

# vSphere-Fehlerbehebung

Update 1

VMware vSphere 6.5

VMware ESXi 6.5

vCenter Server 6.5

**vmware**<sup>®</sup>

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

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

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2010–2017 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

# Inhalt

Grundlegende Informationen zur vSphere-Fehlerbehebung	5
<b>1 Fehlerbehebung – Überblick</b>	<b>7</b>
Richtlinien zur Fehlerbehebung	7
Fehlerbehebung mit Protokollen	9
<b>2 Fehlerbehebung bei virtuellen Maschinen</b>	<b>11</b>
Fehlerbehebung bei fehlertoleranten virtuellen Maschinen	11
Fehlerbehebung bei USB-Passthrough-Geräten	17
Wiederherstellen verwaister virtueller Maschinen	18
Eine virtuelle Maschine wird nach dem Klonen oder der Bereitstellung aus einer Vorlage nicht eingeschaltet	19
<b>3 Fehlerbehebung bei Hosts</b>	<b>21</b>
Fehlerbehebung von vSphere HA-Hostzuständen	21
Fehlerbehebung bei vSphere Auto Deploy	26
Authentifizierungstoken-Manipulationsfehler	32
Active Directory-Regelsatzfehler verursacht einen Fehler bei der Übereinstimmung des Hostprofils	32
Herunterladen von VIBs bei der Verwendung des vCenter Server -Reverse-Proxys ist nicht möglich	33
<b>4 Fehlerbehebung von vCenter Server und vSphere Web Client</b>	<b>35</b>
Fehlerbehandlung von vCenter Server	35
Fehlerbehebung im vSphere Web Client	36
Fehlerbehebung bei vCenter Server- und ESXi -Host-Zertifikaten	38
<b>5 Fehlerbehebung bei der Verfügbarkeit</b>	<b>41</b>
Fehlerbehebung bei der vSphere HA-Zugangsteuerung	41
Fehlerbehebung bei Taktsignal-Datenspeichern	43
Fehlerbehebung bei vSphere HA-Fehlerantwort	45
Fehlerbehebung bei vSphere Fault Tolerance in Netzwerkpartitionen	47
Fehlerbehebung bei VM Component Protection	48
<b>6 Fehlerbehebung bei der Ressourcenverwaltung</b>	<b>51</b>
Fehlerbehebung bei Speicher-DRS	51
Fehlerbehebung bei Storage I/O Control	57
<b>7 Fehlerbehebung beim Speicher</b>	<b>59</b>
Beheben von Anzeigeusername des SAN-Speichers	60
Beheben von SAN-Leistungsproblemen	62
Virtuelle Maschinen mit RDMs müssen den SCSI INQUIRY-Cache ignorieren	66
Der Software-iSCSI-Adapter ist aktiviert, wenn er nicht benötigt wird	67

- Fehler beim Mounten von NFS-Datenspeichern 67
- Fehlerbehebung bei Speicheradaptern 67
- Überprüfen der Metadatenkonsistenz mit VOMA 68
- Kein Failover für den Speicherpfad, wenn der TUR-Befehl nicht erfolgreich ist 70
- Fehlerbehebung bei Flash-Geräten 71
- Fehlerbehebung bei virtuellen Volumes 74
- Fehlerbehebung bei VAIO-Filtern 77

## 8 Fehlerbehebung beim Netzwerk 79

- Fehlerbehebung bei der Zuteilung von MAC-Adressen 80
- Die Konvertierung zur erweiterten LACP-Unterstützung schlägt fehl 83
- Host kann nicht auf einem vSphere Distributed Switch entfernt werden 84
- Für Hosts auf einem vSphere Distributed Switch 5.1 (und höher) wird die Verbindung zu vCenter Server getrennt 85
- Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt 86
- Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host 88
- Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt 88
- Einem vSphere Distributed Switch mit aktiviertem Network I/O Control kann kein physischer Adapter hinzugefügt werden 90
- Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten 90
- Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster 92
- Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen 94
- Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren 96
- Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt 96
- Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt 97

## 9 Fehlerbehebung bei der Lizenzierung 99

- Fehlerbehebung bei der Hostlizenzierung 99
- Einschalten einer virtuellen Maschine fehlgeschlagen 100
- Eine Funktion kann nicht konfiguriert oder verwendet werden 101

Index 103

# Grundlegende Informationen zur vSphere-Fehlerbehebung

---

Das *vSphere-Fehlerbehebungshandbuch* beschreibt Fehlerbehebungsprobleme und -vorgänge für VMware vCenter Server<sup>®</sup>-Implementierungen und verwandte Komponenten.

## Zielgruppe

Diese Informationen richten sich an alle Personen, die Fehler bei virtuellen Maschinen, ESXi-Hosts, Clustern und verwandten Speicherlösungen beheben möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datencenteroperationen vertraut sind.

---

**HINWEIS** Nicht alle Funktionen im vSphere Web Client wurden für den vSphere Client in der Version vSphere 6.5 implementiert. Eine aktuelle Liste nicht unterstützter Funktionen finden Sie im *Handbuch für Funktions-Updates für den vSphere Client* unter <http://www.vmware.com/info?id=1413>.

---



# Fehlerbehebung – Überblick

---

*vSphere-Fehlerbehebung* enthält allgemeine Fehlerbehebungsszenarien und Lösungen für die verschiedenen Probleme. Darüber hinaus finden Sie hier Richtlinien zum Beheben von Problemen, die ähnliche Ursachen haben. Für individuelle Probleme sollten Sie eventuell eine Fehlerbehebungsmethode entwickeln und einführen.

Die folgende Vorgehensweise für eine effektive Fehlerbehebung befasst sich mit der Erfassung von Fehlerbehebungsinformationen, wie etwa dem Identifizieren von Symptomen und dem Definieren des Problembereichs. Die Fehlerbehebung mit Protokolldateien wird ebenfalls behandelt.

Dieses Kapitel behandelt die folgenden Themen:

- „[Richtlinien zur Fehlerbehebung](#)“, auf Seite 7
- „[Fehlerbehebung mit Protokollen](#)“, auf Seite 9

## Richtlinien zur Fehlerbehebung

Für die Fehlerbehebung Ihrer vSphere-Implementierung identifizieren Sie die Symptome des Problems, bestimmen Sie die betroffenen Komponenten und testen Sie mögliche Lösungen.

<b>Identifizieren der Symptome</b>	Eine Reihe potenzieller Ursachen kann zur Leistungsminderung oder zum Leistungsausfall der Implementierung führen. Der erste Schritt für eine effiziente Fehlerbehebung ist die genaue Identifizierung des Problems.
<b>Definieren des Problembereichs</b>	Nachdem Sie die Symptome des Problems isoliert haben, müssen Sie den Problembereich definieren. Identifizieren Sie die betroffenen Software- oder Hardwarekomponenten, durch die das Problem möglicherweise verursacht wird, sowie die nicht betroffenen Software- oder Hardwarekomponenten.
<b>Testen möglicher Lösungen</b>	Wenn Sie die Symptome des Problems und die betroffenen Komponenten kennen, können Sie die Lösungen solange systematisch testen, bis das Problem behoben ist.



Allgemeines zur Fehlerbehebung ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vsphere\\_troubleshooting](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_troubleshooting))

## Identifizieren der Symptome

Bevor Sie versuchen, ein Problem in Ihrer Implementierung zu beheben, müssen Sie die genauen Fehler-symptome identifizieren.

Der erste Schritt bei der Fehlerbehebung ist das Erfassen von Informationen zu den genauen Symptomen. Sie können sich beim Erfassen dieser Informationen die folgende Fragen stellen:

- Welche Aufgabe wird nicht ausgeführt bzw. welches Verhalten ist nicht vorhanden?

- Kann die betroffene Aufgabe in Unteraufgaben unterteilt werden, die Sie separat auswerten können?
- Endet die Aufgabe mit einem Fehler? Ist eine Fehlermeldung damit verbunden?
- Wird die Aufgabe zwar ausgeführt, dauert aber unzumutbar lange?
- Tritt der Fehler kontinuierlich oder sporadisch auf?
- Welche Änderungen gab es in letzter Zeit bei Software oder Hardware, die in Zusammenhang mit dem Fehler stehen könnten?

## Definieren des Problembereichs

Nachdem Sie die Symptome des Problems identifiziert haben, bestimmen Sie die betroffenen Komponenten, die Komponenten, die das Problem verursachen, sowie die nicht beteiligten Komponenten.

Bei der Definition des Problembereichs in einer vSphere-Implementierung müssen Sie die vorhandenen Komponenten berücksichtigen. Neben VMware-Software sollten Sie auf die verwendete Drittanbietersoftware und die mit der virtuellen VMware-Hardware verwendete Hardware achten.

Wenn Sie die Merkmale der Software- und Hardwarekomponenten und deren Auswirkungen auf das Problem kennen, können Sie allgemeine Probleme analysieren, die die Symptome verursachen.

- Fehlkonfiguration der Softwareeinstellungen
- Fehler bei der physischen Hardware
- Inkompatibilität der Komponenten

Schlüsseln Sie den Vorgang auf und erstellen Sie eine separate Analyse jeder Komponente und der Wahrscheinlichkeit, dass die jeweilige Komponente die Ursache sein könnte. Beispielsweise hat ein Problem in Zusammenhang mit einer virtuellen Festplatte im lokalen Speicher wahrscheinlich nichts mit der Konfiguration des Drittanbierrouters zu tun. Allerdings könnte dieses Problem durch eine Einstellung für den lokalen Festplatten-Controller verursacht werden. Wenn eine Komponente nichts mit den spezifischen Symptomen zu tun hat, können Sie sie wahrscheinlich als Kandidat für Lösungstests eliminieren.

Überlegen Sie sich, was zuletzt an der Konfiguration geändert wurde, bevor die Probleme auftauchten. Suchen Sie nach Gemeinsamkeiten bei einem Problem. Wenn mehrere Probleme gleichzeitig auftauchten, sind wahrscheinlich alle Probleme auf dieselbe Ursache zurückzuführen.

## Testen möglicher Lösungen

Wenn Sie die Symptome des Problems und die höchstwahrscheinlich betroffenen Software- oder Hardwarekomponenten kennen, können Sie die Lösungen solange systematisch testen, bis das Problem behoben ist.

Anhand der ermittelten Informationen zu den Symptomen und betroffenen Komponenten können Sie Tests entwickeln, um das Problem ausfindig zu machen und zu beheben. Mithilfe der folgenden Tipps wird dieser Vorgang möglicherweise effektiver ausgeführt.

- Generieren Sie Ideen für möglichst viele potenzielle Lösungen.
- Stellen Sie sicher, dass jede Lösung unmissverständlich bestimmt, ob das Problem behoben wurde. Testen Sie jede potenzielle Lösung, aber fahren Sie unverzüglich fort, falls das Problem durch die Fehlerkorrektur nicht behoben wird.
- Entwickeln und verfolgen Sie eine Hierarchie potenzieller Lösungen auf der Grundlage der Wahrscheinlichkeit. Eliminieren Sie systematisch jedes potenzielle Problem ausgehend von der wahrscheinlichsten Ursache bis hin zur unwahrscheinlichsten Ursache, bis die Symptome verschwinden.
- Ändern Sie beim Testen potenzieller Lösungen immer nur einen Faktor. Wenn das System funktioniert, nachdem Sie viele Faktoren gleichzeitig geändert haben, lässt sich möglicherweise nicht feststellen, auf welche Änderung dies zurückzuführen ist.



- Wenn das Problem durch die für eine Lösung vorgenommenen Änderungen nicht behoben werden kann, setzen Sie die Implementierung auf den vorherigen Status zurück. Für den Fall, dass Sie die Implementierung nicht auf den vorherigen Status zurücksetzen, könnten neue Fehler verursacht werden.
- Suchen Sie eine ähnliche, funktionierende Implementierung und testen Sie sie parallel zu der fehlerhaften Implementierung. Nehmen Sie an beiden Systemen gleichzeitig Änderungen vor, bis nur noch wenige Unterschiede vorhanden sind oder nur noch ein Unterschied vorhanden ist.

## Fehlerbehebung mit Protokollen

Die Protokolle der verschiedenen Dienste und Agenten, die von Ihrer Implementierung verwendet werden, liefern oft hilfreiche Fehlerbehebungsinformationen.

Die meisten Protokolle sind unter `C:\ProgramData\VMware\vCenterServer\logs` für Windows-Bereitstellungen oder `/var/log/` für Linux-Bereitstellungen gespeichert. Gemeinsame Protokolle sind in allen Implementierungen verfügbar. Andere Protokolle gelten speziell für bestimmte Bereitstellungsoptionen (Verwaltungsknoten oder Platform Services Controller).

### Gemeinsame Protokolle

Die folgenden Protokolle werden gemeinsam von allen Bereitstellungen unter Windows oder Linux verwendet.

**Tabelle 1-1.** Verzeichnisse für gemeinsame Protokolle

Protokollverzeichnis	Beschreibung
applmgmt	VMware Appliance Management Service
CloudVM	Protokolle für die Zuteilung und Verteilung von Ressourcen zwischen Diensten
CM	VMware Component Manager
FirstBoot	Speicherort der Protokolle für den erstmaligen Start
rhttpproxy	Reverse Web Proxy
SCA	VMware Service Control Agent
statsmonitor	Vmware Appliance-Überwachungsdienst (nur Linux)
Vapi	VMware-vAPI-Endpoint
vmaffd	VMware Authentication Framework-Daemon
vmdird	VMware Directory Service-Daemon
vmon	VMware Service Lifecycle Manager

### Protokolle des Verwaltungsknotens

Die folgenden Protokolle sind verfügbar, wenn eine Verwaltungsknotenbereitstellung gewählt wird.

**Tabelle 1-2.** Protokolle des Verwaltungsknotens

Protokoll	Beschreibung
Auto Deploy	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
EAM	VMware ESX Agent Manager
InvSvc	VMware Inventory-Dienst
Mbcs	VMware-Meldungs-Bus-Konfigurationsdienst
Netdump	VMware vSphere ESXi Dump Collector

**Tabelle 1-2.** Protokolle des Verwaltungsknotens (Fortsetzung)

<b>Protokoll</b>	<b>Beschreibung</b>
Perfcharts	VMware-Leistungsdiagramme
vmcam	VMware vSphere Authentication Proxy
VMdird	VMware Directory Service-Daemon
vmsyslog collector	vSphere Syslog Collector (nur Windows)
Vmware-sps	VMware vSphere Profile-Driven Storage Service
Vmware-vpx	VMware VirtualCenter Server
vPostgres	vFabric Postgres-Datenbankdienst
MBCS	VMware-Meldungs-Bus-Konfigurationsdienst
vSphere-Client	VMware vSphere Web Client
vcha	VMware High Availability-Dienst (nur Linux)

## Protokolle des Platform Services Controller

Sie analysieren die folgenden Protokolle, wenn eine Platform Services Controller-Knotenbereitstellung gewählt wird.

**Tabelle 1-3.** Protokolle des Platform Services Controller-Knotens

<b>Protokoll</b>	<b>Beschreibung</b>
cis-license	VMware-Lizenzierungsdienst
SSO	VMware Secure Token Service
Vmcaad	VMware Certificate Authority-Daemon
vmdird	VMware Directory Service

Für Platform Services Controller-Knotenbereitstellungen befinden sich zusätzliche Laufzeitprotokolle unter `C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs`.

# Fehlerbehebung bei virtuellen Maschinen

# 2

In den Themen zur Fehlerbehebung bei virtuellen Maschinen finden Sie Lösungen für potenzielle Probleme, die bei der Verwendung Ihrer virtuellen Maschinen auftreten können.

Dieses Kapitel behandelt die folgenden Themen:

- „Fehlerbehebung bei fehlertoleranten virtuellen Maschinen“, auf Seite 11
- „Fehlerbehebung bei USB-Passthrough-Geräten“, auf Seite 17
- „Wiederherstellen verwaister virtueller Maschinen“, auf Seite 18
- „Eine virtuelle Maschine wird nach dem Klonen oder der Bereitstellung aus einer Vorlage nicht eingeschaltet“, auf Seite 19

## 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-Fähigkeit 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-CPU 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 evakuiert wurden

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

**Problem**

Weil 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.



## Fehlerbehebung bei USB-Passthrough-Geräten

Informationen zum Verhalten von Funktionen sind für die Fehlerbehebung nützlich oder können dabei helfen, potenzielle Probleme zu vermeiden, wenn USB-Geräte mit einer virtuellen Maschine verbunden sind.

### Fehlermeldung, wenn Sie versuchen, eine virtuelle Maschine mit angehängten USB-Geräten zu migrieren

Die Migration mit vMotion kann nicht fortgesetzt werden und es wird eine verwirrende Fehlermeldung ausgegeben, wenn mehrere USB-Geräte von einem ESXi-Host mit einer virtuellen Maschine verbunden werden und mindestens ein Gerät nicht für vMotion aktiviert ist.

#### Problem

Der Assistent für das Migrieren einer virtuellen Maschine führt vor dem Starten des Migrationsvorgangs eine Kompatibilitätsprüfung aus. Wenn nicht unterstützte USB-Geräte ermittelt werden, tritt bei der Kompatibilitätsprüfung ein Fehler auf und es wird eine Fehlermeldung nach folgendem Muster ausgegeben: Aktuell verbundenes Gerät 'USB 1' verwendet Backing 'Pfad:1/7/1', auf das nicht zugegriffen werden kann.

#### Ursache

Sie müssen alle USB-Geräte aktivieren, die mit der virtuellen Maschine von einem Host für vMotion verbunden sind, um die vMotion-Kompatibilitätsprüfungen erfolgreich zu bestehen. Wenn ein oder mehrere Geräte nicht für vMotion aktiviert sind, schlägt die Migration fehl.

#### Lösung

- 1 Stellen Sie vor dem Entfernen der Geräte sicher, dass diese keine Daten übertragen.
- 2 Fügen Sie sie wieder hinzu und aktivieren Sie vMotion für jedes betroffene USB-Gerät.

### Daten können nicht von einem ESXi -Host auf ein USB-Gerät kopiert werden, das mit dem Host verbunden ist

Sie können ein USB-Gerät an einen ESXi-Host anschließen und Daten vom Host auf das Gerät kopieren. Sie könnten beispielsweise das vm-support-Paket vom Host sammeln, falls die Netzwerkverbindung des Hosts unterbrochen wird. Um diese Aufgabe auszuführen, müssen Sie den USB-Arbitrator anhalten.

#### Problem

Wenn der USB-Arbitrator für den USB-Passthrough von einem ESXi-Host auf eine virtuelle Maschine verwendet wird, erscheint das USB-Gerät unter `lsusb`, aber es wird nicht ordnungsgemäß gemountet.

#### Ursache

Dieses Problem tritt auf, weil das nicht startfähige USB-Gerät standardmäßig für die virtuelle Maschine reserviert ist. Es erscheint auch dann nicht auf dem Dateisystem des Hosts, wenn `lsusb` das Gerät anzeigt.

#### Lösung

- 1 Halten Sie den `usbarbitrator`-Dienst an: `/etc/init.d/usbarbitrator stop`
- 2 Trennen Sie das USB-Gerät physisch und verbinden Sie es neu.  
Standardmäßig befindet sich das Gerät im Verzeichnis `/vmfs/devices/disks/mpx.vmhbaXX:C0:T0:L0`.
- 3 Starten Sie nach der Wiederherstellung der Verbindung des Geräts den `usbarbitrator`-Dienst neu: `/etc/init.d/usbarbitrator start`
- 4 Starten Sie `hostd` und alle ausgeführten virtuellen Maschinen neu, um den Zugriff auf Passthrough-Geräte in der virtuellen Maschine wiederherzustellen.

## Weiter

Verbinden Sie die USB-Geräte zur virtuellen Maschine neu.

## Wiederherstellen verwaister virtueller Maschinen

Virtuelle Maschinen werden mit dem Zusatz (orphaned) zu ihren Namen angezeigt.

### Problem

Virtuelle Maschinen, die sich auf einem ESXi-Host befinden, der von vCenter Server verwaltet wird, können in seltenen Fällen verwaisten. Solche virtuellen Maschinen sind in der vCenter Server-Datenbank vorhanden, der ESXi-Host erkennt sie jedoch nicht mehr.

### Ursache

Virtuelle Maschinen können verwaisten, wenn ein Host-Failover fehlschlägt oder die Registrierung der virtuellen Maschine direkt auf dem Host aufgehoben wird. In diesem Fall verschieben Sie die verwaiste virtuelle Maschine auf einen anderen Host im Datacenter, auf dem die Dateien der virtuellen Maschine gespeichert sind.

### Lösung

- 1 Bestimmen Sie den Datenspeicher, in dem die VM-Konfigurationsdatei (.vmx) gespeichert ist.
  - a Wählen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client aus und klicken Sie auf die Registerkarte **Datenspeicher**.  
  
Der Datenspeicher bzw. die Datenspeicher, in dem bzw. denen die VM-Dateien gespeichert sind, wird bzw. werden angezeigt.
  - b Falls mehrere Datenspeicher angezeigt werden, wählen Sie jeden Datenspeicher aus und klicken Sie für die .vmx-Datei auf das Dateibrowser-Symbol.
  - c Überprüfen Sie den Speicherort der .vmx-Datei.
- 2 Wechseln Sie wieder zur virtuellen Maschine im vSphere Web Client, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Alle Virtual Infrastructure-Aktionen > Aus Bestandsliste entfernen** aus.
- 3 Klicken Sie auf **Ja**, um das Entfernen der virtuellen Maschine zu bestätigen.
- 4 Registrieren Sie die virtuelle Maschine erneut für vCenter Server.
  - a Klicken Sie mit der rechten Maustaste auf den Datenspeicher, in dem die VM-Datei gespeichert ist, und wählen Sie **VM registrieren** aus.
  - b Navigieren Sie zur .vmx-Datei und klicken Sie auf **OK**.
  - c Wählen Sie den Speicherort für die virtuelle Maschine aus und klicken Sie auf **Weiter**.
  - d Wählen Sie den Host aus, auf dem die virtuelle Maschine ausgeführt werden soll, und klicken Sie auf **Weiter**.
  - e Klicken Sie auf **Beenden**.

## Eine virtuelle Maschine wird nach dem Klonen oder der Bereitstellung aus einer Vorlage nicht eingeschaltet

Virtuelle Maschinen werden nicht eingeschaltet, nachdem Sie im vSphere Web Client den Workflow des Klonens bzw. Bereitstellens aus einer Vorlage abgeschlossen haben.

### Problem

Wenn Sie eine virtuelle Maschine klonen oder eine virtuelle Maschine anhand einer Vorlage bereitstellen, können Sie die virtuelle Maschine nach dem Erstellen möglicherweise nicht einschalten.

### Ursache

Die Größe der Auslagerungsdatei wird nicht reserviert, wenn die VM-Festplatten erstellt werden.

### Lösung

- Verringern Sie die Größe der Auslagerungsdatei, die für die virtuelle Maschine benötigt wird. Sie erreichen dies, indem Sie mehr Arbeitsspeicher für die virtuelle Maschine reservieren.
  - a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
  - b Wählen Sie **Virtuelle Hardware** aus und klicken Sie auf **Arbeitsspeicher**.
  - c Verwenden Sie das Dropdown-Menü „Reservierung“, um die Menge des Arbeitsspeichers zu erhöhen, die der virtuellen Maschine zugeteilt wird.
  - d Klicken Sie auf **OK**.
- Alternativ können Sie die Menge an verfügbarem Speicherplatz für die Auslagerungsdatei erhöhen, indem Sie andere VM-Festplatten aus dem Datenspeicher, der für die Auslagerungsdatei verwendet wird, heraus verschieben.
  - a Navigieren Sie zum Datenspeicher im Objektnavigator von vSphere Web Client.
  - b Wählen Sie die Registerkarte **VMs** aus.
  - c Klicken Sie mit der rechten Maustaste auf jede zu verschiebende virtuelle Maschine und wählen Sie **Migrieren**.
  - d Wählen Sie **Nur Speicher ändern** aus.
  - e Führen Sie den Assistenten Migrieren von virtuellen Maschinen aus.
- Sie können auch die Menge an verfügbarem Speicherplatz für die Auslagerungsdatei erhöhen, indem Sie als Speicherort der Auslagerungsdatei einen Datenspeicher mit entsprechendem Speicherplatz wählen.
  - a Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.
  - b Wählen Sie die Registerkarte **Konfigurieren** aus.
  - c Wählen Sie unter „Virtuelle Maschinen“ die Option **Speicherort der Auslagerungsdatei** aus.
  - d Klicken Sie auf **Bearbeiten**.

---

**HINWEIS** Wenn der Host Teil eines Clusters ist, für den festgelegt ist, dass die Auslagerungsdateien der virtuellen Maschine in demselben Verzeichnis wie die virtuelle Maschine gespeichert werden, können Sie nicht auf **Bearbeiten** klicken. Sie müssen das Dialogfeld „Clustereinstellungen“ verwenden, um die Richtlinie zum Ändern des Speicherorts der Auslagerungsdatei für den Cluster zu ändern.

---

- e Wählen Sie **Bestimmten Datenspeicher verwenden** und wählen Sie einen Datenspeicher aus der Liste aus.
- f Klicken Sie auf **OK**.

## Fehlerbehebung bei Hosts

---

In den Themen zur Fehlerbehebung bei Hosts finden Sie Lösungen für potenzielle Probleme, die bei der Verwendung Ihrer vCenter Server und ESXi-Hosts auftreten können.

Dieses Kapitel behandelt die folgenden Themen:

- [„Fehlerbehebung von vSphere HA-Hostzuständen“](#), auf Seite 21
- [„Fehlerbehebung bei vSphere Auto Deploy“](#), auf Seite 26
- [„Authentifizierungstoken-Manipulationsfehler“](#), auf Seite 32
- [„Active Directory-Regelsatzfehler verursacht einen Fehler bei der Übereinstimmung des Hostprofils“](#), auf Seite 32
- [„Herunterladen von VIBs bei der Verwendung des vCenter Server-Reverse-Proxys ist nicht möglich“](#), auf Seite 33

### Fehlerbehebung von vSphere HA-Hostzuständen

vCenter Server meldet vSphere HA-Hostzustände, die auf einen Fehler auf dem Host hinweisen. Solche Fehler können verhindern, dass vSphere HA die virtuellen Maschinen auf dem Host vollständig schützt, und die Fähigkeit von vSphere HA zum Neustarten virtueller Maschinen nach einem Ausfall beeinträchtigen. Fehler können auftreten, wenn vSphere HA auf einem Host konfiguriert oder die Konfiguration aufgehoben wird, oder in selteneren Fällen während des normalen Betriebs. Wenn dies geschieht, sollten Sie ermitteln, wie der Fehler behoben werden kann, damit vSphere HA voll funktionsfähig ist.

#### Der vSphere HA-Agent befindet sich im Zustand „HA-Agent nicht erreichbar“

Der vSphere HA-Agent auf einem Host befindet sich für eine Minute oder länger im Zustand „HA-Agent nicht erreichbar“. Der Benutzer muss möglicherweise eingreifen, um diesen Zustand zu beheben.

##### Problem

vSphere HA meldet, dass sich ein Agent im Zustand „Agent nicht erreichbar“ befindet, wenn der Agent für den Host nicht vom Master-Host oder vCenter Server kontaktiert werden kann. Folglich ist vSphere HA nicht in der Lage, die virtuellen Maschinen auf dem Host zu überwachen, und kann möglicherweise diese nach einem Ausfall nicht neu starten.

##### Ursache

Es gibt mehrere Gründe, weshalb sich ein vSphere HA-Agent im Zustand „Agent nicht erreichbar“ befinden kann. In der Regel bedeutet dieser Zustand, dass ein Netzwerkproblem vCenter Server oder den Master-Host daran hindert, den Agent auf dem Host zu kontaktieren, oder dass alle Hosts im Cluster ausgefallen sind. Dieser Zustand kann auch auf den eher unwahrscheinlichen Fall hindeuten, dass vSphere HA auf dem

Cluster deaktiviert und anschließend wieder aktiviert wurde, während vCenter Server nicht mit dem vSphere HA-Agenten auf dem Host kommunizieren konnte, oder dass der ESXi-Host-Agent auf dem Host ausgefallen ist und der Watchdog-Prozess ihn nicht neu starten konnte. In jedem dieser Fälle wird kein Failover-Ereignis ausgelöst, wenn ein Host in den Zustand „Unerreichbar“ übergeht.

### Lösung

Überprüfen Sie, ob vCenter Server meldet, dass der Host nicht reagiert. Ist dies der Fall, liegt ein Netzwerkproblem, der Ausfall eines ESXi-Host-Agenten oder der vollständige Ausfall eines Clusters vor. Nach Behebung des Problems sollte vSphere HA ordnungsgemäß funktionieren. Ist dies nicht der Fall, konfigurieren Sie vSphere HA auf dem Host neu. Wenn vCenter Server meldet, dass die Hosts antworten, der Zustand eines Hosts jedoch „Agent nicht erreichbar“ ist, müssen Sie ebenfalls vSphere HA auf dem betreffenden Host neu konfigurieren.

## Der vSphere HA-Agent befindet sich im Zustand „Nicht initialisiert“

Der vSphere HA-Agent auf einem Host befindet sich für eine Minute oder länger im Zustand „Nicht initialisiert“. Der Benutzer muss möglicherweise eingreifen, um diesen Zustand zu beheben.

### Problem

vSphere HA meldet, dass sich ein Agent im Zustand „Nicht initialisiert“ befindet, wenn der Agent für den Host nicht in den Ausführungszustand versetzt werden kann, um zum Master-Host zu werden, oder keine Verbindung zum Master-Host herstellen kann. Folglich ist vSphere HA nicht in der Lage, die virtuellen Maschinen auf dem Host zu überwachen, und kann möglicherweise diese nach einem Ausfall nicht neu starten.

### Ursache

Es gibt einen oder mehrere Gründe, weshalb sich ein vSphere HA-Agent im Zustand „Nicht initialisiert“ befinden kann. In der Regel bedeutet dieser Zustand, dass der Host keinen Zugriff auf die Datenspeicher hat. In wenigen Fällen kann dieser Zustand auch bedeuten, dass der Host keinen Zugriff auf seinen lokalen Datenspeicher hat, auf dem vSphere HA Statusinformationen zwischenspeichert, der Agent auf dem Host nicht erreichbar ist oder der vSphere HA-Agent die erforderlichen Firewallports nicht öffnen kann. Es ist auch möglich, dass der ESXi-Host-Agent gestoppt wurde.

### Lösung

Suchen Sie in der Liste der Hostereignisse nach den jüngsten Vorkommnissen des Ereignisses vSphere HA Agent for the host has an error. Dieses Ereignis gibt den Grund an, weshalb sich der Host im Zustand „Nicht initialisiert“ befindet. Falls der Zustand aufgrund eines Datenspeicherproblems besteht, beheben Sie das Problem, das verhindert, dass der Host auf die betroffenen Datenspeicher zugreifen kann. Wenn der ESXi-Host-Agent gestoppt wurde, müssen Sie ihn neu starten. Falls der Agent nach der Behebung des Problems nicht wieder in einen betriebsbereiten Zustand wechselt, konfigurieren Sie vSphere HA auf dem Host neu.

---

**HINWEIS** Falls der Zustand auf ein Firewallproblem zurückzuführen ist, prüfen Sie, ob ein anderer Dienst auf dem Host Port 8182 verwendet. Ist dies der Fall, beenden Sie diesen Dienst und konfigurieren vSphere HA neu.

---

## Der vSphere HA-Agent befindet sich im Zustand „Initialisierungsfehler“

Der vSphere HA-Agent auf einem Host befindet sich für eine Minute oder länger im Zustand „Initialisierungsfehler“. Der Benutzer muss eingreifen, um diesen Zustand zu beheben.

### Problem

vSphere HA meldet, dass sich ein Agent im Zustand „Initialisierungsfehler“ befindet, wenn der letzte Versuch, vSphere HA für den Host zu konfigurieren, fehlgeschlagen ist. vSphere HA überwacht die virtuellen Maschinen auf einem solchen Host nicht und startet sie nach einem Ausfall möglicherweise nicht.

### Ursache

In der Regel deutet dieser Zustand darauf hin, dass vCenter Server keine Verbindung zum Host herstellen konnte, als der vSphere HA-Agent auf dem Host installiert oder konfiguriert wurde. Er könnte auch bedeuten, dass zwar die Installation und Konfiguration abgeschlossen sind, aber der Agent nicht innerhalb der festgelegten Zeit zum Master-Host oder Slave-Host wurde. Seltener ist der Zustand ein Hinweis darauf, dass nicht genügend Speicherplatz auf dem lokalen Datenspeicher des Hosts vorhanden ist, um den Agenten zu installieren, oder es zu wenig nicht reservierte Arbeitsspeicherressourcen auf dem Host für den Agentenressourcenpool gibt. Schließlich schlägt die Konfiguration für ESXi 5.x-Hosts fehl, wenn durch die vorherige Installation einer anderen Komponente ein Neustart erforderlich war, der Neustart jedoch noch nicht erfolgt ist.

### Lösung

Wenn eine Aufgabe zum Konfigurieren von HA fehlschlägt, wird die Fehlerursache gemeldet.

Fehlerursache	Aktion
Hostkommunikationsfehler	Beheben Sie alle Kommunikationsprobleme mit dem Host und wiederholen Sie den Konfigurationsvorgang.
Zeitüberschreitungsfehler	Mögliche Ursachen sind: Der Host ist während der Konfigurationsaufgabe ausgefallen, der Agent konnte nach der Installation nicht gestartet werden oder der Agent konnte sich nach dem Start nicht initialisieren. Stellen Sie sicher, dass vCenter Server mit dem Host kommunizieren kann. Wenn dies der Fall ist, finden Sie mögliche Lösungen in „Der vSphere HA-Agent befindet sich im Zustand „HA-Agent nicht erreichbar““, auf Seite 21 oder „Der vSphere HA-Agent befindet sich im Zustand „Nicht initialisiert““, auf Seite 22.
Mangel an Ressourcen	Geben Sie ungefähr 75 MB Festplattenspeicher frei. Wenn der Fehler auf unzureichenden nicht reservierten Arbeitsspeicher zurückzuführen ist, geben Sie auf dem Host Arbeitsspeicher frei, indem Sie entweder virtuelle Maschinen auf einen anderen Host verlagern oder deren Reservierungen reduzieren. In beiden Fällen wiederholen Sie die vSphere HA-Konfigurationsaufgabe, nachdem Sie das Problem behoben haben.
Neustart ausstehend	Wenn die Installation eines Hosts der Version 5.0 oder höher fehlschlägt, weil ein Neustart noch aussteht, starten Sie den Host neu und wiederholen Sie die vSphere HA-Konfigurationsaufgabe.

## Der vSphere HA-Agent befindet sich im Zustand „Fehler beim Aufheben der Initialisierung“

Der vSphere HA-Agent auf einem Host befindet sich im Zustand „Fehler beim Aufheben der Initialisierung“. Der Benutzer muss eingreifen, um diesen Zustand zu beheben.

### Problem

vSphere HA meldet, dass sich ein Agent im Zustand „Fehler beim Aufheben der Initialisierung“ befindet, wenn vCenter Server die Konfiguration des Agenten auf dem Host, während die Aufgabe zum Aufheben der Konfiguration von HA ausgeführt wird, nicht aufheben kann. Ein Agent, der in diesem Zustand verbleibt, kann die Betriebsfähigkeit des Clusters beeinträchtigen. Beispielsweise kann der Agent auf dem Host sich selbst zum Master-Host wählen und einen Datenspeicher sperren. Das Sperren eines Datenspeichers hindert den gültigen Cluster-Master-Host daran, die virtuellen Maschinen zu verwalten, deren Konfigurationsdateien sich auf diesem Datenspeicher befinden.

### Ursache

Diese Bedingung bedeutet in der Regel, dass vCenter Server die Verbindung zum Host verloren hat, während die Konfiguration des Agenten aufgehoben wurde.

### Lösung

Fügen Sie den Host wieder zu vCenter Server der Version 5.0 oder höher hinzu. Der Host kann als eigenständiger Host oder einem Cluster hinzugefügt werden.

## Der vSphere HA-Agent befindet sich im Zustand „Host ausgefallen“

Der vSphere HA-Agent auf einem Host befindet sich im Zustand „Host ausgefallen“. Der Benutzer muss eingreifen, um den Zustand zu beheben.

### Problem

Normalerweise deuten diese Berichte darauf hin, dass ein Host tatsächlich ausgefallen ist. Andererseits können Fehlerberichte manchmal falsch sein. Ein ausgefallener Host sorgt für eine Verringerung der verfügbaren Kapazität im Cluster und im Falle eines falschen Berichts wird vSphere HA daran gehindert, die auf dem Host ausgeführten virtuellen Maschinen zu schützen.

### Ursache

Der Hostzustand wird gemeldet, wenn der vSphere HA-Master-Host, mit dem vCenter Server verbunden ist, keine Kommunikation mit dem Host und den für den Host eingesetzten Taktsignal-Datenspeichern aufnehmen kann. Jeder Speicherfehler, der dazu führt, dass die Hosts nicht auf die Datenspeicher zugreifen können, kann diesen Zustand verursachen, wenn gleichzeitig das Netzwerk ausfällt.

### Lösung

Überprüfen Sie die gemeldeten Fehlerzustände und beheben Sie sie.

## Der vSphere HA-Agent befindet sich im Zustand „Netzwerkpartitioniert“

Der vSphere HA-Agent auf einem Host befindet sich im Zustand „Netzwerkpartitioniert“. Der Benutzer muss möglicherweise eingreifen, um diesen Zustand zu beheben.

### Problem

Während die auf dem Host ausgeführten virtuellen Maschinen weiterhin von den Master-Hosts überwacht werden, die für sie verantwortlich sind, wird die Fähigkeit von vSphere HA, die virtuellen Maschinen nach einem Ausfall neu zu starten, beeinträchtigt. Erstens kann jeder Master-Host auf eine Teilmenge der Hosts zugreifen, sodass jedem Host weniger Failover-Kapazitäten zur Verfügung stehen. Zweitens kann vSphere HA eine sekundäre VM von Fault Tolerance nach einem Ausfall möglicherweise nicht neu starten (weitere Informationen erhalten Sie unter [„Primäre virtuelle Maschine verbleibt im Zustand „Sekundäre VM erforderlich““](#), auf Seite 47).

### Ursache

Ein Host wird als partitioniert gemeldet, wenn die beiden folgenden Bedingungen erfüllt sind:

- Der vSphere HA-Master-Host, mit dem vCenter Server verbunden ist, kann nicht über das Verwaltungsnetzwerk (oder das VMware vSAN™-Netzwerk) mit dem Host kommunizieren. Er kann jedoch mithilfe der Taktsignal-Datenspeicher, die für den Host ausgewählt wurden, mit diesem Host kommunizieren.
- Der Host ist nicht isoliert.

Eine Netzwerkpartition kann aus mehreren Gründen eintreten, z. B. auch falsches VLAN-Tagging, den Ausfall einer physischen Netzwerkkarte oder eines Switches, das Konfigurieren eines Clusters mit einigen Hosts, die nur IPv4 verwenden, und anderen, die nur IPv6 verwenden, oder das Verschieben einiger Hosts auf einen anderen virtuellen Switch, ohne vorher den Host in den Wartungsmodus versetzt zu haben.

### Lösung

Beheben Sie das Netzwerkproblem, das verhindert, dass die Hosts über die Verwaltungsnetzwerke kommunizieren.



## Der vSphere HA-Agent befindet sich im Zustand „Netzwerkisoliert“

Der vSphere HA-Agent auf einem Host befindet sich im Zustand „Netzwerkisoliert“. Der Benutzer muss eingreifen, um diesen Zustand zu beheben.

### Problem

Wenn sich ein Host im Zustand „Netzwerkisoliert“ befindet, müssen zwei Dinge berücksichtigt werden: der isolierte Host und der vSphere HA-Agent, der über die Masterrolle verfügt.

- Der vSphere HA-Agent wendet auf dem isolierten Host die konfigurierte Isolierungsreaktion auf die ausgeführten VMs an und bestimmt, ob sie heruntergefahren oder ausgeschaltet werden sollten. Dies erfolgt nach der Überprüfung, ob ein Master-Agent die Verantwortung für jede VM übernehmen kann (durch Sperren des Home-Datenspeichers der VM). Andernfalls verschiebt der Agent das Anwendung der Isolierungsreaktion für die VM und überprüft den Datenspeicher-Zustand nach einer kurzen Verzögerung erneut.
- Falls der vSphere HA-Master-Agent auf Datenspeicher zugreifen kann, werden die VMs überwacht, die auf dem Host ausgeführt wurden, als dieser isoliert wurde. Außerdem wird versucht, VMs neu zu starten, die ausgeschaltet oder heruntergefahren wurden.

### Ursache

Ein Host ist netzwerkisoliert, wenn beide der folgenden Bedingungen erfüllt sind:

- Isolierungsadressen wurden konfiguriert und der Host kann sie nicht anpingen.
- Der vSphere HA-Agent auf dem Host kann auf keinen der Agenten zugreifen, die auf den anderen Clusterhosts ausgeführt werden.

---

**HINWEIS** Wenn für den vSphere HA-Cluster vSAN aktiviert ist, gilt ein Host als isoliert, wenn er weder mit den anderen vSphere HA-Agents im Cluster kommunizieren noch die konfigurierten Isolationsadressen erreichen kann. Obwohl die vSphere HA-Agents das vSAN-Netzwerk für die Kommunikation zwischen Agents verwenden, ist die Standardisolationsadresse weiterhin das Gateway des Hosts. In der Standardkonfiguration müssen deshalb beide Netzwerke ausfallen, damit ein Host als isoliert erklärt wird.

---

### Lösung

Beheben Sie das Netzwerkproblem, das verhindert, dass der Host seine Isolierungsadressen nicht anpingen und nicht mit anderen Hosts kommunizieren kann.

## Konfiguration von vSphere HA führt zu Zeitüberschreitungen auf Hosts

Die Konfiguration eines vSphere HA-Clusters kann bei einige Hosts, die zum Cluster hinzugefügt werden, zu einer Zeitüberschreitung führen.

### Problem

Wenn Sie vSphere HA auf einem vorhandenen Cluster mit einer großen Anzahl Hosts und virtueller Maschinen aktivieren, kann das Setup von vSphere HA möglicherweise auf einigen Hosts fehlschlagen.

### Ursache

Dieser Fehlschlag ist das Ergebnis einer Zeitüberschreitung, die auftritt, bevor die Installation von vSphere HA auf den Hosts abgeschlossen ist.

### Lösung

Legen Sie die erweiterte vCenter Server-Option `config.vpxd.das.electionWaitTimeSec` auf den Wert 240 fest. Nach dieser Änderung treten keine Zeitüberschreitungen mehr auf.

## Fehlerbehebung bei vSphere Auto Deploy

Die Themen zur Fehlerbehebung bei vSphere Auto Deploy bieten Lösungen für Situationen, in denen die Bereitstellung von Hosts mit vSphere Auto Deploy nicht wie erwartet durchgeführt wird.

### vSphere Auto Deploy-TFTP-Zeitüberschreitungsfehler beim Start

Beim Starten eines mit vSphere Auto Deploy bereitgestellten Hosts wird eine Meldung über einen TFTP-Zeitüberschreitungsfehler angezeigt. Der Text der Nachricht richtet sich nach dem jeweiligen BIOS.

#### Problem

Beim Starten eines mit vSphere Auto Deploy bereitgestellten Hosts wird eine Meldung über einen TFTP-Zeitüberschreitungsfehler angezeigt. Der Text der Nachricht richtet sich nach dem jeweiligen BIOS.

#### Ursache

Der TFTP-Server ist heruntergefahren oder nicht erreichbar.

#### Lösung

- ◆ Stellen Sie sicher, dass Ihr TFTP-Dienst ausgeführt wird und über den Host, den Sie starten möchten, erreichbar ist.

### Der vSphere Auto Deploy-Host wird mit der falschen Konfiguration gestartet

Ein Host wird mit einem anderen ESXi-Image, Hostprofil oder Ordnerspeicherort als in den Regeln angegeben gestartet.

#### Problem

Ein Host wird mit einem anderen ESXi-Image-Profil oder einer anderen Konfiguration als dem in den Regeln angegebenen Image-Profil bzw. der angegebenen Konfiguration gestartet. Beispiel: Sie ändern die Regeln, um ein anderes Image-Profil zuzuweisen, aber der Host verwendet nach wie vor das alte Image-Profil.

#### Ursache

Nachdem der Host zum vCenter Server-System hinzugefügt wurde, wird die Startkonfiguration vom vCenter Server-System festgelegt. Das vCenter Server-System ordnet dem Host ein Image-Profil, ein Hostprofil oder einen Ordnerspeicherort zu.

#### Lösung

- ◆ Verwenden Sie die vSphere PowerCLI-Cmdlets `Test-DeployRuleSetCompliance` und `Repair-DeployRuleSetCompliance`, um die Regeln zu überprüfen und dem Host das richtige Image-Profil, Hostprofil oder den richtigen Ordnerspeicherort zuzuordnen.

### Der Host wird nicht an den vSphere Auto Deploy-Server umgeleitet

Während des Startens lädt ein Host, den Sie mit vSphere Auto Deploy bereitstellen möchten, iPXE. Der Host wird nicht an den vSphere Auto Deploy-Server umgeleitet.

#### Problem

Während des Startens lädt ein Host, den Sie mit vSphere Auto Deploy bereitstellen möchten, iPXE. Der Host wird nicht an den vSphere Auto Deploy-Server umgeleitet.

#### Ursache

Die `tramp`-Datei, die in der TFTP-ZIP-Datei enthalten ist, weist die falsche IP-Adresse für den vSphere Auto Deploy-Server auf.

**Lösung**

- ◆ Korrigieren Sie die IP-Adresse des vSphere Auto Deploy-Servers in der `tramp`-Datei. Weitere Informationen dazu finden Sie im Handbuch *Installation und Einrichtung von vSphere*.

**Paket-Warnmeldung, wenn Sie dem vSphere Auto Deploy-Host ein Image-Profil zuweisen**

Wenn Sie ein vSphere PowerCLI-Cmdlet ausführen, das ein nicht vSphere Auto Deploy-fähiges Image-Profil zuweist, wird eine Warnmeldung angezeigt.

**Problem**

Wenn Sie für die Zuweisung eines Image-Profiles zu mindestens einem Host Regeln schreiben oder ändern, wird eine Fehlermeldung ähnlich der folgenden angezeigt:

Warnung: Image-Profil <Name-hier> enthält mindestens ein Software-Paket, das nicht statusfreifähig ist. Wenn Sie dieses Profil mit Auto Deploy verwenden, können Probleme auftreten.

**Ursache**

Jedes VIB in einem Image-Profil hat ein `stateless-ready`-Flag, das angibt, dass dieses VIB zur Verwendung mit vSphere Auto Deploy vorgesehen ist. Dieser Fehler tritt auf, wenn Sie eine vSphere Auto Deploy-Regel schreiben, die ein Image-Profil verwendet, in dem das Flag von mindestens einem VIB auf `FALSE` festgelegt ist.

---

**HINWEIS** Sie können mit vSphere Auto Deploy bereitgestellte Hosts verwenden, die VIBs enthalten, die nicht ohne Probleme „statusfrei“-fähig sind. Das Starten mit einem Image-Profil mit VIBs, die nicht „statusfrei“-fähig sind, wird jedoch als Neuinstallation betrachtet. Bei jedem Hoststart gehen alle Konfigurationsdaten verloren, die beim Neustarten von mit vSphere Auto Deploy bereitgestellten Hosts verfügbar wären.

---

**Lösung**

- 1 Verwenden Sie vSphere ESXi Image Builder-Cmdlets in einer vSphere PowerCLI-Sitzung, um die VIBs im Image-Profil anzuzeigen.
- 2 Entfernen Sie alle VIBs, die nicht „statusfrei“-fähig sind.
- 3 Führen Sie das vSphere Auto Deploy-Cmdlet erneut aus.

**Der vSphere Auto Deploy-Host mit integriertem USB-Flash-Laufwerk sendet keine Core-Dumps an die lokale Festplatte**

Wenn der vSphere Auto Deploy-Host über ein integriertes USB-Flashlaufwerk verfügt und ein Fehler auftritt, der einen Core-Dump verursacht, geht der Core-Dump verloren. Richten Sie das System für die Verwendung von ESXi Dump Collector ein, um Core-Dumps auf einem vernetzten Host zu speichern.

**Problem**

Wenn der vSphere Auto Deploy-Host über ein integriertes USB-Flash-Laufwerk verfügt und ein Fehler auftritt, der einen Core-Dump verursacht, wird der Core-Dump nicht an die lokale Festplatte übermittelt.

**Lösung**

- 1 Installieren Sie ESXi Dump Collector auf einem System Ihrer Wahl.  
ESXi Dump Collector ist im vCenter Server-Installationsprogramm enthalten.
- 2 Verwenden Sie ESXCLI zum Konfigurieren des Hosts für die Verwendung von ESXi Dump Collector.

```
esxcli conn_options system coredump network set IP-addr,port
esxcli system coredump network set -e true
```

- 3 Verwenden Sie ESXCLI zum Deaktivieren lokaler Coredump-Partitionen.

```
esxcli conn_options system coredump partition set -e false
```

## Der vSphere Auto Deploy-Host wird nach fünf Minuten neu gestartet

Ein vSphere Auto Deploy-Host wird gestartet und zeigt iPXE-Informationen an, wird jedoch nach fünf Minuten neu gestartet.

### Problem

Ein Host, der mit vSphere Auto Deploy bereitgestellt werden soll, wird von iPXE gestartet und zeigt iPXE-Informationen an der Konsole an. Nach fünf Minuten wird jedoch die folgende Meldung auf der Konsole angezeigt und der Host wird neu gestartet.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

Der Host zeigt möglicherweise auch die folgenden Details an:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

Auf der Konsole werden dann die Attribute der Hostmaschine angezeigt, darunter Anbieter, Seriennummer, IP-Adresse usw.

### Ursache

Derzeit ist diesem Host kein Image-Profil zugeordnet.

### Lösung

Sie können dem Host ein Image-Profil zuordnen, indem Sie das Cmdlet `Apply-EsxImageProfile` ausführen oder die folgende Regel erstellen:

- 1 Führen Sie das cmdlet `New-DeployRule` aus, um eine Regel zu erstellen, die ein Muster enthält, das dem Host ein Image-Profil zuordnet.
- 2 Führen Sie das cmdlet `Add-DeployRule` aus, um die Regel einem Regelsatz hinzuzufügen.
- 3 Führen Sie das cmdlet `Test-DeployRuleSetCompliance` aus und verwenden Sie die Ausgabe des cmdlets als Eingabe für das cmdlet `Repair-DeployRuleSetCompliance`.

## Der vSphere Auto Deploy-Host kann den TFTP-Server nicht kontaktieren

Der Host, den Sie mit vSphere Auto Deploy bereitstellen, kann den TFTP-Server nicht kontaktieren.

### Problem

Wenn Sie versuchen, einen mit vSphere Auto Deploy bereitgestellten Host zu starten, führt der Host einen Netzwerkstart durch und erhält eine DHCP-Adresse vom DHCP-Server, aber der Host kann den TFTP-Server nicht kontaktieren.

**Ursache**

Der TFTP-Server wird möglicherweise nicht mehr ausgeführt, oder eine Firewall blockiert den TFTP-Port.

**Lösung**

- Wenn Sie den WinAgents TFTP-Server installiert haben, öffnen Sie den WinAgents TFTP-Verwaltungskonsole und stellen Sie sicher, dass der Dienst ausgeführt wird. Wenn der Dienst ausgeführt wird, überprüfen Sie die Windows-Firewallregeln für den eingehenden Datenverkehr, um sicherzugehen, dass der TFTP-Port nicht blockiert ist. Schalten Sie die Firewall vorübergehend aus, um festzustellen, ob das Problem bei der Firewall liegt.
- Sehen Sie im Falle aller anderen TFTP-Server in der Dokumentation zu Debuggen nach.

## vSphere Auto Deploy-Host kann kein ESXi -Image vom vSphere Auto Deploy-Server abrufen

Der Host, den Sie mit vSphere Auto Deploy bereitstellen, wird am iPXE-Startbildschirm angehalten.

**Problem**

Wenn Sie versuchen, einen mit vSphere Auto Deploy bereitgestellten Host zu starten, wird der Startvorgang am iPXE-Startbildschirm angehalten und die Statusmeldung weist darauf hin, dass der Host versucht, das ESXi-Image vom vSphere Auto Deploy-Server abzurufen.

**Ursache**

Der vSphere Auto Deploy-Dienst wurde möglicherweise angehalten oder auf den vSphere Auto Deploy-Server kann nicht zugegriffen werden.

**Lösung**

- 1 Melden Sie sich bei dem System an, auf dem Sie den vSphere Auto Deploy-Server installiert haben.
- 2 Stellen Sie sicher, dass der vSphere Auto Deploy-Server ausgeführt wird.
  - a Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung**.
  - b Doppelklicken Sie auf **Dienste**, um den Bereich „Dienstverwaltung“ zu öffnen.
  - c Suchen Sie im Feld „Dienste“ den Dienst „VMware vSphere Auto Deploy Waiter“ und starten Sie den Dienst erneut, falls er nicht bereits ausgeführt wird.
- 3 Starten Sie einen Webbrowser, geben Sie die folgende URL ein und überprüfen Sie, ob auf den vSphere Auto Deploy-Server zugegriffen werden kann.

`https://IP-Adresse_des_Auto_Deploy_Servers:Port_des_Auto_Deploy_Servers/vmw/rdb`

---

**HINWEIS** Verwenden Sie diese Adresse nur, um zu überprüfen, ob auf den Server zugegriffen werden kann.

---

- 4 Falls der Server nicht erreichbar ist, ist dies wahrscheinlich auf ein Firewall-Problem zurückzuführen.
  - a Versuchen Sie, großzügige Regeln für den eingehenden TCP-Datenverkehr des vSphere Auto Deploy-Serverports einzurichten.  
Die Portnummer lautet 6501, es sei denn, Sie haben während der Installation eine andere Portnummer angegeben.
  - b Als letztes Mittel deaktivieren Sie die Firewall vorübergehend und aktivieren Sie sie wieder, nachdem Sie festgestellt haben, ob sie den Datenverkehr blockiert hat. Deaktivieren Sie die Firewall in Produktionsumgebungen nicht.  
  
Führen Sie den Befehl `netsh firewall set opmode disable` zum Deaktivieren der Firewall aus.  
Führen Sie den Befehl `netsh firewall set opmode enable` zum Aktivieren der Firewall aus.

## vSphere Auto Deploy-Host erhält keine von DHCP zugewiesene Adresse

Der Host, den Sie mit vSphere Auto Deploy bereitstellen, erhält keine DHCP-Adresse.

### Problem

Wenn Sie versuchen, einen mit vSphere Auto Deploy bereitgestellten Host zu starten, führt der Host einen Netzwerkstart durch, ihm wird jedoch keine Adresse von DHCP zugewiesen. Der vSphere Auto Deploy-Server kann den Host mit dem Image-Profil nicht bereitstellen.

### Ursache

Möglicherweise gibt es ein Problem mit dem DHCP-Dienst oder mit der Einrichtung der Firewall.

### Lösung

- 1 Stellen Sie sicher, dass der DHCP-Serverdienst auf dem Windows-System ausgeführt wird, auf dem der DHCP-Server zum Bereitstellen von Hosts eingerichtet ist.
  - a Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung**.
  - b Doppelklicken Sie auf **Dienste**, um den Bereich „Dienstverwaltung“ zu öffnen.
  - c Suchen Sie im Feld „Dienste“ nach dem DHCP-Serverdienst und starten Sie den Dienst neu, falls er nicht ausgeführt wird.
- 2 Wenn der DHCP-Server ausgeführt wird, überprüfen Sie den DHCP-Geltungsbereich und die DHCP-Reservierungen, die Sie für Ihre Zielhosts konfiguriert haben.
 

Wenn der DHCP-Geltungsbereich und die DHCP-Reservierungen ordnungsgemäß konfiguriert sind, liegt das Problem wahrscheinlich bei der Firewall.
- 3 Um das Problem vorübergehend umzugehen, schalten Sie die Firewall aus, um festzustellen, ob dadurch das Problem behoben wurde.
  - a Öffnen Sie die Eingabeaufforderung, indem Sie auf **Start > Programme > Zubehör > Eingabeaufforderung** klicken.
  - b Geben Sie den folgenden Befehl ein, um die Firewall vorübergehend auszuschalten. Deaktivieren Sie die Firewall in Produktionsumgebungen nicht.
 

```
netsh firewall set opmode disable
```
  - c Versuchen Sie, den Host mit vSphere Auto Deploy bereitzustellen.
  - d Geben Sie den folgenden Befehl ein, um die Firewall wieder einzuschalten.
 

```
netsh firewall set opmode enable
```
- 4 Richten Sie Regeln ein, um den DHCP-Netzwerkdatenverkehr für die Zielhosts zu erlauben.
 

Weitere Informationen dazu finden Sie in der Firewall-Dokumentation für DHCP und für das Windows-System, auf dem der DHCP-Server ausgeführt wird.

## Der vSphere Auto Deploy-Host führt keinen Netzwerkstart durch

Der von Ihnen mit vSphere Auto Deploy bereitgestellte Host wird gestartet, er startet jedoch nicht über das Netzwerk.

### Problem

Wenn Sie versuchen, einen mit vSphere Auto Deploy bereitgestellten Host zu starten, initiiert der Host nicht den Netzwerkstartvorgang.

**Ursache**

Sie haben Ihren Host nicht für den Netzwerkstart aktiviert.

**Lösung**

- 1 Starten Sie den Host neu und folgen Sie den auf dem Bildschirm angezeigten Anweisungen, um auf die BIOS-Konfiguration zuzugreifen.
- 2 Aktivieren Sie in der BIOS-Konfiguration die Option „Network Boot“ in der Boot Device-Konfiguration.

## Wiederherstellen einer beschädigten Datenbank auf dem vSphere Auto Deploy-Server

In einigen Situationen tritt möglicherweise ein Problem bei der vSphere Auto Deploy-Datenbank auf. Die effizienteste Wiederherstellungsoption besteht darin, die vorhandene Datenbankdatei durch die letzte Sicherung zu ersetzen.

**Problem**

Wenn Sie vSphere Auto Deploy zum Bereitstellen der ESXi-Hosts in Ihrer Umgebung verwenden, tritt möglicherweise ein Problem bei der vSphere Auto Deploy-Datenbank auf.

**WICHTIG** Dieses Problem tritt nur selten auf. Führen Sie alle anderen Fehlerbehebungsstrategien für vSphere Auto Deploy aus, bevor Sie die aktuelle Datenbankdatei ersetzen. Regeln und Verknüpfungen, die Sie seit der ausgewählten Sicherung erstellt haben, gehen verloren.

**Ursache**

Dieses Problem tritt nur bei Hosts auf, die mit vSphere Auto Deploy bereitgestellt werden.

**Lösung**

- 1 Beenden Sie den vSphere Auto Deploy-Server-Dienst.
- 2 Suchen Sie das vSphere Auto Deploy-Protokoll, indem Sie zur vSphere Auto Deploy-Seite im vSphere Web Client navigieren.
- 3 Durchsuchen Sie die Protokolle nach der folgenden Meldung:

```
DatabaseError: database disk image is malformed.
```

Wenn Sie diese Meldung finden, ersetzen Sie die vorhandene Datenbank durch die letzte Sicherung.

- 4 Navigieren Sie zum vSphere Auto Deploy-Datenverzeichnis.

Betriebssystem	Dateispeicherort
vCenter Server Appliance	/var/lib/rbd
Microsoft Windows	%VMWARE_DATA_DIR%\autodeploy\Data

Das Verzeichnis enthält eine Datei mit dem Namen `db` und Sicherungsdateien mit den Namen `db-jjj-mm-tt`.

- 5 Benennen Sie die aktuelle `db`-Datei um.  
VMware Support wird Sie möglicherweise nach dieser Datei fragen, wenn Sie Assistenz anfordern.
- 6 Benennen Sie die letzte Sicherung in `db` um.
- 7 Starten Sie den vSphere Auto Deploy-Server-Dienst neu.
- 8 Falls die Meldung weiterhin im Protokoll angezeigt wird, wiederholen Sie die Schritte, um die nächste letzte Sicherung zu verwenden, bis bei Verwendung von vSphere Auto Deploy keine Datenbankfehler mehr auftreten.

## Authentifizierungstoken-Manipulationsfehler

Das Erstellen eines Kennworts, das die Authentifizierungsanforderungen des Hosts nicht erfüllt, verursacht einen Fehler.

### Problem

Wenn Sie ein Kennwort auf dem Host erstellen, wird die folgende Fehlermeldung angezeigt: Ein allgemeiner Systemfehler ist aufgetreten: Kennwort: Authentifizierungstoken-Manipulationsfehler.

Die folgende Meldung ist enthalten: Fehler beim Festlegen des Kennworts. Möglicherweise entspricht das Kennwort nicht den vom System festgelegten Komplexitätskriterien.

### Ursache

Der Host überprüft die Einhaltung der Kennwortrichtlinien mithilfe des Standardauthentifizierungs-Plugins `pam_passwdqc`. So. Falls das Kennwort nicht den Richtlinien entspricht, wird ein Fehler angezeigt.

### Lösung

Kennwörter sollten Zeichen aus vier Zeichenklassen enthalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen, wie z. B. Unter- oder Schrägstriche.

Ihr Benutzerkennwort muss die folgenden Längenanforderungen erfüllen.

- Kennwörter mit Zeichen aus drei Zeichenklassen müssen mindestens acht Zeichen lang sein.
- Kennwörter mit Zeichen aus allen vier Zeichenklassen müssen mindestens sieben Zeichen lang sein.

---

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

---

Weitere Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## Active Directory-Regelsatzfehler verursacht einen Fehler bei der Übereinstimmung des Hostprofils

Das Anwenden eines Hostprofils, das eine beizutretende Active Directory-Domäne angibt, führt zu einem Übereinstimmungsfehler.

### Problem

Wenn Sie ein Hostprofil anwenden, das eine beizutretende Active Directory-Domäne angibt, ohne den Regelsatz **activeDirectoryAll** in der Firewallkonfiguration zu aktivieren, tritt ein Übereinstimmungsfehler auf. Der vSphere Web Client zeigt folgende Fehlermeldung an: Fehler im Zusammenhang mit dem Hostprofil: Der Regelsatz „activedirectoryAll“ stimmt nicht mit der Spezifikation überein. Der Übereinstimmungsfehler tritt auch dann auf, wenn Sie ein Hostprofil zum Verlassen einer Active Directory-Domäne anwenden, ohne den Regelsatz **activeDirectoryAll** im Hostprofil zu deaktivieren.

### Ursache

Active Directory benötigt den Firewallregelsatz **activeDirectoryAll**. Sie müssen den Regelsatz in der Firewallkonfiguration aktivieren. Wenn Sie diese Einstellung auslassen, fügt das System die notwendigen Firewallregeln hinzu, wenn der Host der Domäne beitrifft. Aufgrund der Nichtübereinstimmung in den Firewallregeln besteht jedoch keine Übereinstimmung des Hosts. Zudem liegt eine Übereinstimmung des Hosts nicht vor, wenn Sie ihn aus der Domäne entfernen, ohne den Active Directory-Regelsatz zu deaktivieren.



**Lösung**

- 1 Navigieren Sie zum Hostprofil im Navigator von vSphere Web Client.  
Um ein Hostprofil zu suchen, klicken Sie auf der vSphere Web Client-Startseite auf **Richtlinien und Profile > Hostprofile**.
- 2 Klicken Sie mit der rechten Maustaste auf das Hostprofil und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie auf **Weiter**.
- 4 Wählen Sie **Sicherheit und Dienste > Firewall-Konfiguration > Firewall-Konfiguration > Regelsatzkonfiguration** aus.
- 5 Stellen Sie sicher, dass **activeDirectoryAll** ausgewählt ist.
- 6 Wählen Sie im rechten Bereich das Kontrollkästchen **Flag, das angibt, ob der Regelsatz aktiviert werden soll**.  
Heben Sie die Aktivierung des Kontrollkästchens auf, falls der Host die Domäne verlässt.
- 7 Klicken Sie auf **Weiter** und anschließend auf **Beenden**, um die Änderung des Hostprofils abzuschließen.

## Herunterladen von VIBs bei der Verwendung des vCenter Server - Reverse-Proxys ist nicht möglich

Sie können VIBs nicht herunterladen, wenn vCenter Server einen benutzerdefinierten Port für den Reverse-Proxy verwendet.

**Problem**

Wenn Sie den vCenter Server-Reverse-Proxy für die Verwendung eines benutzerdefinierten Ports konfigurieren, schlagen die VIB-Downloads fehl.

**Ursache**

Wenn vCenter Server einen benutzerdefinierten Port für den Reverse-Proxy verwendet, wird der benutzerdefinierte Port nicht automatisch in der ESXi-Firewall aktiviert, und die VIB-Downloads schlagen fehl.

**Lösung**

- 1 Öffnen Sie eine SSH-Verbindung zum Host und melden Sie sich als „root“ an.
- 2 (Optional) Führen Sie die vorhandenen Firewallregeln auf.  
`esxcli network firewall ruleset list`
- 3 (Optional) Sichern Sie die `/etc/vmware/firewall/service.xml`-Datei.  
`cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak`
- 4 Bearbeiten Sie die Zugriffsberechtigungen der `service.xml`-Datei, um Schreibvorgänge zuzulassen. Führen Sie dazu den Befehl `chmod` aus.
  - Um Schreibvorgänge zuzulassen, führen Sie `chmod 644/etc/vmware/firewall/service.xml` aus.
  - Um den Sticky Bit-Flag umzuschalten, führen Sie `chmod +t /etc/vmware/firewall/service.xml` aus.
- 5 Öffnen Sie die Datei `service.xml` in einem Texteditor.

- 6 Fügen Sie eine neue Regel zur Datei `service.xml` hinzu, die den benutzerdefinierten Port für den vCenter Server-Reverse-Proxy aktiviert.

```
<service id='id_value'>
  <id>vcenterrhttpproxy</id>
  <rule id='0000'>
    <direction>outbound</direction>
    <protocol>tcp</protocol>
    <port type='dst'>custom_reverse_proxy_port</port>
  </rule>
  <enabled>true</enabled>
  <required>false</required>
</service>
```

Auch wenn `id_value` ein eindeutiger Wert sein muss, müssen Sie, wenn beispielsweise der zuletzt aufgelistete Dienst in der Datei `service.xml` die ID 0040 aufweist, die ID-Nummer 0041 eingeben.

- 7 Stellen Sie die Zugriffsberechtigungen der Datei `service.xml` auf die standardmäßige Nur-Lesen-Einstellung wiederher.

```
chmod 444 /etc/vmware/firewall/service.xml
```

- 8 Aktualisieren Sie die Firewallregeln, damit die Änderungen wirksam werden.

```
esxcli network firewall refresh
```

- 9 (Optional) Führen Sie den aktualisierten Regelsatz auf, um die Änderung zu bestätigen.

```
esxcli network firewall ruleset list
```

- 10 (Optional) Wenn die Firewallkonfiguration nach einem Neustart des ESXi-Hosts weiterhin bestehen soll, kopieren Sie die Datei `service.xml` in den permanenten Speicher und ändern Sie die Datei `local.sh`.

- a Kopieren Sie die geänderte Datei `service.xml` in den permanenten Speicher, z. B. `/store/`, oder in einen VMFS-Volume, z. B. `/vmfs/volumes/volume/`.

```
cp /etc/vmware/firewall/service.xml location_of_xml_file
```

Sie können einen VMFS-Volume in einem einzelnen Speicherort speichern und ihn auf verschiedene Hosts kopieren.

- b Fügen Sie die Informationen der Datei `service.xml` zur Datei `local.sh` auf dem Host hinzu.

```
cp location_of_xml_file /etc/vmware/firewall
esxcli network firewall refresh
```

Dabei ist `location_of_xml_file` der Speicherort, in den die Datei kopiert wurde.

# Fehlerbehebung von vCenter Server und vSphere Web Client

---

# 4

Die Themen über die Fehlerbehandlung von vCenter Server und vSphere Web Client bieten Lösungen für Probleme, die auftreten können, wenn Sie vCenter Server und vSphere Web Client einrichten und konfigurieren, einschließlich vCenter Single Sign-On.

Dieses Kapitel behandelt die folgenden Themen:

- [„Fehlerbehandlung von vCenter Server“](#), auf Seite 35
- [„Fehlerbehebung im vSphere Web Client“](#), auf Seite 36
- [„Fehlerbehebung bei vCenter Server- und ESXi-Host-Zertifikaten“](#), auf Seite 38

## Fehlerbehandlung von vCenter Server

Diese Themen über die Fehlerbehandlung bieten Lösungen für Probleme, die auftreten können, wenn Sie vCenter Server auf dem Windows-Betriebssystem installieren oder die vCenter Server Appliance auf einem Linux-System bereitstellen.

### Das vCenter Server-Upgrade schlägt fehl, wenn der Tomcat-Dienst nicht gestoppt werden kann

Ein vCenter Server-Upgrade kann fehlschlagen, wenn das Installationsprogramm den Tomcat-Dienst nicht stoppen kann.

#### Problem

Wenn das vCenter Server-Installationsprogramm den Tomcat-Dienst während eines Upgrades nicht stoppen kann, schlägt das Upgrade mit einer Fehlermeldung ähnlich der folgenden fehl: VC Tomcat-Dienst kann nicht gelöscht werden. Das Problem kann selbst dann auftreten, wenn Sie den Tomcat-Dienst manuell vor dem Upgrade stoppen, wenn einige vom Tomcat-Prozess verwendete Dateien gesperrt sind.

#### Lösung

- 1 Wählen Sie in Windows **Start Einstellungen > Systemsteuerung > Verwaltung > Dienste**.
- 2 Klicken Sie mit der rechten Maustaste auf **VMware VirtualCenter Server** und wählen Sie **Manuell**.
- 3 Klicken Sie mit der rechten Maustaste auf **VMware vCenter Management Webservices** und wählen Sie **Manuell**.

- 4 Starten Sie vor dem Upgrade die vCenter Server-Maschine neu.

Dadurch werden gesperrte Dateien freigegeben, die vom Tomcat-Prozess verwendet werden, und das vCenter Server-Installationsprogramm ist in der Lage, den Tomcat-Dienst für das Upgrade zu stoppen.

Alternativ dazu können Sie die vCenter Server-Maschine und den Upgrade-Vorgang neu starten. Wählen Sie dabei aber die Option, die verhindert, dass vCenter Server-Daten überschrieben werden.

## **Eine Microsoft SQL-Datenbank, bei der ein nicht unterstützter Kompatibilitätsmodus festgelegt ist, sorgt dafür, dass das Installieren oder das Upgrade von vCenter Server fehlschlägt**

Die vCenter Server-Installation mit einer Microsoft SQL-Datenbank schlägt fehl, wenn die Datenbank so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird.

### **Problem**

Die folgende Fehlermeldung erscheint: Der eingegebene Datenbankbenutzer verfügt nicht über die erforderlichen Berechtigungen zum Installieren und Konfigurieren von vCenter Server mit der ausgewählten Datenbank. Beheben Sie die folgenden Fehler: %s

### **Ursache**

vCenter Server muss die Datenbankversion unterstützen. Wenn die Datenbank so eingestellt ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird, tritt dieser Fehler bei SQL auch dann auf, wenn es sich bei der Datenbank um eine unterstützte Version handelt. Wenn beispielsweise SQL 2008 für die Ausführung im SQL 2000-Kompatibilitätsmodus eingestellt ist, tritt dieser Fehler auf.

### **Lösung**

- ◆ Stellen Sie sicher, dass es sich bei der vCenter Server-Datenbank um eine unterstützte Version handelt und sie nicht so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter [http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php?](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?)

## **Fehlerbehebung im vSphere Web Client**

Die vSphere Web Client-Themen bieten Lösungen für potenzielle Probleme, die eintreten können, wenn Sie vSphere Web Client verwenden, um vSphere-Komponenten zu verwalten, einschließlich vCenter Single Sign-On und vCenter Server.

### **vCenter Server-System wird nicht in der vSphere Web Client -Bestandsliste angezeigt**

Der vSphere Web Client zeigt die erwarteten vCenter Server-Systeme in der Bestandsliste nicht an.

#### **Problem**

Wenn Sie sich am vSphere Web Client anmelden, ist die Bestandsliste anscheinend leer oder wird das erwartete vCenter Server-System nicht angezeigt.

#### **Ursache**

Melden Sie sich in vSphere 5.1 und höher bei vSphere Web Client an, um mehrere Instanzen von vCenter Server anzuzeigen und zu verwalten. Jedes vCenter Server-System, für das Sie über Berechtigungen verfügen, wird in der Bestandsliste angezeigt, sofern der Server beim selben Komponentenmanager wie der vSphere Web Client angemeldet ist.

## Lösung

- Melden Sie sich als Benutzer mit Berechtigungen für das vCenter Server-System am vSphere Web Client an.

Das vCenter Server-System wird nur dann in der Bestandsliste angezeigt, wenn Sie über entsprechende Berechtigungen verfügen. Wenn Sie sich beispielsweise als der vCenter Single Sign On-Administratorbenutzer anmelden, kann es sein, dass Sie keine Berechtigung für ein vCenter Server-System haben.

- Vergewissern Sie sich, dass das vCenter Server-System beim selben Komponentenmanager wie der vSphere Web Client registriert ist.

Der vSphere Web Client erkennt nur vCenter Server-Systeme, die beim selben Komponentenmanager registriert sind.

## Konsole für die virtuelle Maschine kann nicht gestartet werden

Wenn Sie versuchen, die Konsole für eine virtuelle Maschine vom vSphere Web Client aus zu öffnen, öffnet sich die Konsole nicht.

### Problem

Wenn Sie versuchen, die Konsole für eine virtuelle Maschine vom vSphere Web Client aus zu öffnen, öffnet sich die Konsole nicht. Die folgende Fehlermeldung erscheint:

```
HTTP ERROR 404 Problem accessing /. Reason: Not Found
```

Eine Fehlermeldung ähnlich der folgenden wird in der `virgo-server.log`-Datei angezeigt:

```
[2012-10-03 18:34:19.170] [ERROR] Thread-40 System.err 2012-10-03 18:34:19.167:WARN:oejuc.AbstractLifeCycle:FAILED org.eclipse.jetty.server.Server@315b0333: java.net.BindException: Address already in use [2012-10-03 18:34:19.170] [ERROR] Thread-40 System.err java.net.BindException: Address already in use
```

### Ursache

Ein anderes Programm oder ein anderer Prozess verwendet den Port 9443, den durch die HTML5-Konsole für die virtuelle Maschine verwendeten Standardport.

### Lösung

- ◆ Bearbeiten Sie die Datei `webclient.properties`, um die Zeile `html.console.port=Port` hinzuzufügen, wobei `Port` die neue Portnummer ist.

Die `webclient.properties`-Datei befindet sich, abhängig vom Betriebssystem der Maschine, auf der der vSphere Web Client installiert ist, an einem der folgenden Speicherorte:

Windows 2008	C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\
vCenter Server Appliance	/etc/vmware/vsphere-client/

## Fehlerbehebung bei vCenter Server- und ESXi -Host-Zertifikaten

Bei der Installation von vCenter Server werden automatisch Zertifikate generiert. Diese Standardzertifikate sind nicht von einer kommerziellen Zertifizierungsstelle (CA) zertifiziert und bieten möglicherweise keine hohe Sicherheit. Sie können die standardmäßigen vCenter Server-Zertifikate durch von einer kommerziellen Zertifizierungsstelle signierte Zertifikate ersetzen. Wenn Sie vCenter Server- und ESXi-Zertifikate ersetzen, können Fehler auftreten.

### vCenter Server kann keine Verbindung zu verwalteten Hosts herstellen

Nachdem Sie vCenter Server-Standardzertifikate ersetzt und das System neu gestartet haben, kann vCenter Server möglicherweise keine Verbindung zu verwalteten Hosts herstellen.

#### Problem

vCenter Server kann keine Verbindung zu verwalteten Hosts herstellen, wenn Serverzertifikate ersetzt werden und das System neu gestartet wird.

#### Lösung

Melden Sie sich beim Host als Root-Benutzer an und verbinden Sie den Host erneut mit vCenter Server.

### Neues vCenter Server-Zertifikat scheint nicht geladen zu werden

Nachdem Sie vCenter Server-Standardzertifikate ersetzt haben, scheinen die neuen Zertifikate nicht geladen zu werden.

#### Problem

Wenn Sie neue vCenter Server-Zertifikate installieren, wird das neue Zertifikat möglicherweise nicht angezeigt.

#### Ursache

Vorhandene offene Verbindungen zu vCenter Server werden nicht gezwungenermaßen geschlossen und verwenden möglicherweise weiterhin das alte Zertifikat.

#### Lösung

Um zu erzwingen, dass alle Verbindungen das neue Zertifikat verwenden, gehen Sie nach einer der folgenden Methoden vor.

- Starten Sie den Netzwerk-Stack oder die Netzwerkschnittstellen auf dem Server neu.
- Starten Sie den vCenter Server-Dienst neu.

### Konfigurieren von vSphere HA nicht möglich, wenn benutzerdefinierte SSL-Zertifikate verwendet werden

Nachdem Sie benutzerdefinierte SSL-Zertifikate installiert haben, schlagen die Versuche, vSphere High Availability (HA) zu aktivieren, fehl.

#### Problem

Wenn Sie versuchen, vSphere HA auf einem Host mit installierten benutzerdefinierten SSL-Zertifikaten zu aktivieren, wird die folgende Fehlermeldung angezeigt: vSphere HA kann nicht auf diesem Host konfiguriert werden, weil dessen SSL-Fingerabdruck nicht verifiziert wurde.

**Ursache**

Wenn Sie einen Host zu vCenter Server hinzufügen und vCenter Server dem SSL-Zertifikat des Hosts bereits vertraut, wird `VPX_HOST.EXPECTED_SSL_THUMBPRINT` in der vCenter Server-Datenbank nicht gefüllt. vSphere HA erhält den SSL-Fingerabdruck des Hosts von diesem Feld in der Datenbank. Ohne den Fingerabdruck können Sie vSphere HA nicht aktivieren.

**Lösung**

- 1 Trennen Sie im vSphere Web Client den Host, auf dem benutzerdefinierte SSL-Zertifikate installiert sind.
- 2 Stellen Sie eine erneute Verbindung des Hosts zu vCenter Server her.
- 3 Akzeptieren Sie das SSL-Zertifikat des Hosts.
- 4 Aktivieren Sie vSphere HA auf dem Host.





# Fehlerbehebung bei der Verfügbarkeit

# 5

In den Themen zur Fehlerbehebung bei der Verfügbarkeit finden Sie Lösungen für potenzielle Probleme, die bei der Verwendung von Hosts und Datenspeichern in vSphere HA-Clustern auftreten können.

Möglicherweise erhalten Sie eine Fehlermeldung, wenn Sie versuchen, vSphere HA oder vSphere FT zu verwenden. Informationen zu diesen Fehlermeldungen finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1033634>.

Dieses Kapitel behandelt die folgenden Themen:

- „Fehlerbehebung bei der vSphere HA-Zugangssteuerung“, auf Seite 41
- „Fehlerbehebung bei Taktsignal-Datenspeichern“, auf Seite 43
- „Fehlerbehebung bei vSphere HA-Fehlerantwort“, auf Seite 45
- „Fehlerbehebung bei vSphere Fault Tolerance in Netzwerkpartitionen“, auf Seite 47
- „Fehlerbehebung bei VM Component Protection“, auf Seite 48

## Fehlerbehebung bei der vSphere HA-Zugangssteuerung

vCenter Server verwendet die Zugangssteuerung, um sicherzustellen, dass im Fall eines Hostausfalls genügend Ressourcen in einem vSphere HA-Cluster für die Wiederherstellung von virtuellen Maschinen reserviert sind.

Falls die vSphere HA-Zugangssteuerung nicht ordnungsgemäß funktioniert, gibt es keine Garantie dafür, dass nach einem Hostausfall alle virtuellen Maschinen im Cluster neu gestartet werden können.

### Roter Cluster aufgrund von unzureichenden Failover-Ressourcen

Wenn Sie die Zugangssteuerungsrichtlinie „Vom Cluster tolerierte Hostfehler“ verwenden, können vSphere HA-Cluster aufgrund von unzureichenden Failover-Ressourcen ungültig (rot) werden.

#### Problem

Wenn Sie die Zugangssteuerungsrichtlinie „Vom Cluster tolerierte Hostfehler“ auswählen und bestimmte Probleme auftreten, wird der Cluster rot.

#### Ursache

Dieses Problem kann auftreten, wenn Hosts im Cluster getrennt sind, sich im Wartungsmodus befinden, nicht antworten oder einen vSphere HA-Fehler aufweisen. Wenn Hosts getrennt sind oder sich im Wartungsmodus befinden, ist dies in der Regel auf eine Benutzeraktion zurückzuführen. Wenn Hosts nicht antworten oder Fehler aufweisen, liegt für gewöhnlich ein größeres Problem vor, z. B., dass Hosts oder Agenten fehlgeschlagen sind oder ein Netzwerkproblem besteht.

Eine weitere mögliche Ursache dieses Problems ist, dass Ihr Cluster einzelne virtuelle Maschinen enthält, die deutlich größere Arbeitsspeicher- oder CPU-Reservierungen haben als die anderen. Die Zugangssteuerungsrichtlinie „Vom Cluster tolerierte Hostfehler“ basiert auf der Berechnung einer Slotgröße aus zwei Komponenten, den CPU- und Arbeitsspeicherreservierungen einer virtuellen Maschine. Wenn die Berechnung dieser Slotgröße durch virtuelle Maschinen mit deutlich abweichenden Werten verzerrt wird, ist es möglich, dass die Zugangssteuerungsrichtlinie zu restriktiv wird und einen roten Cluster zur Folge hat. In diesem Fall können Sie die erweiterten vSphere HA-Optionen verwenden, um die Steckplatzgröße zu verringern, eine andere Zugangssteuerungsrichtlinie verwenden oder die Richtlinie dahingehend ändern, dass sie weniger Hostausfälle toleriert.

### Lösung

Stellen Sie sicher, dass alle Hosts im Cluster ordnungsgemäß laufen, d. h., dass sie verbunden sind, sich nicht im Wartungsmodus befinden und keine vSphere HA-Fehler aufweisen. Die vSphere HA-Zugangssteuerung berücksichtigt nur Ressourcen von ordnungsgemäß laufenden Hosts.

## Eine virtuelle Maschine kann wegen unzureichender Failover-Ressourcen nicht eingeschaltet werden

Möglicherweise erhalten Sie die Fehlermeldung, dass nicht genügend Failover-Ressourcen zur Verfügung stehen, wenn Sie versuchen, eine virtuelle Maschine in einem vSphere HA-Cluster einzuschalten.

### Problem

Wenn Sie die Zugangssteuerungsrichtlinie „Vom Cluster tolerierte Hostfehler“ auswählen und bestimmte Probleme auftreten, ist es möglich, dass Sie eine virtuelle Maschine aufgrund von unzureichenden Ressourcen nicht einschalten können.

### Ursache

Dieses Problem kann mehrere Ursachen haben.

- Hosts im Cluster sind getrennt, befinden sich im Wartungsmodus, antworten nicht oder weisen einen vSphere HA-Fehler auf.

Wenn Hosts getrennt sind oder sich im Wartungsmodus befinden, ist dies in der Regel auf eine Benutzeraktion zurückzuführen. Wenn Hosts nicht antworten oder Fehler aufweisen, liegt für gewöhnlich ein größeres Problem vor, z. B., dass Hosts oder Agenten fehlgeschlagen sind oder ein Netzwerkproblem besteht.

- Der Cluster enthält virtuelle Maschinen, die deutlich größere Arbeitsspeicher- oder CPU-Reservierungen haben als die anderen.

Die Zugangssteuerungsrichtlinie „Vom Cluster tolerierte Hostfehler“ basiert auf der Berechnung einer Steckplatzgröße aus zwei Komponenten, den CPU- und Arbeitsspeicherreservierungen einer virtuellen Maschine. Wenn die Berechnung dieser Steckplatzgröße durch virtuelle Maschinen mit deutlich abweichenden Werten verzerrt wird, ist es möglich, dass die Zugangssteuerungsrichtlinie zu restriktiv wird und zur Folge hat, dass virtuelle Maschinen nicht eingeschaltet werden können.

- Keine freien Steckplätze im Cluster.

Es treten Probleme auf, wenn im Cluster keine freien Steckplätze vorhanden sind oder das Einschalten einer virtuellen Maschine zu einem Ansteigen der Steckplatzgröße führt, weil sie eine größere Reservierung hat als die vorhandenen virtuellen Maschinen. In beiden Fällen sollten Sie die erweiterten vSphere HA-Optionen verwenden, um die Steckplatzgröße zu verringern, eine andere Zugangssteuerungsrichtlinie verwenden oder die Richtlinie dahingehend ändern, dass sie weniger Hostausfälle toleriert.

## Lösung

Zeigen Sie den Bereich **Erweiterte Laufzeitinformationen** an, der im Abschnitt „vSphere HA“ der Registerkarte **Überwachen** des Clusters im vSphere Web Client angezeigt wird. In diesem Informationsbereich werden die Steckplatzgröße sowie die Anzahl der verfügbaren Steckplätze im Cluster angezeigt. Falls die Steckplatzgröße zu hoch erscheint, klicken Sie auf die Registerkarte **Ressourcenzuteilung** des Clusters und sortieren Sie die virtuellen Maschinen nach der Reservierung, um zu ermitteln, welche Maschinen die größten CPU- und Arbeitsspeicherreservierungen haben. Falls virtuelle Maschinen vorhanden sind, die deutlich größere Reservierungen haben als die anderen, ziehen Sie in Betracht, eine andere vSphere HA-Zugangssteuerungsrichtlinie zu verwenden (z. B. die Zugangssteuerungsrichtlinie „Prozentsatz der reservierten Clusterressourcen“), oder verwenden Sie die erweiterten vSphere HA-Optionen, um einen absoluten Grenzwert für die Steckplatzgröße festzulegen. Beide Optionen erhöhen jedoch das Risiko der Ressourcenfragmentierung.

## Es werden weniger verfügbare Steckplätze als erwartet angezeigt

Das Feld „Erweiterte Laufzeitinformationen“ zeigt möglicherweise eine geringere Anzahl an verfügbaren Steckplätze im Cluster als erwartet an.

### Problem

Wenn Sie die Richtlinie für die Zugangssteuerung „Vom Cluster tolerierte Hostfehler“ auswählen, wird der Bereich **Erweiterte Laufzeitinformationen** im Abschnitt „vSphere HA“ der Registerkarte **Überwachen** des Clusters im vSphere Web Client angezeigt. In diesem Bereich werden Informationen zum Cluster angezeigt, einschließlich der Anzahl der Steckplätze, die zum Einschalten von weiteren virtuellen Maschinen im Cluster zur Verfügung stehen. Unter bestimmten Voraussetzungen könnte die Anzahl geringer als erwartet ausfallen.

### Ursache

Die Steckplatzgröße wird anhand der größten Reservierungen plus dem Arbeitsspeicher-Overhead einer der eingeschalteten virtuellen Maschinen im Cluster berechnet. Die vSphere HA-Zugangssteuerung berücksichtigt jedoch nur die Ressourcen auf einem Host, die für virtuelle Maschinen zur Verfügung stehen. Diese Anzahl ist geringer als die Gesamtzahl der physischen Ressourcen auf dem Host, da es einiges an Overhead gibt.

### Lösung

Reduzieren Sie, falls möglich, die Anzahl der VM-Reservierungen, verwenden Sie die erweiterten Optionen von vSphere HA, um die Steckplatzgröße zu reduzieren, oder verwenden Sie eine andere Zugangssteuerungsrichtlinie.

## Fehlerbehebung bei Taktsignal-Datenspeichern

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

vCenter Server wählt automatisch eine bevorzugte Gruppe von Datenspeichern für Taktsignale aus. Diese Auswahl wird mit dem Ziel getroffen, die Anzahl der Hosts, die Zugriff auf einen angegebenen Datenspeicher haben, zu maximieren und die Wahrscheinlichkeit, dass die ausgewählten Datenspeicher von demselben Speicher-Array oder NFS-Server gestützt werden, zu minimieren. In den meisten Fällen sollte diese

Auswahl nicht geändert werden. Um festzustellen, welche Datenspeicher vSphere HA für die Verwendung ausgewählt hat, wechseln Sie im vSphere Web Client zur Registerkarte **Überwachen** des Clusters, und wählen Sie „vSphere HA“ und „Taktsignal“ aus. Nur Datenspeicher, die von mindestens zwei Hosts gemountet werden, stehen hier zur Verfügung.

---

**HINWEIS** Es ist kein Taktsignal-Datenspeicher verfügbar, wenn vSAN der einzige gemeinsam genutzte Speicher ist, auf den alle Hosts im Cluster Zugriff haben.

---

## Es ist kein vom Benutzer bevorzugter Datenspeicher ausgewählt

vCenter Server wählt möglicherweise keinen der von Ihnen angegebenen Datenspeicher als Präferenz für vSphere HA-Speicher-Taktsignale aus.

### Problem

Sie können die für Speicher-Taktsignale bevorzugten Datenspeicher angeben. Auf Basis dieser Präferenz ermittelt vCenter Server die endgültig zu verwendenden Datenspeicher. Allerdings wählt vCenter Server möglicherweise nicht die Datenspeicher aus, die Sie angeben.

### Ursache

Dieses Problem kann in den folgenden Fällen auftreten:

- Die angegebene Anzahl an Datenspeichern liegt über der erforderlichen Anzahl. vCenter Server wählt die optimale Anzahl an erforderlichen Datenspeichern aus den angegebenen Benutzereinstellungen aus und ignoriert den Rest.
- Ein angegebener Datenspeicher ist nicht optimal für die Zugriffsfähigkeit auf den Host und für die Speicher-Backing-Redundanz. Genauer ausgedrückt: Der Datenspeicher wird möglicherweise nicht ausgewählt, wenn er nur einer kleinen Gruppe von Hosts im Cluster zugänglich ist. Ein Datenspeicher wird möglicherweise auch dann nicht ausgewählt, wenn er sich auf derselben LUN oder demselben NFS-Server wie Datenspeicher befindet, die vCenter Server bereits ausgewählt hat.
- Ein angegebener Datenspeicher ist aufgrund von Speicherausfällen nicht zugänglich, weil beispielsweise im Speicherarray „Keine Pfade verfügbar (APD)“ sind oder eine dauerhafter Geräteverlust (PDL) vorliegt.
- Falls der Cluster eine Netzwerkpartition enthält oder falls ein Host nicht erreichbar oder isoliert ist, verwendet der Host selbst dann die vorhandenen Taktsignal-Datenspeicher weiter, wenn sich die Benutzereinstellungen ändern.

### Lösung

Stellen Sie sicher, dass alle Hosts im Cluster erreichbar sind und auf ihnen ein vSphere HA-Agent ausgeführt wird. Stellen Sie außerdem sicher, dass die angegebenen Datenspeicher für die meisten, wenn nicht für alle Hosts im Cluster zugänglich sind und dass sich die Datenspeicher auf unterschiedlichen LUNs oder NFS-Servern befinden.

## Das Unmounten oder Entfernen eines Datenspeichers schlägt fehl

Wenn Sie versuchen, ein Unmounten oder Entfernen eines Datenspeichers durchzuführen, schlägt der Vorgang fehl.

### Problem

Das Unmounten oder Entfernen eines Datenspeichers schlägt fehl, wenn der Datenspeicher Dateien geöffnet hat. Für diese Benutzervorgänge schließt der vSphere HA-Agent alle Dateien, die er geöffnet hat, beispielsweise die Taktsignal-Dateien. Falls der Agent nicht von vCenter Server erreicht werden kann oder der Agent ausstehende E/A-Vorgänge nicht auf die Festplatte schreiben kann, um die Dateien zu schließen, wird der Fehler Der vSphere HA-Agent auf Host '{hostName}' konnte die Dateiaktivitäten auf dem Datenspeicher '{dsName}' nicht stilllegen ausgelöst.

### Ursache

Wenn der Datenspeicher, für den ein Unmounten durchgeführt oder der entfernt werden soll, für Taktsignale verwendet wird, schließt vCenter Server ihn als Taktsignal-Datenspeicher aus und wählt dafür einen neuen Datenspeicher aus. Allerdings empfängt der Agent nicht die aktualisierten Taktsignal-Datenspeicher, wenn er nicht erreichbar ist. Dies ist der Fall, wenn der Host isoliert ist oder sich in einer Netzwerkpartition befindet. In diesen Fällen werden die Taktsignal-Dateien nicht geschlossen und der Benutzervorgang schlägt fehl. Der Vorgang kann auch fehlschlagen, wenn der Datenspeicher aufgrund von Speicherausfällen, z. B. „Keine Pfade verfügbar“, nicht zugänglich ist.

---

**HINWEIS** Wenn Sie einen VMFS-Datenspeicher entfernen, wird der Datenspeicher von allen Hosts in der Bestandsliste entfernt. Wenn also Hosts in einem vSphere HA-Cluster nicht erreichbar sind oder Hosts nicht auf den Datenspeicher zugreifen können, schlägt der Vorgang fehl.

---

### Lösung

Stellen Sie sicher, dass der Datenspeicher zugänglich ist und die betreffenden Hosts erreichbar sind.

## Fehlerbehebung bei vSphere HA-Fehlerantwort

vSphere HA bietet virtuellen Maschinen hohe Verfügbarkeit, indem sie die virtuellen Maschinen und die Hosts, auf denen sich diese 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.

Es gibt verschiedene Gründe, weshalb betroffene virtuelle Maschine nicht neu gestartet werden. In diesem Fall sollten Sie eine Fehlerbehebung vornehmen, um die Ursache zu ermitteln.

### Falscher VM-Schutzstatus

Eine virtuelle Maschine in einem vSphere HA-Cluster wird als von vSphere HA ungeschützt gemeldet, obwohl sie seit einigen Minuten eingeschaltet ist.

#### Problem

Wenn eine virtuelle Maschine für einige Minuten eingeschaltet ist und ihr vSphere HA-Schutzstatus „Ungeschützt“ bleibt, versucht vSphere HA möglicherweise nicht, die virtuelle Maschine neu zu starten, falls ein Fehler auftritt.

## Ursache

vCenter Server meldet, dass eine virtuelle Maschine geschützt ist, nachdem der vSphere HA-Master-Host, der für die virtuelle Maschine verantwortlich ist, die Information, dass die virtuelle Maschine nach einem Ausfall neu gestartet werden muss, auf der Festplatte gespeichert hat. Dieser Prozess kann aus einer Reihe von Gründen fehlschlagen.

- Der vSphere HA Master-Host wurde nicht gewählt oder vCenter Server kann nicht mit ihm kommunizieren.

In dieser Situation meldet vCenter Server „Agent nicht erreichbar“ oder „Agent nicht initialisiert“ als vSphere HA-Hostzustand für die Cluster-Hosts sowie das Clusterkonfigurationsproblem, dass ein Master-Host nicht gefunden wurde.

- Es sind mehrere Master-Hosts vorhanden und der Master-Host, mit dem vCenter Server kommuniziert, ist für die virtuelle Maschine nicht verantwortlich.

Probleme treten auf, wenn vCenter Server Kontakt mit einem Master-Host aufnimmt, es aufgrund einer Partition des Verwaltungsnetzwerks mehrere Master-Hosts gibt und der Agent, mit dem vCenter Server kommuniziert, für die virtuelle Maschine nicht verantwortlich ist. Diese Situation ist wahrscheinlich, wenn vCenter Server den vSphere HA-Zustand einiger Hosts als „Netzwerkpartitioniert“ meldet.

- Der Agent kann nicht auf den Datenspeicher zugreifen, auf dem die Konfigurationsdatei der virtuellen Maschine gespeichert ist.

vCenter Server hat möglicherweise Kontakt mit dem vSphere HA Master-Host aufgenommen, der die virtuelle Maschine besitzt, aber der Agent kann nicht auf den Datenspeicher zugreifen, auf dem die Konfigurationsdatei der virtuellen Maschine gespeichert ist. Diese Situation kann eintreten, wenn der Zustand „Keine Pfade verfügbar“ alle Hosts im Cluster betrifft.

## Lösung

- 1 Prüfen Sie, ob vCenter Server Kontakt mit einem vSphere HA-Master-Host aufgenommen hat. Ist dies nicht der Fall, beheben Sie das Problem.
- 2 Wenn vCenter Server den Kontakt mit einem Master-Host aufgenommen hat, stellen Sie fest, ob eine Netzwerkpartition vorliegt, und falls ja, beheben Sie das Problem.
- 3 Falls das Problem weiterhin besteht, prüfen Sie, ob andere virtuelle Maschinen, die den gleichen Datenspeicher für ihre Konfigurationsdateien verwenden, auch ungeschützt sind.
- 4 Falls diese virtuellen Maschinen ungeschützt sind, überprüfen Sie, ob der vSphere HA Master-Host auf den Datenspeicher zugreifen kann.
- 5 Falls keiner der vorhergehenden Schritte das Problem behebt, stellen Sie den Schutz wieder her, indem Sie vSphere HA auf dem Host neu konfigurieren, auf dem die virtuelle Maschine ausgeführt wird.

## Neustart der virtuellen Maschine schlägt fehl

Nach dem Ausfall eines Hosts oder einer virtuellen Maschine kann eine virtuelle Maschine möglicherweise nicht neu gestartet werden.

### Problem

Wenn ein Host ausfällt oder eine virtuelle Maschine fehlschlägt, während ihr Host weiter ausgeführt wird, wird die virtuelle Maschine möglicherweise nicht oder erst nach einer langen Verzögerung neu gestartet.

### Ursache

vSphere HA startet eine virtuelle Maschine nach einem Ausfall möglicherweise nicht neu oder verzögert aus mehreren Gründen ihren Neustart.

- Die virtuelle Maschine ist zum Zeitpunkt des Ausfalls nicht von vSphere HA geschützt

- Auf Hosts, mit denen die virtuelle Maschine kompatibel ist, ist unzureichend Speicherkapazität vorhanden.
- vSphere HA hat versucht, die virtuelle Maschine neu zu starten, aber dabei ist bei jedem Versuch ein schwerwiegender Fehler aufgetreten.
- Der gemeinsam genutzte Speicher Ihres Clusters ist vSAN, und auf eine der Dateien der virtuellen Maschine kann nicht mehr zugegriffen werden, weil mehr als die angegebene Anzahl Hosts ausgefallen sind.
- Der Neustart ist tatsächlich erfolgreich verlaufen.

### Lösung

Um zu vermeiden, dass der Neustart virtueller Maschinen fehlschlägt, stellen Sie sicher, dass virtuelle Maschinen nach dem Einschalten von vSphere HA geschützt werden. Stellen Sie zudem bei Auftreten eines Fehlers sicher, dass die Einstellungen für die Zugangssteuerung mit dem erwarteten Verhalten beim Neustart übereinstimmen. Außerdem kann das Sicherstellen einer maximalen Kompatibilität zwischen virtuellen Maschinen und Hosts im Cluster die Wahrscheinlichkeit verringern, dass Neustarts fehlschlagen.

---

**HINWEIS** Informationen zu den Faktoren, die vSphere HA für Neustarts der virtuellen Maschine berücksichtigt, finden Sie unter „Festlegen von Antworten auf Hostprobleme“ in *vSphere-Verfügbarkeit*.

---

## Fehlerbehebung bei vSphere Fault Tolerance in Netzwerkpartitionen

Wenn bei einem vSphere HA-Cluster in dem Netzwerk, das vSphere für die Kommunikation zwischen den Agenten verwendet (Verwaltungsnetzwerk), ein Fehler auftritt, kann möglicherweise ein Teil der Hosts des Clusters nicht mit anderen Clusterhosts kommunizieren. In diesem Fall werden die Hosts, die miteinander kommunizieren können, als in einer Netzwerkpartition enthalten betrachtet.

Eine Cluster-Partition behindert Cluster-Verwaltungsfunktionen, wie z. B. vMotion, und kann die Fähigkeit von vSphere HA zum Überwachen und Neustarten virtueller Maschinen nach einem Ausfall beeinträchtigen. Dieser Zustand muss so bald wie möglich korrigiert werden.

Netzwerkpartitionen beeinträchtigen ebenfalls die Funktionen von vSphere Fault Tolerance. In einem partitionierten Cluster kann es beispielsweise vorkommen, dass eine primäre virtuelle Maschine (oder ihre sekundäre virtuelle Maschine) in einer Partition landet, die von einem Master-Host verwaltet wird, der für die virtuelle Maschine nicht verantwortlich ist. Wenn eine sekundäre virtuelle Maschine neu gestartet werden muss, wird dies von vSphere HA nur dann ausgeführt, wenn sich die primäre virtuelle Maschine in einer Partition befindet, die von dem Master-Host verwaltet wird, der für die virtuelle Maschine verantwortlich ist. Letztlich müssen Sie die Netzwerkpartition korrigieren. Bis dies möglich ist, müssen Sie jedoch alle Probleme beheben, die bei Ihren fehlertoleranten virtuellen Maschinen auftreten, um sicherzustellen, dass sie ordnungsgemäß geschützt sind.

### Primäre virtuelle Maschine verbleibt im Zustand „Sekundäre VM erforderlich“

Eine fehlertolerante primäre virtuelle Maschine kann selbst dann im Zustand Sekundäre VM erforderlich verbleiben, wenn genügend Ressourcen zum Starten der sekundären virtuellen Maschine verfügbar sind.

#### Problem

vSphere HA kann möglicherweise die sekundäre virtuelle Maschine einer virtuellen vSphere Fault Tolerance-Maschine nicht neu starten, obwohl ausreichend Ressourcen verfügbar sind.

**Ursache**

Beim Neustart einer sekundären virtuellen Maschine wird für vSphere HA vorausgesetzt, dass die primäre virtuelle Maschine auf einem Host ausgeführt wird, der sich in derselben Partition wie der vSphere HA-Master-Host befindet, der für das FT-Paar verantwortlich ist. Außerdem muss der vSphere HA-Agent auf dem Host der primären virtuellen Maschine ordnungsgemäß ausgeführt werden. Wenn alle diese Bedingungen erfüllt sind, ist es für FT zudem erforderlich, dass es mindestens einen weiteren Host in derselben Partition gibt, der mit dem FT-Paar kompatibel ist und über einen funktionierenden vSphere HA-Agenten verfügt.

**Lösung**

Um dieses Problem zu beheben, überprüfen Sie die von vCenter Server gemeldeten vSphere HA-Hostzustände. Falls Hosts als partitioniert, isoliert oder nicht erreichbar identifiziert werden, beheben Sie das Problem, bevor Sie fortfahren. In einigen Situationen können Sie ein Neustartproblem dadurch beheben, indem Sie vSphere HA auf dem Host neu konfigurieren, den vCenter Server als Master-Host meldet. In den meisten Situationen reicht dieser Schritt allerdings nicht aus und Sie müssen alle mit dem Hostzustand verbundenen Probleme lösen.

Nachdem Sie alle mit dem Hostzustand in Verbindung stehenden Probleme behoben haben, überprüfen Sie, ob es neben den Hosts der primären virtuellen Maschine weitere Hosts im Cluster gibt, die mit dem Paar fehlertoleranter virtueller Maschinen kompatibel sind. Sie können die Kompatibilität ermitteln, indem Sie versuchen, die primäre virtuelle Maschine auf andere Hosts zu migrieren. Beheben Sie alle erkannten Inkompatibilitäten.

**Probleme hinsichtlich des Rollenwechselverhaltens**

Es ist möglich, dass vCenter Server meldet, dass die primäre virtuelle Maschine eines Paares von vSphere Fault Tolerance-VMs ausgeschaltet ist, die sekundäre virtuelle Maschine jedoch eingeschaltet ist.

**Problem**

Nach einem Failover ist es möglich, dass vCenter Server fälschlicherweise meldet, dass die primäre virtuelle Maschine ausgeschaltet und bei ihrem ursprünglichen Host registriert und die sekundäre virtuelle Maschine eingeschaltet und bei ihrem ursprünglichen Host registriert ist.

**Ursache**

Dieser Fehler tritt auf, wenn vCenter Server nicht mit den Hosts kommunizieren kann, auf denen die primäre virtuelle Maschine und die sekundäre virtuelle Maschine tatsächlich ausgeführt werden. vCenter Server meldet, dass diese Hosts nicht antworten, und das Problem besteht so lange fort, bis vCenter Server mit den Hosts kommunizieren kann.

**Lösung**

Um dieses Problem zu lösen, müssen Sie das Netzwerkproblem beheben, das verhindert, dass vCenter Server mit den Hosts im Cluster kommuniziert.

**Fehlerbehebung bei VM Component Protection**

Wenn Sie VM Component Protection (VMCP) für Ihren vSphere HA-Cluster aktivieren, bietet dies Schutz vor Problemen beim Zugriff auf Datenspeicher, die eine auf einem der Clusterhosts ausgeführte virtuelle Maschine beeinträchtigen können.

Wenn die von Ihnen für einen derartigen Fehler konfigurierte VMCP-Reaktion nicht ausgeführt wird, sollten Sie eine Fehlerbehebung vornehmen, um die Ursache zu ermitteln.



## Problem, dass eine virtuelle Maschine nicht auf einen Datenspeicher zugreifen kann, wird nicht behoben

Wenn auf einen Datenspeicher nicht mehr zugegriffen werden kann, werden die betroffenen virtuellen Maschinen möglicherweise nicht von VMCP beendet und neu gestartet.

### Problem

Wenn der Fehler „Keine Pfade verfügbar“ (All Paths Down, APD) oder „Dauerhafter Geräteverlust“ (Permanent Device Loss, PDL) auftritt und nicht mehr auf einen Datenspeicher zugegriffen werden kann, behebt möglicherweise VMCP das Problem nicht für die betroffenen virtuellen Maschinen.

### Ursache

Bei einem APD- oder PDL-Fehler wird eine virtuelle Maschine von VMCP aus folgenden Gründen möglicherweise nicht beendet:

- Die virtuelle Maschine ist zum Zeitpunkt des Fehlers nicht durch vSphere HA geschützt.
- VMCP ist für diese virtuelle Maschine deaktiviert.

Wenn es sich um einen APD-Fehler handelt, kann darüber hinaus eine virtuelle Maschine von VMCP aus verschiedenen Gründen nicht beendet werden:

- Der APD-Fehler wird vor dem Beenden der virtuellen Maschine korrigiert.
- Auf Hosts, mit denen die virtuelle Maschine kompatibel ist, ist nicht genügend Kapazität vorhanden.
- Während einer Netzwerkpartitionierung oder -isolierung kann der von dem APD-Fehler betroffene Host vom Master-Host keine verfügbare Kapazität anfordern. In diesem Fall lässt vSphere HA der Benutzerrichtlinie den Vortritt und beendet die virtuelle Maschine bei einer aggressiven Einstellung für VM Component Protection.
- vSphere HA beendet von APD betroffene virtuelle Maschinen erst nach Ablauf der folgenden Zeitüberschreitungen:
  - APD-Zeitüberschreitung (standardmäßig 140 Sekunden).
  - Verzögerung für APD-Failover (standardmäßig 180 Sekunden). Für die schnellere Wiederherstellung kann diese Option auf „0“ festgelegt werden.

---

**HINWEIS** Anhand dieser Standardwerte beendet vSphere HA die betroffene virtuelle Maschine nach 320 Sekunden (APD-Zeitüberschreitung + Verzögerung für APD-Failover)

---

### Lösung

Um dieses Problem zu beheben, sollten Sie die folgenden Punkte überprüfen und anpassen:

- Unzureichende Kapazität für den Neustart der virtuellen Maschine
- Vom Benutzer konfigurierte Zeitüberschreitungen und Verzögerungen
- Benutzereinstellungen, die die VM-Beendigung betreffen
- VM Component Protection-Richtlinie
- Hostüberwachung oder VM-Neustartpriorität muss aktiviert sein



# Fehlerbehebung bei der Ressourcenverwaltung

# 6

In den Themen zur Fehlerbehebung bei der Ressourcenverwaltung finden Sie Lösungen für potenzielle Probleme, die möglicherweise bei der Verwendung der Hosts und Datenspeicher in vSphere DRS- oder vSphere Speicher-DRS-Clustern auftreten können.

Dieses Kapitel behandelt die folgenden Themen:

- [„Fehlerbehebung bei Speicher-DRS“](#), auf Seite 51
- [„Fehlerbehebung bei Storage I/O Control“](#), auf Seite 57

## Fehlerbehebung bei Speicher-DRS

Die Themen zur Fehlerbehebung bei Speicher-DRS bieten Lösungen für potenzielle Probleme, die bei Verwendung Speicher-DRS-fähiger Datenspeicher in einem Datenspeicher-Cluster auftreten können.

### Speicher-DRS ist auf einer virtuellen Festplatte deaktiviert

Selbst wenn Speicher-DRS für einen Datenspeicher-Cluster aktiviert ist, kann sie auf einigen virtuellen Festplatten im Datenspeicher-Cluster deaktiviert sein.

#### Problem

Sie haben Speicher-DRS für einen Datenspeicher-Cluster aktiviert, aber Speicher-DRS ist auf mindestens einer Festplatte virtueller Maschinen im Datenspeicher-Cluster deaktiviert.

#### Ursache

Die folgenden Szenarien können dazu führen, dass Speicher-DRS auf einer virtuellen Festplatte deaktiviert wird.

- Die Auslagerungsdatei einer virtuellen Maschine befindet sich lokal auf dem Host (die Auslagerungsdatei wird in einem bestimmten Datenspeicher abgelegt, der sich auf dem Host befindet). Die Auslagerungsdatei kann nicht verlagert werden und Speicher-DRS ist für die Festplatte mit der Auslagerungsdatei deaktiviert.
- Für die `.vmx`-Auslagerungsdatei einer virtuellen Maschine wird ein bestimmter Speicherort angegeben. Die Auslagerungsdatei kann nicht verlagert werden, und Speicher-DRS ist auf der Festplatte mit der `.vmx`-Auslagerungsdatei deaktiviert.
- Der Vorgang des Verlagerns bzw. der Storage vMotion-Vorgang ist zurzeit für die virtuelle Maschine in vCenter Server deaktiviert (weil beispielsweise andere vCenter Server-Vorgänge auf der virtuellen Maschine ausgeführt werden). Speicher-DRS bleibt so lange deaktiviert, bis die Verlagerung bzw. der Storage VMotion-Vorgang in vCenter Server reaktiviert wird.
- Die Home-Festplatte einer virtuellen Maschine ist durch vSphere HA geschützt und eine Verlagerung derselben führt zu einem Verlust des vSphere HA-Schutzes.

- Bei der Festplatte handelt es sich um eine CD-ROM-/ISO-Datei.
- Wenn es sich bei der Festplatte um eine unabhängige Festplatte handelt, wird Speicher-DRS deaktiviert (ausgenommen im Falle der Verlagerung oder der Klonplatzierung).
- Falls die virtuelle Maschine über Systemdateien auf einem separaten Datenspeicher des Home-Datenspeichers (Legacy) verfügt, wird Speicher-DRS auf der Home-Festplatte deaktiviert. Wenn Sie Storage vMotion zum manuellen Migrieren der Home-Festplatte verwenden, werden die Systemdateien der verschiedenen Datenspeicher auf dem Zieldatenspeicher abgelegt und Speicher-DRS wird auf der Home-Festplatte aktiviert.
- Falls die virtuelle Maschine über eine Festplatte verfügt, deren Base- bzw. Redo-Dateien sich über separate Datenspeicher (Legacy) verteilen, wird Speicher-DRS für die Festplatte deaktiviert. Wenn Sie Storage vMotion zum manuellen Migrieren der Festplatte verwenden, werden alle Dateien der verschiedenen Datenspeicher auf dem Zieldatenspeicher abgelegt und Speicher-DRS wird auf der Festplatte aktiviert.
- Die virtuelle Maschine verfügt über versteckte Festplatten (z. B. Festplatten in älteren Snapshots, nicht im aktuellen Snapshot). Dies führt dazu, dass Speicher-DRS auf der virtuellen Maschine deaktiviert wird.
- Die virtuelle Maschine ist eine Vorlage.
- Auf der virtuellen Maschine ist die vSphere Fault Tolerance aktiviert.
- Die virtuelle Maschine verwendet auf ihren verschiedenen Festplatten Dateien gemeinsam.
- Die virtuelle Maschine wird mit Speicher-DRS mit manuell angegebenen Datenspeichern platziert.

### Lösung

Beheben Sie das Problem, durch das Speicher-DRS auf der Festplatte deaktiviert wird.

## Datenspeicher kann nicht in den Wartungsmodus wechseln

Sie versetzen einen Datenspeicher in den Wartungsmodus, wenn er zwecks Wartung vorübergehend nicht benutzt werden soll. Ein Datenspeicher wird nur auf Benutzeranforderung in den Wartungsmodus versetzt bzw. verlässt diesen nur dann.

### Problem

Ein Datenspeicher in einem Datenspeicher-Cluster kann nicht in den Wartungsmodus versetzt werden. Der Status beim Wechsel in den Wartungsmodus verbleibt bei 1 %.

### Ursache

Eine oder mehrere Festplatten auf dem Datenspeicher können nicht mit Storage vMotion migriert werden. Diese Bedingung kann in den folgenden Fällen auftreten.

- Speicher-DRS ist auf der Festplatte deaktiviert.
- Speicher-DRS-Regeln verhindern, dass Speicher-DRS Migrationsempfehlungen für die Festplatte gibt.

### Lösung

- Wenn Speicher-DRS deaktiviert ist, aktivieren Sie es oder ermitteln Sie, warum es deaktiviert ist. Informationen darüber, warum Speicher-DRS möglicherweise deaktiviert ist, finden Sie unter [„Speicher-DRS ist auf einer virtuellen Festplatte deaktiviert“](#), auf Seite 51.
- Wenn Speicher-DRS-Regeln verhindern, dass Speicher-DRS Migrationsempfehlungen für die Festplatte gibt, können Sie bestimmte Regeln entfernen oder deaktivieren.
  - a Navigieren Sie zum Datenspeicher-Cluster im Objektnavigator von vSphere Web Client.
  - b Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

- c Wählen Sie unter „Konfiguration“ **Regeln** aus und klicken Sie auf die Regel.
- d Klicken Sie auf **Entfernen**.
- Wenn Speicher-DRS-Regeln verhindern, dass Speicher-DRS Migrationsempfehlungen für die Festplatte gibt, können Sie alternativ die erweiterte Speicher-DRS-Option „IgnoreAffinityRulesForMaintenance“ auf 1 setzen.
  - a Navigieren Sie zum Datenspeicher-Cluster im Objektnavigator von vSphere Web Client.
  - b Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
  - c Wählen Sie **SDRS** aus und klicken Sie auf **Bearbeiten**.
  - d Klicken Sie in **Erweiterte Optionen > Konfigurationsparameter** auf **Hinzufügen**.
  - e Geben Sie in der Spalte „Option“ **IgnoreAffinityRulesForMaintenance** ein.
  - f Geben Sie in der Spalte „Wert“ **1** ein, um die Option zu aktivieren.
  - g Klicken Sie auf **OK**.

## Speicher-DRS kann nicht auf einem Datenspeicher betrieben werden

Speicher-DRS generiert einen Alarm, um anzuzeigen, dass sie nicht auf dem Datenspeicher betrieben werden kann.

### Problem

Speicher-DRS generiert ein Ereignis und einen Alarm und Speicher-DRS kann nicht betrieben werden.

### Ursache

Die folgenden Szenarien können dazu führen, dass vCenter Server Speicher-DRS für einen Datenspeicher deaktiviert.

- Der Datenspeicher wird von mehreren Datencentern gemeinsam genutzt.  
Storage DRS wird nicht auf Datenspeichern unterstützt, die von mehreren Datencentern gemeinsam genutzt werden. Diese Konfiguration kann auftreten, wenn ein Host in einem Datacenter einen Datenspeicher in einem anderen Datacenter mountet, oder wenn ein Host, der den Datenspeicher verwendet, auf ein anderes Datacenter verschoben wird. Wenn ein Datenspeicher von mehreren Datencentern gemeinsam genutzt wird, ist der E/A-Lastausgleich für Storage DRS für den gesamten Datenspeicher-Cluster deaktiviert. Allerdings bleibt die Storage DRS-Speicherplatzverteilung auf allen Datenspeichern im Datenspeicher-Cluster aktiv, die nicht von mehreren Datencentern gemeinsam genutzt werden.
- Der Datenspeicher ist mit einem nicht unterstützten Host verbunden.  
Storage DRS wird auf ESX/ESXi 4.1 und früheren Hosts nicht unterstützt.
- Der Datenspeicher ist mit einem Host verbunden, auf dem Storage I/O Control nicht ausgeführt wird.

### Lösung

- Der Datenspeicher darf nur in einem einzigen Datacenter sichtbar sein. Verschieben Sie die Hosts auf dasselbe Datacenter oder unmounten Sie den Datenspeicher von Hosts, die sich auf anderen Datacentern befinden.
- Stellen Sie sicher, dass alle dem Datenspeicher-Cluster zugeordneten Hosts über die Version ESXi 5.0 oder höher verfügen.
- Stellen Sie sicher, dass bei allen dem Datenspeicher-Cluster zugeordneten Hosts Storage I/O Control aktiviert ist.

## Das Verschieben mehrerer virtueller Maschinen in einen Datenspeicher-Cluster schlägt fehl

Das Migrieren von mehr als einem Datenspeicher in einen Datenspeicher-Cluster schlägt mit einer Fehlermeldung fehl, nachdem die erste virtuelle Maschine erfolgreich in den Datenspeicher-Cluster verschoben wurde.

### Problem

Wenn Sie versuchen, mehrere virtuelle Maschinen in einen Datenspeicher-Cluster zu migrieren, werden einige virtuelle Maschinen erfolgreich migriert, aber die Migration der nachfolgenden virtuellen Maschinen schlägt fehl. vCenter Server zeigt die Fehlermeldung `Unzureichender Festplattenspeicher im Datenspeicher an`.

### Ursache

Bis zur Anwendung aller Platzierungsempfehlungen scheinen die Speicherplatzressourcen für Speicher-DRS zur Verfügung zu stehen. Daher teilt Speicher-DRS möglicherweise Speicherplatzressourcen den nachfolgenden Anforderungen zu.

### Lösung

Wiederholen Sie die fehlgeschlagenen Vorgänge nacheinander und stellen Sie sicher, dass jede Empfehlung angewendet wird, bevor die nächste Migration angefordert wird.

## Speicher-DRS generiert Fehler beim Erstellen einer virtuellen Maschine

Beim Erstellen oder Klonen einer virtuellen Maschine auf einem Datenspeicher-Cluster generiert Speicher-DRS möglicherweise einen Fehler.

### Problem

Wenn Sie versuchen, eine virtuelle Maschine auf einem Datenspeicher-Cluster zu erstellen oder zu klonen, erhalten Sie möglicherweise die Fehlermeldung `Vorgang nicht zulässig im aktuellen Zustand`.

### Ursache

Speicher-DRS prüft auf Regelverletzungen, wenn Sie eine virtuelle Maschine auf einem Speicher-DRS-fähigen Datenspeicher erstellen. Speicher-DRS generiert einen Fehler, wenn die Festplatten der neuen virtuellen Maschine nicht in Übereinstimmung mit den Regeln erstellt werden können. Der Fehler wird generiert, weil Speicher-DRS nicht auf die virtuelle Maschine verweisen kann, die gerade erstellt wird und somit noch nicht existiert.

### Lösung

Überarbeiten oder entfernen Sie die Regeln und wiederholen Sie den Vorgang zum Erstellen bzw. Klonen der virtuellen Maschine.

## Speicher-DRS ist auf einer von einer OVF-Vorlage bereitgestellten virtuellen Maschine aktiviert

Speicher-DRS ist auf einer virtuellen Maschine aktiviert, die von einer OVF-Vorlage bereitgestellt wurde, für die Speicher-DRS deaktiviert ist. Dies kann auftreten, wenn Sie eine OVF-Vorlage auf einem Datenspeicher-Cluster bereitstellen.

### Problem

Wenn Sie eine OVF-Vorlage mit deaktiviertem Speicher-DRS auf einem Datenspeicher-Cluster bereitstellen, ist bei der sich daraus ergebenden virtuellen Maschine Speicher-DRS aktiviert.

**Ursache**

Der vSphere Web Client wendet die Standardautomatisierungsebene des Datenspeicher-Clusters auf die von einer OVF-Vorlage bereitgestellten virtuellen Maschinen an.

**Lösung**

- 1 Um die Automationsebene der virtuellen Maschine zu ändern, navigieren Sie zum Datenspeichercluster im vSphere Web Client-Objektnavigators.
- 2 Wählen Sie die Registerkarte **Verwalten** und klicken Sie auf **Einstellungen**.
- 3 Wählen Sie **VM-Außerkräftsetzungen** und klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie die virtuelle Maschine aus und klicken Sie auf **OK**.
- 5 Wählen Sie aus dem Dropdown-Menü **VMDKs zusammenhalten** die Option **Nein** und klicken Sie auf **OK**.

**Speicher-DRS-Regelverletzungsfehler wird mehrmals angezeigt**

Wenn Sie versuchen, einen Datenspeicher in den Wartungsmodus zu versetzen, wird der gleiche Affinitäts- oder Anti-Affinitäts-Regelverletzungsfehler möglicherweise mehrmals im Dialogfeld „Fehler“ aufgeführt.

**Problem**

Im Dialogfeld „Fehler“ scheint es, als ob mehrere Instanzen des gleichen Fehlers angezeigt werden, aber in Wirklichkeit bezieht sich jeder Fehler auf einen anderen Datenspeicher. Das Dialogfeld „Fehler“ führt die Namen der Datenspeicher nicht auf, was den Eindruck erweckt, dass es sich um denselben Fehler handelt.

**Lösung**

Das Dialogfeld „Fehler“ zeigt immer einen separaten Regelverletzungsfehler für jeden Datenspeicher an, der für die Platzierung berücksichtigt wird. Wenn Sie möchten, dass der Datenspeicher in den Wartungsmodus versetzt wird, entfernen Sie die Regel, die verhindert, dass die virtuelle Maschine migriert wird.

**Speicher-DRS-Regeln werden nicht aus dem Datenspeicher-Cluster gelöscht**

Affinitäts- oder Anti-Affinitätsregeln, die für eine virtuelle Maschine gelten, werden nicht gelöscht, wenn Sie die virtuelle Maschine aus dem Datenspeicher-Cluster entfernen.

**Problem**

Wenn Sie eine virtuelle Maschine aus einem Datenspeicher-Cluster entfernen und die virtuelle Maschine einer Affinitäts- oder Anti-Affinitätsregeln in einem Datenspeicher-Cluster unterliegt, gilt die Regel nach wie vor. Dies ermöglicht Ihnen, Konfigurationen virtueller Maschinen in verschiedenen Datenspeicher-Clustern zu speichern. Sollte die virtuelle Maschine wieder in den Datenspeicher-Cluster verschoben werden, wird die Regel angewendet. Sie können die Regel nicht löschen, nachdem Sie die virtuelle Maschine aus dem Datenspeicher-Cluster entfernt haben.

**Ursache**

vCenter Server behält die Regeln für eine virtuelle Maschine bei, die aus einem Datenspeicher-Cluster entfernt wurde, sofern die virtuelle Maschine im vCenter Server verbleibt.

**Lösung**

Zum Entfernen einer Regel aus der Konfiguration eines Datenspeicher-Clusters müssen Sie die Regel löschen, bevor Sie die virtuelle Maschine, für die die Regel gilt, aus dem Datenspeicher-Cluster entfernen.

- 1 Navigieren Sie im vSphere Web Client zum Datenspeichercluster.
- 2 Wählen Sie die Registerkarte **Verwalten** und klicken Sie auf **Einstellungen**.

- 3 Klicken Sie unter „Konfiguration“ auf **Regeln**.
- 4 Wählen Sie die zu löschende Regel aus und klicken Sie auf **Entfernen**.
- 5 Klicken Sie auf **OK**.

## Alternative Speicher-DRS-Platzierungsempfehlungen werden nicht generiert

Beim Erstellen, Klonen oder Verlagern einer virtuellen Maschine generiert Speicher-DRS nur eine Platzierungsempfehlung.

### Problem

Speicher-DRS generiert eine einzige Platzierungsempfehlung, wenn Sie eine virtuelle Maschine erstellen, klonen oder verlagern. Es werden keine alternativen Empfehlungen ausgesprochen, wenn mehrere alternative Empfehlungen erwartet werden.

### Ursache

Wenn der Zielhost explizit den Speicherort der Auslagerungsdatei der virtuellen Maschine als einen Datenspeicher im Ziel-Datenspeicher-Cluster angibt, bilden die Festplatten, die in diesem Cluster platziert werden sollen, keine einzelne Affinitätsgruppe. Speicher-DRS generiert alternative Platzierungsempfehlungen nur für eine einzelne Artikelnummer oder Affinitätsgruppe.

### Lösung

Nehmen Sie die einzelne Empfehlung an. Wählen Sie zum Erhalten von mehreren Empfehlungen einen Zielhost aus, der nicht angibt, dass sich der Speicherort der Auslagerungsdatei der virtuellen Maschine auf einem Datenspeicher im Ziel-Datenspeicher-Cluster befindet.

## Das Übernehmen von Speicher-DRS-Empfehlungen schlägt fehl

Speicher-DRS generiert Empfehlungen zum Speicherplatz oder zum E/A-Lastausgleich, jedoch schlagen Versuche, die Empfehlungen zu übernehmen, fehl.

### Problem

Wenn Sie Speicher-DRS-Empfehlungen zum Speicherplatz oder zum E/A-Lastausgleich übernehmen, schlägt der Vorgang fehl.

### Ursache

Die folgenden Szenarien können das Übernehmen von Speicher-DRS-Empfehlungen verhindern.

- Möglicherweise wurde ein Alarm des Typs „Kapazitätsschwellenwert des Thin Provisioning des Speicheranbieters überschritten“ für den Zieldatenspeicher ausgelöst, was darauf hindeutet, dass der Speicherplatz des Datenspeichers knapp wird und daher keine virtuellen Maschinen dorthin migriert werden.
- Der Zieldatenspeicher befindet sich möglicherweise im Wartungsmodus oder wechselt gerade in diesen.

### Lösung

- Beheben Sie das Problem, das den Alarm des Typs „Kapazitätsschwellenwert des Thin Provisioning des Speicheranbieters überschritten“ ausgelöst hat.
- Stellen Sie sicher, dass sich der Zieldatenspeicher nicht im Wartungsmodus befindet oder gerade in diesen wechselt.



## Fehlerbehebung bei Storage I/O Control

In den Themen zur Fehlerbehebung bei der Verwendung von Storage I/O Control finden Sie Lösungen für potenzielle Probleme, die bei der Verwendung von Storage I/O Control mit Datenspeichern auftreten können.

### Nicht unterstützter Host mit Datenspeicher verbunden

Im vSphere Web Client wird ein Alarm ausgelöst, wenn vCenter Server erkennt, dass die Arbeitslast eines Hosts die Leistung beeinträchtigt.

#### Problem

Der Alarm **Host mit einer Versionsnummer vor 4.1 ist mit dem SIOC-fähigen Datenspeicher verbunden** wird ausgelöst.

#### Ursache

Der Datenspeicher ist für die Speicher-E/A-Steuerung aktiviert, kann aber aufgrund der externen Arbeitslast nicht vollständig von der Speicher-E/A-Steuerung kontrolliert werden.

Dieser Zustand kann eintreten, wenn der für Storage I/O Control-aktivierte Datenspeicher mit einem Host verbunden ist, der Storage I/O Control nicht unterstützt.

#### Lösung

Stellen Sie sicher, dass alle Hosts, die mit dem Datenspeicher verbunden sind, Storage I/O Control unterstützen.

### Nicht verwaltete Arbeitslast auf Datenspeicher erkannt

Im vSphere Web Client wird ein Alarm ausgelöst, wenn vCenter Server erkennt, dass die Arbeitslast eines Hosts die Leistung beeinträchtigt.

#### Problem

Der Alarm **Eine nicht verwaltete Arbeitslast wurde auf dem Datenspeicher erkannt** wird ausgelöst.

#### Ursache

Das Array ist für Nicht-vSphere-Arbeitslasten freigegeben oder das Array führt Systemaufgaben wie z. B. die Replizierung durch.

#### Lösung

Dazu gibt es keine Lösung. vCenter Server reduziert nicht die an das Array gesendete Gesamtmenge an E/A, sorgt aber für die vermehrte Durchsetzung der Anteilssteuerung.

### Leistungsdiagramme für den Datenspeicher können nicht angezeigt werden

Leistungsdiagramme für einen Datenspeicher werden auf der Registerkarte „Leistung“ nicht angezeigt.

#### Problem

Sie können auf der Registerkarte **Leistung** im vSphere Web Client keine Leistungsdiagramme für einen Datenspeicher anzeigen.

#### Ursache

Storage I/O Control für den Datenspeicher ist deaktiviert.

### **Lösung**

- 1 Navigieren Sie zum Datenspeicher im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Storage I/O Control konfigurieren** aus.
- 3 Wählen Sie das Kontrollkästchen **Storage I/O Control aktivieren**.
- 4 Klicken Sie auf **OK**.

## **Aktivieren von Storage I/O Control auf dem Datenspeicher nicht möglich**

Storage I/O Control ist auf einem Datenspeicher deaktiviert und kann nicht aktiviert werden.

### **Problem**

Sie können Storage I/O Control nicht auf einem Datenspeicher aktivieren.

### **Ursache**

Die folgenden Gründe können das Aktivieren von Storage I/O Control auf einem Datenspeicher verhindern.

- Auf mindestens einem der mit dem Datenspeicher verbundenen Hosts wird nicht ESX/ESXi 4.1 oder höher ausgeführt.
- Sie haben nicht die entsprechende Lizenz zum Aktivieren von Storage I/O Control.

### **Lösung**

- Stellen Sie sicher, dass die Hosts, die mit dem Datenspeicher verbunden sind, Hosts der Version ESX/ESXi 4.1 oder höher sind.
- Stellen Sie sicher, dass Sie über die entsprechende Lizenz zum Aktivieren von Storage I/O Control verfügen.

# Fehlerbehebung beim Speicher

---

In den Themen zur Fehlerbehebung beim Speicher finden Sie Lösungen für potenzielle Probleme, die bei der Verwendung von vSphere in verschiedenen Speicherumgebungen (z. B. SAN, vSAN oder Virtual Volumes) auftreten können.

Dieses Kapitel behandelt die folgenden Themen:

- [„Beheben von Anzeigeproblemen des SAN-Speichers“](#), auf Seite 60
- [„Beheben von SAN-Leistungsproblemen“](#), auf Seite 62
- [„Virtuelle Maschinen mit RDMS müssen den SCSI INQUIRY-Cache ignorieren“](#), auf Seite 66
- [„Der Software-iSCSI-Adapter ist aktiviert, wenn er nicht benötigt wird“](#), auf Seite 67
- [„Fehler beim Mounten von NFS-Datenspeichern“](#), auf Seite 67
- [„Fehlerbehebung bei Speicheradaptern“](#), auf Seite 67
- [„Überprüfen der Metadatenkonsistenz mit VOMA“](#), auf Seite 68
- [„Kein Failover für den Speicherpfad, wenn der TUR-Befehl nicht erfolgreich ist“](#), auf Seite 70
- [„Fehlerbehebung bei Flash-Geräten“](#), auf Seite 71
- [„Fehlerbehebung bei virtuellen Volumes“](#), auf Seite 74
- [„Fehlerbehebung bei VAIO-Filtern“](#), auf Seite 77

## Beheben von Anzeigeproblemen des SAN-Speichers

Wenn Sie den vSphere Web Client verwenden, um Fibre-Channel-SAN- oder iSCSI-Speichergeräte anzuzeigen, sind Sie möglicherweise nicht in der Lage, alle für Ihren Host verfügbaren Geräte zu sehen. Es gibt mehrere Fehlerbehebungsaufgaben, die Sie zum Beheben von Speicheranzeigeproblemen ausführen können.

### Beheben von Anzeigeproblemen bei Fibre-Channel-Speichergeräten

Wenn Fibre-Channel-Speichergeräte im vSphere Web Client nicht ordnungsgemäß angezeigt werden, müssen Sie Fehlerbehebungsaufgaben ausführen.

**Tabelle 7-1.** Beheben von Problemen bei der Fibre-Channel-LUN-Anzeige

Fehlerbehebungsaufgabe	Beschreibung
Prüfen Sie die Kabelverbindung.	Wenn ein Port nicht angezeigt wird, ist die Ursache dieses Problems möglicherweise die Kabelverbindung. Überprüfen Sie zunächst die Kabel. Stellen Sie sicher, dass die Ports mit Kabeln verbunden sind und eine Leuchte anzeigt, dass die Verbindung ordnungsgemäß funktioniert. Wenn dies nicht an beiden Enden des Kabels der Fall ist, ersetzen Sie das Kabel.
Prüfen Sie das Zoning.	Das Zoning schränkt den Zugriff auf bestimmte Speichergeräte ein, erhöht die Sicherheit und verringert den Netzwerkdatenverkehr. Einige Speicheranbieter lassen nur Zonen für einzelne Initiatoren zu. In einem solchen Fall kann sich ein HBA in mehreren Zonen für lediglich ein Ziel befinden. Andere Anbieter lassen Zonen für mehrere Initiatoren zu. Weitere Informationen zu den Zoning-Anforderungen finden Sie in der Dokumentation Ihres Speicheranbieters. Verwenden Sie die SAN-Switch-Software, um Zoning zu konfigurieren und zu verwalten.
Prüfen Sie die Konfiguration der Zugriffssteuerung.	<ul style="list-style-type: none"> <li>■ Mit dem Plug-In MASK_PATH können Sie Ihren Host daran hindern, auf ein bestimmtes Speicher-Array oder auf bestimmte LUNs auf einem Speicher-Array zuzugreifen. Wenn Ihr Host Geräte und Pfade erkennt, auf die der Host nicht zugreifen soll, ist die Pfadmaskierung möglicherweise falsch eingerichtet.</li> <li>■ Um über ein SAN zu starten, stellen Sie sicher, dass jedem Host ausschließlich die erforderlichen LUNs angezeigt werden. Legen Sie fest, dass für einen Host keine Start-LUNs mit Ausnahme der eigenen sichtbar sind. Verwenden Sie Speichersystemsoftware, um sicherzustellen, dass dem Host ausschließlich die erforderlichen LUNs angezeigt werden.</li> <li>■ Stellen Sie sicher, dass der Parameter <b>Disk.MaxLUN</b> das Anzeigen der erwarteten LUN zulässt. Informationen zum Parameter finden Sie in der Dokumentation <i>vSphere-Speicher</i>.</li> </ul>
Prüfen Sie die Einrichtung der Speicherprozessoren.	Wenn ein Festplatten-Array über mehrere Speicherprozessoren verfügt, stellen Sie sicher, dass der SAN-Switch mit dem Speicherprozessor verbunden ist, dem die LUNs zugewiesen sind, auf die Sie zugreifen möchten. In einigen Festplatten-Arrays ist lediglich ein Speicherprozessor aktiv, und die anderen Speicherprozessoren sind so lange passiv, bis ein Failover eintritt. Wenn Sie mit dem falschen Speicherprozessor verbunden sind (dem mit dem passiven Pfad), werden die erwarteten LUNs möglicherweise angezeigt, Sie erhalten jedoch eine Fehlermeldung, wenn Sie darauf zugreifen.
Scannen Sie Ihren HBA neu.	<p>Führen Sie eine erneute Prüfung durch, wenn Sie eine der folgenden Aufgaben ausgeführt haben:</p> <ul style="list-style-type: none"> <li>■ Erstellen von neuen LUNs in einem SAN.</li> <li>■ Ändern Sie die Konfiguration der Pfadmaskierung auf dem Host.</li> <li>■ Erneutes Verbinden eines Kabels.</li> <li>■ Ändern eines Hosts in einem Cluster</li> </ul> <p>Weitere Informationen finden Sie in der Dokumentation zu <i>vSphere-Speicher</i>.</p>

## Beheben von Anzeigeproblemen des iSCSI-Speichers

Führen Sie Fehlerbehebungsaufgaben aus, wenn iSCSI-Speichergeräte im vSphere Web Client nicht ordnungsgemäß angezeigt werden.

**Tabelle 7-2.** Fehlerbehebung bei der iSCSI-LUN-Anzeige

Fehlerbehebungsaufgabe	Beschreibung
Prüfen Sie die Kabelverbindung.	Wenn ein Port nicht angezeigt wird, ist die Ursache dieses Problems möglicherweise die Kabelverbindung oder das Routing. Überprüfen Sie zunächst die Kabel. Stellen Sie sicher, dass die Ports mit Kabeln verbunden sind und eine Leuchte anzeigt, dass die Verbindung ordnungsgemäß funktioniert. Wenn dies nicht an beiden Enden des Kabels der Fall ist, ersetzen Sie das Kabel.
Prüfen Sie die Routing-Einstellungen.	Steuert die Konnektivität zwischen verschiedenen Subnetzen in Ihrer Ethernet-Konfiguration. Wenn sich das ESXi-System und der iSCSI-Speicher nicht in demselben Subnetz befinden, stellen Sie sicher, dass das Routing zwischen den Subnetzen ordnungsgemäß funktioniert. Stellen Sie ferner sicher, dass die Subnetzmaske und Gateway-Adresse im iSCSI-Speicher und iSCSI-Initiator auf dem ESXi-Host ordnungsgemäß konfiguriert sind.
Prüfen Sie die Konfiguration der Zugriffssteuerung.	<p>Wenn die erwarteten LUNs nach dem erneuten Überprüfen nicht angezeigt werden, ist die Zugriffssteuerung auf Speichersystemseite möglicherweise nicht ordnungsgemäß konfiguriert.</p> <ul style="list-style-type: none"> <li>■ Wenn CHAP konfiguriert ist, stellen Sie sicher, dass das Protokoll auf dem ESXi-Host aktiviert ist und der Einrichtung des Speichersystems entspricht.</li> <li>■ Wenn die IP-basierte Filterung verwendet wird, stellen Sie sicher, dass die IP-Adresse von iSCSI-HBA oder der VMkernel-Portgruppe zulässig ist.</li> <li>■ Wenn Sie die auf dem Initiator-Namen basierende Filterung verwenden, stellen Sie sicher, dass der Name ein qualifizierter iSCSI-Name ist und der Einrichtung des Speichersystems entspricht.</li> <li>■ Um über ein SAN zu starten, stellen Sie sicher, dass jedem Host ausschließlich die erforderlichen LUNs angezeigt werden. Legen Sie fest, dass für einen Host keine Start-LUNs mit Ausnahme der eigenen sichtbar sind. Verwenden Sie Speichersystemsoftware, um sicherzustellen, dass dem Host ausschließlich die erforderlichen LUNs angezeigt werden.</li> <li>■ Stellen Sie sicher, dass die Einstellung <b>Disk.MaxLUN</b> das Anzeigen der erwarteten LUN zulässt. Weitere Informationen finden Sie in der Dokumentation zu <i>vSphere-Speicher</i>.</li> </ul>
Prüfen Sie die Einrichtung der Speicherprozessoren.	Wenn ein Speicherprozessor über mehrere Speicherprozessoren verfügt, stellen Sie sicher, dass der SAN-Switch mit dem Speicherprozessor verbunden ist, dem die LUNs zugewiesen sind, auf die Sie zugreifen möchten. In einigen Speichersystemen ist lediglich ein Speicherprozessor aktiv, und die anderen Speicherprozessoren sind so lange passiv, bis ein Failover eintritt. Wenn Sie mit dem falschen Speicherprozessor verbunden sind (dem mit dem passiven Pfad), werden die erwarteten LUNs möglicherweise nicht angezeigt, oder die LUNs werden angezeigt, beim Versuch, darauf zuzugreifen, erhalten Sie jedoch Fehlermeldungen.
Überprüfen Sie die Netzwerkkonfiguration für Software- und abhängige Hardware-iSCSI	Die Software-iSCSI-Adapter und die abhängigen Hardwareadapter in ESXi erfordern, dass ein VMkernel-Netzwerkport auf den iSCSI-Speicher zugreifen kann. Die Adapter verwenden den VMkernel für die Datenübertragung zwischen dem ESXi-System und dem iSCSI-Speicher.
Prüfen Sie den iSCSI-Initiator erneut.	<p>Führen Sie eine erneute Prüfung durch, wenn Sie eine der folgenden Aufgaben ausgeführt haben:</p> <ul style="list-style-type: none"> <li>■ Erstellen von neuen LUNs in einem SAN.</li> <li>■ Ändern Sie die LUN-Maskierung.</li> <li>■ Erneutes Verbinden eines Kabels.</li> <li>■ Ändern eines Hosts in einem Cluster</li> <li>■ Ändern der CHAP-Einstellungen oder Hinzufügen neuer Erkennungsadressen.</li> </ul> <p>Weitere Informationen finden Sie in der Dokumentation zu <i>vSphere-Speicher</i>.</p>

## Beheben von SAN-Leistungsproblemen

Verschiedene Faktoren können sich negativ auf die Speicherleistung in der ESXi-SAN-Umgebung auswirken. Zu diesen Faktoren gehören übermäßig viele SCSI-Reservierungen, Pfad-Thrashing und eine unzureichende LUN-Warteschlangentiefe.

Um die Speicherleistung in Echtzeit zu überwachen, verwenden Sie die Befehlszeilendienstprogramme `resxtop` und `esxtop`. Weitere Informationen finden Sie unter *vSphere-Überwachung und -Leistung*.

### Übermäßig viele SCSI-Reservierungen beeinträchtigen die Leistung des Hosts

Wenn Speichergeräte die Hardwarebeschleunigung nicht unterstützen, verwenden ESXi-Hosts den SCSI-Reservierungsmechanismus beim Ausführen von Vorgängen, für die eine Dateisperre oder eine Metadaten-sperre in VMFS erforderlich ist. SCSI-Reservierungen sperren die LUN vollständig. Eine übermäßig hohe Anzahl an SCSI-Reservierungen durch einen Host kann die Leistung auf anderen Servern beeinträchtigen, die auf dasselbe VMFS zugreifen.

#### Problem

Übermäßig viele SCSI-Reservierungen beeinträchtigen die Leistung und verursachen SCSI-Reservierungskonflikte.

#### Ursache

Bei mehreren Vorgängen sind für das VMFS SCSI-Reservierungen erforderlich.

- Erstellen, Neusignieren oder Erweitern eines VMFS-Datenspeichers
- Das Einschalten einer virtuellen Maschine
- Erstellen oder Löschen einer Datei
- Erstellen einer Vorlage
- Bereitstellen einer virtuellen Maschine anhand einer Vorlage
- Erstellen einer neuen virtuellen Maschine
- Migrieren einer virtuellen Maschine mit vMotion
- Vergrößern einer Datei, z. B. einer Thin-bereitgestellten virtuellen Festplatte

---

**HINWEIS** Bei Speichergeräten, die die Hardwarebeschleunigung unterstützen, verwenden die Hosts den ATS-Algorithmus, um die LUN zu sperren. Weitere Informationen zur Hardwarebeschleunigung finden Sie in der Dokumentation *vSphere-Speicher*.

---

#### Lösung

Befolgen Sie zur Beseitigung potenzieller SCSI-Reservierungskonflikte die folgenden Richtlinien:

- Serialisieren Sie, falls möglich, die Vorgänge der gemeinsam genutzten LUNs, um die Anzahl der Vorgänge auf verschiedenen Hosts zu beschränken, die gleichzeitig eine SCSI-Reservierung erfordern.
- Erhöhen Sie die Anzahl der LUNs und begrenzen Sie die Anzahl der Hosts, die auf dieselbe LUN zugreifen.
- Reduzieren Sie die Anzahl der Snapshots. Snapshots verursachen viele SCSI-Reservierungen.
- Reduzieren Sie die Anzahl der virtuellen Maschinen pro LUN. Befolgen Sie die Empfehlungen unter *Maximalwerte für die Konfiguration*.
- Stellen Sie sicher, dass Sie über alle Hosts hinweg über die aktuellste HBA-Firmware verfügen.
- Stellen Sie sicher, dass der Host über das neueste BIOS verfügt.

- Stellen Sie sicher, dass die Einstellung für den Hostmodus auf dem SAN-Array korrekt ist.

Informationen zum Behandeln von SCSI-Reservierungskonflikten auf bestimmten Speicher-Arrays finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1005009>.

## Pfad-Thrashing führt zu langsamem LUN-Zugriff

Wenn Ihr ESXi-Host nicht auf eine LUN zugreifen kann, oder der Zugriff sehr langsam ist, liegt möglicherweise ein Problem mit Pfad-Thrashing (auch als LUN-Thrashing bezeichnet) vor.

### Problem

Ihr Host kann nicht auf eine LUN zugreifen oder der Zugriff ist sehr langsam. Die Protokolldateien des Hosts weisen möglicherweise häufige Änderungen am Pfadzustand aus. Beispiel:

```
Frequent path state changes are occurring for path vmhba2:C0:T0:L3. This may indicate a storage problem. Affected device: naa.600600000000000000edd1. Affected datastores: ds1
```

### Ursache

Das Problem wird möglicherweise durch Pfad-Thrashing verursacht. Ein Pfad-Thrashing kann auftreten, wenn zwei Hosts über unterschiedliche Speicherprozessoren (Sps) auf dieselbe LUN zugreifen und die LUN infolgedessen niemals verfügbar ist.

Das Pfad-Thrashing tritt in der Regel in Aktiv/Passiv-Arrays auf. Pfad-Thrashing kann auch auf einem direkt verbundenen Array mit HBA-Failover auf einem oder mehreren Knoten auftreten. Aktiv/aktiv-Arrays oder Arrays, die transparentes Failover bieten, verursachen kein Pfad-Thrashing.

### Lösung

- 1 Stellen Sie sicher, dass alle Hosts, die eine Gruppe von LUNs in diesen Aktiv/Passiv-Arrays gemeinsam verwenden, gleichzeitig auf denselben Speicherprozessor zugreifen.
- 2 Korrigieren Sie mögliche Inkonsistenzen bei der Verkabelung oder der Maskierung unterschiedlicher Hosts und SAN-Ziele, sodass allen HBAs dieselben Ziele in derselben Reihenfolge angezeigt werden.
- 3 Stellen Sie sicher, dass die Beanspruchungsregeln, die auf allen Hosts definiert sind, die LUNs gemeinsam verwenden, exakt gleich sind.
- 4 Wählen Sie für die Pfadrichtlinie die Option „Zuletzt verwendetes PSP“ (Standardeinstellung).

## Eine erhöhte Latenz für E/A-Anforderungen beeinträchtigt die Leistung virtueller Maschinen

Wenn der ESXi-Host mehr Befehle für eine LUN generiert, als die Warteschlangentiefe der LUN aufnehmen kann, werden die überzähligen Befehle in die Warteschlange von VMkernel eingereiht. Dadurch wird die Latenz bzw. die Dauer, die für das Verarbeiten von E/A-Anforderungen benötigt wird, erhöht.

### Problem

Der Host braucht mehr Zeit für das Verarbeiten von E/A-Anforderungen, was zu einer unbefriedigenden Leistung der virtuellen Maschinen führt.

### Ursache

Möglicherweise wird das Problem durch eine unzureichende LUN-Warteschlangentiefe verursacht. SCSI-Gerätetreiber verfügen über einen konfigurierbaren Parameter, LUN-Warteschlangentiefe, mit dem die Anzahl der Befehle, die bei einer angegebenen LUN gleichzeitig aktiv sein dürfen, festgelegt wird. Wenn der Host mehrere Befehle an eine LUN sendet, werden die überzähligen Befehle in die Warteschlange des VMkernels eingereiht.

## Lösung

- 1 Falls die Gesamtzahl der aktiven Befehle aller virtuellen Maschinen die LUN-Tiefe ständig überschreitet, erhöhen Sie die Warteschlangentiefe.

Das Verfahren, mit dem Sie die Warteschlangentiefe erhöhen, hängt vom Speicheradapertyp ab, den der Host verwendet.

- 2 Wenn mehrere virtuelle Maschinen für eine LUN aktiv sind, ändern Sie den Parameter „Disk.Sched-NumReqOutstanding (DSNRO)“, sodass er mit dem Wert der Warteschlangentiefe übereinstimmt.

## Anpassen der Warteschlangentiefe für QLogic-, Emulex- und Brocade-HBAs

Wenn Sie mit der Leistung Ihrer Hardwarebusadapter (HBAs) nicht zufrieden sind, können Sie die maximale Warteschlangentiefe auf Ihrem ESXi-Host ändern.

Der maximale Werte bezieht sich auf die Warteschlangentiefe, die für verschiedene Pfade zur LUN gemeldet werden. Wenn Sie diesen Wert herabsetzen, wird der Durchsatz des Hosts gedrosselt und das Risiko von SAN-Konflikten wird reduziert, falls mehrere Hosts den Speicher überbeanspruchen und die Befehlswarteschlange auffüllen.

Verwenden Sie zum Anpassen des Parameters für die maximale Warteschlangentiefe die vCLI-Befehle.

In diesem Vorgang wird der Zielsever durch `--server=Servername` angegeben. Der angegebene Zielsever fordert Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Vorgehensweise

- 1 Prüfen Sie, welches HBA-Modul derzeit geladen ist, indem Sie folgenden Befehl eingeben:

```
esxcli --server=Servername system module list | grep Modul
```

Verwenden Sie für *Modul* eine der folgenden Optionen.

Option	Beschreibung
<b>qla</b>	QLogic
<b>qln</b>	Native QLogic-Treiber
<b>lpfc</b>	Emulex
<b>bfa</b>	Brocade

- 2 Passen Sie die Warteschlangentiefe für das entsprechende Modul an.

```
esxcli --server=Servername system module parameters set -p parameter=value -m Modul
```

Verwenden Sie für die Optionen *Parameter* und *Modul* die folgenden Zeichenfolgen.

String	Beschreibung
<b>-p ql2xmaxqdepth=Wert</b> <b>-m qla2xxx</b>	QLogic
<b>-p ql2xmaxqdepth=Wert</b> <b>-m qlnativefc</b>	Native QLogic-Treiber



String	Beschreibung
<b>-p lpfc0_lun_queue_depth=Wert</b> <b>-m lpfc820</b>	Emulex
<b>-p lpfc0_lun_queue_depth=Wert</b> <b>-m lpfc</b>	Native Emulex-Treiber
<b>-p bfa_lun_queue_depth=Wert</b> <b>-m bfa</b>	Brocade

- 3 Starten Sie Ihren Host neu.
- 4 Überprüfen Sie Ihre Änderungen, indem Sie den folgenden Befehl ausführen:  
**esxcli --server=Servername system module parameters list -m=Modul.**

*Modul* ist ein entsprechender Treiber, wie z. B. **qlnativefc** oder **bfa**.

## Anpassen der maximalen Warteschlangentiefe für Software-iSCSI

Wenn Sie für Ihre Software-iSCSI-LUNs eine nicht zufriedenstellende Leistung feststellen, ändern Sie die maximale Warteschlangentiefe, indem Sie die `esxcli`-Befehle ausführen.

### Voraussetzungen

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi-Shell aus.
- Bei dem Vorgang gibt die Verbindungsoption „`--server=Servername`“ den Zielserver an. Bereiten Sie sich darauf vor, einen Benutzernamen und ein Kennwort einzugeben, wenn der Zielserver Sie dazu auffordert. Eine Liste der anderen möglichen Optionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*

### Vorgehensweise

- 1 Führen Sie den folgenden Befehl aus:

```
esxcli --server=server_name system module parameters set -m iscsi_vmk -p iscsivmk_LunQ-Depth=value
```

Der Parameter `iscsivmk_LunQDepth` legt die maximale Anzahl ausstehender Befehle oder die Warteschlangentiefe für jede LUN fest, auf die über den Software-iSCSI-Adapter zugegriffen wird. Der Standardwert ist 128.

- 2 Starten Sie Ihr System neu.
- 3 Überprüfen Sie Ihre Änderungen, indem Sie den Befehl  
**esxcli --server=Servername system module parameters list -m iscsi\_vmk** ausführen.

Die folgende Ausgabe zeigt die Warteschlangentiefe für Software-iSCSI an.

```
iscsivmk_LunQDepth int 64 Maximum Outstanding Commands Per LUN
```



**VORSICHT** Wenn für die Warteschlangentiefe ein höherer Wert als die Standardeinstellung gewählt wird, kann die Gesamtzahl an unterstützten LUNs reduziert sein.

## Ändern der Einstellung für ausstehende E/A-Anforderungen

Falls Sie die LUN-Warteschlangentiefe angepasst haben, ändern Sie den Parameter „Disk.SchedNumReqOutstanding (DSNRO)“, sodass sein Wert mit der Warteschlangentiefe übereinstimmt. Der Parameter steuert die maximale Anzahl der ausstehenden E/A-Anforderungen, die alle virtuellen Maschinen an die LUN übermitteln können.

Ändern Sie diesen Parameter nur dann, wenn auf einer LUN mehrere virtuelle Maschinen aktiv sind. Der Parameter findet keine Anwendung, wenn nur eine virtuelle Maschine aktiv ist. In diesem Fall wird die Bandbreite durch die Warteschlangentiefe des Speicheradapters gesteuert.

Dieser Parameter wird pro Gerät festgelegt.

### Vorgehensweise

- 1 Geben Sie den folgenden Befehl ein, um die aktuelle DSNRO-Einstellung für das angegebene Gerät anzuzeigen:

```
esxcli storage core device list -d Geräte-ID
```

Eine Meldung, die so oder ähnlich aussieht, wird angezeigt:

```
No of outstanding IOs with competing worlds: 32
```

- 2 Ändern Sie den DSNRO-Wert durch Eingabe des folgenden Befehls:

```
esxcli storage core device set -0 | --sched-num-req-outstanding Wert -d Geräte-ID
```

- 3 Überprüfen Sie Ihre Änderungen, indem Sie den folgenden Befehl eingeben:

```
esxcli storage core device list -d Geräte-ID
```

## Virtuelle Maschinen mit RDMs müssen den SCSI INQUIRY-Cache ignorieren

Speicheranbieter setzen möglicherweise voraus, dass virtuelle Maschinen mit RDMs von ESXi zwischengespeicherte SCSI INQUIRY-Daten ignorieren.

### Problem

Bestimmte Gastbetriebssysteme oder Anwendungen, die in virtuellen Maschinen mit RDMs ausgeführt werden, zeigen ein unberechenbares Verhalten.

### Ursache

Dies wird möglicherweise durch zwischengespeicherte SCSI INQUIRY-Daten verursacht, die sich störend auf bestimmte Gastbetriebssysteme und Anwendungen auswirken.

Wenn der ESXi-Host zum ersten Mal eine Verbindung mit einem Zielspeichergerät auf einem SAN herstellt, führt er den SCSI INQUIRY-Befehl aus, um allgemeine Identifikationsdaten vom Gerät abzurufen. Standardmäßig speichert ESXi die empfangenen SCSI INQUIRY-Daten (Standard, Seite 80 und Seite 83) im Cache-Speicher und diese Daten bleiben danach unverändert.

### Lösung

- ◆ Konfigurieren Sie die virtuelle Maschine mit RDM, um den SCSI INQUIRY-Cache zu ignorieren, indem Sie den folgenden Parameter in die `.vmx`-Datei einfügen.

```
scsiox.y.ignoreDeviceInquiryCache = "true"
```

wobei *x* die Nummer des SCSI-Controllers und *y* die SCSI-Zielnummer der RDM ist.

Aktivieren Sie diesen Parameter nur dann, wenn Ihr Speicheranbieter Ihnen dies empfiehlt. Dieser Parameter wird nur für eine begrenzte Anzahl an Speicher-Arrays und nur für bestimmte Gastbetriebssysteme benötigt.

## Der Software-iSCSI-Adapter ist aktiviert, wenn er nicht benötigt wird

Wenn Ihr Host einen Netzwerkadapter mit iBFT verwendet, ist der Software-iSCSI-Adapter standardmäßig immer aktiviert.

### Problem

Nach dem ersten Start Ihres ESXi-Hosts ist der Software-iSCSI-Adapter aktiviert und wird im vSphere Web Client in der Liste der Speicheradapter angezeigt.

### Ursache

Der iBFT-aktivierte Netzwerkadapter auf Ihrem Host sorgt dafür, dass der Software-iSCSI immer vorhanden ist. Dieser Zustand liegt auch dann vor, wenn Sie für den iSCSI-Start nicht iBFT verwenden.

### Lösung

Wenn Sie den iBFT-fähigen Netzwerkadapter nicht für den iSCSI-Start verwenden und nicht möchten, dass der Software-iSCSI-Adapter aktiviert ist, entfernen Sie die iBFT-Konfiguration aus dem Netzwerkadapter. Da dieser Prozess anbieterspezifisch ist, lesen Sie bitte die Dokumentation Ihres Anbieters, um nähere Informationen zu erhalten.

## Fehler beim Mounten von NFS-Datenspeichern

Versuche, NFS-Datenspeicher mit Namen in anderen Sprachen zu mounten, schlagen fehl.

### Problem

Die Verwendung von Nicht-ASCII-Zeichen für Verzeichnis- und Dateinamen auf einem NFS-Speicher kann zu unvorhersehbarem Verhalten führen. Sie können dann möglicherweise einen NFS-Datenspeicher nicht mehr mounten oder eine virtuelle Maschine nicht mehr starten.

### Ursache

ESXi unterstützt die Verwendung von Nicht-ASCII-Zeichen für Verzeichnis- und Dateinamen auf einem NFS-Speicher, damit Sie Datenspeicher und virtuelle Maschinen mit Namen in internationalen Sprachen erstellen können. Wenn allerdings der zugrunde liegende NFS-Server die Internationalisierung nicht unterstützt, kann es zu unvorhersehbaren Ausfällen kommen.

### Lösung

Achten Sie stets darauf, dass der zugrunde liegende NFS-Server die Internationalisierung unterstützt. Ist dies nicht der Fall, verwenden Sie ausschließlich ASCII-Zeichen.

## Fehlerbehebung bei Speicheradaptern

Wenn auf Ihren Speicheradaptern Leistungsbeeinträchtigungen auftreten, verwenden Sie die Befehle `esxc li storage san`, um die Ursache der Probleme zu ermitteln.

### Problem

Leistungs- und E/A-Problem bei Speicheradaptern.

## Lösung

Verwenden Sie die Befehle `esxcli storage san`, um Ereignisse und Statistiken für die Adapter abzufragen und anzuzeigen. Sie können die Ausgabe der Befehle analysieren, um Adapterprobleme zu erkennen und geeignete Lösungen zu finden.

**Tabelle 7-3.** `esxcli storage san`-Befehle

Befehl	Beschreibung	Optionen
<code>esxcli storage san fc   iscsi   fcoe   sas list</code>	Auflisten von Adapterattributen. <b>HINWEIS</b> iSCSI ist nur für Software iSCSI anwendbar.	-- adapter   -A Adaptername (vmhbaX) oder „none“, um Informationen für alle Adapter eines bestimmten Typs anzuzeigen.
<code>esxcli storage san fc   iscsi   fcoe   sas stats get</code>	Abrufen der Adapterstatistiken. <b>HINWEIS</b> iSCSI ist nur für Software iSCSI anwendbar.	-- adapter   -A Adaptername (vmhbaX) oder „none“, um Informationen für alle Adapter eines bestimmten Typs anzuzeigen.
<code>esxcli storage san fc   fcoe   sas reset</code>	Zurücksetzen eines bestimmten Adapters.	-- adapter   -A Adapter name (vmhbaX).
<code>esxcli storage san fc events get</code>	Abruf von Ereignissen für Fibre Channel-Adapter.	-- adapter   -A Adaptername (vmhbaX) oder „none“, um Informationen für alle Fibre Channel-Adapter auf dem System anzuzeigen.

## Überprüfen der Metadatenkonsistenz mit VOMA

Verwenden Sie vSphere On-disk Metadata Analyzer (VOMA), um Metadatenbeschädigungen zu identifizieren, die Dateisysteme oder zugrunde liegende logische Volumes beeinträchtigen.

### Problem

Sie können die Metadatenkonsistenz überprüfen, wenn Probleme mit einem VMFS-Datenspeicher oder einer vFlash-Ressource auftreten. Führen Sie beispielsweise in folgenden Situationen eine Metadatenprüfung durch:

- Es treten Speicherausfälle auf.
- Nach einer erneuten RAID-Erstellung oder dem Ersetzen einer Festplatte.
- Die Datei `vmkernel.log` enthält Metadatenfehler ähnlich den folgenden:
 

```
cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402 ("<Data-store_name>") may be damaged on disk. Corrupt heartbeat detected at offset 3305472: [HB state 0 offset 6052837899185946624 gen 15439450 stampUS 5 $
```
- Sie können nicht auf Dateien auf einem VMFS zugreifen.
- Für einen Datenspeicher wird auf der Registerkarte „Ereignisse“ von vCenter Server eine Beschädigung gemeldet.

## Lösung

Führen Sie zum Überprüfen der Metadatenkonsistenz VOMA von der Befehlszeilenschnittstelle eines ESXi-Hosts aus. Mit VOMA können geringfügige Inkonsistenzprobleme für einen VMFS-Datenspeicher oder eine vFlash-Ressource überprüft und behoben werden. Wenden Sie sich an den VMware-Support, wenn von VOMA gemeldete Fehler behoben werden sollen.

Folgen Sie diesen Anweisungen, wenn Sie das VOMA-Tool verwenden:

- Stellen Sie sicher, dass der VMFS-Datenspeicher, den Sie analysieren, sich nicht über mehrere Erweiterungen erstreckt. Sie können VOMA nur auf einen Datenspeicher mit einer Erweiterung anwenden.
- Schalten Sie alle ausgeführten virtuellen Maschinen aus oder migrieren Sie sie in einen anderen Datenspeicher.

Das folgende Beispiel veranschaulicht die Überprüfung der VMFS-Metadatenkonsistenz mithilfe von VOMA.

- 1 Ermitteln Sie den Namen und die Partitionsnummer des Geräts, das den zu überprüfenden VMFS-Datenspeicher stützt.

```
#esxcli storage vmfs extent list
```

Der Gerätenamen und die Partitionsnummern in der Ausgabe geben das Gerät an. Beispiel:

```
Volume Name XXXXXXXX Device Name Partition
1TB_VMFS5 XXXXXXXX naa.0000000000000000000000000000703 3
```

- 2 Suchen Sie nach VMFS-Fehlern.

Geben Sie den absoluten Pfad zur Gerätepartition an, die den VMFS-Datenspeicher stützt. Geben Sie zudem eine Partitionsnummer mit dem Gerätenamen an. Beispiel:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/naa.0000000000000000000000000000703:3
```

In der Ausgabe werden mögliche Fehler aufgelistet. Beispielsweise deutet die folgende Ausgabe darauf hin, dass die Taktsignaladresse ungültig ist.

```
XXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.
```

```
Total Errors Found: 1
```

Für das VOMA-Tool gibt es die folgenden Befehlsoptionen.

**Tabelle 7-4.** VOMA-Befehlsoptionen

Befehlsoption	Beschreibung
-m   --module	U. a. müssen folgende Module ausgeführt werden:
vmfs	Wenn Sie den Namen des Moduls nicht angeben, wird diese Option standardmäßig verwendet. Sie können VMFS3-, VMFS5- und VMFS6-Dateisysteme sowie Dateisysteme, die vFlash-Ressourcen stützen, überprüfen. Wenn Sie dieses Modul angeben, werden zudem Minimalüberprüfungen für LVM durchgeführt.
lvm	Überprüft logische Volumes, die VMFS-Datenspeicher unterstützen.

**Tabelle 7-4.** VOMA-Befehloptionen (Fortsetzung)

Befehloption	Beschreibung
	ptck Überprüft und validiert VMFS-Partitionen wie MBR oder GPT. Wenn keine Partition vorhanden ist, wird ermittelt, ob Partitionen vorhanden sein sollten.
-f   --func	U. a. müssen folgenden Funktionen ausgeführt werden:
	query Listet die vom Modul unterstützten Funktionen auf.
	check Sucht nach Fehlern.
-d   --device	Zu inspizierendes Gerät bzw. zu inspizierende Festplatte. Stellen Sie sicher, dass Sie den absoluten Pfad zur Gerätepartition angeben, die den VMFS-Datenspeicher stützt. Zum Beispiel: /vmfs/devices/disks/naa.00000000000000000000000000000000:1.
-s   --logfile	Geben Sie die Protokolldatei zum Ausgeben der Ergebnisse an.
-v   --version	Zeigt die VOMA-Version an.
-h   --help	Zeigt einen Hilfetext zum VOMA-Befehl an.

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [2036767](#).

## Kein Failover für den Speicherpfad, wenn der TUR-Befehl nicht erfolgreich ist

Es kommt zu keinem Failover für den Speicherpfad, wenn der TUR-Befehl wiederholt Wiederholungsanforderungen zurückgibt.

### Problem

Wenn bei einem Speicherpfad Probleme auftreten, sendet ein ESXi-Host normalerweise den TUR-Befehl (Test Unit Ready), um zu bestätigen, dass der Pfad vor dem Initiieren eines Pfad-Failovers deaktiviert ist. Wenn jedoch der TUR-Befehl nicht erfolgreich ist und wiederholt eine Anforderung für Wiederholungsvorgänge wiedergibt (VMK\_STORAGE\_RETRY\_OPERATION), wiederholt der Host weiterhin den Befehl, ohne dass der Failover ausgelöst wird. In der Regel wird durch die folgenden Fehler verursacht, dass der Host den TUR-Befehl wiederholt:

- SCSI\_HOST\_BUS\_BUSY 0x02
- SCSI\_HOST\_SOFT\_ERROR 0x0b
- SCSI\_HOST\_RETRY 0x0c

### Ursache

Um dieses Problem zu beheben, können Sie den `enable|disable_action_OnRetryErrors`-Parameter verwenden. Wenn Sie diesen Parameter aktivieren, kann der ESXi-Host den problematischen Pfad als ausgefallen markieren. Wenn der Pfad als ausgefallen markiert wurde, kann der Host den Failover auslösen und einen alternativen funktionierenden Pfad verwenden.

## Lösung

- Legen Sie den Parameter durch Ausführen eines entsprechenden Befehls durch:

Aktion	Befehl
Aktiviert die Funktion, einen problematischen Pfad als ausgefallen zu markieren	<pre># esxcli storage nmp satp generic deviceconfig set -c enable_action_OnRetryErrors -d naa.XXX</pre>
Deaktiviert die Funktion, einen problematischen Pfad als ausgefallen zu markieren	<pre># esxcli storage nmp satp generic deviceconfig set -c disable_action_OnRetryErrors -d naa.XXX</pre>

- Überprüfen Sie den Status des Parameters, indem Sie den folgenden Befehl ausführen:

```
# esxcli storage nmp device list
```

Mit der folgenden Beispielausgabe wird angezeigt, dass der Parameter aktiviert wurde:

```
naa.XXX
Device Display Name: DGC Fibre Channel Disk (naa.XXX)
Storage Array Type: VMW_SATP_CX Storage Array Type Device
Config: {navireg ipfilter action_OnRetryErrors}
```

Der enable|disable\_action\_OnRetryErrors-Parameter ist über Neustarts hinweg persistent.

Sie können diesen Parameter auch beim Konfigurieren einer SATP-Beanspruchungsregel festlegen:

```
# esxcli storage nmp satp rule add -t device -d naa.XXX -s VMW_SATP_EXAMPLE -P VMW_PSP_FIXED -o enable_action_OnRetryErrors
```

## Fehlerbehebung bei Flash-Geräten

vSphere verwendet Flash-Laufwerke für Speicherfunktionen wie vSAN, Hostauslagerungs-Cache und Flash Read Cache.

Die Themen zur Fehlerbehebung helfen, potenzielle Probleme zu vermeiden, und enthalten Lösungen für Probleme, die beim Konfigurieren von Flash-Laufwerken auftreten können.

### Formatierte Flash-Geräte sind möglicherweise nicht mehr verfügbar

Ein lokales Flash-Gerät ist für eine vFlash-Ressource oder Virtual SAN-Konfiguration nicht mehr verfügbar, wenn es mit VMFS oder einem anderen Dateisystem formatiert wurde.

#### Problem

Wenn Sie versuchen, vSAN oder eine vFlash-Ressource zu konfigurieren, ist die Flash-Festplatte nicht mehr in der Liste der verfügbaren Festplatten aufgeführt.

#### Ursache

Dieses Problem kann auftreten, wenn eine Flash-Festplatte, die mit einer der beiden Funktionen verwendet werden soll, bereits mit VMFS formatiert wurde. Virtueller Flash und vSAN dürfen die Flash-Festplatte nicht mit VMFS oder einem anderen Dateisystem gemeinsam verwenden.

Zudem können beide Funktionen nicht dieselbe Flash-Festplatte verwenden, da vFlash und vSAN sich gegenseitig ausschließende Konsumenten von Flash-Festplatten sind. Wenn die Flash-Festplatte bereits von einer Funktion, z. B. vSAN, beansprucht wird, kann sie nicht durch eine andere Funktion, z. B. vFlash, verwendet werden, ohne zuvor freigegeben zu werden.

## Lösung

Verwenden Sie nur unformatierte Flash-Festplatten für vFlash-Ressourcen und vSAN-Konfigurationen.

- Vermeiden Sie während der Installation von ESXi oder der Ausführung von Auto Deploy das Formatieren der Flash-Festplatten mit VMFS.
- Wenn die Flash-Festplatte bereits mit VMFS formatiert ist, entfernen Sie den VMFS-Datenspeicher. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Speicher*.
- Zum Verwenden der Flash-Festplatte als vFlash-Ressource beanspruchen Sie diese Festplatte nicht für vSAN. Wenn die Festplatte von vSAN beansprucht wird, entfernen Sie die Festplatte von vSAN. Die Flash-Festplatte wird aus vSAN freigegeben und steht dann auf der Liste der Festplatten zur Verfügung, die mit virtuellem Flash verwendet werden können. Weitere Informationen zum Entfernen von Festplatten aus vSAN finden Sie in der Dokumentation *Verwalten von VMware vSAN*.
- Wenn Sie beabsichtigen, die Flash-Festplatte mit vSAN zu verwenden, verwenden Sie sie nicht für eine vFlash-Ressource. Wenn die Flash-Festplatte als vFlash-Ressource verwendet wird, entfernen Sie die vFlash-Konfiguration. Die Festplatte wird für vSAN verfügbar. Informationen finden Sie in der Dokumentation *vSphere-Speicher*.

Wenn die Festplatte von ESXi nicht erkannt wird, so ist dies ein weiterer Grund, weshalb die Flash-Festplatte nicht verfügbar ist. Weitere Informationen hierzu finden Sie unter [„Lokale Flash-Festplatten werden nicht gefunden“](#), auf Seite 73.

## Beibehalten VMFS-freier Flash-Festplatten

Wenn Sie beim Installieren oder der automatischen Bereitstellung von ESXi die Startoption für die automatische Partitionierung verwenden, erstellt die Option für die automatische Partitionierung einen VMFS-Datenspeicher im lokalen Speicher Ihres Hosts. In bestimmten Fällen müssen Sie die Flash-Festplatten des lokalen Speichers unformatiert lassen.

### Problem

Standardmäßig stellt die automatische Partitionierung auf allen nicht verwendeten lokalen Speicherfestplatten des Hosts VMFS-Dateisysteme bereit, einschließlich Flash-Festplatten.

Eine mit VMFS formatierte Flash-Festplatte ist jedoch für Funktionen wie vFlash und vSAN nicht mehr verfügbar. Beide Funktionen erfordern eine unformatierte Flash-Festplatte und keine dieser Funktionen kann die Festplatte zusammen mit einem anderen Dateisystem verwenden.

### Lösung

Wenn Sie sicherstellen möchten, dass die Flash-Festplatte bei der automatischen Partitionierung nicht mit VMFS formatiert wird, verwenden Sie beim Installieren von ESXi oder beim erstmaligen Starten des ESXi-Hosts die folgenden Startoptionen:

- `autoPartition=TRUE`
- `skipPartitioningSsds=TRUE`

Wenn Sie Auto Deploy verwenden, legen Sie diese Parameter auf einem Referenzhost fest.

- 1 Wählen Sie im vSphere Web Client den Host aus, den Sie als Referenzhost verwenden möchten, und klicken Sie auf die Registerkarte **Konfigurieren**.
- 2 Klicken Sie auf **System**, um die Systemoptionen zu öffnen, und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 3 Führen Sie einen Bildlauf zu `VMkernel.Boot.autoPartition` durch und legen Sie den Wert auf „True“ fest.
- 4 Führen Sie einen Bildlauf zu `VMkernel.Boot.skipPartitioningSsds` durch und legen Sie den Wert auf „True“ fest.



5 Starten Sie den Host neu.

Falls Flash-Festplatten, die Sie mit Flash Read Cache und vSAN verwenden möchten, bereits VMFS-Datenspeicher aufweisen, entfernen Sie die Datenspeicher.

## Lokale Flash-Festplatten werden nicht gefunden

Wenn Sie nach lokalen Flash-Festplatten abfragen, gibt der ESXi-Host möglicherweise keine vollständige Liste der lokalen Flash-Festplatten zurück.

### Problem

ESXi kann möglicherweise Flash-Festplatten nicht erkennen oder kann sie nicht als lokal erkennen. Dieses Problem kann auftreten, wenn Sie Elemente konfigurieren, die nur lokale Flash-Festplatten wie beispielsweise virtuelle Flash-Ressourcen oder vSAN erfordern.

### Ursache

ESXi erkennt bestimmte Geräte nicht als Flash-Festplatten, wenn die Hersteller die automatische Flash-Festplatten-Erkennung nicht unterstützen. In anderen Fällen werden einige Flash-Festplatten nicht als lokal erkannt, und ESXi markiert sie als „Remote“. Wenn der Host die Festplatten nicht als die lokalen Flash-Festplatten erkennt, werden sie von der Liste der für die Konfiguration verfügbaren Festplatten ausgeschlossen.

### Lösung

Sie müssen Festplatten möglicherweise als Flash-Festplatten oder lokale Festplatten kennzeichnen.

- Falls ESXi Festplatten nicht automatisch als Flash-Festplatten erkennt, kennzeichnen Sie sie als Flash-Festplatten.
- Falls ESXi Flash-Festplatten nicht als lokal erkennt, legen Sie sie manuell als lokal fest.

## Markieren der Speichergeräte als Flash-Gerät

Falls ESXi Geräte nicht als Flash-Geräte erkennt, markieren Sie sie als Flash-Geräte.

ESXi erkennt bestimmte Geräte nicht als Flash-Festplatten, wenn die Hersteller die automatische Flash-Festplatten-Erkennung nicht unterstützen. In der Spalte „Laufwerktyp“ wird für die Geräte „HDD“ als Typ angezeigt.



**VORSICHT** Das Markieren von HDD-Geräten als Flash-Geräte kann die Leistung von Datenspeichern und Diensten, die sie verwenden, verschlechtern. Markieren Sie die Geräte nur dann, wenn Sie sicher sind, dass es sich um Flash-Geräte handelt.

### Voraussetzungen

Stellen Sie sicher, dass das Gerät nicht verwendet wird.

### Vorgehensweise

- 1 Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.
- 4 Wählen Sie in der Liste der Speichergeräte ein oder mehrere HDD-Geräte aus, die als Flash-Geräte markiert werden sollen, und klicken Sie auf das Symbol **Als Flash-Festplatten markieren** (F).
- 5 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

Der Gerätetyp wird in „Flash“ geändert.

**Weiter**

Wenn das Flash-Gerät, das Sie markieren, von mehreren Hosts gemeinsam genutzt wird, stellen Sie sicher, dass Sie das Gerät von allen Hosts aus markieren, die das Gerät gemeinsam nutzen.

**Markieren der Speichergeräte als lokal**

ESXi ermöglicht Ihnen das Markieren von Geräten als lokal. Dieser Vorgang ist nützlich, wenn ESXi nicht ermitteln kann, ob bestimmte Geräte lokal sind.

**Voraussetzungen**

- Stellen Sie sicher, dass das Gerät nicht gemeinsam genutzt wird.
- Schalten Sie auf dem Gerät befindliche virtuelle Maschinen aus und unmounten Sie einen zugewiesenen Datenspeicher.

**Vorgehensweise**

- 1 Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Konfigurieren**.
- 3 Klicken Sie unter **Speicher** auf **Speichergeräte**.
- 4 Wählen Sie in der Liste der Speichergeräte ein oder mehrere Remotegeräte aus, die als lokal markiert werden müssen, und klicken Sie auf das Symbol **Alle Aktionen**.
- 5 Klicken Sie auf **Als lokal markieren** und dann auf **Ja**, um die Änderungen zu speichern.

**Fehlerbehebung bei virtuellen Volumes**

Virtuelle Volumes sind Verkapselungen der Dateien und virtuellen Festplatten von virtuellen Maschinen sowie deren Derivate. Virtuelle Volumes werden systemseitig in einem Speichersystem gespeichert, das über Ethernet oder SAN verbunden ist. Sie werden als Objekte von einem kompatiblen Speichersystem exportiert und vollständig von der Hardware auf Speicherseite verwaltet.

Informationen zur Funktionalität für virtuelle Volumes finden Sie in der Dokumentation zu *vSphere-Speicher*.

**Virtual Volumes und esxcli-Befehle**

Die `esxcli storage vvol`-Befehle verwenden Sie für die Fehlerbehebung Ihrer Umgebung mit den Virtual Volumes.

Die folgenden Befehlsoptionen sind verfügbar:

**Tabelle 7-5.** `esxcli storage vvol`-Befehle

Namespace	Befehlsoption	Beschreibung
<code>esxcli storage core device</code>	<code>list</code>	Protokollendpunkte identifizieren Der Ausgabeeintrag <code>Is VVOL PE: true</code> zeigt an, dass das Speichergerät ein Protokollendpunkt ist.
<code>esxcli storage vvol daemon</code>	<code>unbindall</code>	Hebt die Bindung für alle virtuellen Volumes aller VASA-Anbieter auf, die dem ESXi-Host bekannt sind.
<code>esxcli storage vvol protocolend-point</code>	<code>list</code>	Listet alle Protokollendpunkte auf, auf die Ihr Host zugreifen kann.

**Tabelle 7-5.** `esxcli storage vvol`-Befehle (Fortsetzung)

Namespace	Befehloption	Beschreibung
<code>esxcli storage vvol storagecontainer</code>	<code>list</code> <code>abandonedvvol scan</code>	Listet alle verfügbaren Speichercontainer auf. Durchsucht den angegebenen Speichercontainer auf aufgegebenen VVols.
<code>esxcli storage vvol vasacontext</code>	<code>get</code>	Zeigt den VASA-Kontext (VC-UUID), der mit dem Host verbunden ist, an.
<code>esxcli storage vvol vasaprovider</code>	<code>list</code>	Listet alle mit dem Host verbundenen Speicher-Anbieter (VASA) auf.

## Auf den virtuellen Datenspeicher kann nicht zugegriffen werden

Nachdem Sie einen virtuellen Datenspeicher erstellt haben, kann nicht darauf zugegriffen werden.

### Problem

Im vSphere Web Client wird angezeigt, dass kein Zugriff auf den Datenspeicher möglich ist. Sie können den Datenspeicher nicht für die Bereitstellung virtueller Maschinen verwenden.

### Ursache

Dieses Problem kann auftreten, wenn Sie keine Protokollendpunkte für den SCSI-basierten Speichercontainer konfiguriert haben, der dem virtuellen Datenspeicher zugeordnet ist. Wie bei traditionellen LUNs müssen SCSI-Protokollendpunkte konfiguriert werden, damit ein ESXi-Host diese erkennen kann.

### Lösung

Vor dem Erstellen virtueller Datenspeicher für SCSI-basierte Container müssen Sie auf der Speicherseite Protokollendpunkte erstellen.

## Fehler beim Migrieren von virtuellen Maschinen oder beim Bereitstellen von VM-OVFs auf Datenspeichern für virtuelle Volumes

Versuche, eine virtuelle Maschine zu migrieren oder VM-OVF in virtuellen Datenspeichern bereitzustellen, schlagen fehl

### Problem

Eine OVF-Vorlage oder eine VM, die von einem nicht virtuellen Datenspeicher migriert wird, enthält möglicherweise zusätzliche große Dateien, wie beispielsweise ISO-Festplatten-Images, DVD-Images und Image-Dateien. Falls diese zusätzlichen Dateien bewirken, dass das virtuelle Konfigurations-Volumen den Grenzwert von 4 GB überschreitet, schlägt die Migration oder die Bereitstellung in einem virtuellen Datenspeicher fehl.

### Ursache

Das virtuelle Konfigurations-Volumen bzw. Konfigurations-vVol enthält verschiedene Dateien im Zusammenhang mit virtuellen Maschinen. Auf traditionellen, nicht virtuellen Datenspeichern werden diese Dateien im Stammverzeichnis der virtuellen Maschine gespeichert. Ähnlich wie das Stammverzeichnis der virtuellen Maschine enthält das Konfigurations-vVol in der Regel die VM-Konfigurationsdatei, Deskriptordateien für virtuelle Festplatten und Snapshots, Protokolldateien, Sperrdateien usw.

Auf virtuellen Datenspeichern werden alle anderen großen Dateien, wie beispielsweise für virtuelle Festplatten, Arbeitsspeicher-Snapshots, Auslagerung und Digest, als separate virtuelle Volumes gespeichert.

Konfigurations-vVols werden als virtuelle 4-GB-Volumes erstellt. Der allgemeine Inhalt des Konfigurations-vVol belegt gewöhnlich nur einen Bruchteil der reservierten 4 GB, weshalb Konfigurations-vVols in der Regel Thin-bereitgestellte Volumes sind, um Backing-Speicherplatz zu sparen. Zusätzliche große Dateien, wie beispielsweise ISO-Festplatten-Images, DVD-Images und Image-Dateien, bewirken möglicherweise, dass das Konfigurations-vVol den Grenzwert von 4 GB überschreitet. Falls solche Dateien in einer OVF-Vorlage enthalten sind, schlägt die Bereitstellung von VM-OVF in vSphere Virtual Volumes-Speicher fehl. Falls diese Dateien Bestandteil einer vorhandenen virtuellen Maschine sind, schlägt die Migration dieser virtuellen Maschine von einem traditionellen Datenspeicher zu vSphere Virtual Volumes-Speicher ebenfalls fehl.

### Lösung

- Für die VM-Migration. Entfernen Sie vor der Migration einer virtuellen Maschine von einem traditionellen Datenspeicher zu einem virtuellen Datenspeicher überflüssige Inhalte aus dem Stammverzeichnis der virtuellen Maschine, damit das Konfigurations-vVol unter dem Grenzwert von 4 GB bleibt.
- Für die OVF-Bereitstellung. Eine OVF-Vorlage, die zu viele Dateien enthält, kann nicht direkt in einem virtuellen Datenspeicher bereitgestellt werden. Stellen Sie deshalb zuerst die virtuelle Maschine in einem nicht virtuellen Datenspeicher bereit. Entfernen Sie überflüssige Inhalte aus dem Stammverzeichnis der virtuellen Maschine und migrieren Sie die resultierende virtuelle Maschine zu vSphere Virtual Volumes-Speicher.

## Fehlgeschlagene Versuche beim Migrieren von virtuellen Maschinen mit Arbeitsspeicher-Snapshots zu und von virtuellen Datenspeichern

Beim Versuch, eine virtuelle Maschine mit Hardwareversion 10 oder früher zu und von einem vSphere Virtual Volumes-Datenspeicher zu migrieren, treten Fehler auf, falls die virtuelle Maschine Arbeitsspeicher-Snapshots aufweist.

### Problem

Die folgenden Probleme treten beim Migrieren einer virtuellen Maschine der Version 10 oder früher, die Arbeitsspeicher-Snapshots aufweist, auf:

- Die Migration einer virtuellen Maschine der Version 10 oder früher, die Arbeitsspeicher-Snapshots aufweist, zu einem virtuellen Datenspeicher wird nicht unterstützt und schlägt fehl.
- Die Migration einer virtuellen Maschine der Version 10 oder früher, die Arbeitsspeicher-Snapshots aufweist, von einem virtuellen Datenspeicher zu einem nicht virtuellen Datenspeicher wie z. B. VMFS wird erfolgreich ausgeführt. Wenn Sie später zusätzliche Snapshots erstellen und versuchen, diese virtuelle Maschine wieder zu vSphere Virtual Volumes-Speicher zu migrieren, schlägt der Vorgang fehl.

### Ursache

vSphere Virtual Volumes-Speicher erfordert nicht die Verwendung einer bestimmten Hardwareversion für Ihre virtuellen Maschinen. In der Regel können Sie eine virtuelle Maschine jeder Hardwareversion zu vSphere Virtual Volumes-Speicher migrieren. Wenn Sie jedoch bei einer virtuellen Maschine mit Arbeitsspeicher-Snapshots diese virtuelle Maschine zwischen einem virtuellen Datenspeicher und einem nicht virtuellen Datenspeicher migrieren möchten, sollten Sie die virtuelle Maschine der Hardwareversion 11 verwenden.

Nicht-VVols-VMs der Hardwareversion 11 oder höher verwenden separate Dateien zum Speichern der Arbeitsspeicher-Snapshots. Dieses Verhalten entspricht virtuellen Maschinen auf vSphere Virtual Volumes-Speicher, wo Arbeitsspeicher-Snapshots als separate VVols erstellt werden, anstatt als Bestandteil einer .vmsn-Datei im Stammverzeichnis der virtuellen Maschine gespeichert zu werden. Im Gegensatz dazu speichern Nicht-VVols-VMs mit Hardwareversion 10 ihre Arbeitsspeicher-Snapshots weiterhin als Bestandteil der .vmsn-Datei im Stammverzeichnis der virtuellen Maschine. Demzufolge können beim Versuch, diese virtuellen Maschinen zwischen virtuellen und nicht virtuellen Datenspeichern zu migrieren, Probleme oder Fehler auftreten.

## Lösung

Um bei der Migration von virtuellen Maschinen mit Arbeitsspeicher-Snapshots zwischen virtuellen und nicht virtuellen Datenspeichern Probleme zu vermeiden, sollten Sie Hardwareversion 11 verwenden. Halten Sie sich beim Migrieren von virtuellen Maschinen der Hardwareversion 10 oder früher mit Arbeitsspeicher-Snapshots an die folgenden Richtlinien:

- Die Migration einer virtuellen Maschine der Version 10 oder früher, die Arbeitsspeicher-Snapshots aufweist, zu einem virtuellen Datenspeicher wird nicht unterstützt. Die einzige Problemlösung besteht im Entfernen aller Snapshots. Durch ein Upgrade der Hardwareversion wird dieses Problem nicht behoben.
- Die Migration einer virtuellen Maschine der Version 10 oder früher, die Arbeitsspeicher-Snapshots aufweist, von einem virtuellen Datenspeicher zu einem nicht virtuellen Datenspeicher wie z. B. VMFS wird erfolgreich ausgeführt. Durch die Migration weist die virtuelle Maschine jedoch möglicherweise einen inkonsistenten Zustand auf. Die Snapshots, die auf dem virtuellen Datenspeicher erstellt wurden, verwenden das `vmem`-Objekt. Arbeitsspeicher-Snapshots, die nach der Migration zu VMFS erstellt wurden, werden in der `.vmsn`-Datei gespeichert. Wenn Sie später versuchen, diese virtuelle Maschine wieder zu vSphere Virtual Volumes-Speicher zu migrieren, schlägt der Vorgang fehl. Entfernen Sie wie im vorherigen Fallbeispiel alle Snapshots, um dieses Problem zu umgehen.

## Fehlerbehebung bei VAIO-Filtern

vSphere APIs für E/A-Filter (VAIO) liefern ein Framework, mit dessen Hilfe Drittanbieter als E/A-Filter bezeichnete Softwarekomponenten erstellen können. Die Filter können auf ESXi-Hosts installiert werden und können virtuellen Maschinen zusätzliche Datendienste anbieten, indem E/A-Anforderungen zwischen dem Gastbetriebssystem einer virtuellen Maschine und virtuellen Festplatten verarbeitet werden.

Weitere Informationen zu E/A-Filtern finden Sie in der Dokumentation *vSphere-Speicher*.

## Handhabung von Installationsfehlern bei E/A-Filtern

In der Regel sind für alle ESXi-Hosts in einem Cluster dieselben E/A-Filter installiert. Bei der Installation können gelegentlich Fehler auftreten.

Wenn die Installation eines E/A-Filters auf einem Host fehlschlägt, werden Ereignisse generiert, um den Fehler zu melden. Darüber hinaus zeigt ein Alarm auf dem Host die Ursache für den Fehler an. Beispiele für Fehler:

- Auf dem Host kann nicht auf die VIB-URL zugegriffen werden.
- VIB weist ein ungültiges Format auf.
- VIB erfordert für den Host den Wartungsmodus, um ein Upgrade oder eine Deinstallation durchzuführen.
- VIB erfordert nach der Installation oder Deinstallation einen Neustart des Hosts.
- Versuche, den Host in den Wartungsmodus zu versetzen, schlagen fehl, da die virtuelle Maschine auf dem Host nicht evakuiert werden kann.
- VIB erfordert manuelle Installation oder Deinstallation.

vCenter Server kann einige Fehler beheben. Für andere Fehler ist möglicherweise ein Eingreifen Ihrerseits erforderlich. Beispielsweise müssen Sie möglicherweise die VIB-URL bearbeiten, virtuelle Maschinen manuell evakuieren bzw. ausschalten oder aber VIBs manuell installieren bzw. deinstallieren.

## Installieren von E/A-Filtern auf einem einzelnen ESXi -Host

Zur Fehlerbehebung können Sie eine ESXi-Komponente des E/A-Filters in Form einer VIB-Datei herunterladen und auf dem ESXi-Host installieren. Zum Installieren der VIB-Datei verwenden Sie den Befehl `esxcli`.

Wenn Sie mit `--server=Servername` einen Zielserver angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

### Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

### Vorgehensweise

- 1 Installieren Sie die VIBs durch Ausführen des folgenden Befehls:

```
esxcli --server=server_name software vib install --depot path_to_VMware_vib_ZIP_file
```

Optionen für den Befehl `install` ermöglichen es Ihnen, einen Testlauf durchzuführen, ein bestimmtes VIB anzugeben, die Verifizierung einer Akzeptanzebene zu umgehen usw. Umgehen Sie die Verifizierung nicht auf Produktionssystemen. Informationen finden Sie in der Dokumentation *Referenz zur vSphere Command-Line Interface*.

- 2 Stellen Sie sicher, dass die VIBs auf Ihrem ESXi-Host installiert sind.

```
esxcli --server=Servername software vib list
```

# Fehlerbehebung beim Netzwerk

---

In den Themen zur Fehlerbehebung beim Netzwerk finden Sie Lösungen für potenzielle Probleme, die bei der Konnektivität von ESXi-Hosts, vCenter Server und virtuellen Maschinen auftreten können.

Dieses Kapitel behandelt die folgenden Themen:

- „Fehlerbehebung bei der Zuteilung von MAC-Adressen“, auf Seite 80
- „Die Konvertierung zur erweiterten LACP-Unterstützung schlägt fehl“, auf Seite 83
- „Host kann nicht auf einem vSphere Distributed Switch entfernt werden“, auf Seite 84
- „Für Hosts auf einem vSphere Distributed Switch 5.1 (und höher) wird die Verbindung zu vCenter Server getrennt“, auf Seite 85
- „Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt“, auf Seite 86
- „Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host“, auf Seite 88
- „Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt“, auf Seite 88
- „Einem vSphere Distributed Switch mit aktiviertem Network I/O Control kann kein physischer Adapter hinzugefügt werden“, auf Seite 90
- „Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten“, auf Seite 90
- „Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster“, auf Seite 92
- „Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen“, auf Seite 94
- „Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren“, auf Seite 96
- „Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt“, auf Seite 96
- „Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt“, auf Seite 97

## Fehlerbehebung bei der Zuteilung von MAC-Adressen

In vSphere können bestimmte Einschränkungen bezüglich des MAC-Adressbereichs, der virtuellen Maschinen zugewiesen werden kann, dazu führen, dass die Verbindung getrennt wird oder Arbeitslasten nicht eingeschaltet werden können.

### Doppelte MAC-Adressen von virtuellen Maschinen im gleichen Netzwerk

Paket- und Konnektivitätsverluste treten auf, da für virtuelle Maschinen von vCenter Server doppelte MAC-Adressen generiert werden.

#### Problem

Die MAC-Adressen von virtuellen Maschinen in derselben Broadcast-Domäne oder im selben IP-Subnetz verursachen Konflikte, oder aber vCenter Server generiert eine doppelte MAC-Adresse für eine neu erstellte virtuelle Maschine.

Eine virtuelle Maschine wird eingeschaltet und funktioniert ordnungsgemäß, verwendet aber eine MAC-Adresse gemeinsam mit einer anderen virtuellen Maschine. Dadurch können Paketverluste und sonstige Probleme verursacht werden.

#### Ursache

Es gibt mehrere Ursachen für doppelte MAC-Adressen bei virtuellen Maschinen.

- Zwei vCenter Server-Instanzen mit identischen IDs generieren für VM-Netzwerkadapter überlappende MAC-Adressen.

Jede vCenter Server-Instanz weist eine ID zwischen 0 und 63 auf, die bei der Installation nach dem Zufallsprinzip erzeugt wird, aber nach der Installation neu konfiguriert werden kann. vCenter Server verwendet die Instanz-ID zum Generieren von MAC-Adressen für die Netzwerkadapter der Maschine.

- Eine virtuelle Maschine wurde in ausgeschaltetem Zustand von einer vCenter Server-Instanz an eine andere Instanz im selben Netzwerk übertragen, beispielsweise mithilfe von gemeinsam genutzten Speicher, und ein neuer VM-Netzwerkadapter in der ersten vCenter Server-Instanz erhält die freigegebene MAC-Adresse.

#### Lösung

- Ändern Sie die MAC-Adresse eines VM-Netzwerkadapters manuell.

Wenn eine virtuelle Maschine mit einem MAC-Adressenkonflikt vorhanden ist, müssen Sie in den Einstellungen für **Virtuelle Hardware** eine eindeutige MAC-Adresse eingeben.

- Schalten Sie die virtuelle Maschine aus, konfigurieren Sie für den Adapter die Verwendung einer manuellen MAC-Adresse und geben Sie die neue Adresse ein.
- Falls Sie die virtuelle Maschine nicht für die Konfiguration ausschalten können, erstellen Sie mit aktivierter manueller MAC-Adresszuweisung den Netzwerkadapter neu, der den Konflikt verursacht, und geben Sie die neue Adresse ein. Legen Sie im Gastbetriebssystem wie zuvor dieselbe statische IP-Adresse für den neu hinzugefügten Adapter fest.

Weitere Informationen zum Konfigurieren der Netzwerkadapter von virtuellen Maschinen finden Sie in der Dokumentation *vSphere-Netzwerk* und *vSphere-Administratorhandbuch für virtuelle Maschinen*.



- Falls die vCenter Server-Instanz die MAC-Adressen von virtuellen Maschinen gemäß der Standardzuteilung (VMware OUI) generiert, ändern Sie die vCenter Server-Instanz-ID oder verwenden Sie eine andere Zuteilungsmethode zum Beheben von Konflikten.

---

**HINWEIS** Durch die Änderung der vCenter Server-Instanz-ID oder den Wechsel zu einem anderen Zuteilungsschema werden MAC-Adressenkonflikte bei vorhandenen virtuellen Maschinen nicht behoben. Nur nach der Änderung erstellte virtuelle Maschinen oder hinzugefügte Netzwerkadapter erhalten Adressen gemäß dem neuen Schema.

---

Weitere Informationen zu Zuteilungsschemen von MAC-Adressen und zur Konfiguration von MAC-Adressen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Lösung	Beschreibung
<b>Ändern der vCenter Server-ID</b>	<p>Sie können das VMware-OUI-Zuteilungsschema verwenden, wenn Ihre Bereitstellung nur wenige vCenter Server-Instanzen enthält. Gemäß diesem Schema weisen MAC-Adressen das folgende Format auf:</p> <p>00:50:56:XX:YY:ZZ</p> <p>Dabei stellt 00:50:56 den VMware-OUI dar, XX wird als (80 + vCenter Server-ID) berechnet, und YY:ZZ ist eine Zufallszahl.</p> <p>Zum Ändern der vCenter Server-ID konfigurieren Sie die Option <b>Eindeutige vCenter Server-ID</b> im Abschnitt <b>Laufzeiteinstellungen</b> der Einstellungen <b>Allgemein</b> der vCenter Server-Instanz und starten die Instanz neu. Die VMware-OUI-Zuteilung funktioniert mit bis zu 64 vCenter Server-Instanzen und ist für kleine Bereitstellungen geeignet.</p>
<b>Wechseln zur präfixbasierten Zuteilung</b>	<p>Sie können einen benutzerdefinierten OUI verwenden. Beispielsweise haben für den lokal verwalteten Adressbereich 02:12:34 die MAC-Adressen das Format 02:12:34:XX:YY:ZZ. Sie können das vierte Oktett XX zum Aufteilen des OUI-Adressraums auf die vCenter Server-Instanzen verwenden. Diese Struktur ergibt 255 Adresscluster, wobei jeder Cluster von einer vCenter Server-Instanz verwaltet wird, und etwa 65000 MAC-Adressen pro vCenter Server. Beispielsweise 02:12:34:01:YY:ZZ für vCenter Server A, 02:12:34:02:YY:ZZ für vCenter Server B usw.</p> <p>Die präfixbasierte Zuteilung ist für größere Bereitstellungen geeignet. Für global eindeutige MAC-Adressen muss der OUI in IEEE registriert werden.</p>

- Konfigurieren Sie die MAC-Adressenzuteilung.
- Wenden Sie das neue Zuteilungsschema für MAC-Adressen auf eine vorhandene virtuelle Maschine in den Einstellungen für **Virtuelle Hardware** an.
  - Schalten Sie eine virtuelle Maschine aus, konfigurieren Sie für den Adapter die Verwendung einer manuellen MAC-Adresse, setzen Sie auf die automatische MAC-Adressenzuteilung zurück und schalten Sie die virtuelle Maschine ein.
  - Angenommen, die virtuelle Maschine wird gerade verwendet und kann deshalb nicht für die Konfiguration ausgeschaltet werden. Nachdem Sie die vCenter Server-ID oder das Zuteilungsschema für MAC-Adressen geändert haben, erstellen Sie mit aktivierter automatischer MAC-Adresszuweisung den Netzwerkadapter neu, der den Konflikt verursacht. Legen Sie im Gastbetriebssystem wie zuvor dieselbe statische IP-Adresse für den neu hinzugefügten Adapter fest.

- Erzwingen Sie die Neugenerierung von MAC-Adressen, wenn Sie eine virtuelle Maschine zwischen vCenter Server-Instanzen übertragen, indem Sie die Dateien der virtuellen Maschine aus einem Datenspeicher verwenden.
  - a Schalten Sie eine virtuelle Maschine aus, entfernen Sie sie aus der Bestandsliste und legen Sie in der Konfigurationsdatei (.vmx) den Parameter ethernetX.addressType auf **generated** fest.  
Das X neben ethernet steht für die fortlaufende Nummer der virtuellen Netzwerkkarte in der virtuellen Maschine.
  - b Importieren Sie die virtuelle Maschine aus einem vCenter Server-System in ein anderes System, indem Sie die virtuelle Maschine aus einem Datenspeicher in der vCenter Server-Zielinstanz registrieren.  
Die Dateien der virtuellen Maschine können sich in einem Datenspeicher befinden, der von den beiden vCenter Server-Instanzen gemeinsam genutzt wird. Sie können aber auch in einen Datenspeicher hochgeladen werden, auf den nur vom vCenter Server-Zielsystem aus zugegriffen werden kann.  
Weitere Informationen zum Registrieren einer virtuellen Maschine über einen Datenspeicher finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.
  - c Schalten Sie die virtuellen Maschinen zum ersten Mal ein.  
Während die virtuelle Maschine gestartet wird, wird im vSphere Web Client ein Informationssymbol für die virtuelle Maschine angezeigt.
  - d Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Gastbetriebssystem > Frage beantworten** aus.
  - e Wählen Sie die Option **Ich habe sie kopiert** aus.  
Das vCenter Server-Zielsystem erstellt die MAC-Adresse der virtuellen Maschine neu. Die neue MAC-Adresse beginnt mit dem VMware-OUI 00:0c:29 und basiert auf der BIOS-UUID der virtuellen Maschine. Die BIOS-UUID der virtuellen Maschine wird anhand der BIOS-UUID des Hosts berechnet.
- Falls vCenter Server und Hosts die Version 6.0 und höher aufweisen und die vCenter Server-Instanzen im erweiterten verknüpften Modus miteinander verbunden sind, migrieren Sie virtuelle Maschinen mithilfe von vMotion zwischen vCenter Server-Systemen.  
Bei der Migration einer virtuellen Maschine zwischen vCenter Server-Systemen fügt die vCenter Server-Quellinstanz die MAC-Adresse der virtuellen Maschine zu einer Blacklist hinzu und weist sie keinen anderen virtuellen Maschinen zu.

## Einschalten einer virtuellen Maschine schlägt aufgrund eines MAC-Adressenkonflikts fehl

Nachdem Sie eine statische MAC-Adresse für einen virtuellen Maschinenadapter festgelegt haben, lässt sich die virtuelle Maschine nicht mehr einschalten.

### Problem

Nachdem Sie einer virtuellen Maschine eine MAC-Adresse im Bereich von 00:50:56:40:YY:ZZ – 00:50:56:7F:YY:ZZ zugewiesen haben, schlägt im vSphere Web Client jeder Einschaltversuch fehl. Eine Statusmeldung weist auf einen Konflikt bei der MAC-Adresse hin.

00:50:56:XX:YY:ZZ ist keine gültige statische Ethernet-Adresse. Es besteht ein Konflikt mit für VMware reservierten MACs zur anderweitigen Nutzung.

### Ursache

Sie versuchen, eine MAC-Adresse zuzuweisen, die mit dem VMware OUI-Präfix 00:50:56 beginnt und sich innerhalb des Adressbereichs für Host-VMkernel-Adapter im vCenter Server-System befindet.

## Lösung

Wenn Sie das VMware OUI-Präfix beibehalten möchten, legen Sie eine statische MAC-Adresse im Bereich zwischen 00:50:56:00:00:00 und 00:50:56:3F:FF:FF fest. Andernfalls bestimmen Sie eine willkürliche MAC-Adresse mit einem anderen Präfix als VMware OUI. Informationen über die verfügbaren Bereiche für statische MAC-Adressen mit dem VMware OUI-Präfix erhalten Sie in der Dokumentation zu *vSphere-Netzwerk*.

## Die Konvertierung zur erweiterten LACP-Unterstützung schlägt fehl

Unter bestimmten Bedingungen schlägt die Konvertierung von einer vorhandenen LACP-Konfiguration zur erweiterten LACP-Unterstützung auf einem vSphere Distributed Switch der Version 5.5 und höher möglicherweise fehl.

### Problem

Nachdem Sie ein Upgrade von vSphere Distributed Switch auf die Version 5.5 und höher durchgeführt haben, schlägt die Konvertierung in einer bestimmten Phase des Prozesses fehl, wenn Sie die Konvertierung zur erweiterten LACP-Unterstützung von einer vorhandenen LACP-Konfiguration starten.

### Ursache

Die Konvertierung von einer vorhandenen LACP-Konfiguration zur erweiterten LACP-Unterstützung schließt mehrere Aufgaben für das Neukonfigurieren des Distributed Switch ein. Die Konvertierung schlägt möglicherweise fehl, weil ein anderer Benutzer den Distributed Switch möglicherweise während der Konvertierung neu konfiguriert hat. Zum Beispiel wurden physische Netzwerkkarten von den Hosts unterschiedlichen Uplinks neu zugewiesen oder die Teaming- und Failover-Konfiguration der verteilten Portgruppen wurde möglicherweise geändert.

Ein anderer Grund für den Fehler ist möglicherweise, dass einige Hosts während der Konvertierung getrennt wurden.

### Lösung

Wenn die Konvertierung zur erweiterten LACP-Unterstützung in einer bestimmten Phase fehlschlägt, wurde der Vorgang nur teilweise abgeschlossen. Sie müssen die Konfiguration des Distributed Switch und die teilnehmenden Hosts überprüfen, um die Objekte mit unvollständiger LACP-Konfiguration zu identifizieren.

Überprüfen Sie die Zielkonfiguration, die durch jede Konvertierungsphase in der Reihenfolge erfolgt, in der sie in der Tabelle aufgelistet wird. Wenn Sie die Phase finden, in der die Konvertierung fehlgeschlagen ist, beenden Sie die Zielkonfiguration manuell und fahren Sie mit den darauf folgenden Phasen fort.

**Tabelle 8-1.** Schritte für das manuelle Abschließen der Konvertierung zum erweiterten LACP

Konvertierungsphase	Zielkonfigurationszustand	Lösung
1. Erstellen Sie eine neue Linkzusammenfassungsgruppe.	Eine neu erstellte Linkzusammenfassungsgruppe muss auf dem Distributed Switch vorhanden sein.	Überprüfen Sie die LACP-Konfiguration des Distributed Switch und erstellen Sie eine neue Linkzusammenfassungsgruppe, wenn keine vorhanden ist.
2. Erstellen Sie auf den verteilten Portgruppen eine zwischengeschaltete Konfiguration von LACP-Teaming und -Failover.	Die neu erstellte Linkzusammenfassungsgruppe muss sich im Standby-Modus befinden, sodass Sie die physischen Netzwerkkarten ohne Verlust der Netzwerkkonnektivität zur Linkzusammenfassungsgruppe migrieren können.	Überprüfen Sie die Teaming- und Failover-Konfiguration der verteilten Portgruppe. Legen Sie die neue Linkzusammenfassungsgruppe als Standby fest, wenn dies nicht der Fall ist. Wenn Sie eine Linkzusammenfassungsgruppe nicht verwenden möchten, um den Datenverkehr für alle verteilten Portgruppen zu regeln, setzen Sie die Teaming- und Failover-Konfiguration auf einen Status zurück, in dem eigenständige Uplinks aktiv sind und die Linkzusammenfassungsgruppe nicht verwendet wird.

**Tabelle 8-1.** Schritte für das manuelle Abschließen der Konvertierung zum erweiterten LACP (Fortsetzung)

Konvertierungsphase	Zielkonfigurationszustand	Lösung
3. Weisen Sie physische Netzwerkkarten von eigenständigen Uplinks zu Ports der Linkzusammenfassungsgruppe neu zu.	Alle physischen Netzwerkkarten aus den Ports der Linkzusammenfassungsgruppe müssen von eigenständigen Uplinks zu Ports der Linkzusammenfassungsgruppe neu zugewiesen werden.	Überprüfen Sie, ob physische Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe zugewiesen wurden. Weisen Sie eine physische Netzwerkkarte zu jedem Port der Linkzusammenfassungsgruppe zu. <b>HINWEIS</b> Die Linkzusammenfassungsgruppe muss in der Teaming- und Failover-Reihenfolge der verteilten Portgruppen im Standby-Modus bleiben, während Sie die physischen Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe neu zuweisen.
4. Erstellen Sie die abschließende Konfiguration von LACP-Teaming und -Failover auf den verteilten Portgruppen.	Die abschließende Konfiguration von LACP-Teaming und -Failover sieht wie folgt aus: <ul style="list-style-type: none"> <li>■ Aktiv: nur die neue Linkzusammenfassungsgruppe</li> <li>■ Standby: Leer</li> <li>■ Nicht verwendet: alle eigenständigen Uplinks</li> </ul>	Überprüfen Sie die Teaming- und Failover-Konfiguration der verteilten Portgruppe. Erstellen Sie eine gültige Konfiguration von LACP-Teaming und -Failover für alle verteilten Portgruppen, für die Sie LACP anwenden möchten.

Angenommen, Sie stellen fest, dass eine neue Linkzusammenfassungsgruppe auf dem Distributed Switch erstellt wurde und dass eine Zwischenkonfiguration für Teaming und Failover für verteilte Portgruppen erstellt wurde. Sie fahren damit fort, zu überprüfen, ob physische Netzwerkkarten den Ports der Linkzusammenfassungsgruppe zugewiesen wurden. Sie stellen fest, dass nicht alle Hosts physische Netzwerkkarten den Ports der Linkzusammenfassungsgruppe zugewiesen haben, und Sie weisen die Netzwerkkarten manuell zu. Sie schließen die Konvertierung ab, indem Sie die abschließende Konfiguration von LACP-Teaming und -Failover für die verteilten Portgruppen erstellen.

## Host kann nicht auf einem vSphere Distributed Switch entfernt werden

Unter bestimmten Bedingungen kann ein Host möglicherweise nicht auf einem vSphere Distributed Switch entfernt werden.

### Problem

- Versuche, einen Host von einem vSphere Distributed Switch zu entfernen, schlagen fehl. Außerdem werden Sie informiert, dass Ressourcen weiterhin verwendet werden. Diese Benachrichtigung kann wie folgt aussehen:

```
Die Ressource '16' ist in Gebrauch. vDS DSwitch-Port 16 ist noch auf dem Host 10.23.112.2 verbunden mit MyVM nic=4000 type=vmVnic
```

- Versuche, einen Host-Proxy-Switch zu entfernen, der noch aus einer vorherigen Netzwerkkonfiguration auf dem Host vorhanden ist, schlagen fehl. Angenommen, Sie haben den Host in ein anderes Datacenter oder vCenter Server-System verschoben, ein Upgrade der ESXi- und vCenter Server-Software durchgeführt und eine neue Netzwerkkonfiguration erstellt. Der Versuch, den Host-Proxy-Switch zu entfernen, schlägt fehl, da Ressourcen auf dem Proxy-Switch weiterhin verwendet werden.

### Ursache

Aus folgenden Gründen ist es nicht möglich, den Host vom Distributed Switch zu entfernen oder den Host-Proxy-Switch zu löschen.

- Auf dem Switch sind VMkernel-Adapter vorhanden, die verwendet werden.
- Netzwerkkadapter der virtuellen Maschine sind mit dem Switch verbunden.

## Lösung

Problem	Lösung
Host kann nicht auf einem Distributed Switch entfernt werden	<ol style="list-style-type: none"> <li>1 Navigieren Sie im vSphere Web Client zum Distributed Switch.</li> <li>2 Wählen Sie auf der Registerkarte <b>Konfigurieren Mehr &gt; Ports</b> aus.</li> <li>3 Suchen Sie alle Ports, die noch verwendet werden, und überprüfen Sie, welche VMkernel- oder VM-Netzwerkadapter auf dem Host noch mit den Ports verbunden sind.</li> <li>4 Migrieren oder löschen Sie die VMkernel- und VM-Netzwerkadapter, die noch mit dem Switch verbunden sind.</li> <li>5 Verwenden Sie den Assistenten Hosts hinzufügen und verwalten im vSphere Web Client, um den Host vom Switch zu entfernen.</li> </ol> <p>Nachdem der Host entfernt wurde, wird der Host-Proxy-Switch automatisch gelöscht.</p>
Host-Proxy-Switch kann nicht entfernt werden	<ol style="list-style-type: none"> <li>1 Navigieren Sie im vSphere Web Client zum Host.</li> <li>2 Löschen oder migrieren Sie VMkernel- oder VM-Netzwerkadapter, die noch mit dem Host-Proxy-Switch verbunden sind.</li> <li>3 Löschen Sie den Host-Proxy-Switch in der Netzwerkansicht auf dem Host.</li> </ol>

## Für Hosts auf einem vSphere Distributed Switch 5.1 (und höher) wird die Verbindung zu vCenter Server getrennt

Hosts auf einem vSphere Distributed Switch 5.1 (und höher) können nach der Konfiguration einer Portgruppe keine Verbindung zu vCenter Server herstellen.

### Problem

Nach der Änderung der Netzwerkkonfiguration einer Portgruppe auf einem vSphere Distributed Switch 5.1 (und höher), der die VMkernel-Adapter für das Verwaltungsnetzwerk enthält, wird für Hosts auf dem Switch die Verbindung zu vCenter Server getrennt. Im vSphere Web Client wird als Status angezeigt, dass die Hosts nicht reagieren.

### Ursache

Auf einem vSphere Distributed Switch 5.1 (und höher) in vCenter Server mit deaktiviertem Netzwerk-Rollback ist die Portgruppe mit den VMkernel-Adaptoren für das Verwaltungsnetzwerk in vCenter Server falsch konfiguriert und die ungültige Konfiguration wird an die Hosts auf dem Switch weitergegeben.

**HINWEIS** Das Netzwerk-Rollback ist in vSphere 5.1 und höher standardmäßig aktiviert. Allerdings können Sie Rollbacks auf vCenter Server-Ebene aktivieren bzw. deaktivieren. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

### Lösung

- 1 Konfigurieren Sie über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) für einen betroffenen Host mithilfe der Option **vDS wiederherstellen** im Menü **Optionen der Netzwerkwiederherstellung** die Uplinks und die ID des VLAN für das Verwaltungsnetzwerk.

Die DCUI erstellt einen lokalen flüchtigen Port und wendet die VLAN und die Uplink-Konfiguration auf den Port an. Die DCUI ändert den VMkernel-Adapter für das Verwaltungsnetzwerk, sodass der neue lokale Host-Port verwendet wird, um die Konnektivität mit vCenter Server wiederherzustellen.

Nachdem der Host erneut eine Verbindung zu vCenter Server hergestellt hat, zeigt der vSphere Web Client eine Warnung an, dass einige Hosts auf dem Switch eine andere als die im vSphere Distributed Switch gespeicherte Netzwerkkonfiguration aufweisen.

- 2 Konfigurieren Sie im vSphere Web Client die verteilte Portgruppe mit den richtigen Einstellungen für das Verwaltungsnetzwerk.

Situation	Lösung
<b>Sie haben die Konfiguration der Portgruppe nur einmal geändert</b>	Für die Konfiguration der Portgruppe können Sie ein Rollback um einen Schritt durchführen. Klicken Sie mit der rechten Maustaste auf die Portgruppe, klicken Sie auf <b>Konfiguration wiederherstellen</b> und wählen Sie <b>Auf frühere Konfiguration zurücksetzen</b> aus.
<b>Sie haben eine gültige Konfiguration der Portgruppe gesichert</b>	Mithilfe der Sicherungsdatei können Sie die Konfiguration der Portgruppe wiederherstellen. Klicken Sie mit der rechten Maustaste auf die Portgruppe, klicken Sie auf <b>Konfiguration wiederherstellen</b> und wählen Sie <b>Konfiguration aus einer Datei wiederherstellen</b> aus. Sie können auch die Konfiguration für den gesamten Switch, einschließlich der Portgruppe, mithilfe einer Sicherungsdatei für den Switch wiederherstellen.
<b>Sie haben mehrere Konfigurationsschritte ausgeführt und verfügen nicht über eine Sicherungsdatei</b>	Sie müssen gültige Einstellungen für die Portgruppe manuell eingeben.

Weitere Informationen zum Netzwerk-Rollback und zur Wiederherstellung finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

- 3 Migrieren Sie mit dem Assistenten Hosts hinzufügen und verwalten den VMkernel-Adapter für das Verwaltungsnetzwerk vom lokalen flüchtigen Port des Hosts auf einen verteilten Port des Switches.

Im Gegensatz zu verteilten Ports weist der lokale flüchtige Port des VMkernel eine nicht-numerische ID auf.

Weitere Informationen zum Umgang mit VMkernel-Adaptoren mithilfe des Assistenten Hosts hinzufügen und verwalten finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

- 4 Wenden Sie die Konfiguration der verteilten Portgruppe und den VMkernel-Adapter von vCenter Server auf den Host an.
- Übertragen Sie die richtige Konfiguration der verteilten Portgruppe und den VMkernel-Adapter von vCenter Server an den Host.
    - a Navigieren Sie im vSphere Web Client zum Host.
    - b Klicken Sie auf der Registerkarte **Konfigurieren** auf **Netzwerk**.
    - c Wählen Sie aus der Liste **Virtuelle Switches** den Distributed Switch aus und klicken Sie auf **Zustand des ausgewählten Distributed Switch auf dem Host berichtigen**.
  - Warten Sie, bis vCenter Server die Einstellungen innerhalb der nächsten 24 Stunden anwendet.

## Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt

Hosts auf einem vSphere Distributed Switch 5.0 (und früher) können nach der Konfiguration einer Portgruppe keine Verbindung zu vCenter Server herstellen.

### Problem

Nach der Änderung der Netzwerkkonfiguration einer Portgruppe auf einem vSphere Distributed Switch 5.0 (und früher), der die VMkernel-Adapter für das Verwaltungsnetzwerk enthält, wird für Hosts auf dem Switch die Verbindung zu vCenter Server getrennt. Im vSphere Web Client wird als Status angezeigt, dass die Hosts nicht reagieren.

## Ursache

Auf einem vSphere Distributed Switch 5.0 (und früher) in vCenter Server ist die Portgruppe mit den VMkernel-Adaptoren für das Verwaltungsnetzwerk in vCenter Server falsch konfiguriert und die ungültige Konfiguration wird an die Hosts auf dem Switch weitergegeben.

## Lösung

- 1 Stellen Sie über den vSphere Client eine Verbindung zu einem betroffenen Host her.
- 2 Wählen Sie unter **Konfiguration** die Option **Netzwerk** aus.
- 3 Erstellen Sie in der Ansicht „vSphere Standard-Switch“ einen neuen Standard-Switch, falls der Host keinen geeigneten Standard-Switch für das Verwaltungsnetzwerk aufweist.
  - a Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.
  - b Wählen Sie im Assistenten zum Hinzufügen von Netzwerken unter „Verbindungstypen“ die Option **Virtuelle Maschine** aus und klicken Sie auf **Weiter**.
  - c Wählen Sie **vSphere Standard-Switch erstellen**.
  - d Wählen Sie im Abschnitt **vSphere Standard-Switch erstellen** einen oder mehrere freie physische Adapter auf dem Host für die Übertragung des Verwaltungsdatenverkehrs aus und klicken Sie auf **Weiter**.  
  
Falls bereits alle physischen Adapter mit Datenverkehr von anderen Switches belegt sind, erstellen Sie den Switch ohne verbundenen physischen Netzwerkadapter. Später entfernen Sie den physischen Adapter für das Verwaltungsnetzwerk im Proxy-Switch des Distributed Switch und fügen ihn zu diesem Standard-Switch hinzu.
  - e Geben Sie im Abschnitt „Portgruppeneigenschaften“ eine Netzwerkbezeichnung für die zu erstellende Portgruppe und optional eine VLAN-ID ein.
  - f Klicken Sie auf **Beenden**.
- 4 Migrieren Sie in der Ansicht „vSphere Distributed Switch“ den VMkernel-Adapter für das Netzwerk auf einen Standard-Switch.
  - a Wählen Sie die Ansicht „vSphere Distributed Switch“ aus und klicken Sie für den Distributed Switch auf **Virtuelle Adapter verwalten**.
  - b Wählen Sie im Assistenten Virtuelle Adapter verwalten den VMkernel-Adapter aus der Liste aus und klicken Sie auf **Migrieren**.
  - c Wählen Sie den neu erstellten oder einen anderen Standard-Switch aus, auf den der Adapter migriert werden soll, und klicken Sie auf **Weiter**.
  - d Geben Sie eine Netzwerkbezeichnung, die im Bereich des Hosts eindeutig ist, und optional eine VLAN-ID für das Verwaltungsnetzwerk ein und klicken Sie auf **Weiter**.
  - e Überprüfen Sie die Einstellungen im Ziel-Standard-Switch und klicken Sie auf **Beenden**.
- 5 Konfigurieren Sie im vSphere Web Client die verteilte Portgruppe mit den richtigen Einstellungen für das Verwaltungsnetzwerk.
- 6 Migrieren Sie mit dem Assistenten Hosts hinzufügen und verwalten den VMkernel-Adapter für das Verwaltungsnetzwerk vom Standard-Switch auf einen Port des Distributed Switch.  
  
Weitere Informationen zum Assistenten Hosts hinzufügen und verwalten finden Sie in der Dokumentation zu *vSphere-Netzwerk*.
- 7 Falls Sie den physischen Adapter vom Proxy-Switch auf den Standard-Switch verschoben haben, können Sie ihn mit dem Assistenten Hosts hinzufügen und verwalten erneut zum Distributed Switch hinzufügen.

## Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host

Ein Alarm meldet für einen Host den Verlust der Uplink-Redundanz auf einem vSphere Standard-Switch oder einem Distributed Switch.

### Problem

Für einen Host sind keine redundanten physischen Netzwerkkarten mit einem bestimmten Standard-Switch oder Distributed Switch verbunden und der folgende Alarm wird angezeigt:

*Hostname oder IP-Adresse*      Netzwerk-Uplink-Redundanz verloren

### Ursache

Nur eine physische Netzwerkkarte auf dem Host ist mit einem bestimmten Standard-Switch oder Distributed Switch verbunden. Die redundanten physischen Netzwerkkarten sind entweder nicht betriebsbereit oder nicht dem Switch zugewiesen.

Angenommen, ein Host in Ihrer Umgebung weist die physischen Netzwerkkarten *vmnic0* und *vmnic1* auf, die mit *vSwitch0* verbunden sind. Die physische Netzwerkkarte *vmnic1* wird offline geschaltet, sodass nur *vmnic0* mit *vSwitch0* verbunden ist. Die Uplink-Redundanz für *vSwitch0* geht deshalb auf dem Host verloren.

### Lösung

Überprüfen Sie, für welchen Switch die Uplink-Redundanz auf dem Host verloren geht. Verbinden Sie mindestens eine zusätzliche physische Netzwerkkarte auf dem Host mit diesem Switch und setzen Sie den Alarm auf Grün zurück. Sie können dazu den vSphere Web Client oder die ESXi Shell verwenden.

Wenn eine physische Netzwerkkarte nicht betriebsbereit ist, versuchen Sie mithilfe der ESXi Shell auf dem Host deren Betriebsbereitschaft wiederherzustellen.

Weitere Informationen zur Verwendung der Netzwerkbefehle in der ESXi Shell finden Sie unter *Referenz zur vSphere Command-Line Interface*. Weitere Informationen zum Konfigurieren von Netzwerkeinstellungen auf einem Host im vSphere Web Client finden Sie unter *vSphere-Netzwerk*.

## Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt

Durch Änderungen bei der Failover-Reihenfolge für die Netzwerkkarte in einer verteilten Portgruppe werden die virtuellen Maschinen, die der Gruppe zugeordnet sind, vom externen Netzwerk getrennt.

### Problem

Nachdem Sie die Uplinks in den Failover-Gruppen für eine verteilte Portgruppe in vCenter Server, beispielsweise mit dem vSphere Web Client geändert haben, können einige virtuelle Maschinen in der Portgruppe nicht mehr auf das externe Netzwerk zugreifen.

### Ursache

Nach der Änderung der Failover-Reihenfolge gibt es viele Gründe, weshalb die Verbindung von virtuellen Maschinen zum externen Netzwerk getrennt wird.

- Für den Host, auf dem die virtuellen Maschinen ausgeführt werden, sind den Uplinks keine physischen Netzwerkkarten zugeordnet, die auf „Aktiv“ oder „Standby“ festgelegt sind. Alle Uplinks, denen physische Netzwerkkarten vom Host für die Portgruppe zugeordnet sind, werden nach „Nicht verwendet“ verschoben.



- Eine Linkzusammenfassungsgruppe ohne physische Netzwerkkarten vom Host wird gemäß den Anforderungen für die Verwendung von LACP in vSphere als einziger aktiver Uplink festgelegt.
- Falls der Datenverkehr der virtuellen Maschine auf VLANs verteilt ist, sind die physischen Adapter des Hosts für die aktiven Uplinks möglicherweise mit Trunk-Ports auf dem physischen Switch verbunden, die keinen Datenverkehr von diesen VLANs verarbeiten.
- Falls die Portgruppe über eine IP-Hash-Lastausgleichsrichtlinie konfiguriert wurde, wird ein aktiver Uplink-Adapter mit einem physischen Switch-Port verbunden, der sich möglicherweise nicht in einem „EtherChannel“ befindet.

Mit dem zentralen Topologie-Diagramm des Distributed Switch oder mit dem Proxy-Switch-Diagramm für den Host können Sie die Konnektivität der virtuellen Maschinen in der Portgruppe mit zugehörigen Host-Uplinks und Uplink-Adaptoren analysieren.

### Lösung

- Stellen Sie die Failover-Reihenfolge mit dem Uplink, der einer einzelnen physischen Netzwerkkarte auf dem Host zugeordnet ist, wieder als aktiv her.
- Erstellen Sie eine Portgruppe mit identischen Einstellungen, legen Sie die Verwendung der gültigen Uplink-Nummer für den Host fest und migrieren Sie das Netzwerk der virtuellen Maschine zur Portgruppe.
- Verschieben Sie die Netzwerkkarte in einen Uplink, der an der aktiven Failover-Gruppe beteiligt ist.

Mit dem vSphere Web Client können Sie die physische Netzwerkkarte des Hosts in einen anderen Uplink verschieben.

- Verwenden Sie den Assistenten Hosts hinzufügen und verwalten auf dem Distributed Switch.
  - a Navigieren Sie zum Distributed Switch im vSphere Web Client.
  - b Wählen Sie aus dem Menü **Aktionen Hosts hinzufügen und verwalten** aus.
  - c Wählen Sie auf der Seite **Aufgabe auswählen** die Option **Hostnetzwerk verwalten** und anschließend den Host aus.
  - d Um die Netzwerkkarte des Hosts einem aktiven Uplink zuzuweisen, navigieren Sie zur Seite **Physische Netzwerkadapter verwalten** und ordnen Sie die Netzwerkkarte dem Switch-Uplink zu.
- Verschieben Sie die Netzwerkkarte auf der Hostebene.
  - a Navigieren Sie zum Host im vSphere Web Client und erweitern Sie auf der Registerkarte **Konfigurieren** das Menü **Netzwerk**.
  - b Wählen Sie **Virtuelle Switches** und dann den Distributed Switch-Proxy aus.
  - c Klicken Sie auf **Physische Netzwerkadapter, die mit dem ausgewählten Switch verbunden sind, verwalten** und verschieben Sie die Netzwerkkarte zum aktiven Uplink.

## Einem vSphere Distributed Switch mit aktiviertem Network I/O Control kann kein physischer Adapter hinzugefügt werden

Es kann sein, dass Sie einem vSphere Distributed Switch mit konfiguriertem vSphere Network I/O Control Version 3 keinen physischen Adapter mit geringer Geschwindigkeit (z. B. 1 GBit/s) hinzufügen können.

### Problem

Sie versuchen, einem vSphere Distributed Switch, der mit physischen Adaptern mit hoher Geschwindigkeit (z. B. 10 GBit/s) verbunden ist, einen physischen Adapter mit geringer Geschwindigkeit (z. B. 1 GBit/s) hinzuzufügen. Network I/O Control Version 3 ist auf dem Switch aktiviert und es sind Bandbreitenreservierungen für mindestens einen Systemdatenverkehrstyp vorhanden, z. B. für vSphere-Verwaltungsdatenverkehr, vSphere vMotion-Datenverkehr, vSphere-NFS-Datenverkehr usw. Das Hinzufügen des physischen Adapters schlägt fehl und es wird eine Statusmeldung mit dem Hinweis angezeigt, dass ein Parameter falsch ist.

Ein angegebener Parameter war nicht korrekt: `spec.host[].backing.pnicSpec[]`

### Ursache

Network I/O Control richtet die zur Reservierung verfügbare Bandbreite an der 10-GBit/s-Geschwindigkeit der einzelnen physischen Adapter aus, die bereits mit dem Distributed Switch verbunden sind. Nachdem Sie einen Teil dieser Bandbreite reserviert haben, reicht ein Adapter mit weniger als 10 GBit/s für die Anforderungen eines Systemdatenverkehrstyps möglicherweise nicht mehr aus.

Informationen zu Network I/O Control Version 3 finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

### Lösung

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Erweitern Sie auf der Registerkarte **Konfigurieren** die Gruppe der Einstellungen für **System**.
- 3 Wählen Sie **Erweiterte Systemeinstellungen** aus und klicken Sie auf **Bearbeiten**.
- 4 Geben Sie die physischen Adapter, die außerhalb des Bereichs von Network I/O Control eingesetzt werden sollen, als kommagetrennte Liste für den `Net.IOControlPnicOptOut`-Parameter ein.

Beispiel: `vmnic2,vmnic3`

- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
- 6 Fügen Sie in vSphere Web Client den physischen Adapter zum verteilten Switch hinzu.

## Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten

Unter bestimmten Bedingungen können bei virtuellen Maschinen, die mithilfe von SR-IOV Daten an physische Netzwerkadapter senden, Konnektivitäts- oder Einschaltprobleme auftreten.

### Eine virtuelle Maschine, die eine virtuelle SR-IOV-Funktion verwendet, kann nicht eingeschaltet werden, weil der Host den Status „Out of Interrupt Vectors“ aufweist

Auf einem ESXi-Host werden virtuelle Maschinen, die virtuelle SR-IOV-Funktionen (VFs) für Netzwerke verwenden, ausgeschaltet.

### Problem

Auf einem ESXi-Host können virtuelle Maschinen, die virtuelle SR-IOV-Funktionen (VFs) für Netzwerke verwenden, nicht eingeschaltet werden, wenn die Gesamtanzahl der zugewiesenen virtuellen Funktionen sich der im Handbuch *Maximalwerte für die Konfiguration von vSphere* angegebenen, maximal zulässigen Anzahl von VFs nähert.

Die Protokolldatei `vmware.log` der virtuellen Maschine enthält eine Meldung ähnlich der Folgenden über die VF:

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

Die Protokolldatei `vmkernel.log` von VMkernel enthält Meldungen ähnlich der Folgenden über die der virtuellen Maschine zugewiesenen VF:

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

### Ursache

Die Anzahl der zuteilbaren Interrupt-Vektoren steigt mit der Anzahl der physischen CPUs auf einem ESXi-Host. Ein ESXi-Host mit 32 CPUs kann insgesamt 4096 Interrupt-Vektoren bereitstellen. Wird der Host gestartet, verbrauchen Geräte auf dem Host (z. B. Speichercontroller, physische Netzwerkkadaper und USB-Controller) einen Teil der 4096-Vektoren. Wenn diese Geräte mehr als 1024 Vektoren benötigen, wird die maximale Anzahl der potenziell unterstützten VFs reduziert.

Mit dem Einschalten einer virtuellen Maschine und dem Starten des VF-Treibers des Gastbetriebssystems werden Interrupt-Vektoren verbraucht. Wenn die erforderliche Anzahl der Interrupt-Vektoren nicht verfügbar ist, wird das Gastbetriebssystem unerwartet und ohne Fehlermeldung heruntergefahren.

Derzeit ist keine Regel vorhanden, mit der die Anzahl der verbrauchten oder verfügbaren Interrupt-Vektoren auf einem Host ermittelt werden kann. Diese Anzahl hängt von der Hardwarekonfiguration des Hosts ab.

### Lösung

- ◆ Um die virtuellen Maschinen einschalten zu können, verringern Sie die Gesamtanzahl der den virtuellen Maschinen auf dem Host zugewiesenen VFs.
  - Ändern Sie z. B. den SR-IOV-Netzwerkkadaper einer virtuellen Maschine in einen Adapter, der mit einem vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist.

## SR-IOV-fähige Arbeitslast kann nach der Änderung der MAC-Adresse nicht mehr kommunizieren

Nach dem Ändern der MAC-Adresse im Gastbetriebssystem einer SR-IOV-fähigen virtuellen Maschine wird die Verbindung der virtuellen Maschine unterbrochen.

### Problem

Wenn Sie den Netzwerkkadaper einer virtuellen Maschine mit einer virtuellen SR-IOV-Funktion (VF) verbinden, erstellen Sie einen Passthrough-Netzwerkkadaper für die virtuelle Maschine. Nachdem der (VF-) Treiber im Gastbetriebssystem die MAC-Adresse für den Passthrough-Netzwerkkadaper modifiziert hat, zeigt das Gastbetriebssystem an, dass die Änderung erfolgreich war, aber die Verbindung des VM-Netzwerkkadapters geht verloren. Obwohl das Gastbetriebssystem anzeigt, dass die neue MAC-Adresse aktiviert ist, weist eine Protokollnachricht in der Datei `/var/log/vmkernel.log` darauf hin, dass die Operation fehlgeschlagen ist.

Angeforderte Änderung der MAC-Adresse auf *neue MAC-Adresse* auf Port *Portnummer* der VM-Netzwerkkarte wegen vSwitch-Richtlinie unzulässig.

wo

- *neue MAC-Adresse* ist die MAC-Adresse im Gastbetriebssystem.
- *Portnummer der VM-Netzwerkkarte* ist die Portnummer des VM-Netzwerkkadapters im Hexadezimalformat.

**Ursache**

Die Standardsicherheitsrichtlinie auf der Portgruppe, mit der der Passthrough-Netzwerkadapter verbunden ist, erlaubt keine Änderungen der MAC-Adresse im Gastbetriebssystem. Deshalb kann die Netzwerkschnittstelle im Gastbetriebssystem keine IP-Adresse erhalten und ihre Verbindung geht verloren.

**Lösung**

- ◆ Setzen Sie im Gastbetriebssystem die Schnittstelle zurück, damit der Passthrough-Netzwerkadapter wieder seine gültige MAC-Adresse erhält. Wenn die Schnittstelle für die Verwendung von DHCP für die Adressenzuweisung konfiguriert ist, ruft die Schnittstelle automatisch eine IP-Adresse ab.

Beispiel: Führen Sie auf einer virtuellen Linux-Maschine den Konsolenbefehl `ifconfig` aus.

```
ifconfig ethX down
ifconfig ethX up
```

dabei stellt X in `ethX` die Sequenznummer des Netzwerkadapters der virtuellen Maschine im Gastbetriebssystem dar.

## Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster

Eine virtuelle Maschine, die BPDUs (Bridge Protocol Data Unit) sendet (z. B. ein VPN-Client), bewirkt, dass bei virtuellen Maschinen, die mit derselben Portgruppe verbunden sind, die Verbindung getrennt wird. Die Übertragung von BPDUs kann auch die Verbindung des Hosts oder des übergeordneten vSphere HA-Clusters trennen.

**Problem**

Eine virtuelle Maschine, die BPDUs senden soll, bewirkt, dass der Datenverkehr zum externen Netzwerk der virtuellen Maschinen in derselben Portgruppe blockiert wird.

Falls die virtuelle Maschine auf einem Host ausgeführt wird, der Bestandteil eines vSphere HA-Clusters ist, und falls der Host unter bestimmten Bedingungen vom Netzwerk isoliert wird, treten Denial-of-Service-Fehler (DoS) auf den Hosts im Cluster auf.

**Ursache**

Es empfiehlt sich, für einen physischen Switch-Port, der mit einem ESXi-Host verbunden ist, Port-Fast und BPDUGuard zu aktivieren, um die Begrenzung des Spanning-Tree-Protokolls (STP) zu erzwingen. STP wird von einem Standard-Switch oder Distributed Switch nicht unterstützt, und es werden keine BPDUs an den Switch-Port gesendet. Wenn jedoch ein BPDUs-Frame von einer manipulierten virtuellen Maschine an einem physischen Switch-Port eintrifft, der auf einen ESXi-Host verweist, deaktiviert die BPDUGuard-Funktion den Port, um eine Beeinträchtigung der Spanning-Tree-Topologie des Netzwerks durch die Frames zu verhindern.

In bestimmten Fällen soll eine virtuelle Maschine BPDUs senden, beispielsweise beim Bereitstellen eines VPN, das über ein Windows-Bridge-Gerät oder über eine Bridge-Funktion verbunden ist. Wenn für die Kombination aus physischem Switch-Port und physischem Adapter, von der der Datenverkehr dieser virtuellen Maschine verarbeitet wird, BPDUGuard aktiviert ist, ist der Port aufgrund eines Fehlers deaktiviert. Die virtuellen Maschinen und die VMkernel-Adapter, die den physischen Adapter des Hosts verwenden, können nicht mehr mit dem externen Netzwerk kommunizieren.

Falls die Teaming- und Failover-Richtlinie der Portgruppe mehr aktive Uplinks enthält, wird der BPDUs-Datenverkehr auf den Adapter für den nächsten aktiven Uplink verschoben. Der neue physische Switch-Port wird deaktiviert, weshalb für weitere Arbeitslasten keine Pakete mit dem Netzwerk ausgetauscht werden können. Schließlich sind fast alle Entitäten auf dem ESXi-Host nicht mehr erreichbar.

Falls die virtuelle Maschine auf einem Host ausgeführt wird, der Bestandteil eines vSphere HA-Clusters ist, und falls der Host vom Netzwerk isoliert wird, da die meisten verbundenen physischen Switch-Ports deaktiviert sind, verschiebt der aktive Master-Host im Cluster die virtuelle Maschine des BPDU-Absenders auf einen anderen Host. Die virtuelle Maschine beginnt mit dem Deaktivieren der physischen Switch-Ports, die mit dem neuen Host verbunden sind. Die Migration im vSphere HA-Cluster führt letztlich zu einer Häufung von DoS-Fehlern im gesamten Cluster.

### Lösung

- Falls die VPN-Software noch auf der virtuellen Maschine verwendet werden muss, lassen Sie den ausgehenden Datenverkehr für die virtuelle Maschine zu und konfigurieren Sie den physischen Switch-Port so, dass die BPDU-Frames übertragen werden.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	<p>Legen Sie die Sicherheitseigenschaft „Gefälschte Übertragungen“ in der Portgruppe auf <b>Akzeptieren</b> fest, damit BPDU-Frames aus dem Host übertragen werden und den physischen Switch-Port erreichen.</p> <p>Sie können die Einstellungen und den physischen Adapter für den VPN-Datenverkehr isolieren, indem Sie die virtuelle Maschine einer separaten Portgruppe hinzufügen und den physischen Adapter der Gruppe zuweisen.</p> <p><b>VORSICHT</b> Die Festlegung der Sicherheitseigenschaft „Gefälschte Übertragungen“ auf <b>Akzeptieren</b>, damit BPDU-Frames von einem Host gesendet werden können, beinhaltet ein Sicherheitsrisiko, da eine manipulierte virtuelle Maschine Spoofing-Angriffe ausführen kann.</p>
Physischer Switch	<ul style="list-style-type: none"> <li>■ Lassen Sie Port-Fast aktiviert.</li> <li>■ Aktivieren Sie den BPDU-Filter für den betreffenden Port. Wenn ein BPDU-Frame am Port eintrifft, wird er herausgefiltert.</li> </ul> <p><b>HINWEIS</b> Aktivieren Sie den BPDU-Filter nicht global. Wenn der BPDU-Filter global aktiviert wird, wird der Port-Fast-Modus deaktiviert und alle physischen Switch-Ports führen den kompletten STP-Funktionssatz aus.</p>

- Um ein Bridge-Gerät zwischen zwei VM-Netzwerkkarten bereitzustellen, die mit demselben Layer 2-Netzwerk verbunden sind, lassen Sie den ausgehenden BPDU-Datenverkehr für die virtuellen Maschinen zu und deaktivieren Sie Port-Fast und die Verhinderung von BPDU-Schleifen.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	<p>Legen Sie die Eigenschaft „Gefälschte Übertragungen“ der Sicherheitsrichtlinie in den Portgruppen auf <b>Akzeptieren</b> fest, damit BPDU-Frames aus dem Host übertragen werden und den physischen Switch-Port erreichen.</p> <p>Sie können die Einstellungen und einen oder mehrere physische Adapter für den Bridge-Datenverkehr isolieren, indem Sie die virtuelle Maschine einer separaten Portgruppe hinzufügen und die physischen Adapter der Gruppe zuweisen.</p> <p><b>VORSICHT</b> Die Festlegung der Sicherheitseigenschaft „Gefälschte Übertragungen“ auf <b>Akzeptieren</b>, um die Bridge-Bereitstellung zu ermöglichen, beinhaltet ein Sicherheitsrisiko, da eine manipulierte virtuelle Maschine Spoofing-Angriffe ausführen kann.</p>
Physischer Switch	<ul style="list-style-type: none"> <li>■ Deaktivieren Sie Port-Fast auf den Ports zum virtuellen Bridge-Gerät, um STP darauf auszuführen.</li> <li>■ Deaktivieren Sie BPDU-Guard und filtern Sie nach den Ports, die auf das Bridge-Gerät verweisen.</li> </ul>

- Schützen Sie die Umgebung auf jeden Fall vor DoS-Angriffen, indem Sie den BPDU-Filter auf dem ESXi-Host oder dem physischen Switch aktivieren.
  - Aktivieren Sie auf einem Host mit ESXi 4.1 Update 3, ESXi 5.0 Patch 04 und späteren 5.0-Versionen sowie ESXi 5.1 Patch 01 und höher den Gast-BPDU-Filter mithilfe einer der folgenden Methoden und starten Sie den Host neu:
    - Setzen Sie in der Tabelle für erweiterte Systemeinstellungen auf der Registerkarte **Konfigurieren** für den Host im vSphere Web Client die Eigenschaft „Net.BlockGuestBPDU“ auf **1**.

- Geben Sie in einer ESXi Shell für den Host den folgenden vCLI-Befehl ein:
 

```
esxcli system settings advanced set -o /Net/BlockGuestBPDU -i 1
```
- Aktivieren Sie auf einem Host, für den der Gast-BPDU-Filter nicht implementiert ist, den BPDU-Filter auf dem physischen Switch-Port zum virtuellen Bridge-Gerät.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	Setzen Sie die Eigenschaft „Gefälschte Übertragungen“ der Sicherheitsrichtlinie in der Portgruppe auf <b>Ablehnen</b> .
Physischer Switch	<ul style="list-style-type: none"> <li>■ Behalten Sie die Port-Fast-Konfiguration bei.</li> <li>■ Aktivieren Sie den BPDU-Filter für den betreffenden physischen Switch-Port. Wenn ein BPDU-Frame am physischen Port eintrifft, wird er herausgefiltert.</li> </ul> <p><b>HINWEIS</b> Aktivieren Sie den BPDU-Filter nicht global. Wenn der BPDU-Filter global aktiviert wird, wird der Port-Fast-Modus deaktiviert und alle physischen Switch-Ports führen den kompletten STP-Funktionssatz aus.</p>

## Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen

Wenn eine virtuelle Windows-Maschine in vSphere 5.1 und höher große UDP-Pakete überträgt, ist der Durchsatz geringer als erwartet oder schwankt, auch wenn anderer Datenverkehr zu vernachlässigen ist.

### Problem

Wenn eine virtuelle Windows-Maschine UDP-Pakete größer als 1024 Byte überträgt, ist der Durchsatz geringer als erwartet oder schwankt, auch wenn anderer Datenverkehr zu vernachlässigen ist. Im Falle eines Video-Streaming-Servers hält die Video-Wiedergabe an.

### Ursache

Für jedes UDP-Paket größer als 1024 Byte wartet der Windows-Netzwerkstapel auf einen Übertragungsabschluss-Interrupt, bevor das nächste Paket gesendet wird. Im Gegensatz zu früheren Versionen bieten vSphere 5.1 und höhere Versionen keine transparente Umgehung der Situation.

### Lösung

- Erhöhen Sie den Schwellenwert in Byte, bei dem Windows sein Verhalten in Bezug auf UDP-Pakete ändert, indem Sie die Registrierung des Windows-Gastbetriebssystems ändern.
  - a Suchen Sie den Registrierungsschlüssel HKLM\System\CurrentControlSet\Services\Afd\Parameters.
  - b Fügen Sie einen Wert mit dem Namen FastSendDatagramThreshold vom Typ DWORD gleich 1500 hinzu.

Weitere Informationen zum Beheben dieses Problems in der Windows-Registrierung finden Sie auf <http://support.microsoft.com/kb/235257>.

- Ändern Sie die Vereinigungseinstellungen der Netzwerkkarte der virtuellen Maschine.

Wenn die virtuelle Windows-Maschine über einen VMXNET3 vNIC-Adapter verfügt, konfigurieren Sie einen der folgenden Parameter in der .vmx-Datei der virtuellen Maschine. Verwenden Sie den vSphere Web Client oder ändern Sie direkt die .vmx-Datei.

Aktion	Parameter	Wert
Erhöhen Sie die Interrupt-Rate der virtuellen Maschine auf eine höhere Rate als die erwartete Paketrage. Wenn die erwartete Paketrage beispielsweise 15000 Interrupts pro Sekunde entspricht, legen Sie die Interrupt-Rate auf 16000 Interrupts pro Sekunde fest. Setzen Sie den Parameter <code>ethernetX.coalescingScheme</code> auf <b>rbc</b> und den Parameter <code>ethernetX.coalescingParams</code> auf <b>16000</b> . Die Standard-Interrupt-Rate beträgt 4000 Interrupts pro Sekunde.	<code>ethernetX.coalescingScheme</code> <code>ethernetX.coalescingParams</code>	rbc 16000
Deaktivieren Sie die Vereinigung für geringen Durchsatz oder latenzempfindliche Arbeitslasten. Informationen zum Konfigurieren von Arbeitslasten mit niedriger Latenz finden Sie unter <a href="#">Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs</a> .	<code>ethernetX.coalescingScheme</code>	Deaktiviert
Stellen Sie den Vereinigungsalgorithmus früherer ESXi-Versionen wieder her. <b>HINWEIS</b> In höheren vSphere-Versionen kann ein früherer Algorithmus nicht wiederhergestellt werden.	<code>ethernetX.coalescingScheme</code>	kalibrieren

Das X neben ethernet steht für die fortlaufende Nummer der vNIC in der virtuellen Maschine.

Weitere Informationen zum Konfigurieren von Parametern in der `.vmx`-Datei finden Sie in der *vSphere-Administratorhandbuch für virtuelle Maschinen*-Dokumentation.

- Ändern Sie die Vereinigungseinstellungen des ESXi-Hosts.

Dieser Ansatz betrifft alle virtuellen Maschinen und alle Netzwerkkarten virtueller Maschinen auf dem Host.

Sie können die Liste „Erweiterte Systemeinstellungen“ für den Host im vSphere Web Client oder mithilfe eines vCLI-Konsolenbefehls auf dem Host aus der ESXi Shell bearbeiten.

Aktion	Parameter im vSphere Web Client	Parameter für den Befehl <code>esxcli system settings advanced set</code>	Wert
Legen Sie eine Standard-Interrupt-Rate fest, die höher als die erwartete Paketrage ist. Legen Sie beispielsweise die Interrupt-Rate auf 16000 fest, wenn 15.000 Interrupts pro Sekunde erwartet werden.	<code>Net.CoalesceScheme</code> <code>Net.CoalesceParams</code>	<code>/Net/CoalesceScheme</code> <code>/Net/CoalesceParams</code>	rbc 16000
Deaktivieren Sie die Vereinigung für geringen Durchsatz oder latenzempfindliche Arbeitslasten. Informationen zum Konfigurieren von Arbeitslasten mit niedriger Latenz finden Sie unter <a href="#">Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs</a> .	<code>Net.CoalesceDefaultOn</code>	<code>/Net/CoalesceDefaultOn</code>	0
Stellen Sie das Vereinigungsschema früherer ESXi-Versionen wieder her. <b>HINWEIS</b> In höheren vSphere-Versionen kann ein früherer Algorithmus nicht wiederhergestellt werden.	<code>Net.CoalesceScheme</code>	<code>/Net/CoalesceScheme</code>	calibrate

Weitere Informationen zum Konfigurieren eines Hosts aus dem vSphere Web Client finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation. Weitere Informationen zum Festlegen von Hosteigenschaften mithilfe eines vCLI-Befehls finden Sie in der *Referenz zur vSphere Command-Line Interface*-Dokumentation.

## Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren

Unter bestimmten Bedingungen können die virtuellen Maschinen, die sich in derselben verteilten Portgruppe, aber auf unterschiedlichen Hosts befinden, nicht miteinander kommunizieren.

### Problem

Virtuelle Maschinen, die sich auf unterschiedlichen Hosts und in derselben Portgruppe befinden, können nicht miteinander kommunizieren. Die Ausführung von Ping-Befehlen zwischen virtuellen Maschinen zeigt keine Wirkung. Sie können die virtuellen Maschinen nicht mithilfe von vMotion zwischen den Hosts migrieren.

### Ursache

- Auf einigen Hosts sind aktiven oder Standby-Uplinks in der Teaming- und Failover-Reihenfolge der verteilten Portgruppe keine physischen Netzwerkkarten zugewiesen.
- Die physischen Netzwerkkarten auf den Hosts, die den aktiven oder Standby-Uplinks zugewiesen sind, befinden sich in unterschiedlichen VLANs auf dem physischen Switch. Die physischen Netzwerkkarten in unterschiedlichen VLANs erkennen die jeweils anderen Netzwerkkarten nicht und können deshalb nicht miteinander kommunizieren.

### Lösung

- Überprüfen Sie in der Topologie des Distributed Switch, welchem Host keine physischen Netzwerkkarten zu einem aktiven oder Standby-Uplink in der verteilten Portgruppe zugewiesen sind. Weisen Sie mindestens eine physische Netzwerkkarte auf diesem Host einem aktiven Uplink in der Portgruppe zu.
- Überprüfen Sie in der Topologie des Distributed Switch die VLAN-IDs der physischen Netzwerkkarten, die den aktiven Uplinks in der verteilten Portgruppe zugewiesen sind. Weisen Sie auf allen Hosts physische Netzwerkkarten desselben VLAN einem aktiven Uplink in der verteilten Portgruppe zu.
- Um sicherzustellen, dass auf der physischen Ebene kein Problem vorliegt, migrieren Sie die virtuellen Maschinen zum selben Host und überprüfen Sie die Kommunikation zwischen ihnen. Stellen Sie sicher, dass eingehender und ausgehender ICMP-Datenverkehr im Gastbetriebssystem aktiviert sind. Standardmäßig ist ICMP-Datenverkehr in Windows Server 2008 und Windows Server 2012 deaktiviert.

## Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt

Sie können keine vApp oder virtuelle Maschine einschalten, die Sie an ein Datacenter oder ein vCenter Server-System übertragen haben, weil ein Netzwerkprotokollprofil fehlt.

### Problem

Nach der Cold-Migration einer vApp oder einer virtuellen Maschine zu einem anderen Datacenter oder vCenter Server-System schlägt das Einschalten der vApp bzw. der virtuellen Maschine fehl. Eine Fehlermeldung gibt an, dass eine Eigenschaft nicht initialisiert oder zugewiesen werden kann, weil das Netzwerk der vApp oder virtuellen Maschine kein zugewiesenes Netzwerkprotokollprofil besitzt.

Eigenschaft '*property*' kann nicht initialisiert werden. Netzwerk '*port group*' besitzt kein zugewiesenes Netzwerkprotokollprofil.

IP-Adresse für Eigenschaft '*property*' kann nicht zugewiesen werden. Netzwerk '*port group*' besitzt kein zugewiesenes Netzwerkprotokollprofil.



### Ursache

Mithilfe der OVF-Umgebung ruft die vApp oder virtuelle Maschine die Netzwerkeinstellungen von einem Netzwerkprotokollprofil ab, das mit der Portgruppe der vApp oder virtuellen Maschine verknüpft ist.

Der vCenter Server schafft ein solches Netzwerkprotokollprofil für Sie, wenn Sie das OVF einer vApp installieren, und ordnet das Profil mit der Portgruppe zu, die Sie während der Installation angeben.

Die Zuordnung zwischen dem Protokollprofil und der Portgruppe ist nur im Bereich eines Datencenters zulässig. Wenn Sie vApp verschieben, wird das Protokollprofil aus folgenden Gründen nicht an das Zieldatencenter übertragen:

- Die Netzwerkeinstellungen des Protokollprofils sind möglicherweise in der Netzwerkumgebung des Zieldatencenters nicht zulässig.
- Eine Portgruppe, die den gleichen Namen hat und einem anderen Protokollprofil zugeordnet ist, existiert möglicherweise bereits im Zieldatencenter und vApps und virtuelle Maschinen sind möglicherweise mit dieser Gruppe verbunden. Durch das Ersetzen der Protokollprofile für die Portgruppe kann die Konnektivität dieser vApp und virtuellen Maschinen beeinflusst werden.

### Lösung

- Erstellen Sie mit den erforderlichen Netzwerkeinstellungen ein Netzwerkprotokollprofil im Zieldatencenter oder vCenter Server-System und ordnen Sie das Protokollprofil der Portgruppe zu, mit der vApp oder die virtuelle Maschine verbunden ist. Dieser Ansatz ist beispielsweise geeignet, wenn vApp oder die virtuelle Maschine eine vCenter Server-Erweiterung ist, die den vCenter-Erweiterungs-vService nutzt.

Für Informationen zur Bereitstellung von Netzwerkeinstellungen für vApp oder eine virtuelle Maschine durch ein Netzwerkprotokollprofil, siehe *vSphere-Netzwerk* Dokumentation.

- Verwenden Sie den vSphere Web Client, um die OVF-Datei von vApp oder der virtuellen Maschine vom Quelldatencenter oder vCenter Server-System zu exportieren und im Zieldatencenter oder vCenter Server-System bereitzustellen.

Wenn Sie vSphere Web Client verwenden, um die OVF-Datei bereitzustellen, erstellt das vCenter Server-System das Netzwerkprotokollprofil für vApp.

Für Informationen zur Verwaltung von OVF-Dateien im vSphere Web Client, siehe *vSphere-Administratorhandbuch für virtuelle Maschinen* Dokumentation.

## Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt

Wenn Sie versuchen, Netzwerke auf einem vSphere Distributed Switch auf einem Host hinzuzufügen oder zu konfigurieren, wird für den Vorgang ein Rollback durchgeführt und die Verbindung zwischen Host und vCenter Server wird getrennt.

### Problem

In vSphere 5.1 oder höher führt ein Versuch, einen Netzwerkkonfigurationsvorgang auf einem vSphere Distributed Switch auf einem Host durchzuführen, z. B. einen VM-Adapter oder eine Portgruppe zu erstellen, dazu, dass die Verbindung zwischen Host und vCenter Server getrennt und die Fehlermeldung Für die Transaktion wurde auf dem Host ein Rollback durchgeführt angezeigt wird.

### Ursache

Bei hoher Belastung des Hosts, d. h., wenn viele gleichzeitige Netzwerkvorgänge sich begrenzte Ressourcen teilen müssen, überschreitet die Ausführungsdauer einiger der Vorgänge möglicherweise das Standardzeitlimit für das Rollback von Netzwerkkonfigurationsvorgängen auf dem Distributed Switch. Infolgedessen wird für diese Vorgänge ein Rollback durchgeführt.

Solch eine Bedingung kann beispielsweise eintreten, wenn Sie einen VMkernel-Adapter auf einem Host erstellen, der eine große Zahl von Switch-Ports oder virtuellen Adaptern aufweist, die alle Systemressourcen auf dem Host verbrauchen.

Das Standardzeitlimit für das Rollback eines Vorgangs beträgt 30 Sekunden.

### Lösung

- Verwenden Sie den vSphere Web Client, um die Zeitüberschreitung für das Rollback auf dem vCenter Server zu erhöhen.

Falls dasselbe Problem erneut auftritt, erhöhen Sie die Zeitüberschreitung für das Rollback schrittweise um jeweils 60 Sekunden, bis die Zeit ausreicht, um den Vorgang erfolgreich auszuführen.

- a Erweitern Sie auf der Registerkarte **Konfigurieren** einer vCenter Server-Instanz die Option **Einstellungen**.
- b Wählen Sie **Erweiterte Einstellungen** aus und klicken Sie auf **Bearbeiten**.
- c Wenn die Eigenschaft nicht existiert, fügen Sie den Parameter `config.vpxd.network.rollbackTimeout` zu den Einstellungen hinzu.
- d Geben Sie für den Parameter `config.vpxd.network.rollbackTimeout` einen neuen Wert (in Sekunden) ein.
- e Klicken Sie auf **OK**.
- f Starten Sie das vCenter Server-System neu, um die Änderungen anzuwenden.

- Erhöhen Sie die Zeitüberschreitung für das Rollback durch Bearbeiten der `vpxd.cfg`-Konfigurationsdatei.

Falls dasselbe Problem erneut auftritt, erhöhen Sie die Zeitüberschreitung für das Rollback schrittweise um jeweils 60 Sekunden, bis die Zeit ausreicht, um den Vorgang erfolgreich auszuführen.

- a Navigieren Sie auf einer vCenter Server-Instanz in das Verzeichnis, das die `vpxd.cfg`-Konfigurationsdatei enthält.
  - Navigieren Sie in einem Windows Server-Betriebssystem zu `vCenter Server-Stammverzeichnis\Application Data\VMware\VMware VirtualCenter`.
  - Navigieren Sie auf der vCenter Server-Appliance zu `/etc/vmware-vpx`.
- b Öffnen Sie die Datei `vpxd.cfg` zur Bearbeitung.
- c Erhöhen Sie im Abschnitt `<network>` für das Element `<rollbackTimeout>` die Zeitüberschreitung.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

- d Speichern und schließen Sie die Datei.
- e Starten Sie das vCenter Server-System neu, um die Änderungen anzuwenden.

# Fehlerbehebung bei der Lizenzierung

---

Die Themen zur Fehlerbehebung bei der Lizenzierung bieten Lösungen für Probleme, die möglicherweise aus einem falschen und nicht kompatiblen Setup in vSphere resultieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Fehlerbehebung bei der Hostlizenzierung“, auf Seite 99
- „Einschalten einer virtuellen Maschine fehlgeschlagen“, auf Seite 100
- „Eine Funktion kann nicht konfiguriert oder verwendet werden“, auf Seite 101

## Fehlerbehebung bei der Hostlizenzierung

Es treten möglicherweise unterschiedliche Probleme auf, die von einer inkompatiblen oder falschen Lizenzkonfiguration der ESXi-Hosts verursacht werden.

### Zuweisen einer Lizenz zu einem ESXi -Host fehlgeschlagen

Unter bestimmten Bedingungen sind Sie möglicherweise nicht in der Lage, einem ESXi-Host eine Lizenz zuzuweisen.

#### Problem

Sie versuchen, einem ESXi-Host eine Lizenz zuzuweisen, der Vorgang wird jedoch nicht erfolgreich durchgeführt und Sie erhalten eine Fehlermeldung.

#### Ursache

Folgende Gründe können bewirken, dass Sie dem ESXi-Host keine Lizenz zuweisen können:

- Die berechnete Lizenznutzung für den Host überschreitet die Lizenzkapazität. Sie verfügen beispielsweise über einen vSphere-Lizenzschlüssel mit der Kapazität für zwei CPUs. Sie versuchen, den Schlüssel einem Host zuzuweisen, der über vier CPUs verfügt. Sie können die Lizenz nicht zuweisen, da die erforderliche Lizenznutzung für den Host die Lizenzkapazität überschreitet.
- Die Funktionen auf dem Host stimmen nicht mit der Lizenzedition überein. Beispielsweise können Sie im Testmodus Hosts mit vSphere Distributed Switch und vSphere DRS konfigurieren. Sie versuchen zu einem späteren Zeitpunkt, den Hosts vSphere Standard-Lizenzen zuzuweisen. Dieser Vorgang schlägt fehl, da die vSphere Standard Edition weder vSphere Distributed Switch noch vSphere DRS enthält.
- Der Host ist mit einem vCenter Server-System verbunden, dem eine Lizenz zugewiesen ist, die die Lizenzedition, die Sie zuweisen möchten, nicht erlaubt.

#### Lösung

- Weisen Sie eine Lizenz mit einer größeren Kapazität zu.

- Führen Sie ein Upgrade der Lizenzedition durch, um eine Übereinstimmung der Ressourcen und Funktionen auf dem Host zu erzielen, oder deaktivieren Sie die Funktionen, die nicht mit der Lizenzedition übereinstimmen.
- Weisen Sie eine vSphere-Lizenz zu, deren Edition zu der Lizenzedition von vCenter Server kompatibel ist.

## ESXi -Host wird von vCenter Server getrennt

Ein ESXi-Host trennt möglicherweise die Verbindung zu vCenter Server oder alle ESXi-Hosts trennen möglicherweise gleichzeitig die Verbindung zu vCenter Server.

### Problem

Die Verbindung eines ESXi-Hosts von vCenter Server wird getrennt, wenn der Host-Testzeitraum oder die Lizenz abläuft. Die Verbindung aller ESXi-Hosts von vCenter Server wird getrennt, wenn der Testzeitraum oder die Lizenz von vCenter Server abläuft. Sie erhalten eine Fehlermeldung im Zusammenhang mit der Lizenzierung, wenn die Verbindung eines einzelnen Hosts sowie Verbindung aller Hosts getrennt wird. Sie können keine Hosts zur vCenter Server-Bestandsliste hinzufügen. Die Hosts und die virtuellen Maschinen auf den Hosts werden weiterhin ausgeführt.

### Ursache

- Der Testzeitraum von 60 Tagen des Hosts oder die Hostlizenz ist abgelaufen.
- Der Testzeitraum von 60 Tagen von vCenter Server oder die vCenter Server-Lizenz ist abgelaufen.

### Lösung

- Weisen Sie dem ESXi-Host eine vSphere-Lizenz zu und versuchen Sie erneut, eine Verbindung mit vCenter Server herzustellen.
- Weisen Sie dem vCenter Server-System eine vCenter Server-Lizenz zu.

## Einschalten einer virtuellen Maschine fehlgeschlagen

Sie versuchen, eine virtuelle Maschine einzuschalten, der Vorgang kann jedoch nicht erfolgreich durchgeführt werden und Sie erhalten eine Fehlermeldung.

### Problem

Sie können eine virtuelle Maschine auf Ihrem ESXi-Host nicht einschalten.

### Ursache

Das Einschalten einer virtuellen Maschine schlägt möglicherweise aus folgenden Gründen fehl.

- Die 60-tägige Testphase des Hosts ist abgelaufen.
- Die Lizenz für den Host ist abgelaufen.

### Lösung

**Tabelle 9-1.** Einschalten einer virtuellen Maschine

Ursache	Lösung
Der Testzeitraum für den Host ist abgelaufen.	Weisen Sie dem ESXi-Host eine vSphere-Lizenz zu.
Die Lizenz für den Host ist abgelaufen.	Weisen Sie dem ESXi-Host eine vSphere-Lizenz zu.

## Eine Funktion kann nicht konfiguriert oder verwendet werden

Sie können keine Funktion verwenden oder deren Konfiguration ändern.

### **Problem**

Sie können keine Funktion verwenden oder konfigurieren und eine die Lizenz betreffende Fehlermeldung wird angezeigt.

### **Ursache**

Dem ESXi-Host oder dem vCenter Server-System ist eine Lizenz zugewiesen, die die Funktionen, die Sie konfigurieren möchten, nicht unterstützt.

### **Lösung**

Überprüfen Sie die lizenzierten Funktionen auf dem ESXi-Host und auf dem vCenter Server-System. Führen Sie ein Upgrade der Edition der Lizenz durch, die dem Host oder vCenter Server zugewiesen ist, falls die Funktionen nicht enthalten sind, die Sie konfigurieren bzw. verwenden möchten.



# Index

## A

- Active Directory **32**
- Adresse wird bereits verwendet, Jetty-Server **37**
- Aktivieren von Storage I/O Control nicht möglich **58**
- Anzeige Probleme **60, 61**
- Ausstehende Festplattenanforderungen **66**
- Authentifizierung **61**
- Automatisches Partitionieren, Formatierung von Flash-Festplatten verhindern **72**

## B

- Beheben von Problemen bei Fault Tolerance **11**
- benutzerdefinierter Reverse-Proxy **33**

## C

- CHAP-Authentifizierung **61**
- config.vpxd.das.electionWaitTimeSec **25**

## D

- Datenbankbeschädigung, vSphere Auto Deploy **31**
- Datenspeicher
  - Leistungsdiagramme, Fehlerbehebung **57**
  - Wartungsmodus **52**
- Datenspeicher entfernen **45**
- Datenspeicher unmounten **45**
- Datenspeicher-Cluster, Wartungsmodus **52**
- Datenspeicher-Taktsignale **43, 44**
- Denial-of-Service
  - Virtuelle Maschine, VPN **92**
  - Siehe auch* DoS
- Die Konsole für eine virtuelle Maschine startet nicht, vSphere Web Client **37**
- disable\_action\_OnRetryErrors parameter **70**
- Disk.SchedNumReqOutstanding **66**
- Distributed Switch
  - Host kann nicht entfernt werden **84**
  - Physischer Netzwerkkarte **90**
- DRS platziert keine fehlertolerante VM **15**

## E

- E/A-Filter
  - Fehlerbehebung **77**

Installationsfehler **77**

Installieren **78**

Empfehlungen für Speicher-DRS, Fehlerbehebung **56**

enable\_action\_OnRetryErrors parameter **70**

Enhanced vMotion Compatibility **15**

erweiterte Einstellungen, Disk.SchedNumReqOutstanding **66**

Erweiterte Laufzeitinformationen **43**

ESXi-Protokolle **9**

EVC **15**

## F

- Failover, Verbindung zur virtuellen Maschine wird getrennt **88**
- Fault Tolerance
  - Fehlerbehebung **11, 12**
  - Protokollierung **15**
- Fehler beim VIB-Download **33**
- Fehler von vSphere Fault Tolerance für eingeschaltete VM **14**
- Fehlerbehebung
  - USB-Geräte **17**
  - vCenter Server **35**
  - vSphere Web Client **35, 36**
  - VVols-Datenspeicher **75**
- Fehlerbehebung (Überblick) **7**
- Fehlerbehebung bei der Hostlizenzierung **99**
- Fehlerbehebung bei der Lizenzierung **99**
- Fehlerbehebung bei Hosts **21**
- Fehlerbehebung bei virtuellen Maschinen **11**
- Fehlerbehebung bei virtuellen Volumes
  - OVF-Bereitstellungsfehler **75**
  - VM-Migrationsfehler **75**
- Fehlerbehebung beim Problembereich **8**
- Fehlerbehebung beim Speicher **59**
- Fehlgeschlagene Konvertierung zum erweiterten LACP **83**
- Flash-Geräte, Markieren **73**
- Flash-Laufwerke **71**
- Formatierung von Flash-Festplatten, während der automatischen Partitionierung verhindern **72**
- Formatierung von Flash-Festplatten während der automatischen Partitionierung verhindern **72**

Funktion **101**

## G

Gemeinsame Protokolle **9**  
geringer Durchsatz, virtuelle Windows-Maschine **94**

## H

Hardwarevirtualisierung (HV) **11, 12**  
HBAs, Warteschlangentiefe **64**  
Herunterladen von VIBs, Verwenden eines benutzerdefinierten vCenter Server-Reverse-Proxys **33**  
Hostisolierungsreaktion **25**  
Hostprofile, Übereinstimmungsfehler **32**  
Hosts, keine Verbindung mit vCenter Server **85, 86**  
Hostzertifikate **38**

## I

iBFT **67**  
Identifizieren der Symptome, Fehlerbehebung **7**  
IPv4 **24**  
IPv6 **24**

## J

Jetty-Server, Adresse wird bereits verwendet **37**

## K

Keine Pfade verfügbar (All Paths Down, APD) **49**  
keine Uplink-Redundanz **88**  
Kennwortanforderungen **32**  
Konvertieren zum erweiterten LACP schlägt fehl **83**

## L

Leistung, Probleme **62**  
Leistungsdiagramme für Datenspeicher, Fehlerbehebung für das Anzeigen von Leistungsdiagrammen **57**  
Lizenzedition **99, 101**  
Lizenzkapazität **99, 100**  
Lizenzschlüssel **100**  
Lokale Flash-Festplatten, nicht auffindbar **73**  
Lokale Flash-Festplatten nicht verfügbar **71**  
LUN-Thrashing **63**  
LUNs, die nicht angezeigt werden, Speicherprozessoranzeige **60, 61**

## M

Markieren, Flash-Geräte **73**  
Maximale HBA-Warteschlangentiefe **64**  
Metadatenkonsistenz, Überprüfen mit VOMA **68**

Mit FT-VMs überlastete Hosts **13**

## N

Network I/O Control, Physischer Netzwerkadapter kann nicht hinzugefügt werden **90**  
Netzwerk  
Rollback der Transaktion **97**  
Verbindung zum Host getrennt **97**  
Netzwerklatenz bei FT-VMs **13**  
Netzwerkpartition **43, 45, 47**  
Netzwerkprotokollprofile, Einschalten einer vApp oder einer virtuellen Maschine schlägt fehl **96**  
NFS-Datenspeicher **67**  
Nicht-ASCII-Zeichen **67**

## P

Permanenter Geräteverlust (Permanent Device Loss, PDL) **49**  
Pfad-Thrashing **63**  
Primäre virtuelle Maschine **47, 48**  
Problembereich, Fehlerbehebung **8**  
Probleme  
Anzeige **60, 61**  
Leistung **62**  
Protokolle des Platform Services Controller **9**  
Protokolle des Verwaltungsknotens **9**  
Protokollierung **9**

## R

Reverse-Proxy, benutzerdefiniert **33**  
Richtlinien für die Fehlerbehebung **7**  
Roter Cluster **41**

## S

Schutzstatus der virtuellen Maschine **45**  
SCSI INQUIRY **66**  
SCSI-Reservierungen reduzieren **62**  
Sekundäre virtuelle Maschine **47, 48**  
Single Root I/O Virtualization (SR-IOV), , *siehe* SR-IOV  
Software-iSCSI-Adapter, Warteschlangentiefe **65**  
Speicher-DRS  
Affinitätsregeln **55**  
deaktivieren **54**  
Deaktiviert **51**  
Empfehlungen **56**  
Empfehlungen können nicht übernommen werden **56**  
Fehler **55**  
Fehlerbehebung **51**  
Löschen von Affinitätsregeln **55**  
OVF-Vorlagen **54**



- Platzierung **56**
- Regelverletzung **55**
- Speicher-DRS-Empfehlungen können nicht übernommen werden, Fehlerbehebung **56**
- Speicheradapter, Fehlerbehebung **67**
- Speichergeräte, Anzeige Probleme **60**
- Speichergeräte, als lokal markieren **74**
- Speicherprozessoranzeige, LUN wird nicht angezeigt **60, 61**
- SQL-Kompatibilitätsmodus **36**
- SR-IOV
  - MAC-Adresse, Konnektivität verloren gegangen **91**
  - out of interrupt vectors **90**
  - virtuelle Maschine, Konnektivität verloren gegangen **91**
  - virtuelle Maschinen, Fehlerbehebung **90**
- SR-IOV, virtuelle Maschine ist ausgeschaltet **90**
- SSDs **71**
- SSL-Zertifikate, Fehlerbehebung in vSphere HA **38**
- Steckplatzgröße **41–43**
- Storage I/O Control
  - Fehlerbehebung **57, 58**
  - überwachen **57**

## T

- Testen der Lösungen **8**
- TFTP-Server, vSphere Auto Deploy **28**
- Tomcat-Dienst, vCenter Server-Upgrade-Fehler **35**

## U

- Übereinstimmungsfehler, Hostprofile **32**
- Überlasteter Host **12**
- überwachen, Storage I/O Control **57**
- Ungleichmäßige Verteilung von FT-VMs **13**
- Uplink-Redundanz verloren **88**
- USB-Geräte, Fehlermeldungen **17**
- USB-Passthrough
  - Fehlerbehebung **17**
  - Fehlerbehebung bei Geräteverbindungen **17**
  - Neustart des USB-Arbitrators **17**

## V

- VAIO-Filter, Fehlerbehebung **77**
- vCenter Server
  - benutzerdefinierter Reverse-Proxy **33**
  - Fehlerbehebung **35**
  - keine Verbindung mit Hosts **85, 86**
- vCenter Server-Lizenz **100**
- vCenter Server-System wird nicht angezeigt **36**
- vCenter Server-Upgrade schlägt fehl, Tomcat-Dienst **35**

- vCenter Server-Zertifikate **38**
- vDS, Host kann nicht entfernt werden **84**
- Verbindung zur virtuellen Maschine wird getrennt, Failover **88**
- Verlust der Uplink-Redundanz **88**
- Verlust des Zugriffs auf den FT-Metadaten-Datenspeicher **14**
- Verteilte Portgruppe, virtuelle Maschinen können nicht miteinander kommunizieren **96**
- Verwaiste virtuelle Maschinen, Wiederherstellen **18**
- Virtuelle Datenspeicher
  - OVF-Bereitstellungsfehler **75**
  - VM-Migrationsfehler **75**
- Virtuelle Maschine
  - BPDU **92**
  - Bridge **92**
  - Denial-of-Service **92**
  - doppelte MAC-Adressen **80**
  - geringer Durchsatz **94**
  - MAC-Adresse **80**
  - MAC-Adresse außerhalb des Bereichs **82**
  - MAC-Adressenkonflikt **80**
  - SR-IOV, Konnektivität verloren gegangen **91**
  - UDP **94**
  - VPN **92**
  - Windows **94**
- Virtuelle Maschine ist ausgeschaltet, SR-IOV **90**
- virtuelle Maschinen, SR-IOV, Fehlerbehebung **90**
- Virtuelle Volumes
  - Fehlerbehebung **74**
  - VM-Migrationsfehler **76**
- virtueller Datenspeicher, Fehlerbehebung **75**
- virtueller Flash, lokale Flash-Festplatten nicht verfügbar **71**
- VM Component Protection **48, 49**
- VM-Host-Affinitätsregeln **46**
- VMCP **48**
- VMFS, Überprüfen der Metadatenkonsistenz **68**
- VMware On-disk Metadata Analyzer, , *siehe* VOMA
- VOMA **68**
- vSAN **25, 43, 46**
- vSphere Auto Deploy
  - Coredump **27**
  - DHCP-Adresse **30**
  - Falsches Image **26**
  - Fehlerbehebung **26**
  - Image-Profilwarnung **27**
  - Probleme beim Netzwerkstart **30**
  - Startfehler **29**
  - Startvorgang wird nicht abgeschlossen **28**
  - TFTP-Server **28**

- Umleitungsproblem **26**
- Zeitüberschreitungsfehler **26**
- vSphere Distributed Switch
  - Hosts reagieren nicht **85, 86**
  - Verbindung zur virtuellen Maschine wird getrennt **88**
- vSphere DRS **46**
- vSphere Fault Tolerance **47, 48**
- vSphere HA
  - Denial-of-Service **92**
  - Fehlerbehebung bei SSL-Zertifikaten **38**
- vSphere HA-Agent **21–25**
- vSphere HA-Cluster **47**
- vSphere HA-Failover **45**
- vSphere HA-Hostzustand
  - Agent nicht erreichbar **21**
  - Agent nicht initialisiert **22**
  - Fehler beim Aufheben der Initialisierung **23**
  - Host ausgefallen **24**
  - Initialisierungsfehler **22**
  - Netzwerkisoliert **25**
  - Netzwerkpartitioniert **24**
- vSphere HA-Zugangssteuerung **41**
- vSphere HA, fehlgeschlagene Neustarts **46**
- vSphere Web Client
  - Die Konsole für eine virtuelle Maschine startet nicht **37**
  - Fehlerbehebung **35, 36**
- vSphere-Lizenz **100**
- VVols **76**
- VVols-Datenspeicher **75**
- VVols-Funktionalität, und esxcli-Befehle **74**

## **W**

- Warteschlangentiefe **64, 65**
- Warteschlangentiefe der LUN **63**
- Wartungsmodus, Datenspeicher **52**
- webclient.properties-Datei **37**

## **Z**

- Zeitüberschreitungsfehler, vSphere Auto Deploy **26**
- Zertifikate
  - Hosts **38**
  - vCenter Server **38**
- Zugangssteuerung mit der Richtlinie „Prozentsatz der reservierten Clusterressourcen“ **42**
- Zugangssteuerung mit der Richtlinie „Vom Cluster tolerierte Hostfehler“ **41–43**
- Zugriff auf den FT-Metadaten-Datenspeicher, Verlust **14**