertoleranten VM wird auf die Arbeitsspeichergröße der virtuellen Maschine festgelegt, wenn Fault Tolerance eingeschaltet wird. Stellen Sie sicher, dass ein Ressourcenpool, der fehlertolerante VMs enthält, eine größere Arbeitsspeichermenge als die für die virtuellen Maschinen erforderliche Menge besitzt. Ohne diesen Überschuss im Ressourcenpool ist es möglich, dass kein Arbeitsspeicher mehr zur Verfügung steht, der als Overhead-Arbeitsspeicher genutzt werden kann.
- Verwenden Sie maximal 16 virtuelle Festplatten pro fehlertoleranter virtueller Maschine.
- Um Redundanz und maximalen Fault Tolerance-Schutz zu gewährleisten, sollten sich mindestens drei Hosts im Cluster befinden. Auf diese Weise wird in einer Failover-Situation ein Host bereitgestellt, der die neu erstellte sekundäre virtuelle Maschine aufnehmen kann.

Konfigurieren von Netzwerken für Hostmaschinen

Auf jedem Host, den Sie zu einem vSphere HA-Cluster hinzufügen möchten, müssen Sie zwei verschiedene Netzwerk-Switches (vMotion und Fault Tolerance-Protokollierung) konfigurieren, damit der Host vSphere Fault Tolerance unterstützen kann.

Um Fault Tolerance für einen Host zu aktivieren, müssen Sie diesen Vorgang einmal pro Portgruppenoption (vMotion und Fault Tolerance-Protokollierung) durchführen. Dadurch wird sichergestellt, dass für die Protokollierung der Fault Tolerance genügend Bandbreite zur Verfügung steht. Wählen Sie eine Option, schließen Sie den Vorgang ab, führen Sie den Vorgang dann erneut durch und wählen Sie die andere Portgruppenoption.

Voraussetzungen

Mehrere Gigabit-Netzwerkkarten sind erforderlich. Für jeden Host, der Fault Tolerance unterstützt, werden mindestens zwei physische Netzwerkkarten empfohlen. Sie benötigen beispielsweise eine für Fault Tolerance-Protokollierung und eine für vMotion. Verwenden Sie mindestens drei Netzwerkkarten, um die Verfügbarkeit sicherzustellen.

Hinweis Die vMotion-Netzwerkkarte und die Netzwerkkarte mit Fault Tolerance-Protokollierung müssen sich in unterschiedlichen Subnetzen befinden. Wenn Sie die Fault Tolerance-Legacy-Version verwenden, wird IPv6 auf den Netzwerkkarten für die Fault Tolerance-Protokollierung nicht unterstützt.

Vorgehensweise

1 Navigieren Sie zum Host im vSphere Web Client.

2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Netzwerk**.

3 Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen**.

4 Wählen Sie auf der Seite „Verbindungstyp auswählen“ die Option **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.

5 Wählen Sie **Neuer Standard-Switch** und klicken Sie auf **Weiter**.

6 Weisen Sie freie physische Netzwerkadapter zum Switch hinzu und klicken Sie auf **Weiter**.

7 Geben Sie eine Netzwerkbezeichnung ein, aktivieren Sie die gewünschten Dienste und klicken Sie auf **Weiter**.

8 Geben Sie eine IP-Adresse und Subnetzmaske ein und klicken Sie auf **Beenden**, nachdem Sie die Einstellungen überprüft haben.

Nachdem Sie sowohl einen virtuellen vMotion- als auch einen virtuellen Fault Tolerance-Protokollierungs-Switch erstellt haben, können Sie nach Bedarf weitere virtuelle Switches erstellen. Fügen Sie den Host zum Cluster hinzu und führen Sie die Schritte zum Einschalten von Fault Tolerance aus.

Weiter

Hinweis Wenn Sie das Netzwerk für die Unterstützung von Fault Tolerance konfigurieren, daraufhin jedoch den Port für Fault Tolerance-Protokollierung aussetzen, bleiben die Paare von fehlertoleranten virtuellen Maschinen, die eingeschaltet sind, immer noch eingeschaltet. Falls 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.

Erstellen eines Clusters und Überprüfen der Übereinstimmung

vSphere Fault Tolerance wird im Kontext eines vSphere HA-Clusters verwendet. Erstellen Sie den vSphere HA-Cluster und fügen Sie ihm die Hosts hinzu, nachdem Sie auf allen Hosts die Netzwerke konfiguriert haben. Sie können überprüfen, ob der Cluster richtig konfiguriert ist und den Anforderungen für die Aktivierung von Fault Tolerance entspricht.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum Cluster.

2 Klicken Sie auf die Registerkarte **Überwachen** und klicken Sie dann auf **Profil-Übereinstimmung**.

3 Klicken Sie auf **Jetzt auf Übereinstimmung prüfen**, um die Übereinstimmung zu überprüfen.

Die Ergebnisse des Übereinstimmungstests – d. h. die Übereinstimmung bzw. Nichtübereinstimmung jedes Hosts – werden angezeigt.

Verwenden von Fault Tolerance

Nachdem Sie alle erforderlichen Schritte zum Aktivieren von vSphere Fault Tolerance für Ihren Cluster ausgeführt haben, können Sie die Funktion nutzen, indem Sie sie für individuelle virtuelle Maschinen aktivieren.

Bevor Fault Tolerance eingeschaltet werden kann, werden auf einer virtuellen Maschine Validierungsprüfungen durchgeführt.

Wenn diese Prüfungen bestanden wurden und Sie vSphere Fault Tolerance für eine virtuelle Maschine aktivieren, werden neue Optionen zum Abschnitt „Fault Tolerance“ des Kontextmenüs hinzugefügt. Hierzu zählen Optionen zum Ausschalten oder Deaktivieren von Fault Tolerance, zum Migrieren der sekundären virtuellen Maschine, zum Testen des Failovers und zum Testen des Neustarts der sekundären virtuellen Maschine.

Validierungsprüfungen für das Einschalten von Fault Tolerance

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

Bevor Fault Tolerance 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 vSphere HA-Cluster oder einem gemischten vSphere HA- und DRS-Cluster befinden.
- Auf dem Host muss ESXi 6.x oder höher installiert sein (ESX/ESXi 4.x oder höher für Legacy-FT).
- Die virtuelle Maschine darf nicht über Snapshots verfügen.
- Die virtuelle Maschine darf keine Vorlage sein.
- vSphere HA darf auf der virtuellen Maschine nicht deaktiviert sein.
- Die virtuelle Maschine darf keine 3D-fähige Grafikkarte haben.

Überprüfungen für eingeschaltete virtuelle Maschinen

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 Fault Tolerance unterstützt.
- Ihre Hardware sollte als kompatibel mit Fault Tolerance 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 Konfiguration der virtuellen Maschine muss für die Verwendung mit Fault Tolerance gültig sein (beispielsweise darf sie keine nicht unterstützten Geräte enthalten).

Platzierung sekundärer VM

Wenn Ihr Versuch, Fault Tolerance 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 Fault Tolerance 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 für die virtuelle Maschine angezeigte Fault Tolerance-Status 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 für die virtuelle Maschine angezeigte Fault Tolerance-Status lautet **Nicht geschützt, VM wird nicht ausgeführt**.
- Wenn Sie versuchen, die primäre virtuelle Maschine einzuschalten, nachdem Fault Tolerance eingeschaltet wurde, werden die oben aufgeführten zusätzlichen Validierungsprüfungen durchgeführt.

  Nachdem diese Prüfungen bestanden wurden, werden die primäre und sekundäre virtuelle Maschine eingeschaltet und auf separaten, kompatiblen Hosts platziert. Der Fault Tolerance-Status der virtuellen Maschine wird als **Geschützt** gekennzeichnet.

Fault Tolerance einschalten

Sie können vSphere Fault Tolerance über den vSphere Web Client aktivieren.

Wenn Fault Tolerance eingeschaltet wird, setzt vCenter Server den Grenzwert der virtuellen Maschine für den Arbeitsspeicher zurück und legt die Arbeitsspeicherreservierung auf die Arbeitsspeichergröße der virtuellen Maschine fest. Sie können die Arbeitsspeicherreservierung, -größe, -anteile, den Arbeitsspeichergrenzwert oder die Anzahl der vCPUs nicht ändern, solange Fault Tolerance eingeschaltet ist. Darüber hinaus können Sie für die VM keine Festplatten hinzufügen oder entfernen. Wenn die Fehlertoleranz ausgeschaltet wird, werden geänderte Parameter nicht auf ihre ursprünglichen Werte zurückgesetzt.

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

Voraussetzungen

Die Option zum Einschalten von Fault Tolerance 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.

Vorgehensweise

1. Navigieren Sie im vSphere Web Client zu der virtuellen Maschine, für die Sie Fault Tolerance aktivieren möchten.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Fault Tolerance einschalten** aus.
3. Klicken Sie auf **Ja**.
4. Wählen Sie einen Datenspeicher aus, auf dem die Konfigurationsdateien für die sekundäre VM platziert werden sollen. Klicken Sie anschließend auf **Weiter**.
5. Wählen Sie einen Host aus, auf dem die sekundäre VM platziert werden soll. Klicken Sie anschließend auf **Weiter**.
6. Überprüfen Sie Ihre Auswahl und klicken Sie anschließend auf **Beenden**.

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.

Fault Tolerance ausschalten

Das Ausschalten der vSphere Fault Tolerance löscht die sekundäre virtuelle Maschine, ihre Konfiguration und den Verlauf.

Verwenden Sie die Option **Fault Tolerance ausschalten**, wenn Sie nicht planen, die Funktion wieder zu aktivieren. Verwenden Sie anderenfalls die Option **Fault Tolerance anhalten**.

Hinweis Wenn sich die sekundäre virtuelle Maschine auf einem Host befindet, der im Wartungsmodus bzw. nicht verbunden ist oder nicht antwortet, können Sie die Option **Fault Tolerance ausschalten** nicht verwenden. In diesem Fall sollten Sie stattdessen Fault Tolerance anhalten und fortsetzen.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu der virtuellen Maschine, für die Sie Fault Tolerance deaktivieren möchten.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Fault Tolerance ausschalten** aus.

3 Klicken Sie auf **Ja**.

Fault Tolerance wird für die ausgewählte virtuelle Maschine ausgeschaltet. Der Verlauf und die sekundäre virtuelle Maschine für die ausgewählte virtuelle Maschine werden gelöscht.

Fault Tolerance anhalten

Durch das Anhalten von vSphere Fault Tolerance für eine virtuelle Maschine wird ihr Fault Tolerance-Schutz angehalten. Die sekundäre virtuelle Maschine, ihre Konfiguration und der gesamte Verlauf werden jedoch beibehalten. Verwenden Sie diese Option, um den Fault Tolerance-Schutz später fortzusetzen.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu der virtuellen Maschine, für die Sie Fault Tolerance anhalten möchten.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Fault Tolerance anhalten** aus.

3 Klicken Sie auf **Ja**.

Fault Tolerance wird für die ausgewählte virtuelle Maschine angehalten. Der Verlauf und die sekundäre virtuelle Maschine für die ausgewählte virtuelle Maschine werden beibehalten und verwendet, falls die Funktion fortgesetzt wird.

Weiter

Um Fault Tolerance nach dem Anhalten fortzusetzen, wählen Sie **Fault Tolerance fortsetzen** aus.

Sekundäre VM migrieren

Nachdem vSphere Fault Tolerance für eine primäre virtuelle Maschine aktiviert wurde, können Sie die zugehörige sekundäre virtuelle Maschine migrieren.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu der primären virtuellen Maschine, für die Sie ihre sekundäre virtuelle Maschine migrieren möchten.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Sekundäre VM migrieren** aus.

3 Aktivieren Sie die Optionen im Dialogfeld „Migrieren“ und bestätigen Sie die durchgeführten Änderungen.

4 Klicken Sie auf **Beenden**, um die Änderungen anzuwenden.

Die sekundäre virtuelle Maschine, die der ausgewählten fehlertoleranten virtuellen Maschine zugewiesen ist, wird auf den angegebenen Host migriert.

Failover testen

Sie können eine Failover-Situation für eine ausgewählte primäre virtuelle Maschine herbeiführen, um Ihren Fehlertoleranzschutz zu testen.

Diese Option ist nicht verfügbar (abgeblendet), wenn die virtuelle Maschine ausgeschaltet ist.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu der primären virtuellen Maschine, für die Sie den Failover testen möchten.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Failover testen** aus.

3 Zeigen Sie die Details zum Failover in der Aufgabenkonsole an.

Diese Aufgabe ruft den Ausfall der primären virtuellen Maschine hervor, um sicherzustellen, dass sie durch die sekundäre virtuelle Maschine ersetzt wird. Außerdem wird eine neue sekundäre virtuelle Maschine gestartet und die primäre virtuelle Maschine wird wieder in den Status „Geschützt“ versetzt.

Neustart sekundärer VM testen

Sie können den Ausfall einer sekundären virtuellen Maschine herbeiführen, um den Fehlertoleranzschutz für eine ausgewählte primäre virtuelle Maschine zu testen.

Diese Option ist nicht verfügbar (abgeblendet), wenn die virtuelle Maschine ausgeschaltet ist.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu der primären virtuellen Maschine, für die Sie den Test durchführen möchten.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Fault Tolerance > Neustart sekundärer VM testen** aus.

3 Zeigen Sie die Details zum Test in der Aufgabenkonsole an.

Diese Aufgabe führt zum Beenden der sekundären virtuellen Maschine, die den Fehlertoleranzschutz für die ausgewählte primäre virtuelle Maschine bereitstellte. Eine neue sekundäre virtuelle Maschine wird gestartet und die primäre virtuelle Maschine wird wieder in den Status „Geschützt“ versetzt.

Upgrade von für Fault Tolerance verwendeten Hosts

Führen Sie die folgenden Schritte für das Upgrade von Hosts aus, die für Fault Tolerance verwendet werden.

Voraussetzungen

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

Stellen Sie sicher, dass Sie über Gruppen von vier oder mehr ESXi-Hosts verfügen, die eingeschaltete, fehlertolerante virtuelle Maschinen hosten. 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 fehlertolerante virtuelle Maschinen entfernt wurden, auf dieselbe ESXi-Version durch.

3 Halten Sie Fault Tolerance auf der primären virtuellen Maschine an.

4 Verschieben Sie die primäre virtuelle Maschine, für die Fault Tolerance angehalten wurde, unter Verwendung von vMotion auf einen der aktualisierten Hosts.

5 Setzen Sie Fault Tolerance auf der verschobenen primären virtuellen Maschine fort.

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 ESXi-Hosts in einem Cluster durchgeführt.

Best Practices für Fault Tolerance

Um optimale Fault Tolerance-Ergebnisse erzielen zu können, sollten Sie bestimmte empfohlene Vorgehensweisen einhalten.

Mit den folgenden Empfehlungen für die Host- und Netzwerkkonfiguration lassen sich die Stabilität und Leistung Ihres Clusters verbessern.

Hostkonfiguration

Hosts, auf denen die primären und sekundären virtuellen Maschinen ausgeführt werden, sollten mit annähernd denselben Prozessorfrequenzen arbeiten, anderenfalls könnte es sein, dass die sekundären virtuellen Maschinen häufiger neu gestartet werden. Plattform-Energieverwaltungsfunktionen, die sich nicht abhängig von der Arbeitslast anpassen (z. B. die Energiebeschränkung und erzwungene Niedrigfrequenzmodi zum Einsparen von Energie), können große Abweichungen der Prozessorfrequenzen verursachen. Falls sekundäre virtuelle Maschinen regelmäßig neu gestartet werden, deaktivieren Sie alle Energieverwaltungsmodi auf den Hosts, die fehlertolerante virtuelle Maschinen ausführen, oder stellen Sie sicher, dass alle Hosts im selben Energieverwaltungsmodus laufen.

Hostnetzwerkkonfiguration

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

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

Hinweis Der Datenverkehr für die Fault Toleranceprotokollierung zwischen den primären und sekundären virtuelle Maschinen erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr kann vertrauliche Daten enthalten, wie z. B. Kennwörter im Klartext. Um zu verhindern, dass solche Daten preisgegeben werden, stellen Sie sicher, dass dieses Netzwerk gesichert ist, insbesondere gegen sogenante „Man-in-the-middle“-Angriffe. Verwenden Sie z. B. ein privates Netzwerk für den Datenverkehr für die Fault Toleranceprotokollierung.

Homogene Cluster

vSphere Fault Tolerance kann in Clustern mit uneinheitlichen Hosts arbeiten, am besten funktioniert sie jedoch in Clustern mit kompatiblen Knoten. Wenn Sie Ihren Cluster erstellen, sollten alle Hosts über folgende Konfiguration verfügen:

- Gemeinsamen Zugriff auf Datenspeicher, die von den virtuellen Maschinen verwendet werden.
- Dieselbe Netzwerkkonfiguration für virtuelle Maschinen.
- Die gleichen BIOS-Einstellungen (Energieverwaltung und Hyper-Threading) für alle Hosts.

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

Leistung

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

Speichern von ISOs auf gemeinsam genutztem Speicher für einen unterbrechungsfreien Zugriff

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

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

Vermeiden von Netzwerkpartitionen

Eine Netzwerkpartition tritt ein, wenn bei einem vSphere HA-Cluster ein Fehler des Verwaltungsnetzwerks auftritt, der zur Folge hat, dass einige der Hosts von vCenter Server sowie voneinander isoliert werden. Siehe „Netzwerkpartitionen“, auf Seite 19. Wenn eine Partition eintritt, wird der Schutz durch Fault Tolerance möglicherweise herabgestuft.

In einem partitionierten vSphere HA-Cluster, bei dem Fault Tolerance verwendet wird, kann es vorkommen, dass die primäre virtuelle Maschine (oder ihre sekundäre virtuelle Maschine) in einer Partition landet, die von einem Master-Host verwaltet wird, der für die virtuelle Maschine nicht verantwortlich ist. Wenn ein Failover benötigt wird, wird eine sekundäre virtuelle Maschine nur dann neu gestartet, wenn sich die primäre virtuelle Maschine in einer Partition befunden hat, die von dem Master-Host verwaltet wird, der für die virtuelle Maschine verantwortlich ist.

Um die Chancen zu verringern, dass bei Ihrem Verwaltungsnetzwerk einen Fehler auftritt, der zu einer Netzwerkpartition führt, befolgen Sie die Empfehlungen in „Best Practices für Netzwerke“, auf Seite 41.

Verwenden von Virtual SAN-Datenspeichern

vSphere Fault Tolerance kann Virtual SAN-Datenspeicher verwenden, aber Sie müssen folgende Einschränkungen beachten:

- Ein Mix aus Virtual SAN und anderen Typen von Datenspeichern wird sowohl für primäre VMs als auch für sekundäre VMs nicht unterstützt.
- Virtual SAN-Metro-Cluster werden mit FT nicht unterstützt.

Um die Leistung und Zuverlässigkeit bei der Verwendung von FT mit Virtual SAN zu erhöhen, werden auch folgende Bedingungen empfohlen.

- Virtual SAN und FT sollten getrennte Netzwerke verwenden.
- Verwalten Sie primäre und sekundäre VMs in getrennten Virtual SAN Fault Domains.

Legacy Fault Tolerance

Standardmäßig kann vSphere Fault Tolerance (FT) mit symmetrischen Multiprozessor-VMs (SMP) mit bis zu vier vCPUs eingerichtet werden. Wenn Ihre virtuelle Maschine jedoch nur eine vCPU enthält, können Sie zu Zwecken der Abwärtskompatibilität stattdessen die Fault Tolerance-Legacy-Version verwenden. Sofern es nicht aus technischen Gründen notwendig ist, wird von der Verwendung der Fault Tolerance-Legacy-Version abgeraten.

Um die Fault Tolerance-Legacy-Version verwenden zu können, müssen Sie eine erweiterte Option für die virtuelle Maschine konfigurieren. Nach Abschluss dieser Konfiguration unterscheidet sich die virtuelle Maschine mit der Fault Tolerance-Legacy-Version in einigen Punkten von anderen Fault Tolerance-VMs.

Unterschiede bei VMs, die die Fault Tolerance-Legacy-Version verwenden

VMs mit Fault Tolerance unterscheiden sich in mehreren Punkten von VMs mit der Fault Tolerance-Legacy-Version.

Tabelle 3-2. Unterschiede zwischen der Fault Tolerance-Legacy-Version und Fault Tolerance

	Fault Tolerance-Legacy-Version	FT
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI)	Nicht unterstützt	Erforderlich
IPv6	Nicht unterstützt für Netzwerkkarten für die Fault Tolerance-Legacy-Protokollierung	Unterstützt für Netzwerkkarten für die Fault Tolerance-Protokollierung
DRS	Vollständige Unterstützung für anfängliche Platzierung, Lastausgleich und Wartungsmodussupport	Nur Einschaltplatzierung für sekundäre VM und Wartungsmodus werden unterstützt.
vStorage-APIs - Data Protection-Sicherungen	Nicht unterstützt	Unterstützt
Eager-Zeroed Thick-VMDK-Festplattendateien	Erforderlich	Nicht erforderlich, da Fault Tolerance alle Festplattendateitypen unterstützt, einschließlich Thick und Thin
VMDK-Redundanz	Nur eine Kopie	Primäre VMs und sekundäre VMs pflegen immer unabhängige Kopien, die in verschiedenen Datenspeichern platziert werden können, um die Redundanz zu erhöhen.
Bandbreite der Netzwerkkarte	Dedizierte 1-Gbit-Netzwerkkarte empfohlen	Dedizierte 10-Gbit-Netzwerkkarte empfohlen
CPU- und Hostkompatibilität	Erfordert identisches CPU-Modell und -Familie und praktisch identische Versionen von vSphere auf Hosts.	CPUs müssen mit vSphere vMotion oder EVC kompatibel sein. Versionen von vSphere auf Hosts müssen mit vSphere vMotion kompatibel sein.
Aktivieren von Fault Tolerance auf laufender VM	Nicht immer unterstützt. Möglicherweise müssen Sie zuerst die VM herunterfahren.	Unterstützt
Storage vMotion	Nur auf heruntergefahrenen VMs unterstützt. vCenter Server deaktiviert Fault Tolerance automatisch, bevor eine Storage vMotion-Aktion durchgeführt wird, und aktiviert Fault Tolerance wieder, nachdem die Storage vMotion-Aktion abgeschlossen ist.	Nicht unterstützt. Der Benutzer muss Fault Tolerance für die VM deaktivieren, bevor die Storage vMotion-Aktion ausgeführt wird, und danach wieder aktivieren.
vlance-Netzwerktreiber	Nicht unterstützt	Unterstützt

Zusätzliche Voraussetzungen für die Fault Tolerance-Legacy-Version

Zusätzlich zu den aufgeführten Unterschieden bei der Fault Tolerance-Legacy-Version gelten für diese Version noch die folgenden eindeutigen Voraussetzungen.

- Der Cluster muss mindestens zwei von Fault Tolerance zertifizierte Hosts enthalten, die die gleiche Version von Fault Tolerance ausführen oder die gleiche Host-Build-Nummer aufweisen. Die Versionsnummer von Fault Tolerance wird auf der Registerkarte **Übersicht** eines Hosts im vSphere Web Client angezeigt.
- ESXi-Hosts müssen Zugriff auf dieselben VM-Datenspeicher und -Netzwerke haben.
- 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 Verwenden von Fault Tolerance unternommen wird, gibt eine Meldung an, dass die VMDK-Datei konvertiert werden muss. Sie müssen die virtuelle Maschine ausschalten, um diese Konvertierung auszuführen.

- Hosts müssen Prozessoren aus der FT-kompatiblen Prozessorgruppe besitzen. Überprüfen Sie, dass die Prozessoren der Hosts miteinander kompatibel sind.
- Der Host, der die sekundäre virtuelle Maschine unterstützt, muss über einen Prozessor verfügen, der Fault Tolerance unterstützt und zur selben CPU-Familie bzw. zum selben CPU-Modell gehört wie der Host, der die primäre virtuelle Maschine unterstützt.
- Wenn Sie ein Upgrade für Hosts durchführen, die fehlertolerante VMs enthalten, müssen Sie sicherzustellen, dass die primären und sekundären virtuellen Maschinen auf Hosts mit derselben Versionsnummer für die Fault Tolerance oder derselben Host-Build-Nummer (für Hosts vor ESX/ESXi 4.1) ausgeführt werden.

Hinweis Wenn Sie für eine VM die Verwendung der Fault Tolerance-Legacy-Version festgelegt hatten, bevor Sie die Hosts im Cluster aktualisierten, verwendet diese VM nach dem Host-Upgrade weiterhin die Fault Tolerance-Legacy-Version.

Aktivieren der Fault Tolerance-Legacy-Version

Um die Fault Tolerance-Legacy-Version verwenden zu können, müssen Sie eine erweiterte Option für die virtuelle Maschine konfigurieren.

Die Fault Tolerance-Legacy-Version kann nur auf virtuellen Maschinen mit einer vCPU verwendet werden, die Fault Tolerance nicht bereits verwenden. Um die Fault Tolerance-Legacy-Version für jede VM zu aktivieren, die sie verwenden soll, müssen Sie die erweiterte Option `vm.uselegacyft` auf einen Wert von **true** festlegen.

Vorgehensweise

1. Navigieren Sie im vSphere Web Client zur virtuellen Maschine.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Klicken Sie auf die Registerkarte **VM-Optionen**.
4. Öffnen Sie den Abschnitt **Erweitert** und klicken Sie neben **Konfigurationsparameter** auf **Konfiguration bearbeiten**.
5. Klicken Sie auf **Zeile hinzufügen** und geben Sie als Name `vm.uselegacyft` und als Wert **true** ein.
6. Klicken Sie auf **OK**.

Die Fault Tolerance-Legacy-Version ist jetzt für diese virtuelle Maschine aktiviert.

Index

A

Affinitätsregeln **47, 51**
Aktuelle Failover-Hosts **27**
Aktuelle Failover-Kapazität **22, 25**
Ändern von Clustereinstellungen **33**
anhalten, Fault Tolerance **57**
Anti-Affinitätsregeln **47**
Anwendungsbeispiele, Fault Tolerance **48**
Anwendungsüberwachung **12, 17**
APD **18**
Ausfallzeit
  Geplant **7**
  Ungeplant **8**
Ausfallzeiten minimieren **7**
Auto Deploy **43**

B

Best Practices
  Fault Tolerance **59**
  vSphere HA-Cluster **41**
  vSphere HA-Netzwerk **41**
Betriebsstatus des Clusters **44**
Business Continuity **7**

C

Clustereinstellungen **33**
Clustergültigkeit **44**

D

das.config.fdm.memreservationmb **38**
das.config.fdm.reportfailoverfailevent **38**
das.heartbeatdsperhost **19, 38**
das.ignoreinsufficienthbdatastore **38**
das.iostatsinterval **17, 38**
das.isolationsadresse **38, 41**
das.isolationshutdowntimeout **13, 38**
das.maxftvcpusperhost **49**
das.maxftvmsperhost **49**
das.maxresets **38**
das.maxterminates **38**
das.reservationrequestretryintervalsec **38**
das.respectvmvmantiaffinityrules **38**
das.slotcpuinmhz **22, 38**
das.slotmeminmb **22, 38**
das.terminateretryintervalsec **38**
das.usedefaultisolationaddress **38**
das.vmcpuminmhz **22, 25, 38**
das.vmMemoryMinMB **38**
Datenspeicher für Virtual SAN **59**
Datenspeicher-Taktsignale **12, 19**
Datenspeicher-Taktsignale bei vSphere HA **36**
deaktivieren, Fault Tolerance **57**
Distributed Power Management (DPM) **21, 29**
Distributed Resource Scheduler (DRS)
  Verwenden mit der Fault Tolerance-Legacy-Version **61**
  Verwenden mit vSphere Fault Tolerance **51**
  Verwenden mit vSphere HA **29, 30**
DNS-Suche **32**
DRS-Affinitätsregeln **30**

E

E/A-Statistikintervall **17**
Enhanced vMotion Compatibility **51**
Ereignisse und Alarme, Einstellung **44**
Erstellen eines vSphere HA-Clusters **32**
Erweiterte Laufzeitinformationen **22**
EVC **51**
Extended Page Tables (EPT) **50, 61**

F

Failover testen, Fault Tolerance **58**
Failover-Hosts **27**
Failover-Hosts angeben **27**
Fault Tolerance
  aktivieren **52**
  anhalten **57**
  Anti-Affinitätsregeln **47**
  Anwendungsbeispiele **48**
  Best Practices **59**
  Checkliste **52**
  deaktivieren **57**
  Deaktivieren **56**
  Einschränkungen, einschalten **55**
  Failover testen **58**
  Fehlermeldungen **47**
  Interoperabilität **49**
  Netzwerkkonfiguration **53**
  Neustart sekundärer VM testen **58**
  Optionen **54**

Protokollierung **53**
Sekundäre VM migrieren **58**
Überprüfung der Richtlinieneinhaltung **54**
Übersicht **47**
Unterbrechungsfreie Verfügbarkeit **9**
Validierungsprüfungen **55**
version **52**
Voraussetzungen **52**
vSphere-Konfiguration **52**
Fault Tolerance – Anforderungen **49**
Fault Tolerance – Grenzwerte **49**
Fault Tolerance-Legacy-Version **47, 53, 61**
Fault Tolerance-Legacy-Version aktivieren **63**
Fault Tolerance-Lizenzierung **49**
fdm.isolationpolicydelaysec **38**
Fehlermeldungen
Fault Tolerance **47**
vSphere HA **11**
Fehlertoleranz bei Bedarf **48**
Firewallports **20, 41**

G

Geplante Ausfallzeit **7**

H

Hardwarevirtualisierung (HV) **52, 55**
Hostisolierungsreaktion **35**
Hostisolierungsreaktion, Einstellung **13**
Hosts
Netzwerkisolierung **12**
Wartungsmodus **12, 29**
Hostüberwachung **33, 41**

I

Interoperabilität, Fault Tolerance **49**
IPv4 **31, 32, 50, 61**
IPv6 **31, 32, 50, 53, 61**
iSCSI-SAN **52**
ISO-Images **59**
Isolierungsreaktion, Host **35**

K

Konfigurieren von erweiterten vSphere HA-Optionen **37**
Konfigurierte Failover-Kapazität **22, 25**

M

Master-Host-Wahl **12**
Maximale Rücksetzungen pro VM **17**

N

N_Port-ID-Virtualisierung (NPIV) **50**
Netzwerkbezeichnungen **41**
Netzwerkisolierungsadresse **41**
Netzwerkkonfiguration, Fault Tolerance **53**
Netzwerkpartition **12, 19, 59**
Neustart sekundärer VM testen, Fault Tolerance **58**
NIC-Gruppierung **41**

P

Paravirtualisierung **50**
PDL **18**
Planen eines vSphere HA-Clusters **11**
PortFast **41**
Portgruppennamen **41**
Protokolldateien **20**
Prozentsatz der reservierten Clusterressourcen **25, 44**

R

Rapid Virtualization Indexing (RVI) **50, 61**
RDM **50, 52**
Ressourcenfragmentierung **27**

S

Sekundäre VM migrieren, Fault Tolerance **58**
Snapshots **50**
Speicher
iSCSI **52**
NAS **52**
NFS **52**
SSL-Zertifikate **20**
Standard-Gateway **41**
Starten und Herunterfahren von virtuellen Maschinen **32**
Steckplatz **22**
Steckplatzgrößenberechnung **22**
Storage DRS **43**
Storage vMotion **7, 43, 50**
symmetrische Multiprozessor-VMs (SMP) **61**
Symmetrischer Multiprozessor (SMP) **50**

T

TCP-Port **20**
Tolerieren, Hostausfälle **22**
Transparentes Failover **9, 47**

U

Überprüfung der Richtlinieneinhaltung, Fault Tolerance **54**
Überwachen von vSphere HA **44**
Überwachungsempfindlichkeit **17**
UDP-Port **20**
Ungeplante Ausfallzeiten **8**

Upgrade von Hosts mit fehlertoleranten virtuellen Maschinen **59**

V

VADP-Sicherungen **61**
Validierungsprüfungen **55**
Verwaltungsnetzwerk **32, 41**
Virtual SAN **19, 28, 31, 43**
Virtuelle Maschine, Schutz **12, 19**
virtuelle Maschinen, Neustartpriorität **35**
VM Component Protection **18, 31–33, 35, 50**
VM-Außerkraftsetzungen **13, 40**
VM-Neustartpriorität, Einstellung **13**
VM-Überwachung **12, 17**
VM-VM-Affinitätsregeln **27**
vm.uselegacyft **61**
VMCP **18, 31–33, 35, 50**
VMDK **52, 61**
VMFS **19, 41**
VMware Tools **17**
Vom Cluster tolerierte Hostfehler **22, 44**
Voraussetzungen, Fault Tolerance **52**
vpxd.das.completemetadataupdateinterval-sec **38**
vpxuser-Benutzerkonto **20**
vSphere HA
  Checkliste **32**
  Clustereinstellungen **32**
  Fehlermeldungen **11**
  Konfigurieren von Clustereinstellungen **34**
  überwachen **44**
  Vorteile **8**
  Wiederherstellung nach Ausfällen **8**
vSphere HA-Architektur **11**
vSphere HA-Cluster
  Best Practices **41**
  erstellen **33**
  Erstellen **32, 54**
  Heterogenität **27**
  Master-Host **12, 19**
  planen **11**
  Slave-Host **12**
  Zugangssteuerung **21**
vSphere HA-Interoperabilität **28**
vSphere HA-Netzwerk
  Best Practices **41**
  Pfadredundanz **41**

Z

Zielgruppe **5**
Zugangssteuerung
  konfigurieren **35**
  Richtlinie **35**
  Typen **21**
  vSphere HA **21**
Zugangssteuerungsrichtlinie
  auswählen **27**
  Failover-Hosts angeben **27**
  Prozentsatz der reservierten Clusterressourcen **25**
  Vom Cluster tolerierte Hostfehler **22**