Handbuch zur Verfügbarkeit in vSphere

Update 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter 8.0

vmware
by Broadcom

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

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

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

Inhalt

Handbuch zur vSphere-Verfügbarkeit 6

1 Sie können Ausfallzeiten mit vSphere minimieren 7
- Reduzieren geplanter Ausfallzeiten mit vSphere 7
- Verhindern ungeplanter Ausfallzeiten mit vSphere 8
- vSphere HA bietet eine schnelle Wiederherstellung nach Ausfällen 9
- vSphere Fault Tolerance bietet unterbrechungsfreie Verfügbarkeit 10
- Schützen von vCenter Server mit vCenter High Availability 10
- Schützen von vCenter Server mit VMware Service Lifecycle Manager 11

2 Erstellen und Verwenden von vSphere HA-Clustern 12
- Arbeitsweise von vSphere HA 12
  - Primäre und sekundäre Hosts 13
  - Hostfehlertypen 14
  - Festlegen von Antworten auf Hostprobleme 15
  - VM- und Anwendungsüberwachung 18
  - VM Component Protection 20
  - Netzwerkpartitionen 21
  - Datenspeicher-Taktsignale 21
  - vSphere HA-Sicherheit 22
- vSphere HA-Zugangssteuerung 24
  - Zugangssteuerung für Prozentsatz der Clusterressourcen 25
  - Zugangssteuerung mithilfe der Richtlinie für die Steckplatzgröße 27
  - Zugangssteuerung für dedizierte Failover-Hosts 30
- vSphere HA-Interoperabilität 31
  - Verwenden von vSphere HA mit vSAN 31
  - Gemeinsame Verwendung von vSphere HA und DRS 33
  - Andere Probleme mit der vSphere HA-Interoperabilität 34
- Erstellen eines vSphere HA-Clusters 35
  - vSphere HA-Checkliste 36
  - Erstellen eines vSphere HA-Clusters im vSphere Client 37
- Konfigurieren der Einstellungen für vSphere Availability 39
  - Konfigurieren der Reaktionen auf Fehler 39
  - Konfigurieren von Proactive HA 43
  - Konfigurieren der Zugangssteuerung 44
  - Konfigurieren der Taktsignal-Datenspeicher 45
  - Festlegen erweiterter Optionen 46
- Best Practices für VMware vSphere® High Availability-Cluster 51

Empfohlene Vorgehensweisen für Netzwerke 51
Best Practices für die Interoperabilität 54
Best Practices für die Cluster-Überwachung 55
Verhaltensänderung für HA-VIBs 56

3 Aktivieren der Fault Tolerance für virtuelle Maschinen 57
Wie Fault Tolerance funktionert 57
Beispiele für die Nutzen der Fault Tolerance 58
Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance 59
Fault Tolerance-Interoperabilität 60
vSphere-Funktionen, die für Fault Tolerance nicht unterstützt werden 61
Funktionen und Geräte, die mit Fault Tolerance nicht kompatibel sind 61
Verwendung der Fault Tolerance mit DRS 62
Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance 63
Fault Tolerance-Checkliste 63
Konfigurieren von Netzwerken für Hostmaschinen 65
Verwenden von Fault Tolerance 66
Validierungsprüfungen für das Einschalten von Fault Tolerance 66
Fault Tolerance einschalten 68
Fault Tolerance ausschalten 69
Fault Tolerance anhalten 69
Sekundäre VM migrieren 70
Failover testen 70
Neustart sekundärer VM testen 71
Upgrade von für Fault Tolerance verwendeten Hosts 71
Aktivieren der Fault Tolerance-Verschlüsselung 72
Best Practices für Fault Tolerance 74
Aktivieren der Fault Tolerance für Metro-Cluster 76
Legacy Fault Tolerance 77
Fehlerbehebung bei fehlertoleranten virtuellen Maschinen 78
Hardwarevirtualisierung nicht aktiviert 78
Kompatible Hosts, die für die sekundäre virtuelle Maschine nicht verfügbar sind 79
Sekundäre VM auf einem überlasteten Host beeinträchtigt die Leistung der primären VM 79
Höhere Netzwerklatenz bei Fault Tolerance-VMs 80
Manche Hosts sind mit virtuellen FT-Maschinen überlastet 81
Verlust des Zugriffs auf FT-Metadaten-Datenspeicher 81
Einschalten von vSphere FT für eingeschaltete VM schlägt fehl 82
Fehlertolerante virtuelle Maschinen, die durch vSphere DRS nicht platziert oder entfernt wurden 83
Failover von fehlertoleranten virtuellen Maschinen 83

4 vCenter High Availability 86

Planen der Bereitstellung von vCenter HA 87

vCenter - Übersicht über die Architektur 87

Hardware- und Softwareanforderungen von vCenter HA 88

Konfigurations-Workflow in vSphere Client 89

Konfigurieren des Netzwerks 90

Konfigurieren von vCenter HA mit dem vSphere Client 91

Verwalten der vCenter HA-Konfiguration 94

Einrichten von SNMP-Traps 95

Einrichten der Umgebung für die Verwendung von benutzerdefinierten Zertifikaten 96

Verwalten von vCenter HA SSH-Schlüsseln 97

Einleiten eines vCenter HA-Failovers 97

Bearbeiten der vCenter HA-Clusterkonfiguration 98

Durchführen von Sicherungs- und Wiederherstellungsvorgängen 99

Entfernen einer vCenter HA-Konfiguration 100

Neustarten aller vCenter HA-Knoten 100

Ändern der Serverumgebung 101

Erfassen von Support-Paketen für einen vCenter HA-Knoten 101

Beheben von Fehlern in Ihrer vCenter HA-Umgebung 102

vCenter HA-Klonenvorgang schlägt während der Bereitstellung fehl 102

Erneutes Bereitstellen des passive Knotens oder des Zeugenknotens 103

vCenter HA-Bereitstellung schlägt fehl 104

Fehlerbehebung bei einem fehlerhaften vCenter HA-Cluster 104

Wiederherstellen bei isolierten vCenter HA-Knoten 106

Beheben von Failover-Fehlern 106

VMware vCenter® HA-Alarme und -Ereignisse 107

Patchen einer vCenter-Umgebung mit hoher Verfügbarkeit 109

Upgrade mit reduzierter Ausfallzeit für vCenter HA 109

Handbuch zur vSphere-Verfügbarkeit

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

Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip bei unseren Kunden und Partnern sowie innerhalb der internen Community zu fördern, erstellen wir Inhalte mit neutraler Sprache.

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.

Sie können Ausfallzeiten mit vSphere minimieren

1

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

Mit VMware-Software wird die Bereitstellung von hoher Verfügbarkeit für wichtige Anwendungen einfacher und günstiger. Mithilfe von vSphere können Sie die grundlegende Verfügbarkeit aller Anwendungen problemlos erhöhen und höhere Verfügbarkeitsebenen einfacher und kostengünstiger bereitstellen. Mit vSphere können Sie Folgendes erreichen:

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

Mithilfe von vSphere können geplante Ausfallzeiten reduziert und ungeplante Ausfallzeiten verhindert werden. Zudem wird eine schnelle Wiederherstellung nach Ausfällen ermöglicht.

Lesen Sie als Nächstes die folgenden Themen:

- Reduzieren geplanter Ausfallzeiten mit vSphere
- Verhindern ungeplanter Ausfallzeiten mit vSphere
- vSphere HA bietet eine schnelle Wiederherstellung nach Ausfällen
- vSphere Fault Tolerance bietet unterbrechungsfreie Verfügbarkeit
- Schützen von vCenter Server mit vCenter High Availability
- Schützen von vCenter Server mit VMware Service Lifecycle Manager

Reduzieren geplanter Ausfallzeiten mit vSphere

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 mit vSphere

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 vSAN-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 VMware 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.

Schützen von vCenter Server mit vCenter High Availability

vCenter High Availability (vCenter HA) schützt nicht nur vor Ausfällen des Hosts und der Hardware, sondern auch vor Anwendungsfehlern der vCenter Server-Anwendung. Durch den automatischen Failover von aktiven zu passiven Knoten unterstützt die vCenter HA Hochverfügbarkeit bei minimalen Ausfallzeiten.

Die Konfiguration von vCenter HA erfolgt über den vSphere Client. Diese Optionen stehen über den Konfigurationsassistenten zur Verfügung.

Option	Beschreibung
Automatisch	Die automatische Option klont den aktiven Knoten zum passiven Knoten und zum Zeugenkonten und konfiguriert die Knoten für Sie. Wenn Ihre Umgebung die folgenden Anforderungen erfüllt, können Sie diese Option verwenden. ■ Die vCenter Server, die zum aktiven Knoten wird, verwaltet ihren eigenen ESXi-Host und ihre eigene virtuelle Maschine. Diese Konfiguration wird manchmal als selbstverwalteter vCenter Server bezeichnet.
Manuell	Die manuelle Option bietet größere Flexibilität. Sie können diese Option verwenden, sofern Ihre Umgebung die Hardware- und Softwareanforderungen erfüllt. Wenn Sie diese Option auswählen, sind Sie für das Klonen des aktiven Knoten zu dem passiven Knoten und dem Zeugenknoten verantwortlich. Sie müssen auch das Netzwerk entsprechend konfigurieren.

Schützen von vCenter Server mit VMware Service Lifecycle Manager

Die Verfügbarkeit von vCenter Server wird von VMware Service Lifecycle Manager bereitgestellt.

Wenn ein vCenter-Dienst fehlschlägt, wird er von VMware Service Lifecycle Manager neu gestartet. VMware Service Lifecycle Manager überwacht die Funktion von Diensten und ergreift vorkonfigurierte Standardisierungsmaßnahmen, wenn es einen Fehler erkennt. Der Dienst wird nicht neu gestartet, wenn mehrere Standardisierungsversuche fehlschlagen.

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.

Lesen Sie als Nächstes die folgenden Themen:

- Arbeitsweise von vSphere HA
- vSphere HA-Zugangssteuerung
- vSphere HA-Interoperabilität
- Erstellen eines vSphere HA-Clusters
- Konfigurieren der Einstellungen für vSphere Availability
- Best Practices für VMware vSphere® High Availability-Cluster
- Verhaltensänderung für HA-VIBs

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 primärer Host ausgewählt. Der primäre Host kommuniziert mit vCenter Server und überwacht den Zustand aller geschützten virtuellen Maschinen und der sekundären Hosts. Es sind verschiedene Arten von Hostausfällen möglich. Der primäre Host muss den Ausfall erkennen und angemessen mit ihm umgehen. Der primäre Host muss zwischen einem ausgefallenen Host und einem Host unterscheiden, der sich in einer Netzwerkpartition befindet oder vom Netzwerk isoliert ist. Der primäre Host verwendet Netzwerk- und Datenspeicher-Taktsignale, um die Art des Ausfalls zu ermitteln.

 (vSphere HA-Cluster)

Primäre und sekundäre 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 primärer oder sekundärer 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 primären 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 primären Host pro Cluster. Alle anderen Hosts sind sekundäre Hosts. Falls der primäre Host ausfällt, heruntergefahren, in Standby-Modus versetzt oder aus dem Cluster entfernt wird, findet eine Neuwahl statt.

Der primäre Host in einem Cluster hat mehrere Aufgaben:

- Überwachung des Zustands von sekundären Hosts. Falls ein sekundärer Host ausfällt oder nicht erreichbar ist, identifiziert der primäre Host die virtuellen Maschinen, die neu gestartet werden müssen.
- Überwachung des Betriebszustands aller geschützten virtuellen Maschinen. Falls eine virtuelle Maschine ausfällt, sorgt der primäre Host dafür, dass sie neu gestartet wird. Mithilfe einer Engine für die lokale Platzierung bestimmt der primäre Host auch die Stelle, an der der Neustart erfolgt.
- 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 sekundären Hosts tragen in erster Linie zum Cluster bei, indem sie virtuelle Maschinen lokal ausführen, ihren Laufzeitstatus überwachen und Zustand-Updates an den primären Host melden. Ein primärer Host kann auch virtuelle Maschinen ausführen und überwachen. Sowohl sekundäre Hosts als auch primäre Hosts implementieren die VM- und Anwendungsüberwachungsfunktionen.

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

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

Hostfehlertypen

Der primäre Host eines VMware vSphere® High Availability-Clusters ist verantwortlich für das Erkennen des Ausfalls eines sekundären 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 primären Host wird unterbrochen.

Der primäre Host überwacht, ob die sekundären Hosts im Cluster noch aktiv sind. Die Kommunikation erfolgt über den Austausch von Netzwerktaktsignalen im Sekundentakt. Wenn der primäre Host keine Taktsignale von einem sekundären Host empfängt, überprüft er, ob der Host noch aktiv ist, bevor er den Host als ausgefallen betrachtet. Die vom primären Host durchgeführte Überprüfung auf Aktivität dient der Feststellung, ob der sekundäre Host Taktsignale mit einem der Datenspeicher austauscht. Weitere Informationen hierzu finden Sie unter Datenspeicher-Taktsignale . Der primäre Host überprüft zudem, ob der Host auf ICMP-Pings reagiert, die an seine Verwaltungs-IP-Adressen gesendet werden.

Wenn ein primärer Host nicht direkt mit dem Agent auf einem sekundären Host kommunizieren kann, reagiert der sekundäre Host nicht auf ICMP-Pings. Stellt der Agent keine Taktsignale aus, wird er als fehlgeschlagen eingestuft. Die virtuellen Maschinen des Hosts werden auf alternativen Hosts neu gestartet. Wenn ein solcher sekundärer Host Taktsignale mit einem Datenspeicher austauscht, geht der primäre Host davon aus, dass sich der sekundäre Host in einer Netzwerkpartition befindet oder vom Netzwerk isoliert ist. Der primäre Host setzt dann die Überwachung des Hosts und dessen virtueller Maschinen fort. Weitere Informationen hierzu finden Sie unter Netzwerkpartitionen .

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. Schlägt der Ping-Befehl ebenfalls fehl, erklärt sich der Host als vom Netzwerk isoliert.

Der primäre Host überwacht die virtuellen Maschinen, die auf einem isolierten Host ausgeführt werden. Wenn der primäre Host feststellt, dass die VMs ausgeschaltet werden, und der primäre Host für die VMs verantwortlich ist, startet er sie neu.

Hinweis Wenn Sie sicherstellen, dass die Netzwerkinfrastruktur ausreichend redundant ist, sodass mindestens ein Netzwerkpfad stets zur Verfügung steht, ist die Wahrscheinlichkeit einer Hostnetzwerkisolierung geringer.

Proactive HA-Fehler

Ein Proactive HA-Fehler tritt beim Ausfall einer Hostkomponente auf, was zum Redundanzverlust oder zu einem nicht schwerwiegenden Fehler führt. Das funktionale Verhalten der auf dem Host vorhandenen VMs ist jedoch noch nicht davon betroffen. Wenn beispielsweise ein Netzteil auf dem Host ausfällt, aber andere Netzteile verfügbar sind, handelt es sich hierbei um einen Proactive HA-Fehler.

Bei einem Proactive HA-Fehler können Sie die Problembehebungsaktion im vSphere Availability-Abschnitt des vSphere Client automatisieren. Die VMs auf dem betroffenen Host können auf andere Hosts evakuiert werden. Der Host wird dann entweder in den Quarantänemodus oder in den Wartungsmodus versetzt.

Hinweis In Ihrem Cluster muss vSphere DRS verwendet werden, damit die Überwachung auf Proactive HA-Fehler funktioniert.

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. Sie können zudem Ausnahmen für bestimmte virtuelle Maschinen konfigurieren. Weitere Informationen hierzu finden Sie unter Anpassen einer einzelnen virtuellen Maschine .

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 primären Host isoliert oder partitioniert wird und der primäre Host nicht über Taktsignal-Datenspeicher mit ihm kommunizieren kann. In dieser Situation kann der primäre Host nicht feststellen, ob der Host ausgeführt wird, und erklärt ihn daher für ausgefallen. Der primäre Host versucht dann, die virtuellen Maschinen neu zu starten, die auf dem isolierten oder partitionierten Host ausgeführt werden. 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 VMCP-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.

Abhängigkeiten virtueller Maschinen

Sie können Abhängigkeiten zwischen Gruppen virtueller Maschinen erstellen. Dazu müssen Sie zunächst die VM-Gruppen im vSphere Client erstellen, indem Sie auf der Registerkarte **Konfigurieren** für den Cluster die Option **VM/Host-Gruppen** auswählen. Sobald die Gruppen erstellt sind, können Sie Abhängigkeitsregeln für den Neustart zwischen den Gruppen erstellen, indem Sie zu **VM/Host-Regeln** navigieren und im Dropdown-Menü „Typ“ die Option **Virtuelle Maschinen zu virtuelle Maschinen** auswählen. Mit diesen Regeln können Sie angeben, dass bestimmte VM-Gruppen erst gestartet werden können, wenn andere angegebene VM-Gruppen bereit sind.

Berücksichtigte Faktoren für den Neustart von virtuellen Maschinen

Nach einem Ausfall startet der primäre Host des Clusters die betroffenen virtuellen Maschinen neu, indem ein Host angegeben wird, der sie einschalten kann. Bei der Auswahl eines derartigen Hosts berücksichtigt der primäre Host eine Reihe von Faktoren.

Zugriffsfähigkeit auf Dateien

Bevor eine virtuelle Maschine gestartet werden kann, muss von einem der aktiven Cluster-Hosts, mit dem der primäre Host über das Netzwerk kommunizieren kann, auf die zugehörigen Dateien 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. Vier Arten von Reservierungen werden berücksichtigt: CPU, Arbeitsspeicher, vNIC und Virtual 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 primäre Host ein Ereignis mit dem Hinweis aus, dass nicht genügend Ressourcen zum Starten der VM mithilfe von vSphere HA vorhanden sind. Der primäre Host wiederholt den Versuch, nachdem sich die Clusterbedingungen geändert haben. Wenn zum Beispiel nicht auf die virtuelle Maschine zugegriffen werden kann, wiederholt der primäre Host den Versuch, nachdem sich die Dateizugänglichkeit geändert hat.

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.

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.

VM-Komponentenschutz

Wenn 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 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 werden, 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 virtueller 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 primäre Host ausgeführt wird, der für sie verantwortlich ist. Der primäre Host muss mit vCenter Server kommunizieren. Ein primärer 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 primären Host, aber nur mit einer Untergruppe der sekundären Hosts kommunizieren. 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 primäre Host in einem VMware vSphere® High Availability-Cluster nicht über das Verwaltungsnetzwerk mit einem sekundären Host kommunizieren kann, verwendet der primäre Host Datenspeicher-Taktsignale, um festzustellen, ob der sekundäre Host ausgefallen ist, sich in einer Netzwerkpartition befindet oder vom Netzwerk isoliert ist. Wenn der Datenspeicher des sekundären Hosts keine Taktsignale mehr sendet, wird er als ausgefallen betrachtet und seine virtuellen Maschinen werden an anderer Stelle neu gestartet.

VMware 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. Mit vmfs5 ist die maximale und typische Nutzung 3 MB. Die Verwendung von vSphere HA-Datenspeichern fügt einen vernachlässigbaren Overhead hinzu und hat keine Auswirkungen auf die Leistung der anderen Datenspeichervorgänge.

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 die durch den Grenzwert beschränkten virtuellen Maschinen.

Hinweis Ein Datenspeicher für vSAN 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 vSAN 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-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-Hosts schreibt vSphere HA in `/var/log/vmware/fdm` auf der lokalen Festplatte sowie in syslog, falls dies konfiguriert wurde.

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 zufälliges Kennwort für dieses Konto und ändert das Kennwort regelmäßig. Der Zeitraum wird durch die vCenter Server-Einstellung `VirtualCenter.VimPasswordExpirationInDays` 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 primärer 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

vSphere HA stellt mithilfe der Zugangssteuerung sicher, dass genügend Ressourcen für die Wiederherstellung virtueller Maschinen reserviert sind, wenn ein Host ausfällt.

Mit der Zugangssteuerung werden Beschränkungen für die Ressourcennutzung auferlegt. Aktionen, die gegen diese Beschränkungen verstoßen, sind nicht zulässig. Folgende Aktionen sind möglicherweise nicht zulässig:

- Das Einschalten einer virtuellen Maschine
- Migrieren einer virtuellen Maschine
- Erhöhen der CPU- oder Arbeitsspeicherreservierung einer virtuellen Maschine

Die Grundlage für die vSphere HA-Zugangssteuerung ist die Anzahl der Hostfehler, die Ihr Cluster tolerieren darf, während das Failover weiterhin gewährleistet bleibt. Es gibt drei Methoden, um die Failover-Kapazität des Hosts festzulegen:

- Prozentsatz der Clusterressourcen
- Richtlinie für Steckplatzgröße
- Dedizierte Failover-Hosts

Hinweis Die vSphere HA-Zugangssteuerung kann deaktiviert werden. Ohne sie haben Sie jedoch keine Gewissheit, dass nach einem Hostausfall die erwartete Anzahl an virtuellen Maschinen neu gestartet werden kann. Die Zugangssteuerung sollten Sie nicht permanent deaktivieren.

Hinweis Sie müssen in einem Cluster vorübergehend die HA-Zugangssteuerung, damit vSphere vMotion fortfahren kann. Diese Aktion verhindert einen Ausfall der Maschinen auf den Hosts, die Sie standardisieren. Wenn Sie die HA-Zugangssteuerung deaktivieren, bevor Sie einen Cluster mit zwei Knoten standardisieren, verliert der Cluster praktisch alle Hochverfügbarkeitsgarantien. Das hat folgende Ursache: Wenn einer der beiden Hosts in den Wartungsmodus wechselt, kann vCenter Server kein Failover von virtuellen Maschinen auf diesen Host durchführen, und HA-Failover werden nie erfolgreich sein.

Hinweis Für die Verwendung der vSphere HA-Zugangssteuerung sind mindestens 3 Hosts im Cluster erforderlich.

Unabhängig von der gewählten Option für die Zugangssteuerung ist auch ein Schwellenwert für die VM-Ressourcenreduktion vorhanden. Mithilfe dieser Einstellung geben Sie an, welcher Prozentsatz der Ressourcendegradierung toleriert wird. Diese Einstellung ist jedoch nur verfügbar, wenn vSphere DRS aktiviert ist.

Die Berechnung der Ressourcenreduktion wird für CPU und Arbeitsspeicher geprüft. Dabei werden der reservierte Arbeitsspeicher und die Arbeitsspeicherüberlastung einer virtuellen Maschine berücksichtigt, um zu entscheiden, ob sie eingeschaltet oder migriert werden darf oder ob Reservierungsänderungen vorgenommen werden dürfen. Der tatsächlich von der

virtuellen Maschine belegte Arbeitsspeicher wird bei der Berechnung nicht berücksichtigt, da die Arbeitsspeicherreservierung nicht immer der tatsächlichen Arbeitsspeichernutzung der virtuellen Maschine entspricht. Wenn die tatsächliche Nutzung höher als der reservierte Arbeitsspeicher ist, ist nicht genügend Failover-Kapazität verfügbar, was zu Leistungseinbußen beim Failover führt.

Durch die Festlegung eines Schwellenwerts für die Leistungsreduktion kann das Vorhandensein eines Konfigurationsproblems ermittelt werden. Beispiel:

- Der Standardwert ist 100 %, womit keine Warnungen erstellt werden.
- Wenn Sie den Schwellenwert auf 0 % reduzieren, wird eine Warnung generiert, wenn die Cluster-Nutzung die verfügbare Kapazität überschreitet.
- Wenn Sie den Schwellenwert auf 20 % reduzieren, wird die zulässige Leistungsreduktion wie folgt berechnet: `performance reduction = current utilization * 20%`. Wenn die aktuelle Nutzung abzüglich der Leistungsreduktion die verfügbare Kapazität überschreitet, wird ein Konfigurationshinweis ausgegeben.

Zugangssteuerung für Prozentsatz der 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.

Mit diesem Zugangssteuerungstyp stellt vSphere HA sicher, dass ein bestimmter Prozentsatz der gesamten CPU- und Arbeitsspeicherressourcen für das Failover reserviert wird.

Mit der Option für den Prozentsatz der Clusterressourcen setzt vSphere HA die Zugangssteuerung folgendermaßen durch:

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 Zugangssteuerungsoption für den Prozentsatz der Clusterressourcen überprüft zudem, ob 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.

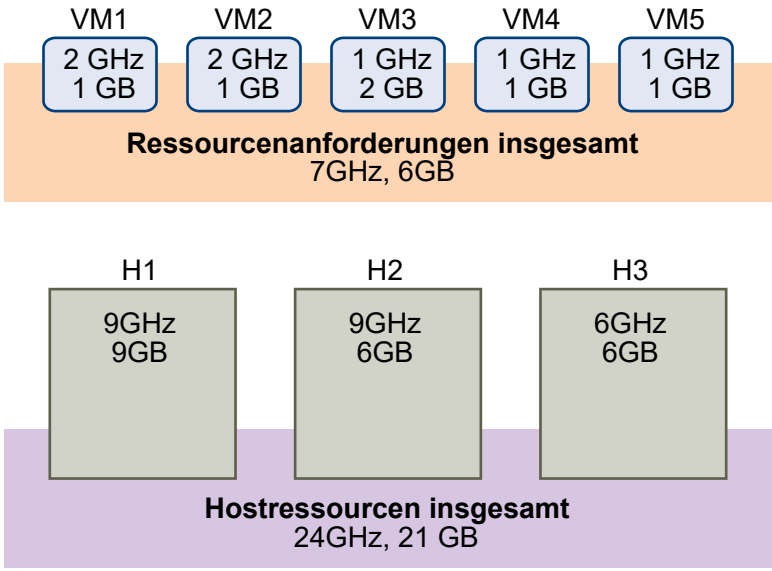
Beispiel: Zugangssteuerung mithilfe des Prozentsatzes der Clusterressourcen

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 verfügbare CPU-Ressourcen und 9 GB verfügbaren Arbeitsspeicher, 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 2-1. 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.

Zugangssteuerung mithilfe der Richtlinie für die Steckplatzgröße

Die Zugangssteuerung von vSphere HA stellt mit der Option für die Richtlinie für die Steckplatzgröße sicher, dass eine angegebene Anzahl an Hosts ausfallen kann und genügend Ressourcen im Cluster verbleiben, um ein Failover aller virtuellen Maschinen für diese Hosts durchzuführen.

Mithilfe der Richtlinie für die Steckplatzgröße führt vSphere HA die Zugangssteuerung wie folgt durch:

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 Client eine spezifische Steckplatzgröße für die CPU und den Arbeitsspeicher festlegen.

Steckplatzgrößenberechnung

 (vSphere HA-Steckplatzgröße und -Zugangssteuerung)

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. Weitere Informationen hierzu finden Sie unter Erweiterte vSphere HA-Optionen.

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 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 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.

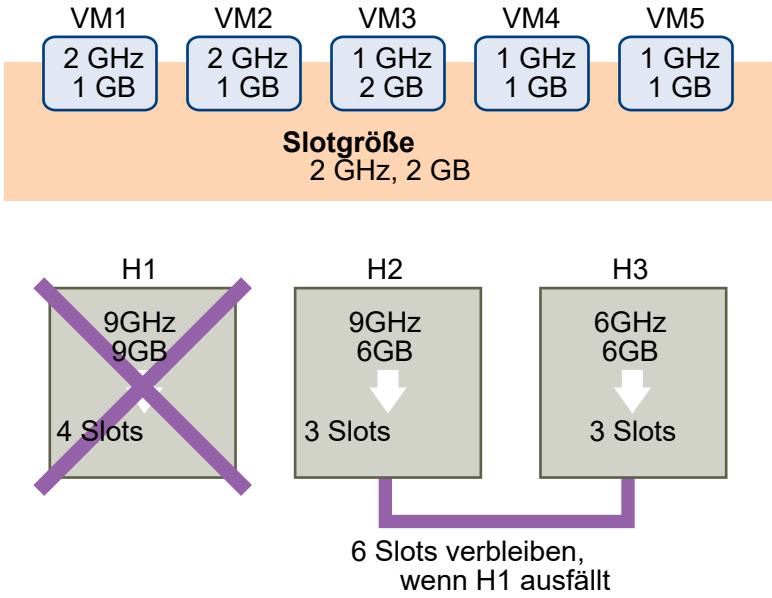
Die aktuelle Failover-Kapazität wird berechnet, indem ermittelt wird, wie viele Hosts (angefangen mit dem größten Host) ausfallen können, damit noch genug Steckplätze zur Verfügung stehen, um den Anforderungen aller eingeschalteten virtuellen Maschinen gerecht zu werden.

Beispiel: Zugangssteuerung mithilfe der Richtlinie für die Steckplatzgröße

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 verfügbare CPU-Ressourcen und 9 GB verfügbaren Arbeitsspeicher, 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 2-2. 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 für dedizierte Failover-Hosts

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

Wenn ein Host ausfällt, versucht vSphere HA mithilfe der Zugangssteuerung für dedizierte Failover-Hosts, die virtuellen Maschinen auf einem der angegebenen Failover-Hosts neu zu starten. Wenn der Neustart der virtuellen Maschinen 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 Zugangssteuerung für dedizierte Failover-Hosts verwenden und dabei mehrere Failover-Hosts auswählen, versucht DRS nicht, die VM-VM-Affinitätsregeln für virtuelle Maschinen zu erzwingen, die auf Failover-Hosts ausgeführt werden.

vSphere HA-Interoperabilität

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

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 vSAN

vSAN kann als gemeinsam genutzter Speicher für einen vSphere HA-Cluster verwendet werden. Wenn vSAN 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 vSAN müssen Sie bestimmte Überlegungen und Einschränkungen für die Interoperabilität dieser beiden Funktionen beachten.

Informationen zu vSAN finden Sie unter *Verwalten von VMware vSAN*.

Hinweis vSphere HA kann zusammen mit ausgeweiteten vSAN-Clustern verwendet werden.

Anforderungen für ESXi-Hosts

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

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

Unterschiede beim Netzwerk

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

Hinweis Sie können vSAN nur aktivieren, wenn vSphere HA deaktiviert ist.

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

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

2 Nehmen Sie die Änderungen am vSAN-Netzwerk 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 die Hostüberwachung für den vSphere HA-Cluster erneut.

Tabelle 2-2. Unterschiede beim vSphere HA-Netzwerk sind die Unterschiede bei vSphere HA-Netzwerken dargestellt, je nachdem, ob vSAN verwendet wird.

Tabelle 2-2. Unterschiede beim vSphere HA-Netzwerk

	vSAN Aktiviert	vSAN Deaktiviert
Von vSphere HA verwendetes Netzwerk	vSAN-Speichernetzwerk	Verwaltungsnetzwerk
Taktsignal-Datenspeicher	Jeder für > 1 Host gemountete Datenspeicher, nicht jedoch Datenspeicher für vSAN	Jeder für > 1 Host gemountete Datenspeicher
Als isoliert erklärter Host	Isolationsadressen können nicht angepingt werden und es besteht kein Zugriff auf das vSAN-Speichernetzwerk	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, müssen Sie diese Einstellung mit der entsprechenden Einstellung für vSAN koordinieren, die den Zugriff auf die Daten bei Fehlern sicherstellt. Insbesondere darf die Einstellung „Anzahl der zu tolerierenden Fehler“ im Regelsatz für vSAN nicht niedriger als die durch die Einstellung für die vSphere HA-Zugangssteuerung reservierte Kapazität sein.

Wenn beispielsweise der Regelsatz für vSAN 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 vSphere 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.

Hinweis Bei vSphere DRS handelt es sich um eine wichtige vSphere-Funktion, die zum Aufrechterhalten der Integrität der in einem vSphere-Cluster ausgeführten Arbeitslasten benötigt wird. Ab vSphere 7.0 Update 1 hängt DRS von der Verfügbarkeit der vCLS-VMs ab. Weitere Informationen finden Sie unter *vSphere Cluster Services (vCLS)* in *Handbuch zur vSphere-Ressourcenverwaltung*.

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, müssen Sie erweiterte vSphere HA-Optionen verwenden, um das gewünschte Failover-Verhalten für vSphere HA durchzusetzen.

- **vSphere HA muss während des Failovers die VM-Anti-Affinitätsregeln respektieren**: Wenn die erweiterte Option für VM-Anti-Affinitätsregeln festgelegt ist, führt vSphere HA kein Failover einer virtuellen Maschine durch, wenn dadurch eine Regel verletzt wird. Stattdessen gibt vSphere HA eine Ereignismeldung aus, wenn nicht genügend Ressourcen zur Durchführung des Failovers vorhanden sind.
- **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.

Weitere Informationen finden Sie unter „Erweiterte vSphere HA-Optionen“.

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:

- Der VM-Komponentenschutz erkennt keine Zugriffsprobleme für Dateien, die sich auf vSAN-Datenspeichern befinden, oder reagiert nicht darauf. Wenn die Konfigurations- und VMDK-Dateien einer virtuellen Maschine sich nur auf vSAN-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 vSAN verwenden.

Zusätzlich zu den obigen Einschränkungen werden die folgenden IPv6-Adresstypen nicht zusammen mit der vSphere HA-Isolierungsadresse bzw. dem Verwaltungsnetzwerk unterstützt: link-local, ORCHID und link-local 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 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 Empfohlene Vorgehensweisen für Netzwerke.

- 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.
- vSphere HA unterstützt sowohl IPv4 als auch IPv6. Überlegungen zur Verwendung von IPv6 finden Sie unter Andere Probleme mit der vSphere HA-Interoperabilität .
- 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 im vSphere Client

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 Client Hosts zum Cluster hinzu und legen die Einstellungen für vSphere HA fest.

Ein vSphere HA-fähiger Cluster ist eine Voraussetzung zur Verwendung von vSphere 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 Empfohlene Vorgehensweisen für Netzwerke.
- 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 Client unter Verwendung eines Kontos mit Clusteradministratorberechtigungen mit vCenter Server.

Verfahren

1. Navigieren Sie im vSphere Client zu dem Datencenter, in dem sich der Cluster befinden soll, und klicken Sie auf **Neuer Cluster**.
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 Client Hosts zum Cluster hinzu.
5. Navigieren Sie zum Cluster und aktivieren Sie vSphere HA.
   a. Klicken Sie auf die Registerkarte **Konfigurieren**.
   b. Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.
   c. Wählen Sie **vSphere HA** aus.
6. Wählen Sie unter **Fehler und Reaktionen** die Option **Hostüberwachung aktivieren** aus.

   Bei aktivierter Hostüberwachung können Hosts im Cluster Netzwerktaktsignale austauschen und vSphere HA kann beim Auftreten von Fehlern entsprechende Maßnahmen ergreifen. Die Hostüberwachung ist erforderlich, damit der vSphere Fault Tolerance-Wiederherstellungsprozess ordnungsgemäß ausgeführt wird.
7. Wählen Sie eine Einstellung für **VM-Überwachung** aus.

   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**.

Ergebnisse

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

Nächste Schritte

Konfigurieren Sie die entsprechenden vSphere HA-Einstellungen für Ihren Cluster.

- Fehler und Reaktionen
- Zugangssteuerung
- Taktsignal-Datenspeicher
- Erweiterte Optionen

Weitere Informationen hierzu finden Sie unter Konfigurieren der Einstellungen für vSphere Availability.

Konfigurieren der Einstellungen für vSphere Availability

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 Client konfigurieren:

Fehler und Reaktionen

Geben Sie hier Einstellungen für Hostfehlerreaktionen, Hostisolierung, VM-Überwachung und VM Component Protection an.

Zugangssteuerung

Aktivieren bzw. deaktivieren Sie die Zugangssteuerung für den vSphere HA-Cluster und wählen Sie eine Richtlinie dafür aus, wie diese erzwungen wird.

Taktsignal-Datenspeicher

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.

Konfigurieren der Reaktionen auf Fehler

Im Fenster **Fehler und Reaktionen** der vSphere HA-Einstellungen können Sie konfigurieren, wie Ihr Cluster beim Auftreten von Problemen funktionieren soll.

In diesem Teil des vSphere Client können Sie die spezifischen Aufgaben festlegen, mit denen der vSphere HA-Cluster auf Hostfehler und -isolierung reagiert. Darüber hinaus können Sie Aktionen für VM Component Protection (VMCP) konfigurieren, wenn Situationen vom Typ „Dauerhafter Geräteverlust“ (Permanent Device Loss, PDL) und „Keine Pfade verfügbar“ (All Paths Down, APD) auftreten. Sie können auch die VM-Überwachung aktivieren.

Die folgenden Aufgaben sind verfügbar:

Weitere Themen zum Lesen

Verfahren

1 Reagieren auf Hostfehler

   Sie können bestimmte Reaktionen auf Hostfehler festlegen, die in Ihrem vSphere HA-Cluster auftreten.

2 Reagieren auf Hostisolierung

   Sie können bestimmte Reaktionen auf die Hostisolierung festlegen, die in Ihrem vSphere HA-Cluster auftreten kann.

3 Konfigurieren der VMCP-Reaktionen

   Konfigurieren Sie, wie VM Component Protection (VMCP) reagiert, wenn bei einem Datenspeicher ein PDL- oder APD-Fehler auftritt.

4 Aktivieren der VM-Überwachung

   Sie können die VM- und Anwendungsüberwachung aktivieren sowie die Überwachungsempfindlichkeit für Ihren vSphere HA-Cluster festlegen.

Reagieren auf Hostfehler

Sie können bestimmte Reaktionen auf Hostfehler festlegen, die in Ihrem vSphere HA-Cluster auftreten.

Diese Seite kann nur bearbeitet werden, wenn Sie vSphere HA aktiviert haben.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **Fehler und Reaktionen** und erweitern Sie dann **Reaktion bei Hostfehler**.

5 Wählen Sie eine der folgenden Konfigurationsoptionen aus.

Option	Beschreibung
Fehlerreaktion	Wenn Sie **Deaktiviert** auswählen, wird mit dieser Einstellung die Hostüberwachung deaktiviert und VMs werden bei Hostfehlern nicht neu gestartet. Wenn Sie **VMs neu starten** auswählen, erfolgt für VMs ein Failover basierend auf ihrer Neustartpriorität, wenn bei einem Host ein Fehler auftritt.
Standardpriorität für den VM-Neustart	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. 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.
Bedingung für VM-Neustartpriorität	Eine bestimmte Bedingung sowie eine Verzögerung nach der Erfüllung dieser Bedingung müssen ausgewählt werden, bevor vSphere HA mit der nächsten VM-Neustartpriorität fortfahren darf.

6 Klicken Sie auf **OK**.

Ergebnisse

Ihre Einstellungen für die Reaktion bei Hostfehlern sind nun wirksam.

Reagieren auf Hostisolierung

Sie können bestimmte Reaktionen auf die Hostisolierung festlegen, die in Ihrem vSphere HA-Cluster auftreten kann.

Diese Seite kann nur bearbeitet werden, wenn Sie vSphere HA aktiviert haben.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **Fehler und Reaktionen** und erweitern Sie **Reaktion bei Hostisolierung**.

5 Um die Reaktion bei Hostisolierung zu konfigurieren, wählen Sie **Deaktiviert**, **VMs herunterfahren und neu starten** oder **VMs ausschalten und neu starten** aus.

6 Klicken Sie auf **OK**.

Ergebnisse

Ihre Einstellung für die Reaktion bei Hostisolierung ist nun wirksam.

Konfigurieren der VMCP-Reaktionen

Konfigurieren Sie, wie VM Component Protection (VMCP) reagiert, wenn bei einem Datenspeicher ein PDL- oder APD-Fehler auftritt.

Diese Seite kann nur bearbeitet werden, wenn Sie vSphere HA aktiviert haben.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **Fehler und Reaktionen** und erweitern Sie entweder **Datenspeicher mit PDL** oder **Datenspeicher mit APD**.

5 Wenn Sie auf **Datenspeicher mit PDL** klicken, können Sie die VMCP-Fehlerreaktion für diesen Problemtyp festlegen, und zwar entweder **Deaktiviert**, **Ereignisse ausgeben** oder **VMs ausschalten und neu starten**.

6 Wenn Sie auf **Datenspeicher mit APD** klicken, können Sie die Reaktion auf VMCP-Fehler für diesen Fehlertyp auf **Deaktiviert**, **Ereignisse ausgeben**, **VMs ausschalten und neu starten – konservative Neustartrichtlinie** oder **VMs ausschalten und neu starten – aggressive Neustartrichtlinie** festlegen. Darüber hinaus können Sie **Reaktion bei Wiederherstellung** festlegen. Hierbei wird angegeben, wie viele Minuten VMCP wartet, bevor eine Aktion ausgeführt wird.

7 Klicken Sie auf **OK**.

Ergebnisse

Ihre Einstellungen für die VMCP-Fehlerreaktion sind nun wirksam.

Aktivieren der VM-Überwachung

Sie können die VM- und Anwendungsüberwachung aktivieren sowie die Überwachungsempfindlichkeit für Ihren vSphere HA-Cluster festlegen.

Diese Seite kann nur bearbeitet werden, wenn Sie vSphere HA aktiviert haben.

Hinweis vSphere HA kann ein Failover einer nicht fehlerfreien VM auf einem fehlerfreien Host durchführen, wenn die VM-Überwachung deaktiviert ist. Der Host konnte aufgrund einer DRS-Empfehlung oder basierend darauf ausgewählt werden, welcher Host über die wenigsten verfügbaren Ressourcen verfügt.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **Fehler und Reaktionen** und erweitern Sie **VM-Überwachung**.

5 Wählen Sie **VM-Überwachung** und **Anwendungsüberwachung** aus.

   Mit diesen Einstellungen werden VMware Tools-Taktsignale bzw. Anwendungstaktsignale aktiviert.

6 Zum Einstellen der Empfindlichkeit der Taktsignal-Überwachung bewegen Sie den Schieberegler zwischen **Niedrig** und **Hoch**, oder wählen Sie **Benutzerdefiniert** aus, um benutzerdefinierte Einstellungen festzulegen.

7 Klicken Sie auf **OK**.

Ergebnisse

Ihre Überwachungseinstellungen sind nun wirksam.

Konfigurieren von Proactive HA

Sie können konfigurieren, wie Proactive HA reagiert, wenn ein Anbieter vCenter seine Beeinträchtigung des Systemzustands gemeldet hat, die auf einen Teilausfall dieses Hosts hinweist.

Diese Seite kann nur bearbeitet werden, wenn Sie vSphere DRS aktiviert haben.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Wählen Sie **Proactive HA einschalten** aus.

5 Klicken Sie auf **Proactive HA - Fehler und Reaktionen**.

6 Wählen Sie eine der folgenden Konfigurationsoptionen aus.

Option	Beschreibung
Automatisierungsebene	Bestimmen Sie, ob der Hostquarantäne- oder Wartungsmodus und VM-Migrationen Empfehlungen sind oder automatisch erfolgen. ■ **Manuell**. vCenter Server gibt Migrationsempfehlungen für virtuelle Maschinen. ■ **Automatisiert**. Virtuelle Maschinen werden auf funktionsfähige Hosts migriert, und fehlerhafte Hosts werden abhängig von der konfigurierten Proactive HA-Automatisierungsebene in den Quarantäne- oder Wartungsmodus versetzt.
Standardisierung	Bestimmen Sie, was mit teilweise fehlerhaften Hosts passiert. ■ **Quarantänemodus für alle Fehler**. Dieser Modus sorgt für Ausgewogenheit zwischen Leistung und Verfügbarkeit, indem die Nutzung von teilweise fehlerhaften Hosts vermieden wird, solange die Leistung der virtuellen Maschine nicht betroffen ist. ■ **Quarantänemodus für leichte und Wartungsmodus für schwerwiegende Fehler (gemischt)**. Dieser Modus sorgt für Ausgewogenheit zwischen Leistung und Verfügbarkeit, indem die Nutzung von leicht fehlerhaften Hosts vermieden wird, solange die Leistung der virtuellen Maschine nicht betroffen ist. Dieser Modus gewährleistet, dass virtuelle Maschinen nicht auf hochgradig fehlerhaften Hosts ausgeführt werden. ■ **Wartungsmodus für alle Fehler**. Dieser Modus gewährleistet, dass virtuelle Maschinen nicht auf teilweise fehlerhaften Hosts ausgeführt werden. Zum Versetzen von Hosts in den Quarantäne- und den Wartungsmodus sind jeweils `Host.Config.Quarantine`- und `Host.Config.Maintenance`-Berechtigungen erforderlich.

Aktivieren Sie die Kontrollkästchen, um Anbieter von Proactive HA für diesen Cluster zu aktivieren. Die Anbieter werden angezeigt, wenn das zugehörige vSphere Client-Plug-In installiert wurde. Die Anbieter überwachen jeden Host im Cluster. Klicken Sie zum Anzeigen oder Bearbeiten der vom Anbieter unterstützten Fehlerbedingungen auf den Bearbeitungslink.

7 Klicken Sie auf **OK**.

Konfigurieren der Zugangssteuerung

Nachdem Sie einen Cluster erstellt haben, können Sie die Zugangssteuerung konfigurieren, um anzugeben, ob virtuelle Maschinen gestartet werden können, wenn sie gegen Verfügbarkeitseinschränkungen 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.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **Zugangssteuerung**, um die Konfigurationsoptionen anzuzeigen.

5 Wählen Sie einen Wert für **Vom Cluster tolerierte Hostfehler** aus. Dieser Wert gibt die maximale Anzahl der Hostfehler an, bei denen der Cluster noch wiederhergestellt oder für die ein Failover garantiert werden kann.

6 Wählen Sie eine Option für **Definition der Failover-Kapazität des Hosts nach** aus.

Option	Beschreibung
Prozentsatz der Clusterressourcen	Geben Sie einen Prozentsatz für die CPU- und Arbeitsspeicherressourcen des Clusters an, der zusätzlich reserviert werden soll, um Failover zu unterstützen.
Richtlinie für Steckplatzgröße (eingeschaltete VMs)	Wählen Sie eine Richtlinie für Steckplatzgröße aus, die alle eingeschalteten VMs abdeckt oder eine bestimmte Größe aufweist. Sie können auch berechnen, wie viele VMs mehrere Steckplätze benötigen.
Dedizierte Failover-Hosts	Wählen Sie Hosts für Failover-Aktionen aus. Failover können immer noch auf anderen Hosts im Cluster erfolgen, wenn ein Standard-Failover-Host nicht über genügend Ressourcen verfügt.
Deaktiviert	Wählen Sie diese Option aus, um die Zugangssteuerung zu deaktivieren und das Einschalten von virtuellen Maschinen zu erlauben, die gegen Verfügbarkeitseinschränkungen verstoßen.

7 Legen Sie den Prozentsatz für die Option **Von VMs tolerierte Leistungseinbußen** fest.

Diese Einstellung bestimmt, welchen Prozentsatz für Leistungseinbußen die VMs im Cluster während eines Ausfalls tolerieren dürfen.

8 Klicken Sie auf **OK**.

Ergebnisse

Ihre Einstellungen für die Zugangssteuerung sind nun wirksam.

Konfigurieren der Taktsignal-Datenspeicher

vSphere HA verwendet Datenspeicher-Taktsignale, um ausgefallene Hosts und Hosts, die sich auf einer Netzwerkpartition befinden, voneinander zu unterscheiden. Mit Datenspeicher-Taktsignalen kann vSphere HA Hosts überwachen, wenn eine Verwaltungsnetzwerkpartition erfolgt, und weiterhin auf Fehler reagieren.

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

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

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

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

Tabelle 2-3.

Datenspeicher-Taktsignaloptionen
Automatisch Datenspeicher auswählen, auf die über den Host zugegriffen werden kann
Nur Datenspeicher 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.

Verfahren

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Wählen Sie **vSphere Availability** aus und klicken Sie auf **Bearbeiten**.

4 Klicken Sie auf **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**.

Ergebnisse

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

Nächste Schritte

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

- Den Wert mit vSphere 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.

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

Option	Beschreibung
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 Zugangssteuerungs-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 einen beliebigen Wert größer oder gleich 0 festgelegt werden. Wenn Sie die Einstellung auf 0 festlegen, 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.
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.
das.config.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.

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

Option	Beschreibung
das.respectvmvmantiaffinityrules	Ermittelt, ob vSphere HA VM-VM-Anti-Affinitätsregeln erzwingt. Der Standardwert ist „true“, und 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. Diese Option kann auch auf „falsch“ festgelegt werden; dann werden die Regeln nicht erzwungen. 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.
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.

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

Option	Beschreibung
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 Wahlen des primären Agenten in einem großen Cluster (mit 6.000 bis 8.000 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.
das.reregisterrestartdisabledvms	Wenn vSphere HA für eine bestimmte VM deaktiviert ist, wird mit dieser Option sichergestellt, dass die VM nach einem Fehler auf einem anderen Host registriert wird. Auf diese Weise können Sie diese VM einschalten, ohne sie erneut manuell registrieren zu müssen. **Hinweis** Bei Verwendung dieser Option schaltet vSphere HA die VM nicht ein, sondern registriert sie lediglich.
das.respectvmhostsoftaffinityrules	Legt fest, ob vSphere HA eine entsprechende virtuelle Maschine auf einem Host neu startet, der zu derselben VM-Host-Gruppe gehört. Wenn kein solcher Host verfügbar ist oder wenn der Wert dieser Option auf „False“ festgelegt ist, startet vSphere HA die VM auf einem beliebigen verfügbaren Host im Cluster neu. In vSphere 6.5 oder höher lautet der Standardwert „true“. In den erweiterten HA-Optionen des Clusters ist dieser Wert möglicherweise nicht sichtbar definiert. Wenn Sie die Option deaktivieren möchten, müssen Sie diese in den erweiterten HA-Optionen für den Cluster manuell als „false“ festlegen.

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.

Verfahren

1. Navigieren Sie im vSphere Client zum vSphere HA-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „Konfiguration“ 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**, **Reaktion bei Hostisolierung**, 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**.

Ergebnisse

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

Best Practices für VMware vSphere® High Availability-Cluster

Um die optimale Leistung eines vSphere HA-Clusters gewährleisten zu können, müssen Sie bestimmte Best Practices berücksichtigen. 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*.

Empfohlene Vorgehensweisen 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 unerwünschten 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, muss der vSphereHA-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, müssen 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 Verwaltungsdatenverkehr des vSphere HA-Agents auf den angegebenen Netzwerken zu halten, 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-Agents 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 daher 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. Verwenden Sie die erweiterte Option `das.isolationaddress[...]`, um weitere Netzwerkisolierungsadressen hinzuzufügen. Weitere Informationen hierzu finden Sie unter Erweiterte vSphere HA-Optionen.

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 potenziellen Fehlerstellen gerechnet werden.

Verwenden von IPv6-Netzwerkkonfigurationen

Nur eine IPv6-Adresse kann 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 ohne entsprechenden Nutzen vom primären Host des Clusters gesendet werden.

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

Im Cluster, in dem sich ESXi 5.x-Hosts und Hosts mit der Version ESX /ESXi 4.1 oder früher befinden und in dem Storage vMotion intensiv genutzt wird oder Storage DRS aktiviert ist, sollten Sie vSphere HA nicht bereitstellen. vSphere HA reagiert möglicherweise auf einen Hostausfall mit einem Neustart einer virtuellen Maschine auf einem Host mit einer ESXi-Version, die sich von der Version des Hosts unterscheidet, auf dem die virtuelle Maschine vor dem Auftreten des Fehlers ausgeführt wurde. Ein Problem kann auftreten, wenn die virtuelle Maschine zum Zeitpunkt des Ausfalls an einer Storage vMotion-Aktion auf einem ESXi 5.x-Host beteiligt war und vSphere HA die virtuelle Maschine auf einem Host mit einer früheren Version als ESXi 5.0 neu startet. Während die virtuelle Maschine möglicherweise eingeschaltet wird, beschädigen alle im Anschluss durchgeführten Snapshot-Vorgänge möglicherweise den vdisk-Zustand, sodass die virtuelle Maschine nicht mehr verwendet werden kann.

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 Hosts installiert wird. Weitere Informationen finden Sie in der Dokumentation zu Auto Deploy im Installations- und Einrichtungshandbuch für vSphere.

Upgrade der Hosts in einem Cluster unter Verwendung von vSAN

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 vSAN verwenden möchten.

1 Führen Sie ein Upgrade für alle Hosts durch.

2 Deaktivieren Sie vSphere HA.

3 Aktivieren Sie vSAN.

4 Aktivieren Sie vSphere HA erneut.

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)
- Primärer Cluster 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.

Verhaltensänderung für HA-VIBs

In vSphere 7.0 oder höher ist es möglich, dass die HA-VIBs möglicherweise in einigen Fällen entfernt werden, wenn HA auf einem Lifecycle Manager (vLCM)-Cluster aktiviert ist. In früheren Versionen versucht vCenter nicht, HA-VIBs von ESXi-Hosts zu entfernen.

Diese Situation kann nur auf vLCM-Clustern mit Aktivierung von vSphere HA erfolgen. Wenn nach der Deaktivierung von vSphere HA auf dem Cluster ein **Standardisieren**-Vorgang für vLCM auftritt (entweder als vom Benutzer initiierter Vorgang oder als API-Aufruf), werden die vSphere HA-VIBs möglicherweise als Folge davon entfernt.

Hinweis Diese Verhaltensänderung ist harmlos, da vCenter die erforderlichen vSphere HA-VIBs verschiebt, wenn HA wieder aktiviert wird.

Aktivieren der Fault Tolerance für virtuelle Maschinen

3

Sie können vSphere Fault Tolerance für Ihre virtuellen Maschinen verwenden, um die Kontinuität mit höherer Verfügbarkeit und besserem Datenschutz sicherzustellen.

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

Um mit Fault Tolerance optimale Ergebnisse zu erzielen, müssen 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.

Lesen Sie als Nächstes die folgenden Themen:

- Wie Fault Tolerance funktionert
- Beispiele für die Nutzen der Fault Tolerance
- Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance
- Fault Tolerance-Interoperabilität
- Vorbereiten Ihrer Cluster und Hosts für Fault Tolerance
- Verwenden von Fault Tolerance
- Aktivieren der Fault Tolerance-Verschlüsselung
- Best Practices für Fault Tolerance
- Aktivieren der Fault Tolerance für Metro-Cluster
- Legacy Fault Tolerance
- Fehlerbehebung bei fehlertoleranten virtuellen Maschinen

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 primäre virtuelle Maschine wird kontinuierlich auf die sekundäre virtuelle Maschine repliziert, sodass die sekundäre virtuelle Maschine jederzeit einspringen kann. Sie bietet dadurch 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 der Host, auf dem die primäre VM ausgeführt wird, ausfällt oder im Arbeitsspeicher der primären VM einen nicht behebbaren Hardwarefehler erkennt. In diesem Fall wird sofort die sekundäre VM aktiviert, um die primäre VM 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 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 acht vCPUs eingerichtet werden.

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. Mit dem von vSphere HA bereitgestellten Failover werden die von dem Fehler betroffenen virtuellen Maschinen neu gestartet.

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 verfügbar sein müssen, vor allem Anwendungen, die langanhaltende Clientverbindungen aufweisen, die Benutzer während 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. 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.

Hinweis Fault Tolerance wird derzeit nicht für die Aktivierung auf einer VM unterstützt, die eine von NSX T erstellte Portgruppe (VLAN oder Overlay-Segment) verwendet. Fault Tolerance wird auch für NSX T Manager und Edge-Knoten nicht unterstützt.

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. Der Standardwert ist 4. Es gibt keine Höchstzahl an FT-VMs pro Host. Sie können eine größere Anzahl verwenden, wenn die Arbeitslast in den FT-VMs ordnungsgemäß ausgeführt wird. Sie können die Überprüfung deaktivieren, indem Sie den Wert auf **0** festlegen.

das.maxftvcpusperhost

Die maximale Anzahl an vCPUs, die für alle fehlertoleranten VMs auf einem Host zusammengefasst werden. Der Standardwert ist 8. Es gibt keine Höchstzahl an FT-vCPUs pro Host. Sie können eine größere Anzahl verwenden, wenn die Arbeitslast ordnungsgemäß ausgeführt wird. Sie können die Überprüfung deaktivieren, indem Sie den Wert auf **0** festlegen.

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 8 vCPUs zulässig

Hinweis Fault Tolerance wird in vSphere Standard-, vSphere Enterprise- und vSphere Enterprise Plus-Editionen unterstützt.

Fault Tolerance-Interoperabilität

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

Hinweis Vor vSphere 7.0 Update 2 wurde vSphere Virtual Machine Encryption nicht mit FT 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.
- Datenspeicher für Virtual Volumes (VVOL)
- Speicherbasierte Richtlinienverwaltung Speicherrichtlinien werden für vSAN-Speicher unterstützt.
- I/O-Filter
- VBS-fähige virtuelle Maschinen
- VM-Namespace-DB und VM-DataSets.

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.
Geräte im laufenden Betrieb wechseln.	Die Funktion zum Wechseln von Geräten im laufenden Betrieb wird für fehlertolerante virtuelle Maschinen automatisch 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.
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 mit vSphere Distributed Resource Scheduler (DRS) verwenden.

Fault Tolerance-VMs benötigen keine EVC, um DRS zu unterstützen. Sie können Fault Tolerance mit DRS auf vSphere 6.5- und 6.0-Hosts verwenden, die von einem vSphere 6.7-VC oder höher verwaltet werden.

Hinweis Bei vSphere DRS handelt es sich um eine wichtige vSphere-Funktion, die zum Aufrechterhalten der Integrität der in einem vSphere-Cluster ausgeführten Arbeitslasten benötigt wird. Ab vSphere 7.0 Update 1 hängt DRS von der Verfügbarkeit der vCLS-VMs ab. Weitere Informationen finden Sie unter *vSphere Cluster Services (vCLS)* in *Handbuch zur vSphere-Ressourcenverwaltung*.

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 einzurichten:

- 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. Weitere Informationen hierzu finden Sie unter Fault Tolerance einschalten.

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. Weitere Informationen hierzu finden Sie unter Konfigurieren von Netzwerken für Hostmaschinen.

- vSphere HA-Cluster wurden erstellt und aktiviert. Weitere Informationen hierzu finden Sie unter Erstellen eines vSphere HA-Clusters. 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 #unique_60 beschrieben sind, um die Kompatibilität der Hosts im Cluster zum Unterstützen von Fault Tolerance zu bestätigen.

VM-Anforderungen für Fault Tolerance

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

- Es dürfen keine nicht unterstützten Geräte mit den virtuellen Maschinen verbunden sein. Weitere Informationen hierzu finden Sie unter Fault Tolerance-Interoperabilität.
- Nicht kompatible Funktionen dürfen nicht mit den fehlertoleranten virtuellen Maschinen ausgeführt werden. Weitere Informationen hierzu finden Sie unter Fault Tolerance-Interoperabilität.
- VM-Dateien (außer VMDK-Dateien) müssen in gemeinsam genutztem Speicher gespeichert werden. Geeignete Lösungen für freigegebenen Speicher sind unter anderem Fibre Channel, iSCSI (Hardware und Software), vSAN, 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.
- 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 einzurichten, 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. Weitere Informationen hierzu finden Sie unter Anforderungen, Grenzwerte und Lizenzierung für Fault Tolerance.

Verfahren

1. Navigieren Sie zum Host im vSphere Client.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Netzwerk**.
3. Wählen Sie **VMkernel-Adapter** aus.
4. Klicken Sie auf das Symbol **Netzwerk hinzufügen**.
5. Geben Sie entsprechende Informationen für Ihren Verbindungstyp an.

6 Klicken Sie auf **Beenden**.

Ergebnisse

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.

Nächste Schritte

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.

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-Zertifikatsprüfung muss in den vCenter Server-Einstellungen aktiviert werden.
- 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.
- 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-aktivierte 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 im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php nach und wählen Sie **Search by Fault Tolerant Compatible Sets** aus.
- 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 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 Fault Tolerance ausgeschaltet wird, werden geänderte Parameter nicht auf ihre ursprünglichen Werte zurückgesetzt.

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

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.

Verfahren

1. Navigieren Sie im vSphere 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**.

Ergebnisse

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.

Hinweis Daten- und Arbeitsspeicher der VM werden während der FT-Aktivierung repliziert. Je nach Umfang der replizierten Daten kann dies einige Minuten dauern. Der Status der VM wird erst nach Abschluss der Replizierung als geschützt angezeigt.

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.

Verfahren

1 Navigieren Sie im vSphere 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**.

Ergebnisse

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

Hinweis Fault Tolerance kann nicht deaktiviert werden, wenn die sekundäre virtuelle Maschine gestartet wird. Da dies die Synchronisierung des vollständigen Status der primären VM auf die sekundäre VM umfasst, kann dieser Vorgang mehr Zeit in Anspruch nehmen als erwartet.

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.

Verfahren

1. Navigieren Sie im vSphere 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**.

Ergebnisse

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.

Nächste Schritte

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.

Verfahren

1. Navigieren Sie im vSphere 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.

Ergebnisse

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.

Verfahren

1. Navigieren Sie im vSphere 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.

Ergebnisse

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.

Verfahren

1 Navigieren Sie im vSphere 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.

Ergebnisse

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.

Verfahren

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.

Ergebnisse

Es wird ein Upgrade aller ESXi-Hosts in einem Cluster durchgeführt.

Aktivieren der Fault Tolerance-Verschlüsselung

Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

vSphere Fault Tolerance führt häufige Prüfungen zwischen einer primären und einer sekundären VM durch, damit die sekundäre VM vom letzten erfolgreichen Prüfpunkt aus schnell fortgesetzt werden kann. Der Prüfpunkt enthält den VM-Status, der seit dem vorherigen Prüfpunkt geändert wurde. Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

Wenn Sie Fault Tolerance aktivieren, ist die FT-Verschlüsselung standardmäßig auf **Opportunistisch** festgelegt. Dies bedeutet, dass die Verschlüsselung nur aktiviert wird, wenn sowohl der primäre als auch der sekundäre Host verschlüsselt werden können. Befolgen Sie dieses Verfahren, wenn Sie den FT-Verschlüsselungsmodus manuell ändern müssen.

Hinweis Fault Tolerance unterstützt vSphere Virtual Machine Encryption mit vSphere 7.0 Update 2 und höher. Gastinterne und Array-basierte Verschlüsselung sind nicht von der VM-Verschlüsselung abhängig und stören sie nicht. Bei Verwendung mehrerer Verschlüsselungsschichten werden zusätzliche Computing-Ressourcen verwendet, was sich auf die Leistung der virtuellen Maschine auswirken kann. Die Auswirkung variiert je nach Hardware sowie der Menge und dem Typ der E/A, aber die Auswirkungen auf die Gesamtleistung sind für die meisten Arbeitslasten vernachlässigbar. Die Effektivität und Kompatibilität von Back-End-Speicherfunktionen wie Deduplizierung, Komprimierung und Replizierung kann auch von der VM-Verschlüsselung betroffen sein.

Voraussetzungen

Die FT-Verschlüsselung erfordert SMP-FT. Eine Verschlüsselung auf Legacy FT (Record-Replay FT) wird nicht unterstützt.

Verfahren

1 Wählen Sie die VM und dann **Einstellungen bearbeiten** aus.

2 Wählen Sie unter **VM-Optionen** das Dropdown-Menü **Verschlüsselte FT** aus.

3 Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Deaktiviert	Schalten Sie die verschlüsselte Fault Tolerance-Protokollierung nicht ein.
Opportunistisch	Aktivieren Sie die Verschlüsselung nur, wenn beide Seiten dazu in der Lage sind. Eine Fault Tolerance-VM kann auf einen ESXi-Host verschoben werden, der keine verschlüsselte Fault Tolerance-Protokollierung unterstützt.
Erforderlich	Wählen Sie Hosts für die primäre und sekundäre Fault Tolerance aus, die beide die verschlüsselte FT-Protokollierung unterstützen.

Hinweis Während die VM-Verschlüsselung aktiviert ist, ist der FT-Verschlüsselungsmodus standardmäßig auf **Erforderlich** festgelegt und kann nicht geändert werden.

Wenn der FT-Verschlüsselungsmodus auf **Erforderlich** festgelegt ist:

- Wenn Sie FT aktivieren, werden nur Hosts für die Platzierung der sekundären FT-Verschlüsselung aufgelistet, welche die FT-Verschlüsselung unterstützen.
- FT-Failover kann nur auf den von der FT-Verschlüsselung unterstützten Hosts erfolgen.

4 Klicken Sie auf **OK**.

Best Practices für Fault Tolerance

Um optimale Fault Tolerance-Ergebnisse erzielen zu können, sollten Sie bestimmte Best Practices 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, andernfalls könnte es sein, dass die sekundären virtuellen Maschinen häufiger neu gestartet werden. Plattform-Energieverwaltungsfunktionen, die sich nicht abhängig von der Arbeitslast anpassen (z. B. die Energiebeschränkung und erzwungene Niedrigfrequenzmodi zum Einsparen von Energie), können große Abweichungen der Prozessorfrequenzen verursachen. Falls sekundäre virtuelle Maschinen regelmäßig neu gestartet werden, deaktivieren Sie alle Energieverwaltungsmodi auf den Hosts, die fehlertolerante virtuelle Maschinen ausführen, oder stellen Sie sicher, dass alle Hosts im selben Energieverwaltungsmodus laufen.

Hostnetzwerkkonfiguration

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

- Verteilen Sie jede Netzwerkkartengruppe über zwei physische Switches, um die L2-Domänenkontinuität für jedes VLAN zwischen den zwei physischen Switches zu gewährleisten.
- Verwenden Sie deterministische Gruppierungsrichtlinien, um sicherzugehen, dass bestimmte Datenverkehrstypen eine Affinität mit einer bestimmten Netzwerkkarte (Aktiv/Standby) bzw. mit mehreren Netzwerkkarten (z. B. ID des virtuellen Quell-Ports) haben.
- Paaren Sie Datenverkehrstypen dort, wo Aktiv/Standby-Richtlinien verwendet werden, um in einer Failoversituation die Auswirkungen zu minimieren, wenn beide Datenverkehrstypen eine 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 Tolerance-Protokollierung zwischen den primären und sekundären virtuellen Maschinen erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr kann vertrauliche Daten enthalten, wie z. B. Kennwörter im Klartext. Um zu verhindern, dass solche Daten preisgegeben werden, stellen Sie sicher, dass dieses Netzwerk gesichert ist, insbesondere gegen so genannte „Man-in-the-middle“-Angriffe. Verwenden Sie z. B. ein privates Netzwerk für den Datenverkehr für die Fault Tolerance-Protokollierung.

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.
- Dieselben 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 Bandbreite, die für den Protokollierungsdatenverkehr zwischen primären und sekundären virtuellen Maschinen verfügbar ist, eine 10 Gbit-Netzwerkkarte und aktivieren Sie die Verwendung von Jumbo-Frames.

Sie können mehrere Netzwerkkarten für das Fault Tolerance-Protokollierungsnetzwerk auswählen. Indem Sie mehrere Netzwerkkarten auswählen, können Sie die Bandbreite mehrerer Netzwerkkarten nutzen, auch wenn nicht alle Netzwerkkarten für die Ausführung von Fault Tolerance reserviert sind.

Speichern von ISOs auf gemeinsam genutztem Speicher für einen unterbrechungsfreien Zugriff

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

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. Weitere Informationen hierzu finden Sie unter Netzwerkpartitionen . Wenn eine Partition eintritt, wird der Schutz durch Fault Tolerance möglicherweise herabgestuft.

In einem partitionierten vSphere HA-Cluster mit Fault Tolerance kann sich die primäre virtuelle Maschine (oder ihre sekundäre virtuelle Maschine) in einer Partition befinden, die von einem primären 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 primären Host verwaltet wird, der für die virtuelle Maschine verantwortlich ist.

Um die Chancen zu verringern, dass bei Ihrem Verwaltungsnetzwerk ein Fehler auftritt, der zu einer Netzwerkpartition führt, befolgen Sie die Empfehlungen unter Empfohlene Vorgehensweisen für Netzwerke.

Verwenden von vSAN-Datenspeichern

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

- Ein Mix aus vSAN und anderen Typen von Datenspeichern wird sowohl für primäre VMs als auch für sekundäre VMs nicht unterstützt.

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

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

Aktivieren der Fault Tolerance für Metro-Cluster

In vSphere 8.0 U3 können Sie die Fault Tolerance des Metro-Clusters im Fault Tolerance-Assistenten aktivieren.

Im Fault Tolerance-Assistenten können Sie ein Kontrollkästchen mit der Bezeichnung **Fault Tolerance für Metro-Cluster aktivieren** aktivieren, um die FT-Metro-Cluster-Funktionalität zu aktivieren. Darüber hinaus steht eine Dropdown-Liste zur Auswahl einer Hostgruppe als bevorzugten Speicherort der FT-VM zur Verfügung. Standardmäßig sind das Kontrollkästchen und die Dropdown-Liste deaktiviert. Das gibt an, dass der FT-Metro-Cluster für die VM deaktiviert ist (`ConfigInfo.metroFtEnabed ist „FALSE“`).

Wenn das Kontrollkästchen aktiviert ist, wird die Dropdown-Liste für die Auswahl einer Hostgruppe aktiviert. Der Assistent verhindert, dass mit dem nächsten Schritt fortgefahren wird, wenn keine Hostgruppe für die VM ausgewählt ist. Um die Rechtmäßigkeit der ausgewählten Hostgruppe sicherzustellen, ruft der Assistent die Funktion `queryFaultToleranceCompatibleHosts` auf und ruft das Ergebnis über die zurückgegebenen Meldungen ab.

Bevor Sie das Kontrollkästchen **Fault Tolerance für Metro-Cluster aktivieren** aktivieren, ist die Dropdown-Liste „Hostgruppe“ deaktiviert. Eine Wegweiserschaltfläche wird neben der Bezeichnung `Hostgruppe` hinzugefügt. Der Inhalt des Wegweisers lautet: `Je nach ausgewählter Hostgruppe kann FT die Hosts im Cluster in zwei Gruppen unterteilen und sicherstellen, dass der primäre FT-Host und der sekundäre FT-Host in verschiedenen Gruppen platziert werden.`

Nach dem Aktivieren des Kontrollkästchens **Fault Tolerance für Metro-Cluster aktivieren** wird die Dropdown-Liste für die Hostgruppenauswahl im Assistenten aktiviert. FT verarbeitet die Validierungsprüfung für „FT-Metro-Cluster“-Flag und Hostgruppe, die durch Klicken auf die Schaltfläche **WEITER** ausgelöst wird. Der Assistent legt **FaultToleranceConfigSpec.metroFtEnabled** auf **TRUE** und **FaultToleranceConfigSpec.preferredLocation** auf die ausgewählte Hostgruppe fest. Anschließend ruft der Assistent die Liste der kompatiblen Hosts ab.

Wenn Sie das Kontrollkästchen **Fault Tolerance für Metro-Cluster aktivieren** aktivieren, aber keine Hostgruppe auswählen, kann der Assistent nicht über die Schaltfläche **WEITER** fortfahren. Es wird folgende Fehlermeldung angezeigt: `Weisen Sie eine Hostgruppe für die Fault Tolerance-VM zu, bevor Sie den Metro-Cluster aktivieren.` FT überprüft auch die Hostgruppe auf die FT-Metro-Cluster-aktivierte VM. Die Aufgabe schlägt möglicherweise fehl, wenn die Hostgruppe nicht konfiguriert ist.

Sie können die konfigurierte Hostgruppe entfernen, während die FT-VM ausgeführt wird. FT-Metro-Cluster ist in diesem Fall deaktiviert. Der Name der Hostgruppe wird jedoch weiterhin auf der FT-Informationskarte angezeigt, da der FT-Metro-Cluster nach der erneuten Konfiguration der Hostgruppe erneut aktiviert werden kann.

Wenn Sie die Hostgruppe für eine ausgeführte FT-VM löschen, wird der FT-Metro-Cluster deaktiviert. Im Falle eines Failovers wird `Status des Metro-Clusters nicht anwendbar, Hostgruppe fehlt.` auf der FT-Informationskarte angezeigt. Wenn Sie die Hostgruppe jedoch wieder hinzufügen, wird der FT-Metro-Cluster erneut aktiviert.

Wenn Sie die Hostgruppe für eine ausgeschaltete FT-VM löschen, kann die sekundäre Fault-Tolerance-VM nicht eingeschaltet werden.

Legacy Fault Tolerance

VMs mit einer Fault Tolerance-Legacy-Version können nur auf ESXi-Hosts vorhanden sein, auf denen ältere vSphere-Versionen als Version 6.5 ausgeführt werden.

Die Unterstützung von vSphere Fault Tolerance basierte bei ESXi-Hosts vor Version 6.5 auf einer anderen Technologie. Wenn Sie derzeit eine dieser Legacy-Versionen von Fault Tolerance verwenden und dies weiterhin erforderlich ist, empfehlen wir Ihnen, eine vCenter 6.0-Instanz zur Verwaltung des Pools von älteren Hosts (vor Version 6.5) zu reservieren, die zur Ausführung dieser virtuellen Maschinen benötigt werden. vCenter 6.0 war die letzte Version, die alle erforderlichen Funktionen zur Verwaltung von virtuellen Maschinen bot, die durch eine Fault Tolerance-Legacy-Version geschützt sind. Weitere Informationen zu Fault Tolerance-Legacy-Versionen finden Sie in der Dokumentation zur vSphere-Verfügbarkeit für Version 6.0.

Fehlerbehebung bei fehlertoleranten virtuellen Maschinen

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

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

Darüber hinaus enthält der VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1033634 Informationen zur Fehlerbehebung bei der Verwendung von Fault Tolerance. Dieser Artikel enthält eine Liste von Fehlermeldungen, die möglicherweise ausgegeben werden, wenn Sie versuchen, diese Funktion zu verwenden, sowie ggf. Hinweise zum Beheben des jeweiligen Fehlers.

Hardwarevirtualisierung nicht aktiviert

Sie müssen die Hardwarevirtualisierung (HV) aktivieren, bevor Sie vSphere Fault Tolerance verwenden können.

Problem

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

Ursache

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

Lösung

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

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

Kompatible Hosts, die für die sekundäre virtuelle Maschine nicht verfügbar sind

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

Problem

Möglicherweise wird die folgende Fehlermeldung angezeigt:

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

Ursache

Dies kann aus mehreren Gründen auftreten, z. B. weil es keine weiteren Hosts im Cluster gibt, weil es keine anderen Hosts mit aktivierter HV gibt, weil die Hardware-MMU-Virtualisierung von Host-CPUs nicht unterstützt wird, weil die Datenspeicher unzugänglich sind, weil keine Kapazität verfügbar ist oder weil sich die Hosts im Wartungsmodus befinden.

Lösung

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

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

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

Problem

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

Ursache

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

Lösung

Wenn sich die sekundäre virtuelle Maschine auf einem überlasteten Host befindet, können Sie die virtuelle Maschine in einen anderen Speicherort ohne Probleme mit Ressourcenkonflikten verschieben. Führen Sie dazu im Einzelnen die folgenden Schritte aus:

- Verwenden Sie für FT-Netzwerkkonflikte die vMotion-Technologie zum Verschieben der sekundären virtuellen Maschine auf einen Host mit weniger FT-VMs, die Konflikte im FT-Netzwerk verursachen. Stellen Sie sicher, dass die Qualität des Speicherzugriffs auf die virtuelle Maschine nicht asymmetrisch ist.
- Bei Problemen mit Speicherkonflikten deaktivieren und aktivieren Sie FT erneut. Ändern Sie bei der Neuerstellung der sekundären virtuellen Maschine deren Datenspeicher in einen Speicherort mit weniger Ressourcenkonflikten und einem besseren Leistungspotenzial.
- Legen Sie zum Beheben eines CPU-Ressourcenproblems eine explizite CPU-Reservierung für die primäre virtuelle Maschine mit einem MHz-Wert fest, der zum Ausführen der Arbeitslast bei dem gewünschten Leistungsniveau ausreicht. Diese Reservierung wird sowohl bei der primären als auch bei der sekundären virtuellen Maschine angewendet, um sicherzustellen, dass beide virtuellen Maschinen mit der angegebenen Geschwindigkeit ausgeführt werden können. Die Leistungsdiagramme der virtuellen Maschinen (bevor Fault Tolerance aktiviert wurde) zeigen auf, wie viele CPU-Ressourcen unter normalen Bedingungen verbraucht werden, und können somit als Hilfe beim Einstellen dieser Reservierung dienen.

Höhere Netzwerklatenz bei Fault Tolerance-VMs

Wenn Ihr Fault Tolerance (FT)-Netzwerk nicht optimal konfiguriert ist, können Latenzprobleme bei den FT-VMs auftreten.

Problem

FT-VMs können eine variable Zunahme der Paketlatenz verzeichnen (im Millisekundenbereich). Bei Anwendungen, die sehr niedrige Werte für Netzwerkpaketlatenz oder Jitter erfordern (z. B. bestimmte Echtzeitanwendungen), kann ein Leistungsabfall auftreten.

Ursache

Eine gewisse Zunahme der Netzwerklatenz entspricht dem erwarteten Overhead für Fault Tolerance, aber bestimmte Faktoren können diese Latenz erhöhen. Wenn beispielsweise das FT-Netzwerk eine Verbindung mit einer besonders hohen Latenz verwendet, wird diese Latenz an die Anwendungen weitergegeben. Darüber hinaus kann eine höhere Latenz auftreten, wenn das FT-Netzwerk nicht genügend Bandbreite aufweist (weniger als 10 GBit/s).

Lösung

Stellen Sie sicher, dass das FT-Netzwerk genügend Bandbreite aufweist (mindestens 10 GBit/s) und eine Verbindung mit niedriger Latenz zwischen der primären virtuellen Maschine und der sekundären virtuellen Maschine verwendet. Durch diese Vorsichtsmaßnahmen wird die Netzwerklatenz nicht minimiert, aber deren potenzielle Auswirkungen werden abgeschwächt.

Manche Hosts sind mit virtuellen FT-Maschinen überlastet

Leistungsprobleme können auftreten, wenn die FT-VMs ungleichmäßig auf die Hosts Ihres Clusters verteilt sind.

Problem

Manche Hosts im Cluster sind möglicherweise mit FT-VMs überlastet, während andere Hosts nicht genutzte Ressourcen aufweisen.

Ursache

vSphere DRS führt für FT-VMs keinen Lastausgleich aus (außer bei Verwendung von Legacy-FT). Aufgrund dieser Beschränkung kann es sein, dass bei einem Cluster die FT-VMs ungleichmäßig auf die Hosts verteilt sind.

Lösung

Verteilen Sie mithilfe von vSphere vMotion die FT-VMs manuell im Cluster. Im Allgemeinen gilt: je weniger FT-VMs auf einem Host vorhanden sind, desto besser ist deren Leistung aufgrund der geringeren Konflikte bei FT-Netzwerkbandbreite und CPU-Ressourcen.

Verlust des Zugriffs auf FT-Metadaten-Datenspeicher

Der Zugriff auf den Fault Tolerance-Metadaten-Datenspeicher spielt für die ordnungsgemäße Funktionsweise einer FT-VM eine wichtige Rolle. Der Verlust dieses Zugriffs kann eine Reihe von Problemen verursachen.

Problem

Hierzu zählen die folgenden Probleme:

- FT wird unerwartet beendet.

- Wenn sowohl die primäre virtuelle Maschine als auch die sekundäre virtuelle Maschine nicht auf den Metadaten-Datenspeicher zugreifen können, schlagen die virtuellen Maschinen möglicherweise unerwartet fehl. In der Regel tritt ein nicht damit in Zusammenhang stehender Fehler, der FT beendet, auch dann auf, wenn beide virtuellen Maschinen nicht mehr auf den FT-Metadaten-Datenspeicher zugreifen können. vSphere HA versucht dann, die primäre virtuelle Maschine auf einem Host mit Zugriff auf den Metadaten-Datenspeicher erneut zu starten.
- Die virtuelle Maschine wird von vCenter Server möglicherweise nicht mehr als FT-VM erkannt. Aufgrund der fehlgeschlagenen Erkennung können möglicherweise nicht unterstützte Vorgänge wie z. B. das Erstellen von Snapshots auf der virtuellen Maschine ausgeführt und Probleme verursacht werden.

Ursache

Der fehlende Zugriff auf den Fault Tolerance-Metadaten-Datenspeicher kann zu den oben aufgeführten unerwünschten Ergebnissen führen.

Lösung

Platzieren Sie bei der Planung Ihrer FT-Bereitstellung den Metadaten-Datenspeicher auf hochverfügbarem Speicher. Wenn während der Ausführung von FT der Zugriff auf den Metadaten-Datenspeicher auf der primären virtuellen Maschine oder der sekundären virtuellen Maschine verloren geht, kümmern Sie sich unverzüglich um das Speicherproblem, bevor der Verlust des Zugriffs eines der vorhergehenden Probleme verursacht. Wenn eine virtuelle Maschine von vCenter Server nicht mehr als FT-VM erkannt wird, sollten Sie auf der virtuellen Maschine keine nicht unterstützten Vorgänge ausführen. Stellen Sie den Zugriff auf den Metadaten-Datenspeicher wieder her. Nachdem der Zugriff für die FT-VMs wiederhergestellt wurde und der Aktualisierungszeitraum abgelaufen ist, werden die virtuellen Maschinen erkannt.

Einschalten von vSphere FT für eingeschaltete VM schlägt fehl

Wenn Sie versuchen, vSphere Fault Tolerance für eine eingeschaltete VM zu aktivieren, kann dieser Vorgang fehlschlagen.

Problem

Wenn Sie **Fault Tolerance einschalten** für eine eingeschaltete VM auswählen, schlägt der Vorgang fehl und die Meldung `Unbekannter Fehler` wird angezeigt.

Ursache

Dieser Vorgang kann fehlschlagen, wenn der Host, auf dem die VM ausgeführt wird, nicht über genügend Arbeitsspeicherressourcen zum Bereitstellen von Fehlertoleranzschutz verfügt. vSphere Fault Tolerance versucht automatisch, den ganzen Arbeitsspeicher auf dem Host für die VM zu reservieren. Für fehlertolerante VMs ist Overhead-Arbeitsspeicher erforderlich,

der manchmal bis zu 1 bis 2 GB groß sein kann. Wenn die eingeschaltete VM auf einem Host ausgeführt wird, der nicht über genügend Arbeitsspeicherressourcen verfügt, um den reservierten Speicher sowie den Overhead-Arbeitsspeicher bereitzustellen, tritt beim Aktivieren von Fault Tolerance ein Fehler auf. Die Meldung `Unbekannter Fehler` wird dann angezeigt.

Lösung

Wählen Sie eine der folgenden Lösungen aus:

- Machen Sie Arbeitsspeicherressourcen auf dem Host verfügbar, damit der reservierte Arbeitsspeicher und der zusätzliche Overhead zur Verfügung stehen.
- Verschieben Sie die virtuelle Maschine auf einen Host mit reichlich freien Arbeitsspeicherressourcen und versuchen Sie es noch einmal.

Fehlertolerante virtuelle Maschinen, die durch vSphere DRS nicht platziert oder entfernt wurden

Fehlertolerante virtuelle Maschinen in einem Cluster, die mit vSphere DRS aktiviert sind, funktionieren nicht ordnungsgemäß, wenn Enhanced vMotion Compatibility (EVC) deaktiviert ist.

Problem

Da EVC eine Voraussetzung für die Verwendung von DRS mit fehlertoleranten virtuellen Maschinen ist, werden diese von DRS nicht platziert oder entfernt, wenn EVC deaktiviert wurde (selbst wenn es später wieder aktiviert wird).

Ursache

Wenn EVC auf einem DRS-Cluster deaktiviert ist, kann eine VM-Außerkraftsetzung, die DRS auf einer fehlertoleranten virtuellen Maschine deaktiviert, hinzugefügt werden. Selbst wenn EVC später wieder aktiviert wird, bleibt diese Außerkraftsetzung wirksam.

Lösung

Wenn DRS fehlertolerante virtuelle Maschinen im Cluster nicht platziert oder entfernt, prüfen Sie die VMs auf eine VM-Außerkraftsetzung, die DRS deaktiviert. Wenn Sie eine Außerkraftsetzung finden, die DRS. deaktiviert, entfernen Sie sie.

Hinweis Weitere Informationen zum Bearbeiten oder Löschen von VM-Außerkraftsetzungen finden Sie unter *vSphere-Ressourcenverwaltung*.

Failover von fehlertoleranten virtuellen Maschinen

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

Teilweiser Hardwareausfall aufgrund von Speicherproblemen

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

Teilweiser Hardwareausfall aufgrund von Netzwerkproblemen

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

Ungenügende Bandbreite der protokollierenden Netzwerkkarte im Netzwerk

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

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

VMotion-Fehler aufgrund der Auslastung von virtuellen Maschinen

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

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

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

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

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

vCenter High Availability

4

vCenter High Availability (vCenter HA) schützt vCenter Server vor Host- und Hardwareausfällen. Die Aktiv-Passiv-Architektur der Lösung kann auch helfen, Ausfallzeiten erheblich zu reduzieren, wenn Sie auf vCenter Server einen Patch anwenden.

Nach einer entsprechenden Konfiguration des Netzwerks erstellen Sie einen Cluster mit einem aktiven, einem passiven und einem Zeugenknoten. Verschiedene Konfigurationspfade stehen zur Verfügung. Ihre Auswahl hängt von Ihrer bestehenden Konfiguration ab.

Verfahren

1 Planen der Bereitstellung von vCenter HA

Bevor Sie vCenter HA konfigurieren können, müssen Sie mehrere Faktoren in Betracht ziehen. Bei einer Bereitstellung mit Komponenten, die unterschiedliche Versionen von vSphere verwenden, sind andere Erwägungen notwendig als bei einer Bereitstellung, die nur vSphere 8.0-Komponenten umfasst. Auch die Anforderungen an Ressourcen und Software sowie an das Netzwerksetup müssen sorgfältig durchdacht werden.

2 Konfigurieren des Netzwerks

Unabhängig von der ausgewählten Bereitstellungsoption und Bestandshierarchie müssen Sie das Netzwerk einrichten, bevor Sie mit der Konfiguration beginnen. Um die Grundlage für das vCenter HA-Netzwerk festzulegen, fügen Sie eine Portgruppe zu jedem ESXi-Host hinzu.

3 Konfigurieren von vCenter HA mit dem vSphere Client

Wenn Sie den vSphere Client verwenden, erstellt und konfiguriert der Assistent zum **Einrichten von vCenter HA** einen zweiten Netzwerkadapter in der vCenter Server, klont den aktiven Knoten und konfiguriert das vCenter HA-Netzwerk.

4 Verwalten der vCenter HA-Konfiguration

Nach der Konfiguration Ihres vCenter HA-Clusters können Sie Verwaltungsaufgaben durchführen. Diese Aufgaben beinhalten die Zertifikatsersetzung, die Ersetzung von SSH-Schlüsseln und das SNMP-Setup. Sie können auch die Clusterkonfiguration bearbeiten, um vCenter HA zu deaktivieren oder zu aktivieren, in den Wartungsmodus zu wechseln und die Clusterkonfiguration zu entfernen.

5 Beheben von Fehlern in Ihrer vCenter HA-Umgebung

Falls Probleme auftreten, können Sie Fehler in Ihrer Umgebung beheben. Die auszuführende Aufgabe hängt von den Fehlersymptomen ab. Weitere Informationen über das Beheben von Problemen finden Sie im VMware-Knowledgebase-System.

6 Patchen einer vCenter-Umgebung mit hoher Verfügbarkeit

Sie können einen vCenter Server, der sich in einem vCenter High Availability-Cluster befindet, mithilfe des Dienstprogramms **`software-packages`** patchen, das in der vCenter Server-Shell zur Verfügung steht.

7 Upgrade mit reduzierter Ausfallzeit für vCenter HA

In vSphere 8.0 U3 ist das Upgrade mit reduzierter Ausfallzeit in die automatische vCenter HA-Bereitstellung integriert.

Planen der Bereitstellung von vCenter HA

Bevor Sie vCenter HA konfigurieren können, müssen Sie mehrere Faktoren in Betracht ziehen. Bei einer Bereitstellung mit Komponenten, die unterschiedliche Versionen von vSphere verwenden, sind andere Erwägungen notwendig als bei einer Bereitstellung, die nur vSphere 8.0-Komponenten umfasst. Auch die Anforderungen an Ressourcen und Software sowie an das Netzwerksetup müssen sorgfältig durchdacht werden.

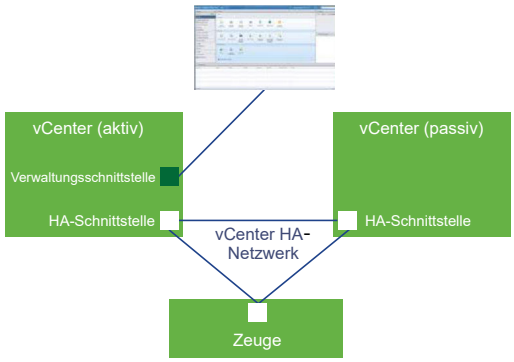
vCenter - Übersicht über die Architektur

Ein vCenter HA Cluster besteht aus drei vCenter Server-Instanzen. Die erste Instanz, die ursprünglich als der aktive Knoten genutzt wird, wird zweimal geklont: als passiver Knoten und als Zeugenknoten. Zusammen bilden die drei Knoten eine Aktiv/Passiv-Failoverlösung.

Die Bereitstellung jedes der Knoten auf einer anderen ESXi-Instanz schützt gegen Hardware-Ausfälle. Das Hinzufügen der drei ESXi-Hosts zu einem DRS-Cluster kann Ihre Umgebung zusätzlich schützen.

Wenn die vCenter HA-Konfiguration abgeschlossen ist, hat nur der aktive Knoten eine aktive Verwaltungsschnittstelle (öffentliche IP). Die drei Knoten kommunizieren über ein privates Netzwerk, das als vCenter HA-Netzwerk bezeichnet wird und als Teil der Konfiguration eingerichtet wird. Der aktive Knoten repliziert kontinuierlich Daten auf den passiven Knoten.

Abbildung 4-1. vCenter-Cluster mit drei Knoten



Alle drei Knoten sind erforderlich, damit diese Funktion ordnungsgemäß ausgeführt wird. Die folgende Tabelle enthält einen Vergleich der Aufgaben der einzelnen Knoten.

Tabelle 4-1. vCenter HA-Knoten

Knoten	Beschreibung
Aktiv	■ Führt die aktive vCenter Server-Instanz aus ■ Verwendet eine öffentliche IP-Adresse für die Verwaltungsschnittstelle ■ Verwendet das vCenter HA-Netzwerk zur Replizierung der Daten zum passiven Knoten. ■ Verwendet das vCenter HA-Netzwerk zur Kommunikation mit dem Zeugenknoten.
Passiv	■ Ist anfangs ein Klon des aktiven Knotens ■ Empfängt kontinuierlich Aktualisierungen vom aktiven Knoten über das vCenter HA-Netzwerk und synchronisiert den Zustand mit dem aktiven Knoten ■ Übernimmt bei einem Fehler automatisch die Rolle des aktiven Knotens
Zeuge	■ Ist ein Lightweight-Klon des aktiven Knotens ■ Stellt ein Quorum für den Schutz vor einer Split-Brain-Situation bereit

Hardware- und Softwareanforderungen von vCenter HA

Stellen Sie vor der Einrichtung von vCenter HA sicher, dass Sie über ausreichend Arbeitsspeicher, CPU-Leistung und Datenspeicherressourcen verfügen und dass Sie Versionen von vCenter Server und ESXi verwenden, die vCenter HA unterstützen.

Ihre Umgebung muss folgende Anforderungen erfüllen:

Tabelle 4-2. Anforderungen von vCenter HA

Komponente	Anforderungen
ESXi	■ ESXi 6.0 oder höher ist erforderlich. ■ Mindestens drei ESXi-Hosts werden dringend empfohlen. Um einen besseren Schutz zu gewährleisten, kann jeder vCenter HA-Knoten auf einem eigenen Host laufen.
Management vCenter Server (falls verwendet)	Ihre Umgebung kann ein Management vCenter Server-System umfassen oder Sie können Ihre vCenter Server so einrichten, dass sie den ESXi-Host verwaltet, auf dem sie ausgeführt wird (selbstverwaltetes vCenter Server) ■ vCenter Server 6.0 oder höher ist erforderlich.

Tabelle 4-2. Anforderungen von vCenter HA (Fortsetzung)

Komponente	Anforderungen
vCenter Server	■ vCenter Server 6.5 oder höher ist erforderlich. ■ Bereitstellungsgröße „Klein“ (4 CPU und 16 GB RAM) oder größer ist erforderlich, um die RTO zu erfüllen. Verwenden Sie „Sehr klein“ nicht in Produktionsumgebungen. ■ vCenter HA wird unterstützt von den Datenspeichern VMFS, NFS sowie vSAN und wurde für diese getestet. ■ Stellen Sie sicher, dass ausreichend Festplattenspeicher zur Verfügung steht, um Support-Pakete für alle drei Knoten auf dem aktiven Knoten zu sammeln und zu speichern. Weitere Informationen hierzu finden Sie unter Erfassen von Support-Paketen für einen vCenter HA-Knoten.
Netzwerkkonnektivität	■ Die Netzwerklatenz von vCenter HA zwischen aktiven, passiven und Zeugenknoten muss unter 10 ms liegen. ■ Das vCenter HA-Netzwerk muss sich auf einem anderen Subnetz als das Verwaltungsnetzwerk befinden.
Lizenzierung für vCenter HA erforderlich	■ Für vCenter HA ist eine einzelne vCenter Server-Lizenz erforderlich. ■ Für vCenter HA ist eine Standardlizenz erforderlich.

Konfigurations-Workflow in vSphere Client

Sie können den Assistenten zum **Einrichten von vCenter HA** in vSphere Client verwenden, um die passiven Knoten und Zeugenknoten zu konfigurieren. Der Assistent zum **Einrichten von vCenter HA** erstellt automatisch die passiven Knoten und die Zeugenknoten Knoten als Teil der vCenter HA-Konfiguration. Bei der manuellen Konfiguration sind Sie für das manuelle Klonen des aktiven Knotens verantwortlich, um den passiven Knoten und den Zeugenknoten zu erstellen.

Automatische Konfiguration mit vSphere Client

Für die automatische Konfiguration müssen die folgenden Anforderungen erfüllt sein.

- Die vCenter Server, die zum aktiven Knoten wird, verwaltet ihren eigenen ESXi-Host und ihre eigene virtuelle Maschine. Diese Konfiguration wird manchmal als selbstverwalteter vCenter Server bezeichnet.

Wenn diese Anforderungen erfüllt sind, wird folgender automatischer Workflow verwendet.

1. Der Benutzer stellt die erste vCenter Server bereit, die zum aktiven Knoten wird.
2. Der Benutzer fügt auf jedem ESXi-Host ein zweites Netzwerk (Portgruppe) für vCenter HA-Datenverkehr hinzu.
3. Der Benutzer beginnt mit der vCenter HA-Konfiguration und gibt die IP-Adressen, den zielseitigen ESXi-Host oder -Cluster und den Datenspeicher für jeden Klon an.
4. Das System klont den aktiven Knoten und erstellt einen passiven Knoten mit exakt denselben Einstellungen einschließlich desselben Hostnamens.
5. Das System klont den aktiven Knoten erneut und erstellt einen weiteren Light-Weight-Zeugenknoten.

6 Das System richtet das vCenter HA-Netzwerk ein, in dem die drei Knoten miteinander kommunizieren, beispielsweise durch Austausch von Taktsignalen und weiteren Informationen.

Manuelle Konfiguration mit vSphere Client

Wenn Sie mehr Kontrolle über Ihre Bereitstellung möchten, können Sie eine manuelle Konfiguration durchführen. Bei dieser Option sind Sie für das Klonen des aktiven Knotens im Rahmen der vCenter HA-Einrichtung selbst verantwortlich. Wenn Sie diese Option wählen und die vCenter HA-Konfiguration später entfernen, sind Sie für das Löschen der von Ihnen erstellten Knoten verantwortlich.

Bei der manuellen Konfiguration kommt folgender Workflow zum Einsatz.

1 Der Benutzer stellt die erste vCenter Server bereit, die zum aktiven Knoten wird.

2 Der Benutzer fügt auf jedem ESXi-Host ein zweites Netzwerk (Portgruppe) für vCenter HA-Datenverkehr hinzu.

3 Der Benutzer muss dem aktiven Knoten einen zweiten Netzwerkadapter (Netzwerkkarte) hinzufügen, wenn die Anmeldedaten für das aktive Management vCenter Server unbekannt sind.

4 Der Benutzer meldet sich mit dem vSphere Client bei der vCenter Server (aktiver Knoten) an.

5 Der Benutzer beginnt mit der vCenter HA-Konfiguration, aktiviert das Kästchen für manuelle Konfiguration und gibt die IP-Adresse und die Subnetzinformationen für den passiven und den Zeugenknoten an. Optional kann der Benutzer die IP-Adressen für das Failover-Management überschreiben.

6 Der Benutzer meldet sich beim Management vCenter Server an und erstellt zwei Klone der vCenter Server (aktiver Knoten).

7 Das System richtet das vCenter HA-Netzwerk ein, in dem die drei Knoten Taktsignale und Replikationsinformationen austauschen.

8 Die vCenter Server ist durch vCenter HA geschützt.

Weitere Informationen finden Sie unter Konfigurieren von vCenter HA mit dem vSphere Client.

Konfigurieren des Netzwerks

Unabhängig von der ausgewählten Bereitstellungsoption und Bestandshierarchie müssen Sie das Netzwerk einrichten, bevor Sie mit der Konfiguration beginnen. Um die Grundlage für das vCenter HA-Netzwerk festzulegen, fügen Sie eine Portgruppe zu jedem ESXi-Host hinzu.

Nach Abschluss der Konfiguration verfügt der vCenter HA-Cluster über zwei Netzwerke, das Verwaltungsnetzwerk auf der ersten virtuellen Netzwerkkarte und das vCenter HA-Netzwerk auf der zweiten virtuellen Netzwerkkarte.

Verwaltungsnetzwerk

Das Verwaltungsnetzwerk bedient Clientanforderungen (öffentliche IP). Die IP-Adressen des Verwaltungsnetzwerks müssen statisch sein.

vCenter HA-Netzwerk

Das vCenter HA-Netzwerk verbindet den aktiven, passiven und Zeugenknoten und repliziert den Serverzustand. Es überwacht auch die Taktsignale.

- Die IP-Adressen für das vCenter HA-Netzwerk für den aktiven Knoten, den passiven Knoten und den Zeugenknoten müssen statisch sein.
- Das vCenter HA-Netzwerk muss sich auf einem anderen Subnetz als das Verwaltungsnetzwerk befinden. Die drei Knoten können sich im gleichen oder in verschiedenen Subnetzen befinden.
- Die Netzwerklatenz zwischen dem aktiven Knoten, dem passiven Knoten und dem Zeugenknoten muss weniger als 10 Millisekunden betragen.
- Sie dürfen keinen Standard-Gateway-Eintrag für das Clusternetzwerk hinzufügen.

Voraussetzungen

- Die vCenter Server, die später zum aktiven Knoten wird, wird bereitgestellt.
- Sie können auf diese vCenter Server und auf den ESXi-Host, auf dem sie ausgeführt wird, zugreifen und haben Änderungsberechtigungen.
- Während der Netzwerkeinrichtung benötigen Sie statische IP-Adressen für das Verwaltungsnetzwerk. Die Verwaltungs- und Clusternetzwerkadressen müssen IPv4 oder IPv6 sein. Es dürfen keine IP-Adressen im Mischmodus verwendet werden.

Verfahren

1. Melden Sie sich beim vCenter Server für die Verwaltung an und suchen Sie den ESXi-Host, auf dem der aktive Knoten ausgeführt wird.
2. Fügen Sie dem ESXi-Host eine Portgruppe hinzu.

   Die Portgruppe kann sich auf einem vorhandenen virtuellen Switch befinden, oder Sie können für eine verbesserte Netzwerkisolierung einen neuen virtuellen Switch erstellen. Er muss sich vom Verwaltungsnetzwerk unterscheiden.
3. Wenn Ihre Umgebung die empfohlenen drei ESXi-Hosts umfasst, fügen Sie die Portgruppe jedem der Hosts hinzu.

Konfigurieren von vCenter HA mit dem vSphere Client

Wenn Sie den vSphere Client verwenden, erstellt und konfiguriert der Assistent zum **Einrichten von vCenter HA** einen zweiten Netzwerkadapter in der vCenter Server, klont den aktiven Knoten und konfiguriert das vCenter HA-Netzwerk.

Voraussetzungen

- Stellen Sie die vCenter Server bereit, die Sie als anfänglichen aktiven Knoten verwenden möchten.
  - Die vCenter Server benötigt eine statische IP-Adresse.
  - SSH muss auf dem vCenter Server aktiviert sein.
- Überprüfen Sie, ob die Umgebung die folgenden Anforderungen erfüllt:
  - Die vCenter Server, die zum aktiven Knoten wird, verwaltet ihren eigenen ESXi-Host und ihre eigene virtuelle Maschine. Diese Konfiguration wird manchmal als selbstverwalteter vCenter Server bezeichnet.
- Richten Sie die Infrastruktur für das vCenter HA-Netzwerk ein. Weitere Informationen hierzu finden Sie unter Konfigurieren des Netzwerks.
- Bestimmen Sie, welche statischen IP-Adressen für die beiden vCenter Server-Knoten verwendet werden, die zum passiven Knoten und zum Zeugenknoten werden.

Hinweis Zur Verwendung eines NSX-T-Segments auf dem aktiven Knoten müssen Sie NIC2/eth1 erstellen, indem Sie mithilfe von **VM-Einstellungen bearbeiten** die zweite Netzwerkkarte mit dem NSX-T-Segment hinzufügen. Sie brauchen keine Ressourcen für passive oder Zeugenknoten anzugeben, da der Klon mithilfe von **VM klonen** erstellt werden muss, nachdem Sie die erforderlichen Gastanpassungsspezifikationen für passive und Zeugenknoten hinzugefügt haben, die NIC1/eth0 und NIC2/eth1 mit IP-Adressen enthalten. Wenn Sie VCHA-IP-Adressen für eth1 in vCenter Server konfigurieren, wird eth1 auf dem aktiven Knoten automatisch ausgefüllt.

Verfahren

1. Melden Sie sich beim aktiven Knoten mit dem vSphere Client an.
2. Wählen Sie das vCenter Server-Objekt in der Bestandsliste aus und klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie **vCenter HA** unter „Einstellungen“ aus.
4. Klicken Sie auf die Schaltfläche **vCenter HA einrichten**, um den Setup-Assistenten zu starten.
   - Wenn der vCenter Server selbstverwaltet ist, wird die Seite **Ressourceneinstellungen** angezeigt. Fahren Sie mit Schritt 7 fort.
   - Wenn der vCenter Server von einem anderen vCenter Server in derselben SSO-Domäne verwaltet wird, fahren Sie mit Schritt 7 fort.
   - Wenn Ihr vCenter Server von einem anderen vCenter Server in einer anderen SSO-Domäne verwaltet wird, geben Sie den Speicherort und die Anmeldedaten dieses Management vCenter Server ein.

5 Klicken Sie auf **Anmeldedaten des Management vCenter Server**. Geben Sie den FQDN oder die IP-Adresse sowie den Single Sign-On-Benutzernamen und das Kennwort des Management vCenter Server ein und klicken Sie auf **Weiter**.

   Wenn Sie nicht über Single Sign-On-Administratoranmeldedaten verfügen, wählen Sie das zweite Aufzählungszeichen und klicken Sie auf **Weiter**.

6 Es wird möglicherweise eine **Zertifikatswarnung** angezeigt. Überprüfen Sie den SHA1-Fingerabdruck und wählen Sie **Ja** aus, um fortzufahren.

7 Wählen Sie im Abschnitt **Ressourceneinstellungen** zunächst das vCenter HA-Netzwerk für den aktiven Knoten aus dem Dropdown-Menü aus.

   Hinweis Die Netzwerkauswahl wird nicht mehr angezeigt, nachdem NIC2/eth1 erstellt wurde.

8 Klicken Sie auf das Kontrollkästchen, wenn Sie automatisch Klone für passive und Zeugenknoten erstellen möchten.

   Hinweis Wenn Sie das Kontrollkästchen nicht aktivieren, müssen Sie nach dem Klicken auf **Fertig stellen** manuell Klone für passive und Zeugenknoten erstellen.

9 Klicken Sie für den passiven Knoten auf **Bearbeiten**.

   a Legen Sie einen eindeutigen Namen und einen Zielspeicherort fest.

   b Wählen Sie die Ziel-Computing-Ressource für diesen Vorgang aus.

   c Wählen Sie den Datenspeicher für die Konfigurations- und Festplattendateien aus.

   d Wählen Sie Netzwerke für die Verwaltung der virtuellen Maschine (Netzwerkkarte 0) und vCenter HA (Netzwerkkarte 1) aus.

      Wenn Probleme bei der Auswahl auftreten, werden Fehler oder Kompatibilitätswarnungen angezeigt.

   e Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.

10 Klicken Sie für den Zeugenknoten auf **Bearbeiten**.

   a Legen Sie einen eindeutigen Namen und einen Zielspeicherort fest.

   b Wählen Sie die Ziel-Computing-Ressource für diesen Vorgang aus.

   c Wählen Sie den Datenspeicher für die Konfigurations- und Festplattendateien aus.

   d Wählen Sie das vCenter HA-Netzwerk (Netzwerkkarte 1) aus:

      Wenn Probleme bei der Auswahl auftreten, werden Fehler oder Kompatibilitätswarnungen angezeigt.

   e Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.

11 Klicken Sie auf **Weiter**.

12 Wählen Sie im Abschnitt **IP-Einstellungen** die IP-Version aus dem Dropdown-Menü aus.

13 Geben Sie die IPv4-Adresse (Netzwerkkarte 1) und die Subnetzmaske oder die Präfixlängeninformationen für die aktiven, passiven und Zeugenknoten ein.

   Sie können die Einstellungen für das Verwaltungsnetzwerk für den passiven Knoten bearbeiten. Das Anpassen von diesen Einstellungen ist optional. Standardmäßig werden die Einstellungen für das Verwaltungsnetzwerk des aktiven Knotens angewendet.

14 Klicken Sie auf **Beenden**.

Ergebnisse

Der passive Knoten und der Zeugenknoten werden erstellt. Wenn das **Einrichten von vCenter HA** abgeschlossen ist, hat die vCenter Server Hochverfügbarkeitsschutz. Nachdem vCenter-HA aktiviert wurde, können Sie auf **Bearbeiten** klicken, um in den Wartungsmodus zu wechseln oder vCenter HA zu aktivieren bzw. zu deaktivieren. Es gibt separate Schaltflächen zum Entfernen von vCenter HA oder zum Initiieren eines vCenter HA-Failover.

Nächste Schritte

Unter Verwalten der vCenter HA-Konfiguration finden Sie eine Liste der Clusterverwaltungsaufgaben.

Eine kurze Übersicht der Verbesserungen im vSphere Client beim Arbeiten mit vCenter HA finden Sie unter:

(Verbesserungen bei der Arbeit mit vCenter HA im vSphere Client)

Verwalten der vCenter HA-Konfiguration

Nach der Konfiguration Ihres vCenter HA-Clusters können Sie Verwaltungsaufgaben durchführen. Diese Aufgaben beinhalten die Zertifikatsersetzung, die Ersetzung von SSH-Schlüsseln und das SNMP-Setup. Sie können auch die Clusterkonfiguration bearbeiten, um vCenter HA zu deaktivieren oder zu aktivieren, in den Wartungsmodus zu wechseln und die Clusterkonfiguration zu entfernen.

- Einrichten von SNMP-Traps

  Sie können SNMP-Traps einrichten, um SNMP-Benachrichtigungen für Ihren vCenter HA-Cluster zu erhalten.

- Einrichten der Umgebung für die Verwendung von benutzerdefinierten Zertifikaten

  Das Maschinen-SSL-Zertifikat auf den einzelnen Knoten wird für die Clustermanagement-Kommunikation sowie für das Verschlüsseln des Replizierungsdatenverkehrs verwendet. Wenn Sie benutzerdefinierte Zertifikate verwenden möchten, müssen Sie die vCenter HA-Konfiguration entfernen, die passiven und Zeugenknoten löschen, den aktiven Knoten mit dem benutzerdefinierten Zertifikat versehen und den Cluster neu konfigurieren.

- Verwalten von vCenter HA SSH-Schlüsseln

  vCenter HA verwendet SSH-Schlüssel für die Authentifizierung zwischen dem aktiven Knoten, dem passiven Knoten und dem Zeugenknoten. Die Authentifizierung wird für den Austausch von Taktsignalen und zur Replizierung von Dateien und Daten verwendet. Um die SSH-Schlüssel in den Knoten eines vCenter HA-Clusters zu ersetzen, deaktivieren Sie den Cluster, generieren neue SSH-Schlüssel auf dem aktiven Knoten, übertragen die Schlüssel an den passiven Knoten und aktivieren den Cluster.

- Einleiten eines vCenter HA-Failovers

  Sie können ein Failover manuell einleiten, sodass der passive Knoten zum aktiven Knoten wird.

- Bearbeiten der vCenter HA-Clusterkonfiguration

  Wenn Sie die vCenter HA-Clusterkonfiguration bearbeiten, können Sie den Cluster deaktivieren oder aktivieren, den Cluster in den Wartungsmodus versetzen oder den Cluster entfernen.

- Durchführen von Sicherungs- und Wiederherstellungsvorgängen

  Zur Steigerung der Sicherheit können Sie den aktiven Knoten im vCenter HA-Cluster sichern. Bei einem schwerwiegenden Fehler können Sie den Knoten dann wiederherstellen.

- Entfernen einer vCenter HA-Konfiguration

  Sie können eine vCenter HA-Konfiguration vom vSphere Client entfernen.

- Neustarten aller vCenter HA-Knoten

  Wenn Sie alle Knoten im Cluster herunterfahren und neu starten müssen, müssen Sie eine bestimmte Reihenfolge beim Herunterfahren einhalten, um zu verhindern, dass der passive Knoten die Rolle des aktiven Knotens übernimmt.

- Ändern der Serverumgebung

  Wenn Sie eine vCenter Server bereitstellen, wählen Sie eine Umgebung aus. Für vCenter HA werden kleine, mittlere, große und sehr große Produktionsumgebungen unterstützt. Falls Sie mehr Platz benötigen und die Umgebung wechseln möchten, müssen Sie vor dem Ändern der Konfiguration die virtuelle Maschine des passiven Knotens löschen.

- Erfassen von Support-Paketen für einen vCenter HA-Knoten

  Das Erfassen eines Support-Pakets für alle Knoten in einem vCenter HA-Cluster hilft bei der Fehlerbehebung.

Einrichten von SNMP-Traps

Sie können SNMP-Traps einrichten, um SNMP-Benachrichtigungen für Ihren vCenter HA-Cluster zu erhalten.

Die Standardeinstellung für die Traps ist SNMP Version 1.

Richten Sie SNMP-Traps für den aktiven Knoten und den passiven Knoten ein. Sie geben durch einen entsprechenden Eintrag für das Ziel in der snmpd-Konfiguration das Ziel an, an das der Agent entsprechende Traps senden soll.

Verfahren

1. Melden Sie sich mithilfe der Konsole für die virtuelle Maschine oder von SSH beim aktiven Knoten an.
2. Führen Sie den Befehl `vicfg-snmp` aus, z. B.:

   ```
   vicfg-snmp -t 10.160.1.1@1166/public
   ```

   In diesem Beispiel ist `10.160.1.1` die Überwachungsadresse des Clients, `1166` ist der Überwachungsport des Clients und `public` ist der Community-String.
3. Aktivieren Sie den SNMP-Agenten (snmpd), indem Sie den folgenden Befehl ausführen.

   ```
   vicfg-snmp -e
   ```

Nächste Schritte

Diese Befehle könnten ebenfalls hilfreich sein:

- Führen Sie **`vicfg-snmp -h`** aus, um eine umfassende Hilfe zum Befehl zu erhalten.
- Um den SNMP-Agenten zu deaktivieren, führen Sie **`vicfg-snmp -D`** aus.
- Führen Sie **`vicfg-snmp -s`** aus, um die Konfiguration des SNMP-Agenten anzuzeigen.
- Um die Konfiguration auf die Standardwerte zurückzusetzen, führen Sie **`vicfg-snmp -r`** aus.

Einrichten der Umgebung für die Verwendung von benutzerdefinierten Zertifikaten

Das Maschinen-SSL-Zertifikat auf den einzelnen Knoten wird für die Clustermanagement-Kommunikation sowie für das Verschlüsseln des Replizierungsdatenverkehrs verwendet. Wenn Sie benutzerdefinierte Zertifikate verwenden möchten, müssen Sie die vCenter HA-Konfiguration entfernen, die passiven und Zeugenknoten löschen, den aktiven Knoten mit dem benutzerdefinierten Zertifikat versehen und den Cluster neu konfigurieren.

Wenn möglich, ersetzen Sie Zertifikate in der vCenter Server, die der aktive Knoten wird, bevor Sie den Knoten klonen.

Verfahren

1. Bearbeiten Sie die Clusterkonfiguration und wählen Sie **Entfernen**.
2. Löschen Sie den passiven Knoten und den Zeugenknoten.
3. Ersetzen Sie auf dem aktiven Knoten, der jetzt ein eigenständiger vCenter Server ist, das Maschinen-SSL-Zertifikat durch ein benutzerdefiniertes Zertifikat.

4 Konfigurieren Sie den Cluster neu.

Verwalten von vCenter HA SSH-Schlüsseln

vCenter HA verwendet SSH-Schlüssel für die Authentifizierung zwischen dem aktiven Knoten, dem passiven Knoten und dem Zeugenknoten. Die Authentifizierung wird für den Austausch von Taktsignalen und zur Replizierung von Dateien und Daten verwendet. Um die SSH-Schlüssel in den Knoten eines vCenter HA-Clusters zu ersetzen, deaktivieren Sie den Cluster, generieren neue SSH-Schlüssel auf dem aktiven Knoten, übertragen die Schlüssel an den passiven Knoten und aktivieren den Cluster.

Verfahren

1 Bearbeiten Sie den Cluster und ändern Sie den Modus in **Deaktiviert**.

2 Melden Sie sich mithilfe der Konsole für die virtuelle Maschine oder von SSH beim aktiven Knoten an.

3 Aktivieren Sie die Bash-Shell.

```
bash
```

4 Führen Sie den folgenden Befehl aus, um neue SSH-Schlüssel auf dem aktiven Knoten zu erzeugen.

```
/usr/lib/vmware-vcha/scripts/resetSshKeys.py
```

5 Verwenden Sie SCP, um die Schlüssel zum passiven Knoten und zum Zeugenknoten zu kopieren.

```
scp /vcha/.ssh/*
```

6 Bearbeiten Sie die Cluster-Konfiguration und legen Sie den vCenter HA-Cluster auf **Aktiviert** fest.

Einleiten eines vCenter HA-Failovers

Sie können ein Failover manuell einleiten, sodass der passive Knoten zum aktiven Knoten wird.

Ein vCenter HA-Cluster unterstützt zwei Arten von Failover.

Automatisches Failover

Der passive Knoten versucht, beim Ausfall eines aktiven Knotens die Rolle des aktiven Knotens zu übernehmen.

Manuelles Failover

Der Benutzer kann einen passiven Knoten mithilfe der Aktion „Failover einleiten“ zwingen, die aktive Rolle zu übernehmen.

Leiten Sie ein manuelles Failover zur Fehlerbehebung und für Tests ein.

Verfahren

1. Melden Sie sich bei der vCenter Server für den aktiven Knotens mit dem vSphere Client an und klicken Sie auf **Konfigurieren** bei dem vCenter Server, auf dem Sie ein Failover initiieren müssen.
2. Wählen Sie unter **Einstellungen** die Option **vCenter HA** aus und klicken Sie auf **Failover einleiten**.
3. Klicken Sie auf **Ja**, um das Failover zu starten.

   In einem Dialogfeld steht die Option zum Erzwingen eines Failovers ohne Synchronisierung bereit. In den meisten Fällen ist es empfehlenswert, zunächst die Synchronisierung durchzuführen.
4. Nach dem Failover können Sie überprüfen, ob der passive Knoten die Rolle des aktiven Knotens im vSphere Client übernimmt.

Bearbeiten der vCenter HA-Clusterkonfiguration

Wenn Sie die vCenter HA-Clusterkonfiguration bearbeiten, können Sie den Cluster deaktivieren oder aktivieren, den Cluster in den Wartungsmodus versetzen oder den Cluster entfernen.

Der Betriebsmodus einer vCenter Server steuert die Failover-Funktionen und die Zustandsreplizierung in einem vCenter HA-Cluster.

Ein vCenter HA-Cluster kann in einem der folgenden Modi verwendet werden.

Tabelle 4-3. Betriebsmodi für den vCenter HA-Cluster

Modus	Automatisches Failover	Manuelles Failover	Replizierung	
Aktiviert	Ja	Ja	Ja	Dieser Standardbetriebsmodus schützt die vCenter Server durch ein automatisches Failover vor Hardware- und Softwarefehlern.
Wartung	Nein	Ja	Ja	Wird für einige Wartungsaufgaben verwendet. Für andere Aufgaben müssen Sie vCenter HA deaktivieren.
Deaktiviert	Nein	Nein	Nein	Wenn der passive Knoten oder der Zeugenknoten verloren geht oder nach einem Fehler wiederhergestellt wird, kann eine vCenter HA-Konfiguration deaktiviert werden. Der aktive Knoten wird als eigenständige vCenter Server weiter ausgeführt.

Hinweis Wenn der Cluster im Wartungsmodus oder im deaktivierten Modus arbeitet, kann ein aktiver Knoten weiterhin Clientanforderungen verarbeiten, selbst wenn der passive Knoten und der Zeugenknoten verlorengehen oder nicht erreichbar sind.

Voraussetzungen

Stellen Sie sicher, dass der vCenter HA-Cluster bereitgestellt ist und den aktiven Knoten, den passiven Knoten und den Zeugenknoten enthält.

Verfahren

1 Melden Sie sich beim aktiven Knoten vCenter Server über den vSphere Client an und klicken Sie auf **Konfigurieren**.

2 Wählen Sie unter **Einstellungen** die Option **vCenter HA** aus und klicken Sie auf **Bearbeiten**.

3 Wählen Sie eine der Optionen aus.

Option	Ergebnis
vCenter HA aktivieren	Ermöglicht die Replikation zwischen dem aktiven und dem passiven Knoten. Wenn der Cluster einen ordnungsgemäßen Zustand aufweist, wird der aktive Knoten durch automatisches Failover vom passiven Knoten geschützt.
Wartungsmodus	Im Wartungsmodus erfolgt die Replizierung weiterhin zwischen dem aktiven Knoten und dem passiven Knoten. Das automatische Failover ist jedoch deaktiviert.
vCenter HA deaktivieren	Deaktiviert Replikation und Failover. Behält die Konfiguration des Clusters bei. Sie können vCenter HA später erneut aktivieren.
vCenter HA-Cluster entfernen	Entfernt den Cluster. Replizierung und Failover werden nicht mehr bereitgestellt. Der aktive Knoten wird weiterhin als eigenständige vCenter Server ausgeführt. Weitere Informationen finden Sie unter Entfernen einer vCenter HA-Konfiguration.

4 Klicken Sie auf OK.

Durchführen von Sicherungs- und Wiederherstellungsvorgängen

Zur Steigerung der Sicherheit können Sie den aktiven Knoten im vCenter HA-Cluster sichern. Bei einem schwerwiegenden Fehler können Sie den Knoten dann wiederherstellen.

Hinweis Entfernen Sie die Clusterkonfiguration, bevor Sie den aktiven Knoten wiederherstellen. Wenn Sie den aktiven Knoten wiederherstellen und der passive Knoten weiterhin ausgeführt wird oder eine andere Clusterkonfiguration weiterhin verwendet wird, sind die Ergebnisse nicht vorhersehbar.

Voraussetzungen

Überprüfen Sie die Interoperabilität von vCenter HA und der Sicherungs- und Wiederherstellungslösung. Bei einer Lösung handelt es sich um eine dateibasierte Wiederherstellung dervCenter Server.

Verfahren

1 Sichern Sie den aktiven Knoten.

   Führen Sie keine Sicherung des passiven Knotens und des Zeugenknotens durch.

2 Bevor Sie den Cluster wiederherstellen, schalten Sie alle Knoten aus und löschen Sie alle vCenter HA-Knoten.

3 Stellen Sie den aktiven Knoten wieder her.

   Der aktive Knoten wird als eigenständige vCenter Server wiederhergestellt.

Entfernen einer vCenter HA-Konfiguration

Sie können eine vCenter HA-Konfiguration vom vSphere Client entfernen.

Verfahren

1 Melden Sie sich beim aktiven Knoten vCenter Server an und klicken Sie auf **Konfigurieren**.

2 Wählen Sie unter **Einstellungen** die Option **vCenter HA** aus und klicken Sie auf **VCHA entfernen**.

   - Die Konfiguration des vCenter HA-Clusters wird auf dem aktiven Knoten, passiven Knoten und Zeugenknoten entfernt.
   - Sie können den passiven Knoten und den Zeugenknoten löschen.
   - Der aktive Knoten wird weiterhin als eigenständige vCenter Server ausgeführt.
   - In einer neuen vCenter HA-Konfiguration können Sie die passiven Knoten und Zeugenknoten nicht wiederverwenden.
   - Wenn Sie eine manuelle Konfiguration durchgeführt haben oder die passiven Knoten und Zeugenknoten nicht erkennbar sind, müssen Sie diese Knoten explizit löschen.
   - Auch dann, wenn die zweite virtuelle Netzwerkkarte durch den Konfigurationsprozess hinzugefügt wurde, wird während des Entfernungsvorgangs die virtuelle Netzwerkkarte nicht entfernt.

Neustarten aller vCenter HA-Knoten

Wenn Sie alle Knoten im Cluster herunterfahren und neu starten müssen, müssen Sie eine bestimmte Reihenfolge beim Herunterfahren einhalten, um zu verhindern, dass der passive Knoten die Rolle des aktiven Knotens übernimmt.

Verfahren

1 Fahren Sie die Knoten in dieser Reihenfolge herunter.

   - Passiver Knoten
   - Aktiver Knoten
   - Zeugenknoten

2 Starten Sie jeden Knoten neu.

   Sie können Knoten in einer beliebigen Reihenfolge neu starten.

3 Überprüfen Sie, ob alle Knoten erfolgreich zum Cluster hinzugefügt wurden und dass der vorherige aktive Knoten diese Rolle übernimmt.

Ändern der Serverumgebung

Wenn Sie eine vCenter Server bereitstellen, wählen Sie eine Umgebung aus. Für vCenter HA werden kleine, mittlere, große und sehr große Produktionsumgebungen unterstützt. Falls Sie mehr Platz benötigen und die Umgebung wechseln möchten, müssen Sie vor dem Ändern der Konfiguration die virtuelle Maschine des passiven Knotens löschen.

Verfahren

1 Melden Sie sich mit dem vSphere Client beim aktiven Knoten an, bearbeiten Sie die Clusterkonfiguration und wählen Sie **Deaktivieren** aus.

2 Löschen Sie die virtuelle Maschine des passiven Knotens.

3 Ändern Sie die Konfiguration der vCenter Server für den aktiven Knoten, beispielsweise von einer kleinen Umgebung zu einer mittleren Umgebung.

4 Konfigurieren Sie vCenter HA neu.

Erfassen von Support-Paketen für einen vCenter HA-Knoten

Das Erfassen eines Support-Pakets für alle Knoten in einem vCenter HA-Cluster hilft bei der Fehlerbehebung.

Wenn Sie ein Support-Paket des aktiven Knotens in einem vCenter HA-Cluster erfassen, geht das System wie folgt vor.

- Die Support-Paket-Informationen werden vom aktiven Knoten selbst erfasst.
- Support-Pakete werden vom passiven Knoten und vom Zeugenknoten erfasst und im Verzeichnis `commands` im Support-Paket des aktiven Knotens abgelegt.

Hinweis Die Erfassung von Support-Paketen vom passiven Knoten und vom Zeugenknoten erfolgt auf der Basis eines „besten Versuchs“ und wird durchgeführt, wenn die Knoten erreichbar sind.

Beheben von Fehlern in Ihrer vCenter HA-Umgebung

Falls Probleme auftreten, können Sie Fehler in Ihrer Umgebung beheben. Die auszuführende Aufgabe hängt von den Fehlersymptomen ab. Weitere Informationen über das Beheben von Problemen finden Sie im VMware-Knowledgebase-System.

- vCenter HA-Klonenvorgang schlägt während der Bereitstellung fehl

  Falls der vCenter HA-Konfigurationsprozess die Klone nicht ordnungsgemäß erstellt, müssen Sie den Fehler beim Klonen beheben.

- Erneutes Bereitstellen des passive Knotens oder des Zeugenknotens

  Wenn der passive Knoten oder der Zeugenknoten ausfallen und das vCenter HA-Cluster mithilfe der automatischen Klonmethode konfiguriert wurde, können Sie sie auf der Seite **vCenter HA-Einstellungen** erneut bereitstellen.

- vCenter HA-Bereitstellung schlägt fehl

  Bereitstellungsfehler können durch Konfigurationsprobleme verursacht werden, vor allem Probleme mit der Netzwerkeinrichtung.

- Fehlerbehebung bei einem fehlerhaften vCenter HA-Cluster

  Damit ein vCenter HA-Cluster fehlerfrei ist, müssen der aktive Knoten, der passive Knoten und der Zeugenknoten voll funktionsfähig und über das Netzwerk des vCenter HA-Clusters erreichbar sein. Wenn einer der Knoten ausfällt, gilt der Cluster als fehlerhaft.

- Wiederherstellen bei isolierten vCenter HA-Knoten

  Wenn alle Knoten in einem vCenter HA-Cluster nicht miteinander kommunizieren können, bedient der aktiver Knoten keine Clientanforderungen mehr.

- Beheben von Failover-Fehlern

  Wenn ein passiver Knoten während eines Failovers nicht zum aktiven Knoten wird, können Sie den passiven Knoten dazu zwingen, die Rolle des aktiven Knotens zu übernehmen.

- VMware vCenter® HA-Alarme und -Ereignisse

  Wenn ein vCenter HA-Cluster sich in einem fehlerhaften Zustand befindet, zeigen Alarme und Ereignisse Fehler an.

vCenter HA-Klonenvorgang schlägt während der Bereitstellung fehl

Falls der vCenter HA-Konfigurationsprozess die Klone nicht ordnungsgemäß erstellt, müssen Sie den Fehler beim Klonen beheben.

Problem

Klonvorgang schlägt fehl.

Hinweis Das Klonen einer passiven oder Zeugen-VM für eine VCHA-Bereitstellung auf demselben NFS 3.1-Datenspeicher wie der Quellknoten der aktiven VM schlägt fehl. Sie müssen NFS4 verwenden oder die passiven und Zeugen-VMs in einem Datenspeicher klonen, der sich von der aktiven VM unterscheidet.

Ursache

Sehen Sie nach der Klonausnahme nach. Dies könnte eines der folgenden Probleme bedeuten.

- Sie haben einen DRS-fähigen Cluster, aber keine drei Hosts.
- Die Verbindung zum Host oder zur Datenbank wurde unterbrochen.
- Nicht genügend Speicherplatz.
- Andere Fehler beim **Klonen einer virtuellen Maschine**

Lösung

1. Beheben Sie den Fehler, der das Problem verursacht hat.
2. Entfernen Sie den Cluster und starten Sie die Konfiguration erneut.

Erneutes Bereitstellen des passive Knotens oder des Zeugenknotens

Wenn der passive Knoten oder der Zeugenknoten ausfallen und das vCenter HA-Cluster mithilfe der automatischen Klonmethode konfiguriert wurde, können Sie sie auf der Seite **vCenter HA-Einstellungen** erneut bereitstellen.

Verfahren

1. Melden Sie sich beim aktiven Knoten mit dem vSphere Client an.
2. Wählen Sie das vCenter Server-Objekt in der Bestandsliste aus und klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie **vCenter HA** unter **Einstellungen** aus.
4. Klicken Sie auf die Schaltfläche **ERNEUT BEREITSTELLEN** neben dem Knoten, um den Assistenten für die erneute Bereitstellung zu starten.
5.
   - Wenn Ihr vCenter Server von einem anderen vCenter Server in derselben SSO-Domäne verwaltet wird, fahren Sie mit Schritt 6 fort.
   - Wenn Ihr vCenter Server von einem anderen vCenter Server in einer anderen SSO-Domäne verwaltet wird, geben Sie den Speicherort und die Anmeldedaten dieses Management vCenter Server ein. Geben Sie **Management vCenter Server-FQDN oder IP-Adresse** und **Single Sign-On**-Anmeldedaten ein.
6. Legen Sie einen eindeutigen Namen und einen Zielspeicherort fest.

7 Wählen Sie die Ziel-Computing-Ressource für diesen Vorgang aus.

8 Wählen Sie den Datenspeicher für die Konfigurations- und Festplattendateien aus.

9 Konfigurieren Sie die Netzwerke der virtuellen Maschine.

- Wenn Sie den passiven Knoten erneut bereitstellen, wählen Sie die Netzwerke für die Verwaltung der virtuellen Maschine (Netzwerkkarte 0) und vCenter HA (Netzwerkkarte 1) aus.
- Wenn Sie den Zeugenknoten erneut bereitstellen, wählen Sie das Netzwerk vCenter HA (Netzwerkkarte 1) aus.

Wenn Probleme bei der Auswahl auftreten, werden Fehler oder Kompatibilitätswarnungen angezeigt.

10 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertig stellen**, um den Knoten erneut bereitzustellen.

vCenter HA-Bereitstellung schlägt fehl

Bereitstellungsfehler können durch Konfigurationsprobleme verursacht werden, vor allem Probleme mit der Netzwerkeinrichtung.

Problem

Sie starten eine vCenter HA-Clusterkonfiguration und sie schlägt fehl. Möglicherweise gibt die entsprechende Fehlermeldung die Ursache des Problems wieder, z. B. eine Meldung, die besagt, dass eine SSH-Verbindung fehlgeschlagen ist.

Lösung

Falls die Bereitstellung fehlschlägt, ergreifen Sie die entsprechenden Maßnahmen, um die Netzwerkprobleme zu beheben.

1 Stellen Sie sicher, dass vom aktiven Knoten aus auf die passiven Knoten und Zeugenknoten zugegriffen werden kann.

2 Stellen Sie sicher, dass das Routing zwischen den Knoten ordnungsgemäß eingerichtet ist.

3 Überprüfen Sie die Netzwerklatenz.

Fehlerbehebung bei einem fehlerhaften vCenter HA-Cluster

Damit ein vCenter HA-Cluster fehlerfrei ist, müssen der aktive Knoten, der passive Knoten und der Zeugenknoten voll funktionsfähig und über das Netzwerk des vCenter HA-Clusters erreichbar sein. Wenn einer der Knoten ausfällt, gilt der Cluster als fehlerhaft.

Problem

Wenn sich der Cluster in einem fehlerhaften Zustand befindet, ist kein Failover möglich. Informationen zu Fehlerszenarios eines Clusters, der sich in einem fehlerhaften Zustand befindet, finden Sie unter Beheben von Failover-Fehlern.

Ursache

Der Cluster kann aus mehreren Gründen fehlerhaft sein.

Einer der Knoten fällt aus

- Wenn der aktive Knoten ausfällt, erfolgt automatisch ein Failover des aktiven Knotens auf den passiven Knoten. Nach dem Failover wird der passive Knoten zum aktiven Knoten.

  Zu diesem Zeitpunkt befindet sich der Cluster in einem fehlerhaften Zustand, da der ursprüngliche aktive Knoten nicht verfügbar ist.

  Sobald der ausgefallene Knoten repariert wurde oder online kommt, wird er zum neuen passiven Knoten und der Cluster kehrt zu einem fehlerfreien Zustand zurück, nachdem die aktiven und passiven Knoten synchronisiert wurden.
- Wenn der passive Knoten ausfällt, ist der aktive Knoten weiterhin funktionsbereit, aber es ist kein Failover möglich und der Cluster ist fehlerhaft.

  Wenn der passive Knoten repariert wurde oder online kommt, wird er automatisch wieder dem Cluster hinzugefügt und der Cluster befindet sich in einem fehlerfreien Zustand, nachdem der aktive Knoten und der passive Knoten synchronisiert wurden.
- Wenn der Zeugenknoten ausfällt, ist der aktive Knoten weiterhin funktionsbereit und die Replizierung zwischen dem aktiven und dem passiven Knoten wird fortgesetzt, aber es kann kein Failover durchgeführt werden.

  Wenn der Zeugenknoten repariert wurde oder online kommt, wird er automatisch wieder dem Cluster hinzugefügt und der Cluster befindet sich in einem fehlerfreien Zustand.

Datenbankreplizierung schlägt fehl

Falls die Replizierung zwischen dem aktiven Knoten und dem passiven Knoten fehlschlägt, gilt der Cluster als fehlerhaft. Der aktive Knoten wird weiterhin mit dem passiven Knoten synchronisiert. Wenn die Synchronisierung gelingt, kehrt der Cluster zu einem fehlerfreien Zustand zurück. Dieser Zustand kann auf Probleme bei der Netzwerkbandbreite oder andere fehlende Ressourcen zurückzuführen sein.

Replizierungsprobleme mit Konfigurationsdateien

Wenn Konfigurationsdateien nicht ordnungsgemäß zwischen den aktiven und passiven Knoten repliziert werden, befindet sich der Cluster in einem fehlerhaften Zustand. Der aktive Knoten versucht weiterhin, sich mit dem passiven Knoten zu synchronisieren. Dieser Zustand kann auf Probleme bei der Netzwerkbandbreite oder andere fehlende Ressourcen zurückzuführen sein.

Lösung

Wie die Wiederherstellung erfolgt, hängt von der Ursache des fehlerhaften Clusters ab. Wenn sich der Cluster in einem fehlerhaften Zustand befindet, wird durch Ereignisse, Alarme und SNMP-Traps auf Fehler hingewiesen.

Wenn einer der Knoten ausgefallen ist, kann dies an einem Hardwarefehler oder der Netzwerkisolierung liegen. Überprüfen Sie, ob der ausgefallene Knoten eingeschaltet ist.

Überprüfen Sie im Falle von Replizierungsfehlern, ob das vCenter HA-Netzwerk über eine ausreichende Bandbreite verfügt, und stellen Sie sicher, dass die Netzwerklatenz nicht mehr als 10 ms beträgt.

Wiederherstellen bei isolierten vCenter HA-Knoten

Wenn alle Knoten in einem vCenter HA-Cluster nicht miteinander kommunizieren können, bedient der aktiver Knoten keine Clientanforderungen mehr.

Problem

Bei der Knotenisolierung handelt es sich um ein Netzwerk-Konnektivitätsproblem.

Lösung

1. Versuchen Sie, das Verbindungsproblem zu beheben. Wenn Sie die Konnektivität wiederherstellen können, treten die isolierten Knoten dem Cluster automatisch neu bei und der aktive Knoten bedient Client-Anforderungen wieder.
2. Wenn Sie das Konnektivitätsproblem nicht beheben können, müssen Sie sich direkt an der Konsole des aktiven Knoten anmelden.
   a. Schalten Sie die virtuellen Maschinen des passiven Knotens und des Zeugenknotens aus und löschen Sie sie.
   b. Melden Sie sich mithilfe von SSH oder über die VM-Konsole beim aktiven Knoten an.
   c. Um die Bash-Shell zu aktivieren, geben Sie **`shell`** an der Eingabeaufforderung `appliancesh` ein.
   d. Führen Sie den folgenden Befehl aus, um die vCenter HA-Konfiguration zu entfernen.

      ```
      vcha-destroy -f
      ```

   e. Starten Sie den aktiven Knoten neu.

      Der aktive Knoten ist jetzt ein eigenständiger vCenter Server
   f. Führen Sie die vCenter HA-Clusterkonfiguration erneut durch.

Beheben von Failover-Fehlern

Wenn ein passiver Knoten während eines Failovers nicht zum aktiven Knoten wird, können Sie den passiven Knoten dazu zwingen, die Rolle des aktiven Knotens zu übernehmen.

Problem

Der passive Knoten schlägt fehl, während er versucht, die Rolle des aktiven Knotens zu übernehmen.

Ursache

Ein vCenter HA-Failover kann aus den folgenden Gründen fehlschlagen.

- Der Zeugenknoten ist nicht verfügbar, wenn der passive Knoten versucht, die Rolle des aktiven Knotens zu übernehmen.
- Es liegt ein Synchronisierungsfehler hinsichtlich des Serverzustands der beiden Knoten vor.

Lösung

Dieses Problem kann wie folgt behoben werden.

1 Wenn der aktive Knoten nach einem Ausfall wiederhergestellt wird, wird er erneut zum aktiven Knoten.

2 Wenn der Zeugenknoten nach einem Ausfall wiederhergestellt wird, führen Sie diese Schritte aus.

   a Melden Sie sich über die Konsole der virtuellen Maschine beim passiven Knoten an.

   b Um die Bash-Shell zu aktivieren, geben Sie **`shell`** an der Eingabeaufforderung `appliancesh` ein.

   c Führen Sie den folgenden Befehl aus.

   ```
   vcha-reset-primary
   ```

   d Starten Sie den passiven Knoten neu.

3 Wenn der aktive Knoten und der Zeugenknoten nicht wiederhergestellt werden können, können Sie den passiven Knoten zwingen, die Rolle eines eigenständigen vCenter Server zu übernehmen.

   a Löschen Sie die virtuellen Maschinen des aktiven Knotens und des Zeugenknotens.

   b Melden Sie sich über die Konsole der virtuellen Maschine beim passiven Knoten an.

   c Um die Bash-Shell zu aktivieren, geben Sie **`shell`** an der Eingabeaufforderung `appliancesh` ein.

   d Führen Sie den folgenden Befehl aus.

   ```
   vcha-destroy
   ```

   e Starten Sie den passiven Knoten neu.

VMware vCenter® HA-Alarme und -Ereignisse

Wenn ein vCenter HA-Cluster sich in einem fehlerhaften Zustand befindet, zeigen Alarme und Ereignisse Fehler an.

Problem

Tabelle 4-4. Die folgenden Ereignisse lösen den VCHA-Systemzustandsalarm in vpxd aus:

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
vCenter HA-Clusterzustand ist derzeit fehlerfrei	vCenter HA-Clusterzustand ist derzeit fehlerfrei	com.vmware.vcha.cluster.state.healthy	Info
vCenter HA-Clusterzustand ist derzeit fehlerhaft	vCenter HA-Clusterzustand ist derzeit fehlerhaft	com.vmware.vcha.cluster.state.degraded	Warnung
vCenter HA-Clusterzustand ist derzeit isoliert	vCenter HA-Clusterzustand ist derzeit isoliert	com.vmware.vcha.cluster.state.isolated	Fehler
vCenter HA-Cluster wird dauerhaft gelöscht	vCenter HA-Cluster wird dauerhaft gelöscht	com.vmware.vcha.cluster.state.destroyed	Info

Tabelle 4-5. Die folgenden Ereignisse lösen den PSC HA-Systemzustandsalarm in vpxd aus:

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
PSC HA-Zustand ist derzeit fehlerfrei	PSC HA-Zustand ist derzeit fehlerfrei	com.vmware.vcha.psc.ha.health.healthy	Info
PSC HA-Zustand ist derzeit fehlerhaft	PSC HA-Zustand ist derzeit fehlerhaft	com.vmware.vcha.psc.ha.health.degraded	Info
PSC HA wird nicht überwacht, nachdem der vCenter HA-Cluster gelöscht wurde	PSC HA-Zustand wird nicht überwacht	com.vmware.vcha.psc.ha.health.unknown	Info

Tabelle 4-6. Ereignisse im Zusammenhang mit dem Clusterstatus

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
Knoten {nodeName} wurde wieder zum Cluster hinzugefügt	Ein Knoten wurde wieder zum Cluster hinzugefügt	com.vmware.vcha.node.joined	Info
Knoten {nodeName} hat den Cluster verlassen	Ein Knoten hat den Cluster verlassen	com.vmware.vcha.node.left	Warnung
Failover erfolgreich	Failover erfolgreich	com.vmware.vcha.failover.succeeded	Info
Failover kann nicht fortgesetzt werden, wenn der Cluster sich im deaktivierten Modus befindet	Failover kann nicht fortgesetzt werden, wenn der Cluster sich im deaktivierten Modus befindet	com.vmware.vcha.failover.failed.disabled.mode	Warnung
Failover kann nicht fortgesetzt werden, wenn für den Cluster nicht alle drei Knoten verbunden sind	Failover kann nicht fortgesetzt werden, wenn für den Cluster nicht alle drei Knoten verbunden sind	com.vmware.vcha.failover.failed.node.lost	Warnung

Tabelle 4-6. Ereignisse im Zusammenhang mit dem Clusterstatus (Fortsetzung)

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
Failover kann nicht fortgesetzt werden, wenn vPostgres auf dem passiven Knoten nicht zur Übernahme bereit ist	Das Failover kann nicht fortgesetzt werden, wenn der passive Knoten nicht zur Übernahme bereit ist	com.vmware.vcha.failover.failed.passive.not.ready	Warnung
vCenter HA-Cluster-Modus wurde in {clusterMode} geändert	vCenter HA-Cluster-Modus wurde geändert	com.vmware.vcha.cluster.mode.changed	Info

Tabelle 4-7. Ereignisse im Zusammenhang mit der Datenbankreplikation

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
Datenbankreplikationsmodus zu {newState} geändert	Datenbankreplikationsstatus wurde geändert: synchron, asynchron oder keine Replikation	com.vmware.vcha.DB.replication.state.changed	Info

Tabelle 4-8. Ereignisse im Zusammenhang mit der Dateireplikation

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie
Die Appliance {fileProviderType} ist {state}.	Replikationsstatus der Appliance-Datei geändert	com.vmware.vcha.file.replication.state.changed	Info

Patchen einer vCenter-Umgebung mit hoher Verfügbarkeit

Sie können einen vCenter Server, der sich in einem vCenter High Availability-Cluster befindet, mithilfe des Dienstprogramms **`software-packages`** patchen, das in der vCenter Server-Shell zur Verfügung steht.

Weitere Informationen finden Sie unter *Patchen einer vCenter-Umgebung mit Hochverfügbarkeit* unter *vSphere-Upgrade*.

Upgrade mit reduzierter Ausfallzeit für vCenter HA

In vSphere 8.0 U3 ist das Upgrade mit reduzierter Ausfallzeit in die automatische vCenter HA-Bereitstellung integriert.

Das Upgrade mit reduzierter Ausfallzeit (Reduced Downtime Upgrade, RDU) ist ein migrationsbasiertes VCSA-Upgrade mit dem primären Ziel, die Ausfallzeiten für Upgrades zu reduzieren. Während des RDU-Upgrades werden die VCSA-Konfiguration, VCDB-Datenbank und die Netzwerkinformationen von der alten VCSA in die neue VCSA-Version kopiert, bevor

die Quell-VCSA heruntergefahren und zur Ziel-VCSA geswitcht wird. Während des Migrations-Upgrades wird in der Staging-Phase vor dem RDU-Switchover die Bereitstellung von VCHA automatisch aufgehoben. Für die Dauer des Upgrades ist keine VCHA vorhanden. Nach erfolgreichem RDU-Switchover wird die VCHA auf dem Zielknoten erneut bereitgestellt.

Das RDU-Upgrade ist in die automatische vCenter HA-Bereitstellung integriert, einschließlich selbstverwalteter vCenter- und nicht selbstverwalteter vCenter-Instanzen. Sie können vCenter ohne vCenter-Anmeldedaten aktualisieren, wenn die vCenter-Instanz selbstverwaltet ist. Sie müssen die Anmeldedaten für das Dienstkonto für die Verwaltung der vCenter-Instanz verwenden, die vom RDU-Framework bereitgestellt wird, wenn Sie ein Upgrade einer nicht selbstverwalteten vCenter-Instanz durchführen. Sie können ein Upgrade von vCenter Appliance vornehmen, die die VCHA enthält, ohne vCenter HA vor und nach dem Upgrade entfernen oder einrichten zu müssen. Wenn Sie das Upgrade abbrechen, führt das RDU-Rollback zu einer funktionsfähigen vCenter HA-Bereitstellung, wie sie vor dem Upgrade vorhanden war.