vSphere-Speicher

Update 3
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

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

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

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

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

Inhalt

Grundlegende Informationen zum vSphere-Speicher

Unter *vSphere-Speicher* werden virtualisierte und softwaredefinierte Speichertechnologien beschrieben, die von VMware ESXi™ und VMware vCenter Server® angeboten werden. Außerdem wird erläutert, wie diese Technologien konfiguriert und verwendet werden können.

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

Zielgruppe

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und der Speichervirtualisierung, den Vorgängen in Datencentern und SAN-Speicherkonzepten vertraut sind.

Aktualisierte Informationen

vSphere-Speicher wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *vSphere-Speicher*.

Revision	Beschreibung
29. NOV. 2022	Einschränkungen für vSAN Stretched Cluster wurden aus Anforderungen für Cloud Native Storage und Erstellen einer Speicherrichtlinie für Kubernetes entfernt.
28. OKT. 2022	■ Grafik in Beispiel einer Netzwerktopologie mit NVMe over TCP wurde aktualisiert. ■ Geringfügige Aktualisierungen für Ändern der Einstellungen für die Speicherplatzrückforderung.
24. August 2022	Nebenversionen.
16. August 2022	Es wurde eine Anforderung zum erneuten Mounten eines Datenspeichers in Ändern der Einstellungen für die Speicherplatzrückforderung hinzugefügt.
29. JUL 2022	In Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten wurde die Anforderung einer Replizierungsgruppe für die Speicherrichtlinie für Virtual Volumes verdeutlicht.
26. JUL 2022	Nebenversionen.
28. APR 2022	Nebenversionen.
14. Dez. 2021	Kleinere Updates.
29. Nov. 2021	Die folgende Anweisung wurde aus VMware High Performance-Plug-In und Pfadauswahlschemas entfernt: „Aktivieren Sie das HPP nicht für HDDs oder langsamere Flash-Geräte. Vom HPP wird nicht erwartet, dass es alle Leistungsvorteile mit Geräten bietet, die nicht mindestens einen IOPS-Durchsatz von 200.000 aufweisen.“
17. Nov. 2021	Kleinere Updates.
29. OKT. 2021	Kleinere Updates.
21. OKT. 2021	Konfigurieren von Netzwerkzugriff auf die vSAN-Dateifreigabe wurde aktualisiert, um darauf hinzuweisen, dass die Verwendung einer dedizierten vNIC für den Dateidatenverkehr nicht obligatorisch ist.
05. OKT. 2021	Erstversion.

Einführung in die Speicherung 1

vSphere unterstützt verschiedene Speicheroptionen und Funktionen in herkömmlichen und softwaredefinierten Speicherumgebungen. Eine allgemeine Übersicht über vSphere-Speicherelemente und -Aspekte unterstützt Sie bei der Planung einer geeigneten Speicherstrategie für Ihr virtuelles Datencenter.

Dieses Kapitel enthält die folgenden Themen:

- Herkömmliche Speichervirtualisierungsmodelle
- Softwaredefinierte Speichermodelle
- vSphere Storage APIs

Herkömmliche Speichervirtualisierungsmodelle

Im Allgemeinen handelt es sich bei der Speichervirtualisierung um eine logische Abstraktion von physischen Speicherressourcen und -kapazitäten aus virtuellen Maschinen und deren Anwendungen. ESXi bietet Speichervirtualisierung auf Hostebene.

In einer vSphere -Umgebung wird ein herkömmliches Modell um die folgenden Speichertechnologien und ESXi und vCenter Server-Virtualisierungsfunktionen ausgebaut.

Lokaler und Netzwerkspeicher

In herkömmlichen Speicherumgebungen beginnt der ESXi-Speichermanagement-Prozess mit dem Speicherplatz, den der Speicheradministrator auf verschiedenen Speichersystemen zuweist. ESXi unterstützt sowohl den lokalen als auch den Netzwerkspeicher.

Weitere Informationen hierzu finden Sie unter Physische Speichertypen.

Storage Area Network (SAN)

Ein SAN (Storage Area Network) ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Computersysteme oder ESXi-Hosts mit Hochleistungsspeichersystemen verbindet. ESXi kann Fibre-Channel- oder iSCSI-Protokolle verwenden, um Verbindungen zu Speichersystemen herzustellen.

Weitere Informationen hierzu finden Sie unter Kapitel 3 Übersicht über die Verwendung von ESXi in einem SAN.

Fibre-Channel

Fibre Channel (FC) Ist ein Speicherprotokoll, das das SAN zum Übertragen von Datenverkehr von ESXi-Hostservern in den gemeinsam genutzten Speicher verwendet. Das Protokoll verpackt SCSI-Befehle in FC-Frames. Für den Anschluss an das FC-SAN verwendet der Host Fibre-Channel-HBAs (Hostbusadapter).

Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwenden von ESXi mit Fibre-Channel-SAN.

Internet-SCSI

Internet-SCSI (iSCSI) ist ein SAN-Transport, der Ethernet-Verbindungen zwischen Computersystemen oder ESXi-Hosts und Hochleistungsspeichersystemen nutzen kann. Zum Herstellen der Verbindung mit den Speichersystemen verwenden die Hosts Hardware-iSCSI-Adapter oder Software-iSCSI-Initiatoren mit Standard-Netzwerkadaptern.

Weitere Informationen hierzu finden Sie unter Kapitel 10 Verwenden von ESXi mit iSCSI-SAN.

Speichergerät oder LUN

Im Kontext von ESXi werden die Begriffe „Gerät“ und „LUN“ synonym verwendet. Allgemein stehen beide Begriffe für ein Speicher-Volume, das dem Host von einem Blockspeichersystem zur Verfügung gestellt wird und formatiert werden kann.

Siehe Ziel- und Gerätedarstellungen und Kapitel 14 Verwalten von Speichergeräten.

Virtuelle Festplatten

Eine virtuelle Maschine auf einem ESXi-Host verwendet eine virtuelle Festplatte, um das Betriebssystem, die Anwendungsdateien und andere Daten für ihren Betrieb zu speichern. Virtuelle Festplatten sind große physische Dateien bzw. Gruppen von Dateien, die wie jede andere Datei kopiert, verschoben, archiviert und gesichert werden können. Sie können virtuelle Maschinen mit mehreren virtuellen Festplatten konfigurieren.

Für den Zugriff auf virtuelle Festplatten verwendet eine virtuelle Maschine virtuelle SCSI-Controller. Zu diesen virtuellen Controllern gehören BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS und VMware Paravirtual. Diese Controller sind die einzigen SCSI-Controllertypen, die eine virtuelle Maschine anzeigen und auf die sie zugreifen kann.

Jede virtuelle Festplatte befindet sich in einem Datenspeicher, der auf physischem Speicher bereitgestellt wird. Jede virtuelle Festplatte wird vom Standpunkt der virtuellen Maschine aus so angezeigt, als wäre ein SCSI-Laufwerk mit einem SCSI-Controller verbunden. Ob auf den physischen Speicher über Speicher- oder Netzwerkadapter auf dem Host zugegriffen wird, ist für das VM-Gastbetriebssystem und die Anwendungen normalerweise transparent.

VMware vSphere® VMFS

Die Datenspeicher, die Sie auf Blockspeichergeräten bereitstellen, verwenden das native VMFS-Format (vSphere Virtual Machine File System). Es handelt sich dabei um ein spezielles Hochleistungs-Dateisystemformat, das für die Speicherung virtueller Maschinen optimiert ist.

Weitere Informationen hierzu finden Sie unter Grundlegende Informationen VMFS-Datenspeicher.

NFS

In ESXi integrierte NFS-Clients verwenden das Network File System-Protokoll (NFS) über TCP/IP, um auf ein NFS-Volume auf einem NAS-Server zuzugreifen. Der ESXi-Host kann das Volume mounten und es als NFS-Datenspeicher verwenden.

Weitere Informationen hierzu finden Sie unter Informationen zu NFS-Datenspeichern.

Raw-Gerätezuordnung

Zusätzlich zu virtuellen Festplatten bietet vSphere einen Mechanismus, der als Raw Device Mapping (RDM) bezeichnet wird. RDM ist nützlich, wenn ein Gastbetriebssystem in einer virtuellen Maschine direkten Zugriff auf ein Speichergerät anfordert. Informationen zu RDMs finden Sie unter Kapitel 19 Raw-Gerätezuordnung.

Softwaredefinierte Speichermodelle

Zusätzlich zu der von traditionellen Speichermodellen durchgeführten Abstrahierung von zugrunde liegenden Speicherkapazitäten von VMs werden Speicherfunktionen durch Software-Defined Storage abstrahiert.

Mit dem softwaredefinierten Speichermodell wird eine virtuelle Maschine zu einer Speicherbereitstellungseinheit und kann über einen flexiblen richtlinienbasierten Mechanismus verwaltet werden. Das Modell umfasst die folgenden vSphere -Technologien.

VMware vSphere® Virtual Volumes™ (vVols)

Mit der Funktionalität für Virtual Volumes wird bei der Speicherverwaltung nicht mehr der Speicherplatz innerhalb von Datenspeichern verwaltet, sondern es werden abstrakte, von Speicher-Arrays gehandhabte Speicherobjekte verwaltet. Mit Virtual Volumes wird eine einzelne virtuelle Maschine (nicht der Datenspeicher) ein Teil der Speicherverwaltung. Speicherhardware gewinnt somit die vollständige Kontrolle über den Inhalt der virtuellen Festplatten, das Layout und die Verwaltung.

Weitere Informationen hierzu finden Sie unter Kapitel 22 Arbeiten mit VMware vSphere Virtual Volumes.

VMware vSAN

Bei vSAN handelt es sich um eine Software-Ebene, die im Rahmen des Hypervisors ausgeführt wird. vSAN fasst lokale oder direkt angeschlossene Kapazitätsgeräte eines ESXi-Hostclusters zusammen und erstellt einen einzelnen Speicherpool, der von allen Hosts im vSAN-Cluster verwendet wird.

Weitere Informationen hierzu finden Sie unter *Verwalten von VMware vSAN*.

Speicherrichtlinienbasierte Verwaltung

Die speicherrichtlinienbasierte Verwaltung (SPBM – Storage Policy Based Management) ist ein Framework, das eine einzelne Steuerungskomponente für verschiedene Datendienste und Speicherlösungen bereitstellt, zum Beispiel für vSAN und Virtual Volumes. Bei der

Verwendung von Speicherrichtlinien passt das Framework den Anwendungsbedarf der virtuellen Maschinen an die von den Speicherentitäten bereitgestellten Funktionen an.

Weitere Informationen hierzu finden Sie unter Kapitel 20 Speicherrichtlinienbasierte Verwaltung.

E/A-Filter

E/A-Filter sind Softwarekomponenten, die auf ESXi-Hosts installiert werden und zusätzliche Datendienste für virtuelle Maschinen anbieten können. Je nach Implementierung enthalten die Dienste möglicherweise Replikation, Verschlüsselung, Zwischenspeicherung und usw.

Weitere Informationen hierzu finden Sie unter Kapitel 23 Filtern der E/A einer virtuellen Maschine.

vSphere Storage APIs

Bei den Speicher-APIs (Storage APIs) handelt es sich um eine Reihe von APIs, die von Drittanbieterhardware, -software und Speicheranbietern zur Entwicklung von Komponenten genutzt wird, die zahlreiche vSphere-Funktionen und -Lösungen erweitern.

In dieser Dokumentation zum Speicher werden einige Speicher-APIs beschrieben, die Teil Ihrer Speicherumgebung sind. Informationen zu weiteren APIs dieser Familie, einschließlich „vSphere APIs - Data Protection“, finden Sie auf der VMware-Website.

vSphere APIs for Storage Awareness

Diese auch als VASA bezeichneten APIs, die entweder von externen Anbietern oder von VMware angeboten werden, ermöglichen die Kommunikation zwischen vCenter Server und dem zugrunde liegenden Speicher. Durch VASA können Speicherelemente vCenter Server über ihre Konfiguration, ihre Funktionen sowie den Speicherzustand und Ereignisse informieren. Im Gegenzug kann VASA VM-Speicheranforderungen von vCenter Server an ein Speicherelement übermitteln und sicherstellen, dass die Speicherebene die Anforderungen erfüllt.

VASA wird unverzichtbar, wenn Sie mit Virtual Volumes, vSAN, vSphere APIs für E/A-Filter (VAIO) und VM-Speicherrichtlinien arbeiten. Weitere Informationen hierzu finden Sie unter Kapitel 21 Verwenden von Speicheranbietern.

vSphere APIs for Array Integration

Diese auch als VAAI bezeichneten APIs enthalten die folgenden Komponenten:

- APIs für die Hardwarebeschleunigung. Unterstützende Arrays für die Integration in vSphere, sodass vSphere bestimmte Speichervorgänge auf das Array auslagern kann. Durch diese Vernetzung wird der CPU-Overhead auf dem Host erheblich reduziert. Weitere Informationen hierzu finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.

- Array-Thin Provisioning-APIs. Helfen bei der Überwachung der Speicherplatznutzung auf per Thin Provisioning bereitgestellten Speicher-Arrays, um Situationen zu verhindern, in denen kein Speicherplatz mehr vorhanden ist, und um die Speicherplatzrückforderung durchzuführen. Weitere Informationen hierzu finden Sie unter ESXi und Array-Thin Provisioning.

vSphere APIs für Multipathing

Diese auch als Pluggable Storage Architecture (PSA) bezeichneten APIs ermöglichen Partnern im Speichersektor das Erstellen und Bereitstellen von Plug-Ins zur Unterstützung mehrerer Pfade und des Lastausgleichs, die für jedes Array optimiert sind. Plug-Ins kommunizieren mit Speicher-Arrays und ermitteln die beste Strategie zur Pfadauswahl, um die E/A-Leistung und die Zuverlässigkeit vom ESXi-Host bis zum Speicher-Array zu verbessern. Weitere Informationen finden Sie unter Pluggable Storage Architecture (PSA) und Pfadverwaltung.

Erste Schritte mit einem herkömmlichen Speichermodell

2

Die Einrichtung des ESXi-Speichers in herkömmlichen Umgebungen umfasst die Konfiguration von Speichersystemen und -geräten, die Aktivierung von Speicheradaptern und die Erstellung von Datenspeichern.

Dieses Kapitel enthält die folgenden Themen:

Physische Speichertypen

In herkömmlichen Speicherumgebungen beginnt der ESXi-Speichermanagement-Prozess mit dem Speicherplatz, den der Speicheradministrator auf verschiedenen Speichersystemen zuweist. ESXi unterstützt sowohl den lokalen als auch den Netzwerkspeicher.

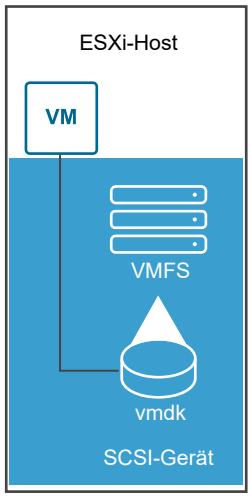
Lokaler Speicher

Bei lokalem Speicher kann es sich um interne Festplatten auf Ihrem ESXi-Host handeln. Sie können auch externe Speichersysteme aufnehmen, die sich außerhalb befinden und über Protokolle wie SAS oder SATA direkt mit dem Host verbunden sind.

Lokale Speichergeräte benötigen kein Speichernetzwerk für die Kommunikation mit Ihrem Host. Sie benötigen ein an die Speichereinheit angeschlossenes Kabel und möglicherweise einen kompatiblen HBA in Ihrem Host.

In der folgenden Abbildung wird eine virtuelle Maschine angezeigt, die lokalen SCSI-Speicher verwendet.

Abbildung 2-1. Lokaler Speicher



Bei diesem Beispiel einer lokalen Speichertopologie verwendet der ESXi-Host eine einzelne Verbindung zu einer Speicherfestplatte. Auf diesem Gerät können Sie einen VMFS-Datenspeicher erstellen, der zur Speicherung der Festplattendateien der virtuellen Maschine verwendet wird.

Obwohl diese Speicherkonfiguration möglich ist, wird sie nicht empfohlen. Die Verwendung einzelner Verbindungen zwischen Speichergeräten und Hosts sorgt für einzelne Ausfallstellen, die Störungen verursachen können, wenn eine Verbindung unzuverlässig wird oder ausfällt. Da die meisten lokalen Speichergeräte jedoch keine Unterstützung für mehrere Verbindungen bieten, können Sie für den Zugriff auf den lokalen Speicher nicht mehrere Pfade verwenden.

ESXi unterstützt verschiedene lokale Speichergeräte einschließlich SCSI-, IDE-, SATA-, USB-, SAS-Flash- und NVMe-Geräten.

Hinweis Virtuelle Maschinen können nicht auf IDE-/ATA- oder USB-Laufwerken gespeichert werden.

Lokaler Speicher unterstützt die gemeinsame Nutzung auf mehreren Hosts nicht. Nur ein Host hat Zugriff auf einen Datenspeicher auf einem lokalen Speichergerät. Infolgedessen können Sie zwar lokalen Speicher verwenden, um VMs zu erstellen, aber keine VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, z. B. HA und vMotion.

Wenn Sie jedoch einen Cluster von Hosts verwenden, die nur über lokale Speichergeräte verfügen, können Sie vSAN implementieren. vSAN wandelt lokale Speicherressourcen in softwaredefinierten freigegebenen Speicher um. Mit vSAN können Sie Funktionen verwenden, die freigegebenen Speicher benötigen. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware vSAN*.

Netzwerkspeicher

Netzwerkspeicher bestehen aus externen Speichersystemen, die Ihr ESXi-Host zur Remotespeicherung von Dateien der virtuellen Maschinen verwendet. In der Regel greift der Host über ein Hochgeschwindigkeitsnetzwerk auf diese Systeme zu.

Netzwerkspeichergeräte werden gemeinsam genutzt. Auf Datenspeicher auf Netzwerkspeichergeräten können mehrere Hosts gleichzeitig zugreifen. ESXi unterstützt mehrere Netzwerkspeichertechnologien.

Zusätzlich zu dem in diesem Thema behandelten traditionellen Netzwerkspeicher unterstützt VMware virtualisierten gemeinsam genutzten Speicher, wie beispielsweise vSAN. vSAN wandelt die internen Speicherressourcen Ihrer ESXi-Hosts in gemeinsam genutzten Speicher um, der Funktionen wie High Availability und vMotion für virtuelle Maschinen bereitstellt. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware vSAN*.

Hinweis Dieselbe LUN kann einem ESXi-Host oder mehreren Hosts nicht von verschiedenen Speicherprotokollen präsentiert werden. Um auf die LUN zuzugreifen, müssen Hosts immer ein einziges Protokoll, z. B. entweder nur Fibre-Channel oder nur iSCSI verwenden.

Fibre-Channel (FC)

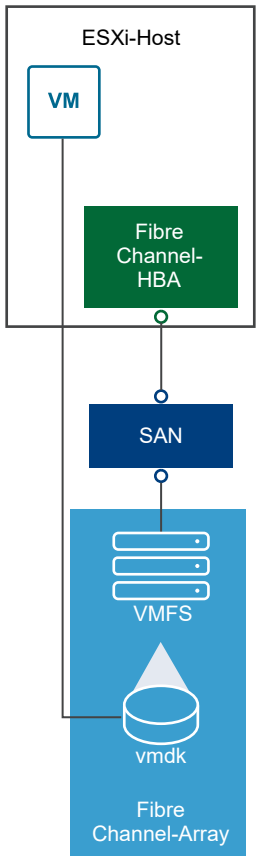
Speichert Dateien virtueller Maschinen extern in einem FC-Speichernetzwerk (Storage Area Network, SAN). Ein FC-SAN ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Ihre Hosts mit Hochleistungsspeichergeräten verbindet. Das Netzwerk nutzt das Fibre-Channel-Protokoll zur Übertragung von SCSI-Datenverkehr virtueller Maschinen an FC-SAN-Geräte.

Für den Anschluss an das FC-SAN muss der Host mit Fibre-Channel-HBAs (Hostbusadaptern) ausgestattet sein. Sofern Sie nicht mit Fibre-Channel-Direktverbindungsspeicher arbeiten, benötigen Sie Fibre-Channel-Switches für die Weiterleitung der zu speichernden Daten. Wenn der Host FCoE-Adapter (Fibre Channel-over-Ethernet-Adapter) enthält, können Sie mithilfe eines Ethernet-Netzwerks eine Verbindung zu Ihren gemeinsam genutzten Fibre-Channel-Geräten herstellen.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Fibre-Channel-Speicher zeigt virtuelle Maschinen, die einen Fibre-Channel-Speicher verwenden.

Abbildung 2-2. Fibre-Channel-Speicher



Bei dieser Konfiguration ist der Host mithilfe eines Fibre-Channel-Adapters mit einem SAN-Fabric verbunden, das aus Fibre-Channel-Switches und Speicher-Arrays besteht. LUNs eines Speicherarrays können vom Host verwendet werden. Sie können auf die LUNs zugreifen und Datenspeicher für Ihre Speicheranforderungen erstellen. Die Datenspeicher verwenden das VMFS-Format.

Weitere Informationen über das Einrichten des Fibre-Channel-SANs finden Sie unter Kapitel 4 Verwenden von ESXi mit Fibre-Channel-SAN.

Internet-SCSI (iSCSI)

Speichert Dateien virtueller Maschinen auf Remote-iSCSI-Speichergeräten. iSCSI packt SCSI-Speicherdatenverkehr in das TCP/IP-Protokoll, sodass dieser über standardmäßige TCP/IP-Netzwerke anstatt über ein spezielles Fibre-Channel-Netzwerk übertragen werden kann. Bei einer iSCSI-Verbindung dient der Host als Initiator, der mit einem Ziel kommuniziert, das sich in externen iSCSI-Speichersystemen befindet.

ESXi unterstützt die folgenden iSCSI-Verbindungstypen:

Hardware-iSCSI

Der Host stellt eine Verbindung mit dem Speicher über einen Drittanbieter-Adapter her, der zur Auslagerung der iSCSI- und Netzwerkverarbeitung geeignet ist. Hardwareadapter können sowohl abhängig als auch unabhängig sein.

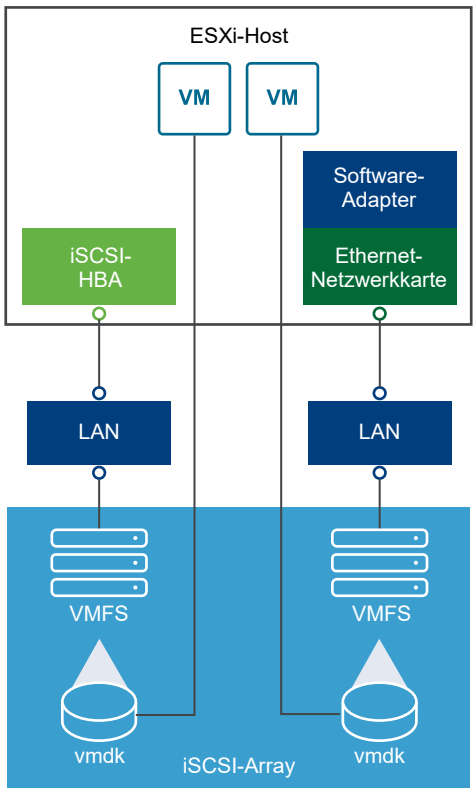
Software-iSCSI

Ihr Host verwendet einen auf Software basierenden iSCSI-Initiator im VMkernel für die Verbindung mit dem Speicher. Bei diesem iSCSI-Verbindungstyp benötigt der Host nur einen Standardnetzwerkadapter zum Herstellen der Netzwerkverbindung.

Sie müssen iSCSI-Initiatoren konfigurieren, damit der Host auf iSCSI-Speichergeräte zugreifen und diese anzeigen kann.

iSCSI-Speicher stellt verschiedene Typen von iSCSI-Initiatoren dar.

Abbildung 2-3. iSCSI-Speicher



Im linken Beispiel verwendet der Host einen Hardware-iSCSI-Adapter für die Verbindung zum iSCSI-Speichersystem.

Im rechten Beispiel verwendet der Host zum Verbinden mit dem iSCSI-Speicher einen Software-iSCSI-Adapter und eine Ethernet-Netzwerkkarte.

Die iSCSI-Speichergeräte des Speichersystems stehen dem Host nun zur Verfügung. Sie können auf die Speichergeräte zugreifen und VMFS-Datenspeicher erstellen, die Sie zur Speicherung benötigen.

Weitere Informationen über das Einrichten des iSCSI-SANs finden Sie unter Kapitel 10 Verwenden von ESXi mit iSCSI-SAN.

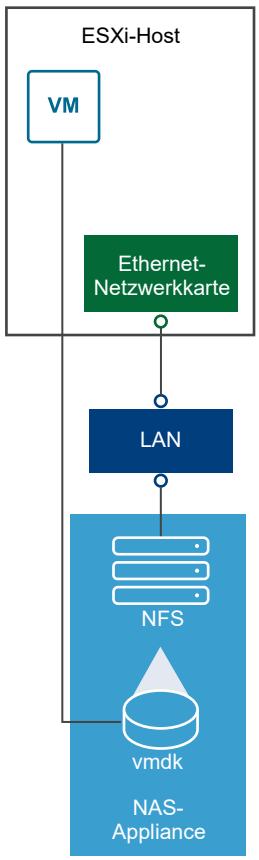
Network-Attached Storage (NAS)

Speichert Dateien von virtuellen Maschinen auf Remotedateiservern, auf die über ein standardmäßiges TCP/IP-Netzwerk zugegriffen wird. Der in ESXi integrierte NFS-Client verwendet das NFS (Network File System)-Protokoll, Version 3 oder 4.1, um mit den NAS-/NFS-Servern zu kommunizieren. Für die Netzwerkverbindung benötigt der Host einen Standardnetzwerkadapter.

Sie können ein NFS-Volume direkt auf dem ESXi-Host mounten. Sie können dann mit dem NFS-Datenspeicher virtuelle Maschinen ebenso wie mithilfe von VMFS-Datenspeichern speichern und verwalten.

NFS-Speicher zeigt eine virtuelle Maschine, die einen NFS-Datenspeicher zur Speicherung ihrer Dateien verwendet. In dieser Konfiguration stellt der Host über einen regulären Netzwerkadapter eine Verbindung zu dem NAS-Server her, auf dem die virtuellen Festplattendateien gespeichert sind.

Abbildung 2-4. NFS-Speicher



Weitere Informationen über das Einrichten eines NFS-Speichers finden Sie unter Informationen zu NFS-Datenspeichern.

Gemeinsam genutztes Serial Attached SCSI (SAS)

Speichert virtuelle Maschinen auf direkt angeschlossenen SAS-Speichersystemen, die gemeinsamen Zugriff auf mehrere Hosts bieten. Diese Art des Zugriffs ermöglicht mehreren Hosts, auf denselben VMFS-Dateispeicher auf eine LUN zuzugreifen.

NVMe over Fabrics-Speicher

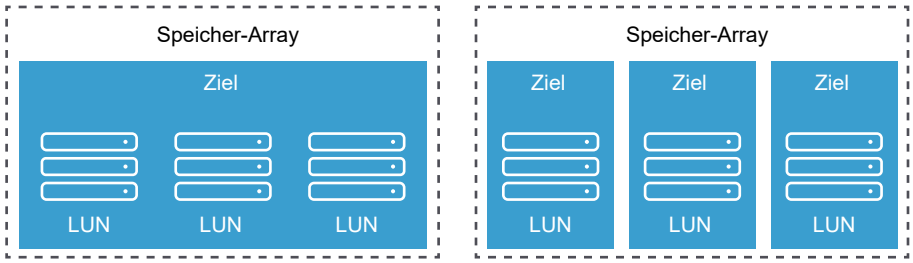
VMware NVMe over Fabrics (NVMe-oF) stellt Konnektivität über Entfernungen zwischen einem Host und einem Zielspeichergerät auf einem freigegebenen Speicher-Array bereit. VMware unterstützt NVMe over RDMA (mit RoCE v2-Technologie), NVMe over Fibre-Channel-Transporte (FC-NVMe) und die NVMe over TCP/IP-Technologie. Weitere Informationen finden Sie unter Kapitel 16 NVMe-Speicher von VMware.

Ziel- und Gerätedarstellungen

Im ESXi-Kontext beschreibt der Begriff „Ziel“ eine einzelne Speichereinheit, auf die der Host zugreifen kann. Die Begriffe „Speichergerät“ und „LUN“ beschreiben ein logisches Volume, das Speicherplatz auf einem Ziel darstellt. Im ESXi-Kontext bedeuten beide Begriffe auch ein Speichervolume, das mit dem Host von einem Speicherziel bereitgestellt wird und zur Formatierung zur Verfügung steht. Speichergerät und LUN sind häufig austauschbar.

Verschiedene Speicheranbieter bieten ESXi-Hosts die Speichersysteme unterschiedlich an. Einige Anbieter bieten mehrere Speichergeräte bzw. LUNs auf einem einzigen Ziel, während andere Anbieter mehrere Ziele mit je einer LUN verknüpfen.

Abbildung 2-5. Ziel- und LUN-Darstellungen



In der vorliegenden Abbildung sind in jeder dieser Konfigurationen drei LUNs verfügbar. Im ersten Fall stellt der Host eine Verbindung zum Ziel her, obwohl in diesem Ziel drei LUNs vorhanden sind, die verwendet werden können. Jede LUN steht für ein einzelnes Speicher-Volume. Im zweiten Fall erkennt der Host drei unterschiedliche Ziele mit je einer LUN.

Ziele, auf die über das Netzwerk zugegriffen wird, besitzen eindeutige Namen, die von den Speichersystemen angegeben werden. Die iSCSI-Ziele verwenden die iSCSI-Namen, während Fibre-Channel-Ziele World Wide Names (WWNs) verwenden.

Hinweis ESXi unterstützt keinen Zugriff auf dieselbe LUN über unterschiedliche Übertragungsprotokolle wie iSCSI und Fibre-Channel.

Ein Gerät oder eine LUN wird durch den UUID-Namen identifiziert. Wenn eine LUN von mehreren Hosts gemeinsam verwendet wird, muss sie für alle Hosts mit der gleichen UUID bereitgestellt werden.

Speicherzugriff durch virtuelle Maschinen

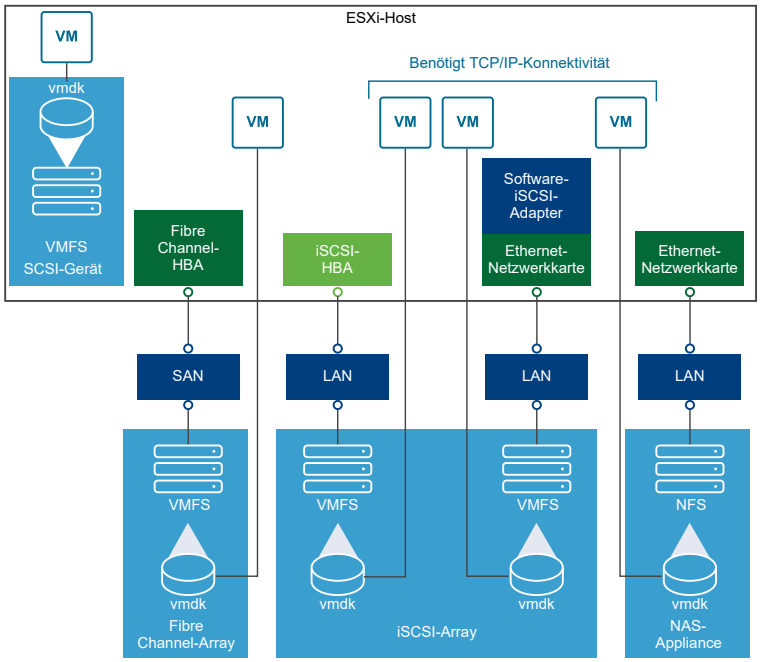
Wenn eine virtuelle Maschine mit ihrer virtuellen Festplatte kommuniziert, die in einem Datenspeicher gespeichert ist, ruft sie SCSI-Befehle auf. Da sich die Datenspeicher auf verschiedenen Arten physischer Speicher befinden können, werden diese Befehle je nach Protokoll, das der ESXi-Host zur Anbindung an ein Speichergerät verwendet, umgewandelt.

ESXi unterstützt die Protokolle Fibre Channel (FC), Internet SCSI (iSCSI), Fibre Channel over Ethernet (FCoE) und NFS. Die virtuelle Festplatte wird unabhängig vom Typ des Speichergeräts, den Ihr Host verwendet, immer als gemountetes SCSI-Gerät angezeigt. Die virtuelle Festplatte verbirgt die physische Speicherebene vor dem Betriebssystem der virtuellen Maschine. Dadurch können in der virtuellen Maschine Betriebssysteme ausgeführt werden, die nicht für bestimmte Speichersysteme, z. B. SAN, zertifiziert sind.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Die folgende Abbildung zeigt die Unterschiede zwischen den Speichertypen: Fünf virtuelle Maschinen verwenden unterschiedliche Arten von Speichern.

Abbildung 2-6. Virtuelle Maschinen mit Zugriff auf verschiedene Speichertypen



Hinweis Diese Abbildung dient nur zur Veranschaulichung. Es handelt sich nicht um eine empfohlene Konfiguration.

Eigenschaften des Speichergeräts

Wenn der ESXi-Host mit blockbasierten Speichersystemen verbunden wird, verfügt der Host über LUNs oder Speichergeräte, die ESXi unterstützen.

Nachdem die Geräte bei Ihrem Host registriert wurden, können Sie alle verfügbaren lokalen und vernetzten Geräte anzeigen und deren Informationen überprüfen. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

Hinweis Wenn ein Array impliziten Asymmetric Logical Unit Access (ALUA) unterstützt und nur über Standby-Pfade verfügt, schlägt die Registrierung des Geräts fehl. Das Gerät kann beim Host registriert werden, nachdem das Ziel einen Standby-Pfad aktiviert und es vom Host als aktiv erkannt wurde. Der erweiterte `/Disk/FailDiskRegistration`-Systemparameter steuert dieses Verhalten des Hosts.

Sie können für jeden Speicheradapter eine separate Liste von Speichergeräten anzeigen, die für diesen Adapter verfügbar sind.

In der Regel wird Ihnen beim Überprüfen von Speichergeräten Folgendes angezeigt.

Tabelle 2-1. Informationen zum Speichergerät

Informationen zum Speichergerät	Beschreibung
Name	Auch als Anzeigename bezeichnet. Es ist ein Name, den der ESXi-Host dem Gerät anhand des Speichertyps und Herstellers zuweist. Im Allgemeinen können Sie diesen Namen durch einen Namen Ihrer Wahl ersetzen. Weitere Informationen hierzu finden Sie unter Umbenennen von Speichergeräten.
Bezeichner	Eine für ein bestimmtes Gerät spezifische UUID. Weitere Informationen hierzu finden Sie unter Namen und Bezeichner von Speichergeräten.
Betriebszustand	Gibt an, ob das Gerät angeschlossen bzw. nicht angeschlossen ist. Weitere Informationen hierzu finden Sie unter Speichergeräte trennen.
LUN	Logical Unit Number (LUN) innerhalb des SCSI-Ziels. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.
Laufwerkstyp	Gibt an, ob das Gerät ein Flash-Laufwerk oder ein reguläres HDD-Laufwerk ist. Weitere Informationen zu Flash-Laufwerken und NVMe-Geräten finden Sie unter Kapitel 15 Arbeiten mit Flash-Geräten.
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet. Das Protokoll hängt vom Typ des verwendeten Speichers ab. Weitere Informationen hierzu finden Sie unter Physische Speichertypen.
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten der Pfade zum Speichergerät verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In. Weitere Informationen hierzu finden Sie unter Pluggable Storage Architecture (PSA) und Pfadverwaltung.

Tabelle 2-1. Informationen zum Speichergerät (Fortsetzung)

Informationen zum Speichergerät	Beschreibung
Hardwarebeschleunigung	Informationen dazu, ob das Speichergerät den Host bei Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen hierzu finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.
Sektorformat	Gibt an, ob das Gerät ein herkömmliches, 512n- oder erweitertes Sektorformat wie 512e oder 4Kn verwendet. Weitere Informationen hierzu finden Sie unter Gerätesektorformate.
Speicherort	Ein Pfad zum Speichergerät im Verzeichnis `/vmfs/devices/`.
Partitionsformat	Ein Partitionsschema, das vom Speichergerät verwendet wird. Es kann sich hierbei um einen Master Boot Record (MBR) oder eine GUID-Partitionstabelle (GPT) handeln. Die GPT-Geräte unterstützen Datenspeicher größer als 2 TB. Weitere Informationen hierzu finden Sie unter Gerätesektorformate.
Partitionen	Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.
Mehrfachpfad-Richtlinien	Pfadauswahlrichtlinie und Speicher-Array-Typ-Richtlinie, die der Host für die Pfade zum Speicher verwendet. Weitere Informationen hierzu finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.
Pfade	Pfade, die zum Zugriff auf den Speicher verwendet werden, und ihr Status. Weitere Informationen hierzu finden Sie unter Deaktivieren von Speicherpfaden.

Anzeigen von Speichergeräten für einen ESXi-Host

Zeigen Sie alle für einen ESXi-Host verfügbaren Speichergeräte an. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

In der Ansicht „Speichergeräte“ können Sie die Speichergeräte des Hosts anzeigen, ihre Informationen analysieren und ihre Eigenschaften ändern.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speichergeräte**.

   Alle für den Host verfügbaren Speichergeräte werden in der Tabelle „Speichergeräte“ aufgeführt.
4. Wählen Sie ein Gerät in der Liste aus, um Details zu diesem Gerät anzuzeigen.
5. Verwenden Sie die Symbole, um allgemeine Speicherverwaltungsaufgaben durchzuführen.

   Die Verfügbarkeit bestimmter Symbole richtet sich nach dem Gerätetyp und der Konfiguration.

Symbol	Beschreibung
Aktualisieren	Aktualisiert die Informationen zu Speicheradaptern, zur Topologie und zu Dateisystemen.
Trennen	Trennt das ausgewählte Gerät vom Host
Anhängen	Verbindet das ausgewählte Gerät mit dem Host.
Umbenennen	Ändert den Anzeigenamen des ausgewählten Geräts.
LED einschalten	Schaltet die Locator-LED der ausgewählten Geräte ein.
LED ausschalten	Schaltet die Locator-LED der ausgewählten Geräte aus.
Als Flash-Festplatte markieren	Markiert die ausgewählten Geräte als Flash-Festplatten.
Als HDD-Festplatte markieren	Markiert die ausgewählten Geräte als HDD-Festplatten.
Als lokal markieren	Markiert die ausgewählten Geräte als lokale Geräte relativ zum Host.
Als Remote markieren	Markiert die ausgewählten Geräte als Remotegeräte relativ zum Host.
Partitionen löschen	Löscht Partitionen auf den ausgewählten Geräten.
Als dauerhaft reserviert markieren	Markieren Sie das ausgewählte Gerät als dauerhaft reserviert.
Markierung als dauerhaft reserviert aufheben	Dauerhafte Reservierung aus ausgewähltem Gerät löschen.

6 Nutzen Sie die folgenden Registerkarten, um auf zusätzliche Informationen zuzugreifen und Eigenschaften für das ausgewählte Gerät zu ändern.

Registerkarte	Beschreibung
Eigenschaften	Anzeigen von Geräteeigenschaften und -merkmalen. Anzeigen und Ändern von Multipathing-Richtlinien für das Gerät.
Pfade	Anzeigen der für das Gerät verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads.
Partitionsdetails	Zeigt Informationen zu Partitionen und ihren Formaten an.

Anzeigen von Speichergeräten für einen Adapter

Zeigen Sie eine Liste der Speichergeräte an, auf die über einen bestimmten Speicheradapter auf dem ESXi-Host zugegriffen werden kann.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter**.

Alle auf dem Host installierten Speicheradapter werden in der Tabelle „Speicheradapter“ aufgeführt.

4 Wählen Sie den Adapter in der Liste aus und klicken Sie auf die Registerkarte **Geräte**.

Die Speichergeräte, auf die der Host über den Adapter zugreifen kann, werden angezeigt.

5 Verwenden Sie die Symbole, um allgemeine Speicherverwaltungsaufgaben durchzuführen.

Die Verfügbarkeit bestimmter Symbole richtet sich nach dem Gerätetyp und der Konfiguration.

Symbol	Beschreibung
Aktualisieren	Aktualisiert die Informationen zu Speicheradaptern, zur Topologie und zu Dateisystemen.
Trennen	Trennt das ausgewählte Gerät vom Host
Anhängen	Verbindet das ausgewählte Gerät mit dem Host.
Umbenennen	Ändert den Anzeigenamen des ausgewählten Geräts.

Vergleich der Speichertypen

Welche vSphere-Funktionen unterstützt werden ist abhängig von der verwendeten Speichertechnologie.

In der folgenden Tabelle werden die Netzwerkspeichertechnologien verglichen, die ESXi unterstützt.

Tabelle 2-2. Von ESXi unterstützter Netzwerkspeicher

Technologie	Protokolle	Übertragungen	Schnittstelle
Fibre-Channel	FC/SCSI	Blockzugriff für Daten/LUN	FC-HBA
Fibre-Channel über Ethernet	FCoE/SCSI	Blockzugriff für Daten/LUN	■ Converged Network Adapter (Hardware-FCoE) ■ Netzwerkkarte mit FCoE-Unterstützung (Software-FCoE) **Hinweis** Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.
iSCSI	IP/SCSI	Blockzugriff für Daten/LUN	■ iSCSI-HBA oder iSCSI-fähige Netzwerkkarte (Hardware-iSCSI) ■ Netzwerkadapter (Software-iSCSI)
NAS	IP/NFS	Datei (kein direkter LUN-Zugriff)	Netzwerkadapter

In der folgenden Tabelle werden die von verschiedenen Speichertypen unterstützen vSphere-Funktionen verglichen.

Tabelle 2-3. Von Speichertypen unterstützte vSphere-Funktionen

Speichertyp	Starten von VMs	vMotion	Datenspeicher	RDM	VM-Cluster	vSphere HA und DRS	Storage APIs - Data Protection
Lokaler Speicher	Ja	Nein	VMFS	Nein	Ja	Nein	Ja
Fibre-Channel	Ja	Ja	VMFS	Ja	Ja	Ja	Ja
iSCSI	Ja	Ja	VMFS	Ja	Ja	Ja	Ja
NAS über NFS	Ja	Ja	NFS 3 und NFS 4.1	Nein	Nein	Ja	Ja

Hinweis Der lokale Speicher unterstützt einen Cluster von virtuellen Maschinen auf einem einzelnen Host (auch als „systeminterner Cluster“ bekannt). Eine gemeinsam genutzte virtuelle Festplatte ist erforderlich. Weitere Informationen zu dieser Konfiguration finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Unterstützte Speicheradapter

Mithilfe von Speicheradaptern können Sie Ihren ESXi-Host mit einer speziellen Speichereinheit oder einem Netzwerk verbinden.

ESXi unterstützt verschiedene Adapterklassen, wie z. B. SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE) und Ethernet. ESXi greift über die Gerätetreiber im VMkernel direkt auf die Adapter zu.

Je nach verwendetem Speichertyp müssen Sie unter Umständen einen Speicheradapter auf Ihrem Host aktivieren und konfigurieren.

Informationen zum Einrichten von Software-FCoE-Adaptern finden Sie unter Kapitel 6 Konfigurieren von Fibre-Channel über Ethernet.

Weitere Informationen zum Konfigurieren verschiedener iSCSI-Adaptertypen finden Sie unter Kapitel 11 Konfigurieren von iSCSI- und iSER-Adapter und -Speicher.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Anzeigen von Informationen zu Speicheradaptern

Ein ESXi-Host verwendet Speicheradapter zum Zugreifen auf verschiedene Speichergeräte. Sie können Details zu den verfügbaren Speicheradaptern anzeigen und die Informationen überprüfen.

Voraussetzungen

Sie müssen bestimmte Adapter aktiveren, beispielsweise Software-iSCSI oder FCoE, bevor Sie deren Informationen anzeigen können. Weitere Informationen zum Konfigurieren von Adaptern:

- Kapitel 11 Konfigurieren von iSCSI- und iSER-Adapter und -Speicher
- Kapitel 6 Konfigurieren von Fibre-Channel über Ethernet

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter**.
4. Verwenden Sie die Symbole, um Speicheradapteraufgaben durchzuführen.

   Das Vorhandensein bestimmter Symbole hängt von der Speicherkonfiguration ab.

Symbol	Beschreibung
Softwareadapter hinzufügen	Speicheradapter hinzufügen. Ist nur für Software-iSCSI und Software-FCoE anwendbar.
Aktualisieren	Aktualisieren Sie die Informationen zu Speicheradaptern, Topologie und Dateisystemen auf dem Host.
Speicher erneut prüfen	Prüft alle Speicheradapter auf dem Host neu, um neu hinzugefügte Speichergeräte oder VMFS-Volumes zu ermitteln.
Adapter erneut prüfen	Prüfen Sie die ausgewählten Adapter erneut auf neu hinzugefügte Speichergeräte.

5. Wählen Sie einen Adapter in der Liste aus, um Details dazu anzuzeigen.
6. Auf den Registerkarten unter „Adapterdetails“ können Sie auf zusätzliche Informationen zugreifen und Eigenschaften für den ausgewählten Adapter ändern.

Registerkarte	Beschreibung
Eigenschaften	Überprüfen allgemeiner Adaptereigenschaften, die in der Regel den Adapternamen und das -modell enthalten sowie eindeutige Bezeichner gemäß den entsprechenden Speicherstandards. Verwenden Sie bei iSCSI- und FCoE-Adaptern diese Registerkarte zum Konfigurieren allgemeiner Eigenschaften, beispielsweise der Authentifizierung.
Geräte	Anzeigen von Speichergeräten, auf die der Adapter zugreifen kann. Verwenden Sie diese Registerkarte für die Durchführung grundlegender Geräteverwaltungsaufgaben. Weitere Informationen hierzu finden Sie unter Anzeigen von Speichergeräten für einen Adapter.
Pfade	Auflisten und Verwalten aller Pfade, die der Adapter für den Zugriff auf Speichergeräte verwendet.
Ziele (Fibre Channel und iSCSI)	Überprüfen und Verwalten der Ziele, auf die über den Adapter zugegriffen werden.

Registerkarte	Beschreibung
Netzwerk-Port-Bindung (nur iSCSI)	Konfigurieren der Port-Bindung für Software- und abhängige Hardware-iSCSI-Adapter.
Erweiterte Optionen (nur iSCSI)	Konfigurieren erweiterter Parameter für iSCSI.

Merkmale von Datenspeichern

Datenspeicher sind besondere logische Container (analog zu Dateisystemen), bei denen Angaben zu den einzelnen Speichergeräten verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Sie können alle auf den Hosts verfügbaren Datenspeicher anzeigen und deren Eigenschaften analysieren.

Es gibt folgende Möglichkeiten, Datenspeicher zu vCenter Server hinzuzufügen:

- Mit dem Assistenten für neue Datenspeicher können Sie VMFS-, NFS-3-, NFS-4.1- oder Virtual Volumes-Datenspeicher erstellen. Ein vSAN-Datenspeicher wird automatisch erstellt, wenn Sie vSAN aktivieren.
- Wenn Sie einen ESXi-Host zu vCenter Server hinzufügen, werden alle Datenspeicher auf dem Host zu vCenter Server hinzugefügt.

In der folgenden Tabelle werden die Datenspeicherdetails aufgeführt, die Ihnen beim Prüfen von Datenspeichern im vSphere Client angezeigt werden. Bestimmte Eigenschaften sind möglicherweise nicht für alle Typen von Datenspeichern verfügbar oder anwendbar.

Tabelle 2-4. Informationen zu Datenspeichern

Informationen zu Datenspeichern	Anwendbarer Datenspeichertyp	Beschreibung
Name	VMFS NFS vSAN vVol	Bearbeitbarer Name, den Sie einem Datenspeicher zuweisen können. Weitere Informationen zum Umbenennen eines Datenspeichers finden Sie unter Ändern des Datenspeichernamens.
Typ	VMFS NFS vSAN vVol	Das vom Datenspeicher verwendete Dateisystem. Weitere Informationen über VMFS- und NFS-Datenspeicher und deren Verwaltung finden Sie unter Kapitel 17 Arbeiten mit Datenspeichern. Informationen zu Datenspeichern für vSAN finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*. Weitere Informationen zu Virtual Volumes finden Sie unter Kapitel 22 Arbeiten mit VMware vSphere Virtual Volumes.
Geräte-Backing	VMFS NFS vSAN	Weitere Informationen zum zugrunde liegenden Speicher, z. B. einem Speichergerät, auf dem der Datenspeicher bereitgestellt wird (VMFS), Server und Ordner (NFS) oder Festplattengruppen (vSAN).

Tabelle 2-4. Informationen zu Datenspeichern (Fortsetzung)

Informationen zu Datenspeichern	Anwendbarer Datenspeichertyp	Beschreibung
Protokollendpunkte	vVol	Informationen zu den entsprechenden Protokollendpunkten. Weitere Informationen hierzu finden Sie unter Protokollendpunkte.
Erweiterungen	VMFS	Einzelne Erweiterungen, aus denen der Datenspeicher besteht, samt Kapazität.
Laufwerkstyp	VMFS	Typ des zugrunde liegenden Speichergeräts: zum Beispiel Flash-Laufwerk oder herkömmliche HHD-Festplatte. Weitere Informationen finden Sie unter Kapitel 15 Arbeiten mit Flash-Geräten.
Kapazität	VMFS NFS vSAN vVol	Umfasst die Gesamtkapazität, bereitgestellten Speicherplatz und freien Speicherplatz.
Mount-Punkt	VMFS NFS vSAN vVol	Ein Pfad zum Datenspeicher im Verzeichnis `/vmfs/volumes/` des Hosts.
Funktionssätze	VMFS **Hinweis** Ein VMFS-Datenspeicher mit mehreren Erweiterungen übernimmt die Funktionalität von nur einer seiner Erweiterungen. NFS vSAN vVol	Informationen zu den Speicherdatendiensten, die vom zugrunde liegenden Speicherelement zur Verfügung gestellt werden. Sie können sie nicht ändern.
Storage I/O Control	VMFS NFS	Informationen darüber, ob die clusterweite Speicher-E/A-Priorisierung aktiviert ist. Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.
Hardwarebeschleunigung	VMFS NFS vSAN vVol	Informationen darüber, ob das zugrunde liegende Speicherelement die Hardwarebeschleunigung unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung. **Hinweis** NFS 4.1 bietet keine Unterstützung für Hardwarebeschleunigung.
Tags	VMFS NFS vSAN vVol	Datenspeicherfunktionen, die Sie definieren und in Form von Tags Datenspeichern zuordnen. Weitere Informationen hierzu finden Sie unter Zuweisen von Tags zu Datenspeichern.

Tabelle 2-4. Informationen zu Datenspeichern (Fortsetzung)

Informationen zu Datenspeichern	Anwendbarer Datenspeichertyp	Beschreibung
Konnektivität mit Hosts	VMFS NFS vVol	Hosts, auf denen der Datenspeicher gemountet wird.
Multipathing	VMFS vVol	Pfadauswahlrichtlinie, die der Host zum Zugriff auf den Speicher verwendet. Weitere Informationen finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.

Anzeigen von Informationen zu Datenspeichern

Greifen Sie mit dem vSphere Client-Navigator auf die Datenspeicheransicht zu.

In der Datenspeicheransicht können Sie alle Datenspeicher auflisten, die in der vSphere-Infrastruktur verfügbar sind, die Informationen analysieren und die Eigenschaften ändern.

Verfahren

1 Navigieren Sie zu einem beliebigen Bestandslistenobjekt, das ein gültiges übergeordnetes Objekt eines Datenspeichers ist, wie z. B. ein Host, ein Cluster oder ein Datencenter, und klicken Sie auf die Registerkarte **Datenspeicher** .

Datenspeicher, die in der Bestandsliste verfügbar sind, werden im mittleren Bereich angezeigt.

2 Verwenden Sie die Optionen aus dem Kontextmenü eines Datenspeichers, um grundlegende Aufgaben für einen ausgewählten Datenspeicher durchzuführen.

Das Vorhandensein bestimmter Optionen hängt vom Typ des Datenspeichers und dessen Konfiguration ab.

Option	Beschreibung
VM registrieren	Eine vorhandene virtuelle Maschine in der Bestandsliste registrieren. Informationen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.
Datenspeicherkapazität erhöhen	Erhöhen Sie die Kapazität des VMFS-Datenspeichers oder fügen Sie eine Erweiterung hinzu. Weitere Informationen hierzu finden Sie unter Erhöhen der VMFS-Datenspeicherkapazität.
Dateien durchsuchen	Navigieren Sie zum Datei-Browser des Datenspeichers. Weitere Informationen hierzu finden Sie unter Verwenden des Datenspeicherbrowsers.
Umbenennen	Ändern Sie den Namen des Datenspeichers. Weitere Informationen hierzu finden Sie unter Ändern des Datenspeichernamens.
Datenspeicher mounten	Mounten Sie den Datenspeicher auf bestimmte Hosts. Weitere Informationen hierzu finden Sie unter Mounten von Datenspeichern.
Datenspeicher unmounten	Unmounten Sie den Datenspeicher aus bestimmten Hosts. Weitere Informationen hierzu finden Sie unter Unmounten von Datenspeichern.

Option	Beschreibung
Wartungsmodus	Verwenden Sie den Datenspeicher-Wartungsmodus. Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.
Storage I/O Control konfigurieren (VMFS)	Aktivieren Sie Storage I/O Control für den VMFS-Datenspeicher. Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.
Speicherplatzrückforderung bearbeiten (VMFS)	Ändern Sie die Einstellungen für die Speicherplatzrückforderung für den VMFS-Datenspeicher. Weitere Informationen hierzu finden Sie unter Ändern der Einstellungen für die Speicherplatzrückforderung.
Datenspeicher löschen (VMFS)	Entfernen Sie den VMFS-Datenspeicher. Weitere Informationen hierzu finden Sie unter Entfernen von VMFS-Datenspeichern.
Tags und benutzerdefinierte Attribute	Verwenden Sie Tags, um Informationen über den Datenspeicher zu kodieren. Weitere Informationen hierzu finden Sie unter Zuweisen von Tags zu Datenspeichern.

3 Um spezielle Datenspeicherdetails anzuzeigen, klicken Sie auf einen ausgewählten Datenspeicher.

4 Verwenden Sie Registerkarten, um auf zusätzliche Informationen zuzugreifen und Datenspeichereigenschaften zu ändern.

Registerkarte	Beschreibung
Übersicht	Zeigen Sie Statistiken und die Konfiguration für den ausgewählten Datenspeicher an.
Überwachen	Anzeigen von Alarmen, Leistungsdaten, Ressourcenzuteilung, Ereignissen und anderen Statusinformationen für den Datenspeicher.
Konfigurieren	Anzeigen und Ändern von Datenspeichereigenschaften. Die verfügbaren Menüelemente hängen vom Datenspeichertyp ab.
Berechtigungen	Zuweisen oder Ändern von Berechtigungen für den ausgewählten Datenspeicher.
Dateien	Navigieren Sie zum Datei-Browser des Datenspeichers.
Hosts	Anzeigen von Hosts, auf denen der Datenspeicher gemountet wird.
VMs	Anzeigen von virtuellen Maschinen, die sich im Datenspeicher befinden.

Verwenden von Geräten mit dauerhaftem Arbeitsspeicher mit ESXi

ESXi unterstützt die nächste Generation von Geräten mit persistentem Arbeitsspeicher, die auch als Non-Volatile Memory (NVM)-Geräte bezeichnet werden. Diese Geräte kombinieren die Leistung und Geschwindigkeit des Arbeitsspeichers mit der Persistenz des herkömmlichen Speichers. Sie können gespeicherte Daten nach Neustarts oder Stromausfällen beibehalten.

Virtuelle Maschinen, die hohe Bandbreite, geringe Latenz und Persistenz erfordern, können von dieser Technologie profitieren. Beispiele hierfür sind VMs mit Beschleunigungsdatenbanken und Analysearbeitslasten.

Um persistenten Arbeitsspeicher mit Ihrem ESXi-Host zu verwenden, müssen Sie mit den folgenden Konzepten vertraut sein.

PMem-Datenspeicher

Nachdem Sie Ihrem ESXi-Host persistenten Arbeitsspeicher hinzugefügt haben, erkennt der Host die Hardware und formatiert und mountet diese anschließend als lokalen PMem-Datenspeicher. ESXi verwendet VMFS-L als Dateisystemformat. Pro Host wird nur ein lokaler PMem-Datenspeicher unterstützt.

Hinweis Wenn Sie physischen persistenten Speicher verwalten, stellen Sie sicher, dass Sie alle VMs vom Host entfernen und den Host in den Wartungsmodus versetzen.

Um den Verwaltungsaufwand zu reduzieren, bietet der PMem-Datenspeicher ein vereinfachtes Verwaltungsmodell. Herkömmliche Datenspeicheraufgaben gelten in der Regel nicht für den Datenspeicher, da der Host automatisch alle erforderlichen Vorgänge im Hintergrund ausführt. Als Administrator können Sie den Datenspeicher in der Ansicht „Datenspeicher“ des vSphere Client nicht anzeigen bzw. keine anderen regulären Datenspeicheraktionen durchführen. Der einzige für Sie ausführbare Vorgang ist die Überwachung von Statistiken für den PMem-Datenspeicher.

Der PMem-Datenspeicher wird zum Speichern von virtuellen NVDIMM-Geräten und herkömmlichen virtuellen Festplatten einer virtuellen Maschine verwendet. Das Stammverzeichnis der virtuellen Maschine mit den `vmx-` und `vmware.log`-Dateien kann nicht im PMem-Datenspeicher platziert werden.

PMem-Zugriffsmodi

ESXi stellt einer VM den persistenten Arbeitsspeicher in zwei verschiedenen Modi zur Verfügung. PMem-fähige VMs können direkten Zugriff auf den persistenten Arbeitsspeicher haben. Herkömmliche VMs können schnelle virtuelle Festplatten verwenden, die im PMem-Datenspeicher gespeichert sind.

Modus für Direktzugriff

In diesem Modus, der auch als virtueller PMem-Modus (vPMem) bezeichnet wird, kann eine PMem-Region einer VM als ein virtuelles NVDIMM-Modul (Non-Volatile Dual In-Line Memory Module) zur Verfügung gestellt werden. Die VM verwendet das NVDIMM-Modul als einen mit Standard-Byte adressierbaren Arbeitsspeicher, der über Ein- und Ausschaltzyklen hinweg beibehalten wird.

Während der Bereitstellung der VM können Sie ein oder mehrere NVDIMM-Module hinzufügen.

Die VMs müssen über die Hardwareversion ESXi 6.7 oder höher und über ein PMem-fähiges Gastbetriebssystem verfügen. Das NVDIMM-Gerät ist kompatibel mit den neuesten Gastbetriebssystemen, die persistenten Arbeitsspeicher unterstützen, wie zum Beispiel Windows 2016.

Jedes NVDIMM-Gerät wird automatisch im PMem-Datenspeicher gespeichert.

Virtueller Festplattenmodus

Dieser Modus, der auch als virtueller PMem-Festplattenmodus (vPMemDisk) bezeichnet wird, ist für jede herkömmliche VM verfügbar und unterstützt alle Hardwareversionen, einschließlich aller Vorgängerversionen. VMs müssen nicht PMem-fähig sein. Wenn Sie diesen Modus verwenden, erstellen Sie eine reguläre virtuelle SCSI-Festplatte und fügen der Festplatte eine PMem-VM-Speicherrichtlinie an. Die Richtlinie platziert die Festplatte automatisch im PMem-Datenspeicher.

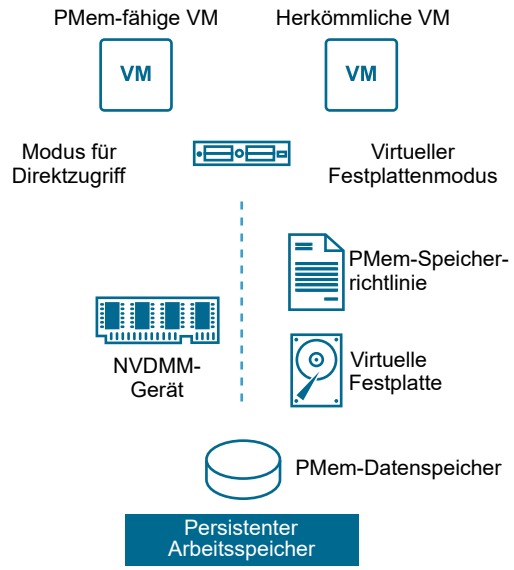
PMem-Speicherrichtlinie

Um die virtuelle Festplatte im PMem-Datenspeicher zu platzieren, müssen Sie die standardmäßige PMem-Speicherrichtlinie für den lokalen Host auf die Festplatte anwenden. Die Richtlinie lässt sich nicht bearbeiten.

Die Richtlinie kann nur auf virtuelle Festplatten angewendet werden. Da sich das VM-Stammverzeichnis nicht im PMem-Datenspeicher befindet, stellen Sie sicher, dass Sie es in einem beliebigen Standarddatenspeicher platzieren.

Nach dem Zuweisen der PMem-Speicherrichtlinie zur virtuellen Festplatte können Sie die Richtlinie nicht mehr im Dialogfeld **VM-Bearbeitungseinstellungen** ändern. Um die Richtlinie zu ändern, müssen Sie die VM migrieren oder klonen.

In der folgenden Abbildung werden die Interaktionen der Komponenten für persistenten Arbeitsspeicher veranschaulicht.



Weitere Informationen zum Konfigurieren und Verwalten von virtuellen Maschinen mit NVDIMMs oder virtuellen Festplatten für persistenten Arbeitsspeicher finden Sie in der Dokumentation zu *Handbuch zur vSphere-Ressourcenverwaltung* und in der *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Überwachen der PMem-Datenspeicher-Statistiken

Sie können vSphere Client und den `esxcli`-Befehl verwenden, um die Kapazität des PMem-Datenspeichers und einige seiner anderen Attribute zu überprüfen.

Allerdings wird im Gegensatz zu regulären Datenspeichern wie VMFS oder vVol der PMem-Datenspeicher nicht in der Ansicht „Datenspeicher“ des vSphere Client angezeigt. Die im Zusammenhang mit regulären Datenspeichern anfallenden Aufgaben entfallen bei PMem-Datenspeichern.

Verfahren

- Überprüfen Sie die PMem-Datenspeicher-Informationen.

Option	Beschreibung
vSphere Client	a Navigieren Sie zum ESXi-Host und klicken Sie auf **Übersicht**. b Vergewissern Sie sich, dass im Bereich „Hardware“ persistenter Arbeitsspeicher angezeigt wird, und überprüfen Sie dessen Kapazität.
esxcli-Befehl	Verwenden Sie den Befehl `esxcli storage filesystem list`, um den PMem-Datenspeicher aufzulisten.

Beispiel: Anzeigen des PMem-Datenspeichers

Bei Verwendung des Befehls `esxcli storage filesystem list` zur Auflistung des Datenspeichers wird die folgende Beispielausgabe angezeigt.

```
# esxcli storage filesystem list
Mount Point              Volume Name          UUID          Mounted   Type      Size
Free
-----------------------  -----------------  -------------  --------- -------- ------------
------------

/vmfs/volumes/5xxx...     ds01-102          5xxx...       true     VMFS-6  14227079168
12718178304
/vmfs/volumes/59ex...     ds02-102          59ex...       true     VMFS-6  21206401024
19697500160
/vmfs/volumes/59bx...                       59bx...       true     vfat    4293591040
4274847744
/vmfs/volumes/pmem:5ax... PMemDS-56ax...    pmem:5a0x...  true     PMEM    12880707584
11504975872
```

Übersicht über die Verwendung von ESXi in einem SAN

3

Die Verwendung von ESXi in einem SAN erhöht die Flexibilität, Effizienz und Zuverlässigkeit. Bei der Verwendung von ESXi mit einem SAN werden eine zentrale Verwaltung sowie Failover- und Lastausgleichstechnologien ebenfalls unterstützt.

Im Folgenden werden die Vorteile der Verwendung von ESXi mit einem SAN zusammengefasst:

- Sie haben die Möglichkeit, Daten sicher zu speichern und mehrere Pfade zu Ihrem Speicher zu konfigurieren, um solch eine Fehlerquelle auszuschließen.
- Die Fehlerresistenz wird durch die Verwendung eines SAN mit ESXi-Systemen auf die Server erweitert. Wenn Sie einen SAN-Speicher einsetzen, können alle Anwendungen nach einem Ausfall des ursprünglichen Hosts umgehend auf einem anderen Host neu gestartet werden.
- Mit VMware VMotion können Sie während des laufenden Systembetriebs Migrationen virtueller Maschinen durchführen.
- Verwenden Sie VMware High Availability (HA) zusammen mit einem SAN, um die virtuellen Maschinen mit ihrem zuletzt bekannten Status auf einem anderen Server neu zu starten, falls ihr Host ausfällt.
- Verwenden Sie VMware Fault Tolerance (FT), um geschützte virtuelle Maschinen auf zwei unterschiedlichen Hosts zu replizieren. Die virtuellen Maschinen werden weiterhin unterbrechungsfrei auf dem sekundären Host ausgeführt, falls der primäre Host ausfällt.
- Verwenden Sie VMware DRS (Distributed Resource Scheduler), um virtuelle Maschinen für den Lastausgleich von einem Host auf einen anderen Host zu migrieren. Da sich der Speicher in einem freigegebenen SAN-Array befindet, werden Anwendungen ohne Unterbrechung weiter ausgeführt.
- Wenn Sie VMware DRS-Cluster verwenden, versetzen Sie einen ESXi-Host in den Wartungsmodus, damit das System alle laufenden virtuellen Maschinen auf andere ESXi-Hosts migriert. Anschließend können Sie auf dem ursprünglichen Host Upgrades oder andere Wartungsvorgänge durchführen.

Die Portabilität und Kapselung von virtuellen VMware-Maschinen ergänzt die Eigenschaften des Speichers hinsichtlich der gemeinsamen Nutzung. Wenn sich virtuelle Maschinen in einem SAN-basierten Speicher befinden, können Sie eine virtuelle Maschine auf einem Server herunterfahren und diese auf einem anderen Server starten oder diese auf einem Server anhalten und den Betrieb auf einem anderen Server im selben Netzwerk wieder aufnehmen – und das in nur wenigen Minuten. Auf diese Weise können Sie Rechenressourcen migrieren und gleichzeitig einen konsistenten gemeinsamen Zugriff aufrechterhalten.

Dieses Kapitel enthält die folgenden Themen:

Anwendungsbeispiele für ESXi und SAN

Wenn mit einem SAN verwendet, kann ESXi von mehreren vSphere-Funktionen profitieren, wie z. B. Storage vMotion, DRS (Distributed Resource Scheduler), HA (High Availability) usw.

Die Verwendung von ESXi mit einem SAN ist für die folgenden Aufgaben hilfreich:

Speicherkonsolidierung und Vereinfachung des Speicherlayouts

Wenn Sie mit mehreren Hosts arbeiten und auf jedem Host mehrere virtuelle Maschinen ausgeführt werden, reicht der Speicher des Hosts nicht mehr aus. Sie müssen möglicherweise externen Speicher verwenden. Das SAN kann eine einfache Systemarchitektur bereitstellen und sonstige Vorteile bieten.

Wartung ohne Ausfallzeiten

Verwenden Sie bei der Wartung von ESXi-Hosts oder -Infrastrukturen vMotion für die Migration virtueller Maschinen auf einen anderen Host. Falls im SAN ein gemeinsamer Speicher vorhanden ist, kann die Wartung für Benutzer virtueller Maschinen ohne Unterbrechungen durchgeführt werden. Die aktiven Prozesse der virtuellen Maschine werden während einer Migration weiterhin ausgeführt.

Lastausgleich

Sie können einen Host zu einem DRS-Cluster hinzufügen. Die Hostressourcen werden dann Teil der Clusterressourcen. Die Verteilung und Verwendung von CPU- und Arbeitsspeicherressourcen für alle Hosts und virtuelle Maschinen im Cluster werden kontinuierlich überwacht. DRS vergleicht diese Metriken mit denen einer idealen

Ressourcennutzung. Die ideale Nutzung berücksichtigt die Attribute der Ressourcenpools und der virtuellen Maschinen des Clusters, des aktuellen Bedarfs sowie des Ziels des Ungleichgewichts. Bei Bedarf führt DRS Migrationen von virtuellen Maschinen aus oder empfiehlt diese.

Notfallwiederherstellung

Sie können VMware High Availability verwenden, um mehrere ESXi-Hosts als Cluster zu konfigurieren. Der Cluster bietet eine schnelle Wiederherstellung nach Ausfällen und kostengünstige Hochverfügbarkeit für Anwendungen, die auf virtuellen Maschinen ausgeführt werden.

Vereinfachte Array-Migrationen und Speicher-Upgrades

Wenn Sie ein neues Speichersystem kaufen, verwenden Sie Storage vMotion, um Live-Migrationen von virtuellen Maschinen vom vorhandenen Speicher zu den neuen Zielen durchzuführen. Sie können die Migrationen ohne Unterbrechungen der virtuellen Maschinen durchführen.

Besonderheiten bei der Verwendung von SAN-Speicher mit ESXi

Die Verwendung eines SAN mit einem ESXi-Host unterscheidet sich von der Verwendung eines herkömmlichen SAN auf verschiedene Arten.

Wenn Sie Speicheranbieter mit ESXi verwenden, ist Folgendes zu beachten:

- Sie können SAN-Verwaltungstools nicht verwenden, um auf Betriebssysteme von virtuellen Maschinen zuzugreifen, die den Speicher verwenden. Mit herkömmlichen Tools können Sie ausschließlich das VMware ESXi-Betriebssystem überwachen. Über den vSphere Client können Sie virtuelle Maschinen überwachen.
- Der für die SAN-Verwaltungstools sichtbare HBA gehört zum ESXi-System und nicht zum Teil der virtuellen Maschine.
- Das ESXi-System führt in der Regel für Sie ein Multipathing durch.

ESXi-Hosts und mehrere Speicher-Arrays

Ein ESXi-Host kann auf Speichergeräte aus mehreren Speicher-Arrays zugreifen, auch auf Speicher von verschiedenen Anbietern.

Wenn Sie mehrere Arrays von verschiedenen Anbietern verwenden, gilt Folgendes:

- Wenn der Host dasselbe SATP für mehrere Arrays verwendet, seien Sie beim Ändern des Standard-PSP für dieses SATP vorsichtig. Die Änderung gilt für alle Arrays. Weitere Information über SATP und PSP finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.

- Einige Speicher-Arrays empfehlen spezifische Warteschlangentiefen und andere Einstellungen. In der Regel werden diese Einstellungen global auf ESXi-Hostebene konfiguriert. Geänderte Einstellungen für ein Array wirken sich auf andere Arrays aus, die LUNs für den Host darstellen. Weitere Informationen zur Warteschlangentiefe finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1267.
- Verwenden Sie das Einzel-Initiator-Einzel-Ziel-Zoning, wenn Sie ESXi-Hosts in Fibre-Channel-Arrays einteilen. Bei dieser Art der Konfiguration nehmen Fabric-spezifische Ereignisse, die in einem Array auftreten, keinen Einfluss auf die anderen Arrays. Weitere Informationen zum Zoning finden Sie unter Verwenden von Zoning mit Fibre-Channel-SANs.

Entscheidungen zur Verwendung von LUNs

Bevor Sie LUNs mit einem VMFS-Datenspeicher formatieren, müssen Sie zunächst festlegen, wie Sie den Speicher für Ihre ESXi-Systeme einrichten möchten.

Wenn Sie Ihre Entscheidungen zur Verwendung von LUNs treffen, ist Folgendes zu beachten:

- Jede LUN muss über das richtige RAID-Level und die richtigen Speichermerkmale für die Anwendungen verfügen, die in virtuellen Maschinen ausgeführt werden, die die LUN verwenden.
- Jede LUN darf nur einen einzigen VMFS-Datenspeicher enthalten.
- Wenn mehrere virtuelle Maschinen auf dieselbe VMFS zugreifen, lassen sich mithilfe von Festplattenfreigaben Prioritäten für virtuelle Maschinen festlegen.

Die folgenden Gründe sprechen für weniger und dafür größere LUNs:

- Mehr Flexibilität beim Erstellen virtueller Maschinen, ohne beim Speicheradministrator mehr Speicherplatz anfordern zu müssen.
- Mehr Flexibilität bei der Größenänderung virtueller Festplatten, dem Erstellen von Snapshots usw.
- Weniger zu verwaltende VMFS-Datenspeicher.

Die folgenden Gründe sprechen für mehr und dafür kleinere LUNs:

- Weniger falsch genutzter Speicherplatz.
- Unterschiedliche Anwendungen könnten unterschiedliche RAID-Merkmale erfordern.
- Mehr Flexibilität, da die Multipathing-Richtlinie und gemeinsam genutzte Festplattenfreigaben pro LUN festgelegt werden.
- Für den Einsatz von Microsoft Clusterdienst muss jede Clusterfestplattenressource in ihrer eigenen LUN eingerichtet sein.
- Bessere Leistung aufgrund weniger Konflikte auf den einzelnen Volumes.

Wenn die Speichermerkmale für eine virtuelle Maschine nicht verfügbar sind, kann es unter Umständen nicht einfach sein, die Anzahl und die Größe der bereitzustellenden LUNs zu ermitteln. Sie können experimentieren, indem Sie entweder ein Vorhersagemodell oder ein adaptives Modell verwenden.

Verwenden eines Vorhersagemodells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESXi-Systeme einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden und welche Größe diese besitzen sollen. Sie können experimentieren, indem Sie das Vorhersagemodell verwenden.

Verfahren

1. Stellen Sie mehrere LUNs mit unterschiedlichen Speichereigenschaften bereit.
2. Erstellen Sie einen VMFS-Datenspeicher in jeder LUN und benennen Sie jedes Volume entsprechend seinen Eigenschaften.
3. Erstellen Sie virtuelle Festplatten, um Kapazität für die Daten der Anwendungen virtueller Maschinen in den VMFS-Datenspeichern zu schaffen, die auf LUNs mit dem entsprechenden RAID-Level für die Anwendungsanforderungen erstellt wurden.
4. Sie verwenden Festplattenfreigaben, um virtuelle Maschinen mit hoher Priorität von denen mit niedriger Priorität zu unterscheiden.

   Hinweis Festplattenfreigaben sind nur innerhalb eines bestimmten Hosts entscheidend. Die den virtuellen Maschinen auf einem Host zugeordneten Freigaben haben keine Auswirkungen auf virtuelle Maschinen auf anderen Hosts.
5. Sie führen die Anwendungen aus, um zu ermitteln, ob die Leistung der virtuellen Maschine zufriedenstellend ist.

Verwenden des adaptiven Modells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESXi-Hosts einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden und welche Größe sie besitzen sollen. Sie können experimentieren, indem Sie das adaptive Modell verwenden.

Verfahren

1. Stellen Sie eine große LUN (RAID 1+0 oder RAID 5) mit aktiviertem Schreibcache bereit.
2. Erstellen Sie in dieser LUN ein VMFS.
3. Erstellen Sie vier oder fünf virtuelle Festplatten im VMFS.
4. Sie führen die Anwendungen aus, um zu ermitteln, ob die Festplattenleistung ausreichend ist.

Ergebnisse

Wenn die Leistung ausreicht, können Sie zusätzliche virtuelle Festplatten im VMFS einrichten. Reicht die Leistung nicht aus, haben Sie die Möglichkeit, eine neue, große LUN zu erstellen (eventuell mit einer anderen RAID-Ebene) und den Vorgang zu wiederholen. Verwenden Sie die Migrationsfunktion, damit keine Daten virtueller Maschinen bei der Neuerstellung der LUN verloren gehen.

Auswählen von Speicherorten für virtuelle Maschinen

Bei der Leistungsoptimierung der virtuellen Maschinen ist der Speicherort ein wichtiger Faktor. In Abhängigkeit von Ihren Speicheranforderungen können Sie Speicher mit hoher Leistung und Hochverfügbarkeit oder Speicher mit geringerer Leistung auswählen.

Die Speichereinteilung in verschiedene Qualitätsstufen ist von zahlreichen Faktoren abhängig:

- Hoch. Bietet hohe Leistung und Verfügbarkeit. Bietet unter Umständen auch integrierte Snapshots, um Sicherungen und PiT-Wiederherstellungen (Point-in-Time) zu vereinfachen. Unterstützt Replizierungen, vollständige Speicherprozessorredundanz und SAS-Laufwerke. Verwendet teure Spindeln.
- Mittel. Bietet durchschnittliche Leistung, niedrigere Verfügbarkeit, geringe Speicherprozessorredundanz und SCSI- bzw. SAS-Laufwerke. Bietet möglicherweise Snapshots. Verwendet Spindeln mit durchschnittlichen Kosten.
- Niedrig. Bietet niedrige Leistung, geringe interne Speicherredundanz. Verwendet Low-End-SCSI-Laufwerke oder SATA.

Nicht alle virtuellen Maschinen müssen sich während ihres gesamten Lebenszyklus im Speicher mit höchster Leistung und größter Verfügbarkeit befinden.

Bevor Sie entscheiden, wo Sie eine virtuelle Maschine platzieren möchten, ist Folgendes zu beachten:

- Die Wichtigkeit der virtuellen Maschine
- Anforderungen an Leistung und Verfügbarkeit
- PiT-Wiederherstellungsanforderungen
- Sicherungs- und Replizierungsanforderungen

Die Ebenen einer virtuellen Maschine können sich aufgrund von Änderungen bei der Wichtigkeit oder der Technologie im Verlauf Ihres Lebenszyklus ändern. Die Wichtigkeit ist relativ und kann sich aus verschiedenen Gründen ändern, beispielsweise bei Änderungen im Unternehmen, betriebswirtschaftlichen Abläufen, gesetzlichen Anforderungen oder Erstellung eines Notfallplans.

Verwaltungsanwendungen von Drittanbietern

Sie können Verwaltungssoftware von Drittanbietern mit Ihrem ESXi-Host verwenden.

Häufig ist im Lieferumfang der SAN-Hardware eine Speicherverwaltungssoftware enthalten. Hierbei handelt es sich in der Regel um eine Webanwendung, die mit einem beliebigen Webbrowser ausgeführt werden kann, der mit dem Netzwerk verbunden ist. In anderen Fällen wird die Software typischerweise auf dem Speichersystem oder einem Einzelserver ausgeführt, der unabhängig von den Servern betrieben wird, die das SAN zum Speichern nutzen.

Verwenden Sie diese Verwaltungssoftware von Drittanbietern für die folgenden Aufgaben:

- Speicher-Array-Verwaltung, einschließlich LUN-Erstellung, Cacheverwaltung des Arrays, LUN-Zuordnung und LUN-Sicherheit.
- Einrichtung von Replikations-, Prüfpunkt-, Snapshot- oder Spiegelungsfunktionen.

Wenn Sie die SAN-Verwaltungssoftware auf einer virtuellen Maschine ausführen, nutzen Sie die Vorteile der Ausführung einer virtuellen Maschine, einschließlich Failover mit vMotion und VMware HA. Aufgrund der zusätzlichen Indirektionsebene ist das SAN jedoch für die Verwaltungssoftware möglicherweise nicht sichtbar. In diesem Fall können Sie eine RDM verwenden.

Hinweis Die erfolgreiche Ausführung der Verwaltungssoftware durch eine virtuelle Maschine hängt letztlich von dem betreffenden Speichersystem ab.

Überlegungen zu SAN-Speichersicherungen

Das Vorhandensein einer guten Sicherungsstrategie ist einer der wichtigsten Aspekte der SAN-Verwaltung. In der SAN-Umgebung haben Sicherungen zwei Ziele. Das erste Ziel ist die Archivierung von Onlinedaten als Offlinemedien. Dieser Vorgang wird gemäß eines festgelegten Zeitplans regelmäßig für alle Onlinedaten wiederholt. Das zweite Ziel ist der Zugriff auf Offlinedaten zu Wiederherstellungszwecken. Für die Datenbankwiederherstellung müssen z.B. häufig archivierte Protokolldateien abgerufen werden, die gegenwärtig nicht online sind.

Die Planung von Sicherungen hängt von mehreren Faktoren ab:

- Ermittlung von kritischen Anwendungen, die häufigere Sicherungszyklen innerhalb eines bestimmten Zeitraums erfordern.
- Ziele für Wiederherstellungspunkte und -zeiten. Überlegen Sie, wie präzise Ihr Wiederherstellungspunkt sein muss und wie lange Sie darauf warten können.
- Die mit den Daten verknüpfte Änderungsrate (Rate of Change, RoC). Wenn Sie beispielsweise die synchrone bzw. asynchrone Replikation verwenden, beeinflusst die RoC die erforderliche Bandbreite zwischen den primären und den sekundären Speichergeräten.
- Auswirkungen insgesamt auf die SAN-Umgebung, Speicherleistung und andere Anwendungen.
- Ermittlung von Spitzenzeiten für den Datenverkehr im SAN. Sicherungen, die während dieser Spitzenzeiten geplant werden, können die Anwendungen und den Sicherungsprozess verlangsamen.
- Zeit für das Planen aller Sicherungen im Datencenter.

- Zeit für das Sichern einer einzelnen Anwendung.
- Ressourcenverfügbarkeit für die Datenarchivierung, z. B. Zugriff auf Offlinedaten.

Planen Sie für jede Anwendung ein Wiederherstellungszeitziel (Recovery Time Objective, RTO), wenn Sie die Sicherungsstrategie entwerfen. Das heißt, berücksichtigen Sie die Zeit und Ressourcen, die zum Durchführen einer Sicherung benötigt werden. Wenn eine geplante Sicherung beispielsweise eine so große Datenmenge speichert, dass die Wiederherstellung sehr lange dauert, überprüfen Sie die geplante Sicherung. Führen Sie die Sicherung häufiger durch, um die gespeicherte Datenmenge pro Sicherungsvorgang und die Wiederherstellungszeit zu reduzieren.

Wenn eine Anwendung innerhalb eines bestimmten Zeitraums wiederhergestellt werden muss, muss der Sicherungsvorgang einen Zeitplan und eine spezielle Datenverarbeitung bieten, um die Anforderung zu erfüllen. Eine schnelle Wiederherstellung kann die Verwendung von Wiederherstellungs-Volumes in einem Onlinespeicher erfordern. Dieser Vorgang hilft, die Notwendigkeit zu minimieren oder zu eliminieren, auf langsame Offline-Medien für fehlende Datenkomponenten zuzugreifen.

Verwenden von Drittanbieter-Sicherungspaketen

Sie können in Ihren virtuellen Maschinen Sicherungslösungen von Drittanbietern zum Schutz des Systems, der Anwendung und der Benutzerdaten verwenden.

Die „Storage APIs - Data Protection“ von VMware kann mit Drittanbieterprodukten verwendet werden. Bei Verwendung von APIs kann Drittanbietersoftware Sicherungen durchführen, ohne dass ESXi-Hosts mit der Verarbeitung der Sicherungsaufgaben belastet werden.

Die Drittanbieterprodukte, die „Storage APIs - Data Protection“ verwenden, können die folgenden Sicherungsaufgaben durchführen:

- Vollständige, differenzielle und inkrementelle Image-Sicherung und Wiederherstellen virtueller Maschinen.
- Sicherung virtueller Maschinen, die unterstützte Windows- und Linux-Betriebssysteme verwenden, auf Dateiebene.
- Sicherstellen der Datenkonsistenz durch Verwendung von Microsoft Volume Shadow Copy Service (VSS) für virtuelle Maschinen, die unterstützte Microsoft Windows-Betriebssysteme ausführen.

Da „Storage APIs - Data Protection“ die Snapshot-Funktionen von VMFS verwendet, ist es für Sicherungen nicht erforderlich, dass Sie virtuelle Maschinen beenden. Diese Sicherungen wirken sich nicht störend aus, können jederzeit durchgeführt werden und benötigen keine erweiterten Sicherungsfenster.

Weitere Informationen zu „Storage APIs - Data Protection“ und zur Integration mit Sicherungsprodukten finden Sie auf der VMware-Website oder wenden Sie sich an Ihren Anbieter.

Verwenden von ESXi mit Fibre-Channel-SAN

4

Bei der Einrichtung von ESXi-Hosts für die Verwendung von FC-SAN-Speicher-Arrays sollten Sie bestimmte Überlegungen anstellen. In diesem Abschnitt finden Sie Informationen zur Verwendung von ESXi mit einem FC-SAN-Array.

Dieses Kapitel enthält die folgenden Themen:

- Fibre-Channel-SAN-Konzepte
- Verwenden von Zoning mit Fibre-Channel-SANs
- Zugriff auf Daten in einem Fibre-Channel-SAN durch virtuelle Maschinen

Fibre-Channel-SAN-Konzepte

Wenn Sie ein ESXi-Administrator sind, der Hosts zusammen mit SANs einsetzen möchte, müssen Sie über Anwendungserfahrungen mit SAN-Konzepten verfügen. Weitere Informationen zur SAN-Technologie finden Sie in Printmedien oder dem Internet. Rufen Sie diese Quellen regelmäßig ab, um sich über Neuerungen in dieser Branche zu informieren.

Falls Sie sich mit der SAN-Technologie noch nicht auskennen, sollten Sie sich mit den Grundbegriffen vertraut machen.

Ein SAN (Storage Area Network) ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Hostserver mit Hochleistungsspeicher-Subsystemen verbindet. Zu den SAN-Komponenten zählen Hostbusadapter (HBAs) in den Hostservern, Switches, die Speicherdatenverkehr weiterleiten, Verkabelung, Speicherprozessoren (SP) und Festplattenspeicher-Arrays.

Eine SAN-Topologie mit mindestens einem Switch im Netzwerk stellt ein SAN-Fabric dar.

Für den Datentransfer von Hostservern auf gemeinsamen Speicher wird vom SAN das Fibre-Channel-Protokoll verwendet, das SCSI-Befehle in Fibre-Channel-Frames bündelt.

Um den Serverzugriff auf Speicher-Arrays einzuschränken, die diesem Server nicht zugeteilt sind, wird im SAN das Zoning verwendet. Normalerweise werden Zonen für jede Servergruppe erstellt, die auf eine gemeinsam genutzte Gruppe von Speichergeräten und LUNs zugreift. Über Zonen wird festgelegt, welche HBAs mit welchen Speicherprozessoren verbunden werden können. Geräte außerhalb einer Zone sind für Geräte in einer Zone nicht sichtbar.

Das Zoning ist mit der LUN-Maskierung vergleichbar, die häufig zur Verwaltung von Berechtigungen verwendet wird. LUN-Maskierung ist ein Prozess, über den eine LUN für einige Hosts bereitgestellt wird – für andere Hosts jedoch nicht.

Bei der Datenübertragung zwischen dem Hostserver und dem Speicher nutzt das SAN eine Technik, die als Multipathing bezeichnet wird. Multipathing bietet die Möglichkeit, mehr als einen physischen Pfad vom ESXi-Host zu einer LUN in einem Speichersystem bereitzustellen.

In der Regel besteht ein einzelner Pfad von einem Host zu einer LUN aus einem HBA, Switch-Ports, Verbindungskabeln und dem Speicher-Controller-Port. Falls eine Komponente des Pfads ausfällt, wählt der Host für E/A-Vorgänge einen anderen verfügbaren Pfad. Der Prozess der Erkennung eines ausgefallenen Pfads und des Wechsels auf einen anderen Pfad wird als Pfad-Failover bezeichnet.

Ports im Fibre-Channel-SAN

Im Kontext dieses Dokuments ist ein Port die Verbindung von einem Gerät mit dem SAN. Jeder Knoten im SAN, z. B. ein Host, ein Speichergerät oder eine Fabric-Komponente, verfügt über einen oder mehrere Ports, die ihn mit dem SAN verbinden. Ports werden auf verschiedene Arten identifiziert.

WWPN (World Wide Port Name)

Ein global eindeutiger Bezeichner für einen Port, der bestimmten Anwendungen den Zugriff auf den Port ermöglicht. Die FC-Switches erkennen den WWPN eines Geräts oder Hosts und weisen dem Gerät eine Portadresse zu.

Port_ID (oder Portadresse)

Innerhalb eines SAN verfügt jeder Port über eine eindeutige Port-ID, die als FC-Adresse für den Port dient. Diese eindeutige ID ermöglicht das Routing von Daten über das SAN zu diesem Port. Die FC-Switches weisen die Port-ID zu, wenn sich das Gerät bei der Fabric anmeldet. Die Port-ID ist nur gültig, wenn das Gerät angemeldet ist.

Wenn die N-Port-ID-Virtualisierung (NPIV) verwendet wird, kann ein einzelner FC-HBA-Port (N-Port) mithilfe mehrerer WWPNs beim Fabric registriert werden. Mit dieser Methode kann ein N-Port mehrere Fabric-Adressen beanspruchen, die jeweils als eindeutiges Element angezeigt werden. Wenn ESXi-Hosts ein SAN verwenden, bieten diese mehreren eindeutigen Bezeichner die Möglichkeit, WWPNs einzelnen virtuellen Maschinen als Teil ihrer Konfiguration zuzuweisen.

Typen von Fibre-Channel-Speicher-Arrays

ESXi unterstützt verschiedene Speichersysteme und Arrays.

Zu den Speichertypen, die Ihr Host unterstützt, gehören Aktiv-Aktiv, Aktiv-Passiv und ALUA-konform.

Aktiv-Aktiv-Speichersystem

Unterstützt den gleichzeitigen Zugriff auf die LUNs über alle Speicherports, die ohne wesentlichen Leistungsabfall verfügbar sind. Alle Pfade sind aktiv, es sei denn, ein Pfad schlägt fehl.

Aktiv-Passiv-Speichersystem

Ein System, in dem ein Speicherprozessor aktiv den Zugriff auf eine vorhandene LUN ermöglicht. Die anderen Prozessoren fungieren als Sicherung für die LUN und können den Zugriff auf andere LUN-E/A-Vorgänge aktiv bereitstellen. E/A-Daten können ausschließlich an einen aktiven Port gesendet werden. Falls der Zugriff über den aktiven Speicherport fehlschlägt, kann einer der passiven Speicherprozessoren durch die Server, die auf ihn zugreifen, aktiviert werden.

Asymmetrisches Speichersystem

Unterstützt Asymmetric Logical Unit Access (ALUA). ALUA-konforme Speichersysteme bieten verschiedene Zugriffsebenen für einzelne Ports. Mit ALUA kann der Host die Zustände von Zielports bestimmen und Pfade priorisieren. Der Host verwendet einige der aktiven Pfade als primäre Pfade und andere als sekundäre Pfade.

Verwenden von Zoning mit Fibre-Channel-SANs

Das Zoning ermöglicht die Zugriffssteuerung in der SAN-Topologie. Über Zonen wird festgelegt, welche HBAs mit welchen Zielen verbunden werden können. Wenn Sie bei der SAN-Konfiguration Zoning verwenden, sind Geräte außerhalb einer Zone für Geräte in einer Zone nicht sichtbar.

Zoning wirkt sich folgendermaßen aus:

- Verringert die Anzahl an Zielen und LUNs, die einem Host angegeben werden.
- Steuert und isoliert Pfade in einem Fabric.
- Kann verhindern, dass andere Systeme als das ESXi-System auf ein bestimmtes Speichersystem zugreifen und möglicherweise VMFS-Daten löschen.
- Kann zum Trennen verschiedener Umgebungen verwendet werden, z. B. zum Trennen einer Testumgebung von einer Produktionsumgebung.

Verwenden Sie für ESXi-Hosts ein Zoning mit einem einzelnen Initiator oder ein Zoning mit einem einzelnen Initiator und einem einzelnen Ziel. Letzteres ist eine bevorzugte Vorgehensweise für das Zoning. Die Verwendung des restriktiveren Zonings verhindert Probleme und falsche Konfigurationen, die im SAN auftreten können.

Ausführliche Anweisungen und die besten Vorgehensweisen für das Zoning erhalten Sie beim Speicher-Array- oder Switch-Anbieter.

Zugriff auf Daten in einem Fibre-Channel-SAN durch virtuelle Maschinen

ESXi speichert Festplattendateien einer virtuellen Maschine in einem VMFS-Datenspeicher, der sich auf einem SAN-Speichergerät befindet. Sobald Gastbetriebssysteme der virtuellen Maschine SCSI-Befehle an die virtuellen Festplatten senden, übersetzt die SCSI-Virtualisierungsebene diese Befehle in VMFS-Dateivorgänge.

Wenn eine virtuelle Maschine mit seinen auf einem SAN gespeicherten virtuellen Festplatten interagiert, finden die folgenden Prozesse statt:

1 Wenn das Gastbetriebssystem in einer virtuellen Maschine zum Lesen oder Schreiben auf eine SCSI-Festplatte zugreifen muss, sendet dieses SCSI-Befehle an die virtuelle Festplatte.

2 Gerätetreiber im Betriebssystem der virtuellen Maschine kommunizieren mit den virtuellen SCSI-Controllern.

3 Der virtuelle SCSI-Controller leitet den Befehl an den VMkernel weiter.

4 Der VMkernel führt die folgenden Aufgaben aus.

   a sucht im VMFS-Volume nach einer entsprechenden virtuellen Festplattendatei.

   b ordnet die Anforderungen für die Blöcke auf der virtuellen Festplatte den Blöcken auf dem entsprechenden physischen Gerät zu.

   c Sendet die geänderte E/A-Anforderung vom Gerätetreiber im VMkernel an den physischen HBA.

5 Der physische HBA führt die folgenden Aufgaben aus.

   a Bündelt die E/A-Anforderungen gemäß den Regeln des FC-Protokolls in Pakete.

   b übermittelt die Anforderung an das SAN.

6 Abhängig vom Port, den der HBA für die Verbindung zum Fabric verwendet, empfängt einer der SAN-Switches die Anforderung. Der Switch leitet die Anforderung an das entsprechende Speichergerät weiter.

Konfigurieren des Fibre-Channel-Speichers

5

Wenn Sie ESXi-Systeme mit SAN-Speicher verwenden, müssen bestimmte Hardware- und Systemanforderungen eingehalten werden.

Dieses Kapitel enthält die folgenden Themen:

- Anforderungen des Fibre-Channel-SAN von ESXi
- Installations- und Konfigurationsschritte
- N-Port-ID-Virtualisierung

Anforderungen des Fibre-Channel-SAN von ESXi

Um die Konfiguration des SAN und die Einrichtung des ESXi-Systems für die Verwendung eines SAN-Speichers vorzubereiten, sollten Sie die Anforderungen und Empfehlungen lesen.

- Stellen Sie sicher, dass ESXi-Systeme die verwendete Kombination aus SAN-Speicher-Hardware und -Firmware unterstützt. Eine aktuelle Liste finden Sie unter *VMware-Kompatibilitätshandbuch*.
- Konfigurieren Sie Ihr System, sodass nur ein VMFS-Volume pro LUN vorhanden ist.
- Wenn Sie keine Server ohne Festplatte verwenden, dürfen Sie keine Diagnosepartition auf einer SAN-LUN einrichten.

  Wenn Sie festplattenlose Server verwenden, die über ein SAN gestartet werden, ist eine gemeinsame Diagnosepartition geeignet.
- Verwenden Sie RDMs für den Zugriff auf Raw-Festplatten. Weitere Informationen hierzu finden Sie unter Kapitel 19 Raw-Gerätezuordnung.
- Damit das Multipathing ordnungsgemäß funktioniert, muss jede LUN allen ESXi-Hosts dieselbe LUN-ID-Nummer anzeigen.
- Stellen Sie sicher, dass für den Speichergerätetreiber eine ausreichend große Warteschlange angegeben ist. Sie können die Warteschlangentiefe für den physischen HBA während der Systeminstallation festlegen.

- Erhöhen Sie auf virtuellen Maschinen unter Microsoft Windows den Wert des SCSI-Parameters `TimeoutValue` auf 60. Aufgrund dieser Erhöhung kann Windows E/A-Verzögerungen tolerieren, die aus einem Pfad-Failover resultieren. Weitere Informationen hierzu finden Sie unter Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen.

Einschränkungen des Fibre-Channel-SAN von ESXi

Für die Verwendung von ESXi in einem SAN gelten gewisse Einschränkungen.

- ESXi unterstützt keine über FC verbundenen Bandlaufwerke.
- Sie können keine Multipathing-Software für virtuelle Maschinen verwenden, um einen E/A-Lastenausgleich für eine einzelne physische LUN durchzuführen. Wenn jedoch Ihre virtuelle Microsoft Windows-Maschine dynamische Datenträger verwendet, gilt diese Einschränkung nicht. Weitere Informationen über das Konfigurieren dynamischer Datenträger finden Sie unter Dynamische Festplattenspiegelung einrichten.

Festlegen der LUN-Zuordnungen

Dieses Thema bietet einige grundlegende Informationen zum Zuweisen von LUNs bei Ausführung des ESXi mit SAN.

Beachten Sie beim Festlegen von LUN-Zuordnungen die folgenden Punkte:

Bereitstellen von Speicher

Damit das ESXi-System die LUNs beim Start erkennt, müssen alle LUNs für die entsprechenden HBAs bereitgestellt werden, bevor das SAN mit dem ESXi-System verbunden wird.

Stellen Sie alle LUNs allen ESXi-HBAs gleichzeitig bereit. HBA-Failover funktioniert nur, wenn für alle HBAs dieselben LUNs sichtbar sind.

Stellen Sie für LUNs, die von mehreren Hosts gemeinsam genutzt werden, sicher, dass die LUN-IDs über alle Hosts hinweg konsistent sind.

vMotion und VMware DRS

Wenn Sie vCenter Server und vMotion oder DRS verwenden, sollten Sie sicherstellen, dass die LUNs für die virtuellen Maschinen allen ESXi-Hosts bereitgestellt werden. Diese Aktion bietet die höchste Flexibilität beim Verschieben virtueller Maschinen.

Aktiv/Aktiv- im Vergleich zu Aktiv/Passiv-Arrays

Bei der Verwendung von vMotion oder DRS mit einem SAN-Speichergerät vom Typ „Aktiv/Passiv“ sollten Sie sicherstellen, dass alle ESXi-Systeme über einheitliche Pfade zu allen Speicherprozessoren verfügen. Anderenfalls kann es bei vMotion-Migrationen zu einem Pfad-Thrashing kommen.

Für Aktiv/Passiv-Speicher-Arrays, die in der Speicher-/SAN-Kompatibilität nicht aufgelistet sind, werden keine Speicherport-Failover von VMware unterstützt. In solchen Fällen müssen Sie den Server am aktiven Port des Speicher-Arrays anschließen. Durch diese Konfiguration wird sichergestellt, dass die LUNs dem ESXi-Host angezeigt werden.

Festlegen von Fibre-Channel-HBAs

In der Regel funktionieren FC-HBAs, die Sie auf Ihrem ESXi-Host verwenden, mit den Standardkonfigurationseinstellungen ordnungsgemäß.

Sie sollten die von Ihrem Speicher-Array-Anbieter bereitgestellten Konfigurationsrichtlinien befolgen. Beachten Sie beim Einrichten von Fibre-Channel-HBA die folgenden Aspekte.

- Verwenden Sie in einem einzelnen Host keine FC-HBAs von verschiedenen Anbietern. Zwar wird der Einsatz verschiedener Modelle desselben HBAs unterstützt, auf eine einzelne LUN kann jedoch nur von HBAs desselben Typs zugegriffen werden.
- Stellen Sie sicher, dass die Firmware-Ebenen aller HBAs einheitlich sind.
- Legen Sie den Zeitüberschreitungswert für das Erkennen eines Failovers fest. Um eine optimale Leistung zu erzielen, ändern Sie den Standardwert nicht.
- ESXi unterstützt End-to-End-Konnektivität für Fibre Channel (32 GBit/s).

Installations- und Konfigurationsschritte

Dieses Kapitel bietet eine Übersicht über Installations- und Konfigurationsschritte zur Einrichtung Ihrer SAN-Umgebung für die Kompatibilität mit ESXi.

Führen Sie zur Konfiguration Ihrer ESXi SAN-Umgebung die folgenden Schritte aus.

1 Entwerfen Sie Ihr SAN, falls noch nicht konfiguriert. Die meisten SANs erfordern für die Kompatibilität mit ESXi nur geringe Änderungen.

2 Stellen Sie sicher, dass alle SAN-Komponenten die Anforderungen erfüllen.

3 Nehmen Sie die erforderlichen Änderungen am Speicher-Array vor.

   Für die Konfiguration eines SAN zur Verwendung mit VMware ESXi bieten die meisten Anbieter spezifische Dokumentationen.

4 Richten Sie die HBAs für die Hosts ein, die mit dem SAN verbunden sind.

5 Installieren Sie ESXi auf den Hosts.

6 Erstellen Sie virtuelle Maschinen und installieren Sie Gastbetriebssysteme.

7 (Optional) Konfigurieren Sie das System für vSphere HA-Failover oder für die Verwendung von Microsoft Cluster-Diensten.

8 Aktualisieren oder ändern Sie ggf. die Umgebung.

N-Port-ID-Virtualisierung

N-Port-ID-Virtualisierung (NPIV) ist ein ANSI T11-Standard, der beschreibt, wie ein einzelner Fibre-Channel-HBA-Port mit dem Fabric über mehrere WWPNs (Worldwide Port Names) verbunden werden kann. Auf diese Weise kann ein Fabric-gebundener N-Port mehrere Fabric-Adressen beanspruchen. Jede Adresse zeigt eine eindeutige Einheit auf dem Fibre-Channel-Fabric.

Funktionsweise des NPIV-basierten LUN-Zugriffs

NPIV bietet die Möglichkeit, dass ein einziger FC-HBA-Port mehrere eindeutige World Wide Name (WWN)-Bezeichnern mit dem Fabric registriert, von denen jeder einer einzelnen virtuellen Maschine zugewiesen werden kann. Durch die Verwendung von NPIV kann ein SAN-Administrator den Speicherzugriff für jede virtuelle Maschine überwachen und weiterleiten.

Nur virtuelle Maschinen mit RDMs können über WWN-Zuweisungen verfügen und diese Zuweisungen für den gesamten RDM-Datenverkehr verwenden.

Wenn eine virtuelle Maschine über einen zugewiesenen WWN verfügt, wird die Konfigurationsdatei der virtuellen Maschine (.vmx) zur Aufnahme eines WWN-Paars aktualisiert. Das WWN-Paar besteht aus einem World Wide Port Name (WWPN) und einem World Wide Node Name (WWNN). Wenn diese virtuelle Maschine eingeschaltet wird, erstellt der VMkernel einen virtuellen Port (VPORT) auf dem physischen HBA, der für den Zugriff auf die LUN verwendet wird. Der VPORT ist ein virtueller HBA, der dem FC-Fabric als physischer HBA angezeigt wird. Als eindeutiger Bezeichner verwendet der VPORT das WWN-Paar, das der virtuellen Maschine zugewiesen wurde.

Für die virtuelle Maschine ist jeder VPORT spezifisch. Sobald die virtuelle Maschine ausgeschaltet ist, wird der VPORT auf dem Host gelöscht und dem FC-Fabric nicht mehr angezeigt. Wenn eine virtuelle Maschine von einem Host zu einem anderen migriert wird, wird der VPORT auf dem ersten Host geschlossen und auf dem Zielhost geöffnet.

Sind für virtuelle Maschinen keine WWN-Zuweisungen vorhanden, erfolgt der Zugriff auf Speicher-LUNs über die WWNs der physischen HBAs des Hosts.

Anforderungen für die Verwendung von NPIV

Wenn Sie NPIV auf Ihren virtuellen Maschinen aktivieren möchten, sollten Sie bestimmte Anforderungen berücksichtigen.

- NPIV wird nur für virtuelle Maschinen mit Raw-Gerätezuordnungsfestplatten unterstützt. Virtuelle Maschinen mit herkömmlichen virtuellen Festplatten verwenden die WWNs der physischen HBAs des Hosts.
- Die HBAs auf Ihrem Host müssen NPIV unterstützen.

Hinweise finden Ihr unter *VMware-Kompatibilitätshandbuch* und in der Dokumentation des Anbieters.

- Verwenden Sie HBAs desselben Typs. VMware unterstützt den Zugriff von heterogenen HBAs auf dieselben LUNs auf demselben Host nicht.
- Wenn ein Host mehrere physische HBAs als Speicherpfade verwendet, teilen Sie alle physischen Pfade zur virtuellen Maschine in Zonen auf. Dies ist erforderlich, damit das Multipathing selbst dann unterstützt wird, wenn nur ein Pfad aktiv ist.
- Stellen Sie sicher, dass die physischen HBAs auf dem Host alle LUNs erkennen können, auf die von NPIV-aktivierten virtuellen Maschinen zugegriffen werden soll, die auf dem Host ausgeführt werden.

- Die Switches in der Fabric müssen NPIV erkennen können.
- Stellen Sie bei der Konfiguration einer LUN für den NPIV-Zugriff auf Speicherebene sicher, dass die NPIV-LUN-Nummer und die NPIV-Ziel-ID mit der physischen LUN und der Ziel-ID übereinstimmen.
- Legen Sie Zonen für die NPIV WWPNs fest, sodass sie eine Verbindung zu allen Speichersystemen herstellen, auf die die Cluster-Hosts Zugriff haben, selbst wenn die VM den Speicher nicht verwendet. Wenn Sie neue Speichersysteme zu einem Cluster mit einer oder mehreren NPIV-fähigen VMs hinzufügen, fügen Sie die neuen Zonen hinzu, damit die NPIV-WWPNs die Zielports des neuen Speichersystems erkennen können.

NPIV-Funktionen und -Einschränkungen

Erfahren Sie mehr über die spezifischen Funktionen und Einschränkungen der Verwendung von NPIV mit ESXi.

ESXi mit NPIV unterstützt die folgenden Elemente:

- NPIV unterstützt vMotion. Wenn Sie vMotion zum Migrieren einer virtuellen Maschine verwenden, wird der zugewiesene WWN beibehalten.

  Wenn Sie eine NPIV-aktivierte virtuelle Maschine auf einen Host migrieren, der NPIV nicht unterstützt, verwendet VMkernel wieder einen physischen HBA zum Weiterleiten des E/A.
- Wenn Ihre FC-SAN-Umgebung die gleichzeitige E/A auf den Festplatten eines Aktiv-Aktiv-Arrays unterstützt, wird die gleichzeitige E/A auf zwei verschieden NPIV-Ports ebenfalls unterstützt.

Für die Verwendung von ESXi mit NPIV gelten folgende Einschränkungen:

- Weil die NPIV-Technologie eine Erweiterung des FC-Protokolls ist, benötigt sie einen FC-Switch und funktioniert nicht auf den direkt angehängten FC-Festplatten.
- Wenn eine virtuelle Maschine oder Vorlage mit einer WWN-Zuweisung geklont wird, behält der Klon den WWN nicht bei.
- NPIV unterstützt Storage vMotion nicht.

- Wenn während der Laufzeit virtueller Maschinen die NPIV-Fähigkeit eines FC-Switches deaktiviert und anschließend erneut aktiviert wird, kann ein FC-Link fehlschlagen und die Ein-/Ausgabe gestoppt werden.

Konfigurieren bzw. Ändern von WWN-Zuweisungen

Weisen Sie WWN-Einstellungen einer virtuellen Maschine zu. Sie können die WWN-Zuweisungen zu einem späteren Zeitpunkt ändern.

Sie können bis zu 16 WWN-Paare erstellen, die jeweils den ersten 16 physischen FC-HBAs auf dem Host zugeordnet werden können.

In der Regel müssen Sie die vorhandenen WWN-Zuweisungen auf Ihrer virtuellen Maschine nicht ändern. Unter bestimmten Umständen, wenn beispielsweise manuell zugewiesene WWNs Konflikte auf dem SAN verursachen, müssen Sie möglicherweise WWNs ändern oder entfernen.

Voraussetzungen

- Stellen Sie vor der WWN-Konfiguration sicher, dass der ESXi-Host auf die auf Array-Seite konfigurierte Zugriffssteuerungsliste (Access Control List, ACL) der Speicher-LUN zugreifen kann.
- Wenn Sie die vorhandenen WWNs bearbeiten möchten, schalten Sie die virtuelle Maschine aus.

Verfahren

1. Klicken Sie in der Bestandsliste mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.
2. Klicken Sie auf **VM-Optionen** und erweitern Sie **Fibre-Channel-NPIV**.
3. Erstellen oder bearbeiten Sie die WWN-Zuweisungen, indem Sie eine der folgenden Optionen auswählen:

Option	Beschreibung
NPIV für diese virtuelle Maschine vorübergehend deaktivieren	Deaktivieren Sie die vorhandenen WWN-Zuweisungen für die virtuelle Maschine, aber entfernen Sie sie nicht.
Unverändert lassen	Behalten Sie die vorhandenen WWN-Zuweisungen bei. Im Abschnitt mit den schreibgeschützten WWN-Zuweisungen werden die Knoten- und Portwerte aller vorhandenen WWN-Zuweisungen angezeigt.
Neue WWNs generieren	Generieren Sie neue WWNs und überschreiben Sie dabei vorhandene WWNs. Die WWNs des HBA sind davon nicht betroffen. Geben Sie die Anzahl der WWNNs und WWPNs an. Zur Unterstützung von Failover mit NPIV werden mindestens zwei WWPNs benötigt. In der Regel wird nur ein WWNN für jede virtuelle Maschine erstellt.
WWN-Zuweisung entfernen	Entfernen Sie die der virtuellen Maschine zugewiesenen WWNs. Die virtuelle Maschine verwendet anschließend für den Zugriff auf die Speicher-LUN die HBA-WWNs.

4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Nächste Schritte

Registrieren Sie neu erstellte WWNs in der Fabric.

Konfigurieren von Fibre-Channel über Ethernet

6

Mithilfe des Fibre Channel over Ethernet-(FCoE-)Protokolls kann ein ESXi-Host auf den Fibre-Channel-Speicher zugreifen.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Das FCoE-Protokoll kapselt Fibre-Channel-Frames in Ethernet-Frames ein. Ihr Host benötigt daher keine speziellen Fibre-Channel-Verknüpfungen, um eine Verbindung zum Fibre-Channel-Speicher herzustellen. Der Host kann 10 Gbit Lossless Ethernet verwenden, um Fibre-Channel-Datenverkehr bereitstellen zu können.

Dieses Kapitel enthält die folgenden Themen:

- Adapter für Fibre-Channel über Ethernet
- Konfigurationsrichtlinien für Software-FCoE
- Einrichten des Netzwerks für Software-FCoE
- Hinzufügen von Software-FCoE-Adaptern

Adapter für Fibre-Channel über Ethernet

Um Fibre-Channel über Ethernet (FCoE) zu verwenden, konfigurieren Sie entsprechende Adapter auf dem Host.

Die von VMware unterstützten Adapter lassen sich in der Regel in zwei Kategorien einteilen: Hardware-FCoE-Adapter und Software-FCoE-Adapter, die den nativen FCoE-Stack in ESXi verwenden.

Informationen zu Adaptern, die mit VMware-FCoE verwendet werden können, finden Sie im *VMware-Kompatibilitätshandbuch*

Hardware-FCoE-Adapter

Diese Kategorie enthält verlagerte spezialisierte CNAs (Converged Network Adapters), die Netzwerk- und Fibre-Channel-Funktionalität auf derselben Karte enthalten.

Wenn solch ein Adapter installiert ist, erkennt Ihr Host beide CNA-Komponenten und kann diese verwenden. Im vSphere Client wird die Netzwerkkomponente als Standardnetzwerkadapter (vmnic) und die Fibre-Channel-Komponente als FCoE-Adapter (vmhba) angezeigt. Sie müssen den Hardware-FCoE-Adapter nicht konfigurieren, um ihn verwenden zu können.

Software-FCoE-Adapter

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Ein Software-FCoE-Adapter verwendet den nativen FCoE-Protokoll-Stack in ESXi, um einige der FCoE-Verarbeitungen durchzuführen. Sie müssen den Software-FCoE-Adapter mit einer kompatiblen Netzwerkkarte verwenden.

VMware unterstützt zwei Kategorien von Netzwerkkarten mit dem Software-FCoE-Adapter.

Netzwerkkarten mit FCoE-Offload (teilweise)

Das Ausmaß der Offload-Funktionen richtet sich nach dem Typ der Netzwerkkarte. Die Netzwerkkarten bieten in der Regel Data Center Bridging (DCB) und E/A-Offload-Funktionen.

Netzwerkkarten ohne FCoE-Offload

Alle Netzwerkkarten, die Data Center Bridging (DCB) bieten und eine minimale Geschwindigkeit von 10 Gbit/s aufweisen. Die Netzwerkadapter müssen FCoE-Offload-Funktionen nicht zwangsläufig unterstützen.

Im Gegensatz zum Hardware-FCoE-Adapter muss der Software-Adapter aktiviert werden. Bevor Sie den Adapter aktivieren, müssen Sie das Netzwerk ordnungsgemäß konfigurieren.

Hinweis Die Anzahl an Software-FCoE-Adaptern, die Sie aktivieren, entspricht der Anzahl der physischen Netzwerkkarten-Ports. ESXi unterstützt maximal vier Software-FCoE-Adapter auf einem Host.

Konfigurationsrichtlinien für Software-FCoE

Befolgen Sie beim Einrichten einer Netzwerkumgebung für ESXi-Software-FCoE die Richtlinien und Best Practices von VMware.

Richtlinien für Netzwerk-Switches

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Befolgen Sie diese Richtlinien, wenn Sie einen Netzwerk-Switch für eine FCoE-Softwareumgebung konfigurieren:

- Deaktivieren Sie das Spanning-Tree-Protokoll (STP) auf den Ports, die mit Ihrem ESXi-Host kommunizieren. Durch das Aktivieren des STP wird möglicherweise die Antwort des FCoE-Initialisierungsprotokolls (FIP) am Switch verzögert und der Zustand „Keine Pfade verfügbar“ verursacht.

  FIP ist ein Protokoll, das FCoE zum Ermitteln und Initialisieren von FCoE-Elementen im Ethernet verwendet.
- Schalten Sie die prioritätsbasierte Flusssteuerung (Priority-based Flow Control, PFC) ein und legen Sie sie auf „AUTO“ fest.
- Vergewissern Sie sich, dass Sie über eine kompatible Firmware-Version auf dem FCoE-Switch verfügen.
- Legen Sie den MTU-Wert auf dem vSwitch auf 2500 oder höher fest.

Richtlinien und Best Practices für Netzwerkadapter

Wenn Sie planen, Software-FCoE-Adapter für den Einsatz mit Netzwerkadaptern zu aktivieren, gelten besondere Erwägungen.

- Unabhängig davon, ob Sie eine Netzwerkkarte mit partieller E/A-Offload-Fähigkeit oder eine nicht-FCoE-fähige Netzwerkkarte verwenden, sollten Sie sicherstellen, dass der neueste Mikrocode auf dem Netzwerkadapter installiert ist.
- Wenn Sie eine nicht-FCoE-fähige Netzwerkkarte verwenden, sollten Sie sich vergewissern, dass diese über die für die Software-FCoE-Aktivierung erforderliche DCB-Funktionalität verfügt.
- Wenn der Netzwerkadapter über mehrere Ports verfügt, fügen Sie bei der Konfiguration von Netzwerken jeden Port zu einem eigenen vSwitch hinzu. Dadurch vermeiden Sie den Zustand „Keine Pfade verfügbar“, wenn ein störendes Ereignis, wie z. B. eine MTU-Änderung, eintritt.
- Verschieben Sie einen Netzwerkadapter-Port nicht von einem vSwitch zu einem anderen vSwitch, wenn der FCoE-Datenverkehr aktiv ist. Falls Sie diese Änderung vornehmen, starten Sie danach den Host neu.
- Falls das Ändern des vSwitches für einen Netzwerkadapter-Port einen Ausfall verursacht, verschieben Sie den Port auf den ursprünglichen vSwitch zurück, um das Problem zu beheben.

Einrichten des Netzwerks für Software-FCoE

Bevor Sie die Software-FCoE-Adapter auf Ihrem ESXi-Host aktivieren, erstellen Sie VMkernel-Netzwerkadapter für alle physischen FCoE-Netzwerkkarten, die auf dem Host installiert sind.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Dieses Verfahren erklärt, wie ein einzelner VMkernel-Netzwerkadapter erstellt wird, der mit einem einzelnen physischen FCoE-Netzwerkadapter über einen vSphere Standard-Switch verbunden ist. Wenn Ihr Host mehrere Netzwerkadapter oder mehrere Ports auf dem Adapter hat, verbinden Sie jede FCoE-Netzwerkkarte mit einem getrennten Standard Switch. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

2 Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.

3 Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.

4 Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.

5 Um Jumbo-Frames zu aktivieren, ändern Sie **MTU (Byte)** in den Wert 2500 oder höher und klicken Sie auf **Weiter**.

6 Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie den Netzwerkadapter (vmnic#) aus, der FCoE unterstützt.

   Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.

7 Geben Sie eine Netzwerkbezeichnung ein.

   Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. „FCoE“.

8 Geben Sie eine VLAN-ID an und klicken Sie auf **Weiter**.

   Der FCoE-Datenverkehr erfordert ein isoliertes Netzwerk. Stellen Sie sicher, dass sich die von Ihnen eingegebene VLAN-ID von derjenigen unterscheidet, die für das normale Netzwerk auf Ihrem Host verwendet wird. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

9 Prüfen Sie nach dem Abschließen der Konfiguration die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Sie haben den virtuellen VMkernel-Adapter für den auf Ihrem Host installierten physischen FCoE-Netzwerkadapter erstellt.

Hinweis Um Störungen im FCoE-Datenverkehr zu vermeiden, sollten Sie den FCoE-Netzwerkadapter (vmnic #) nicht aus dem vSphere Standard-Switch entfernen, nachdem Sie das FCoE-Netzwerk eingerichtet haben.

Hinzufügen von Software-FCoE-Adaptern

Sie müssen Software-FCoE-Adapter aktivieren, damit der ESXi-Host sie für den Zugriff auf den Fibre-Channel-Speicher verwenden kann.

Hinweis Ab vSphere 7.0 bietet VMware keine weitere Unterstützung für Software-FCoE-Adapter in Produktionsumgebungen.

Die Anzahl an Software-FCoE-Adaptern, die Sie aktivieren können, entspricht der Anzahl der physischen FCoE-Netzwerkkarten-Ports auf Ihrem Host. ESXi unterstützt maximal vier Software-FCoE-Adapter auf einem Host.

Voraussetzungen

Richten Sie das Netzwerk für den Software-FCoE-Adapter ein.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und anschließend auf das Symbol **Softwareadapter hinzufügen**.
4. Wählen Sie **Software-FCoE-Adapter**.
5. Wählen Sie im Dialogfeld „Hinzufügen von Software-FCoE-Adaptern“ eine entsprechende vmnic aus der Dropdown-Liste der physischen Netzwerkadapter aus.

   Nur diejenigen Adapter, die noch nicht für den FCoE-Datenverkehr verwendet werden, werden aufgelistet.
6. Klicken Sie auf **OK**.

   Der Software-FCoE-Adapter wird in der Liste der Speicheradapter angezeigt.

Ergebnisse

Nachdem Sie den Software-FCoE-Adapter aktiviert haben, können Sie seine Eigenschaften anzeigen. Wenn Sie den Adapter nicht verwenden, können Sie ihn aus der Liste der Adapter entfernen.

Starten von ESXi aus einem Fibre-Channel-SAN

7

Wenn Sie Ihren Host so einrichten, dass er von einem SAN gestartet wird, wird das Start-Image des Hosts auf einer oder mehreren LUNs im SAN-Speichersystem gespeichert. Wenn der Host startet, wird er nicht von seiner lokalen Festplatte aus, sondern von der LUN im SAN aus gestartet.

ESXi bietet Unterstützung für den Start über einen Fibre-Channel-HBA (Host Bus Adapter) oder einen FCoE-CNA (Fibre Channel over Ethernet Converged Network Adapter).

Dieses Kapitel enthält die folgenden Themen:

Starten über ein SAN – Vorteile

Das Starten über ein SAN kann Ihrer ESXi-Umgebung viele Vorteile bieten. In bestimmten Fällen ist das Starten über ein SAN jedoch nicht kompatibel mit Ihren Hosts. Bevor Sie Ihr System zum Starten über ein SAN einrichten, sollten Sie zunächst überlegen, ob dies Ihrer Umgebung angemessen ist.

Vorsicht Wenn das Starten über ein SAN mit mehreren ESXi-Hosts erfolgt, muss jeder Host über eine eigene Start-LUN verfügen. Wenn Sie mehrere Hosts für die Verwendung derselben Start-LUN konfigurieren, werden wahrscheinlich ESXi-Images beschädigt.

Wenn Sie über ein SAN starten, gibt es u.a. folgende Vorteile für Ihre Umgebung:

- Günstigere Server. Höhere Serverdichte und bessere Ausführung ohne internen Speicher.
- Einfacherer Serveraustausch. Sie können Server problemlos austauschen und den neuen Server so einrichten, dass sie auf den alten Speicherort der Start-Image-Datei verweisen.
- Weniger ungenutzter Speicherplatz. Server ohne lokale Festplatten benötigen oft weniger Speicherplatz.

- Einfachere Sicherungsvorgänge. Sie können die Systemstart-Images im SAN als Teil der allgemeinen SAN-Sicherungsverfahren sichern. Außerdem können Sie fortschrittliche Array-Funktionen verwenden, wie z. B. Snapshots auf dem Start-Image.
- Verbesserte Verwaltung. Das Erstellen und Verwalten des Betriebssystem-Images ist einfacher und effizienter.
- Noch zuverlässiger. Sie können über mehrere Pfade auf das Startlaufwerk zugreifen, was verhindert, dass das Laufwerk zur einzelnen Fehlerquelle wird.

Anforderungen und Überlegungen beim Starten von Fibre-Channel-SAN

Ihre ESXi-Startkonfiguration muss bestimmte Anforderungen erfüllen.

Tabelle 7-1. Anforderungen für das Starten über ein SAN

Anforderung	Beschreibung
Anforderungen an das ESXi-System	Halten Sie sich an die Herstellerempfehlungen für das Starten des Servers über ein SAN.
Adapteranforderungen	Konfigurieren Sie den Adapter ordnungsgemäß, damit er auf die Start-LUN zugreifen kann. Informationen finden Sie in der Dokumentation des Anbieters.
Zugriffssteuerung	■ Jeder Host darf nur auf seine eigene LUN zugreifen, nicht auf die Start-LUNs anderer Hosts. Verwenden Sie Speichersystemsoftware, um sicherzustellen, dass der Host nur auf die zugewiesenen LUNs zugreift. ■ Eine Diagnosepartition kann von mehreren Servern gemeinsam genutzt werden. Um diese Konfiguration zu erzielen, können Sie die Array-spezifische LUN-Maskierung verwenden.
Unterstützung von Multipathing	Das Multipathing auf eine Start-LUN auf Aktiv-Passiv-Arrays wird nicht unterstützt, weil das BIOS Multipathing nicht unterstützt und keinen Standby-Pfad aktivieren kann.
Überlegungen zum SAN	Wenn das Array nicht für eine direkte Verbindungstopologie zertifiziert ist, müssen die SAN-Verbindungen über eine Switch-Topologie hergestellt werden. Wenn das Array für die direkte Verbindungstopologie zertifiziert ist, können die SAN-Verbindungen direkt zum Array hergestellt werden. Start über ein SAN wird für sowohl für die Switch-Topologie als auch für die direkte Verbindungstopologie unterstützt.
Hardwarespezifische Überlegungen	Wenn Sie ein eServer BladeCenter von IBM ausführen und das System über das SAN starten, müssen Sie die IDE-Laufwerke der Blades deaktivieren.

Vorbereiten des Starts über ein SAN

Wenn Sie den ESXi-Host für den Start über ein SAN vorbereiten, führen Sie mehrere Aufgaben durch.

In diesem Abschnitt wird der generische Aktivierungsprozess zum Starten über SAN auf den im Rack montierten Servern beschrieben. Weitere Informationen zum Aktivieren des Starts über die SAN-Option auf Cisco Unified Computing System FCoE-Blade-Servern finden Sie in der Cisco-Dokumentation.

Verfahren

1 Konfigurieren von SAN-Komponenten und des Speichersystems

Bevor Sie Ihren ESXi-Host zum Starten von einer SAN-LUN einrichten, konfigurieren Sie die SAN-Komponenten und ein Speichersystem.

2 Konfigurieren eines Speicheradapters für das Starten über ein SAN

Wenn Sie Ihren Host zum Starten über ein SAN einrichten, aktivieren Sie den Startadapter im BIOS des Hosts. Sie können den Startadapter zum Initiieren einer einfachen Verbindung mit der Ziel-Start-LUN konfigurieren.

3 Einrichten des Systems zum Starten vom Installationsmedium

Wenn Sie Ihren Host zum Starten vom SAN einrichten, starten Sie den Host zuerst vom VMware-Installationsmedium. Um vom Installationsmedium aus zu starten, ändern Sie die Startreihenfolge in den BIOS-Einstellungen des Systems.

Konfigurieren von SAN-Komponenten und des Speichersystems

Bevor Sie Ihren ESXi-Host zum Starten von einer SAN-LUN einrichten, konfigurieren Sie die SAN-Komponenten und ein Speichersystem.

Weil das Konfigurieren der SAN-Komponenten anbieterspezifisch ist, sollten Sie die Produktdokumentation eines jeden Elements zu Rate ziehen.

Verfahren

1 Schließen Sie das Netzwerkkabel an, wie in den Handbüchern der betreffenden Geräte beschrieben.

Überprüfen Sie ggf. die Switch-Verkabelung.

2 Konfigurieren Sie das Speicher-Array.

a Machen Sie den ESXi-Host über das SAN-Speicher-Array für das SAN sichtbar. Dieser Vorgang wird häufig als das Erstellen eines Objekts bezeichnet.

b Richten Sie den Host über das SAN-Speicher-Array so ein, sodass dieser die WWPNs der Hostadapter als Port- oder Knotennamen verwendet.

c Erstellen Sie LUNs.

d Weisen Sie LUNs zu.

e Erfassen Sie die IP-Adressen der Switches und der Speicher-Arrays.

f Erfassen Sie den WWPN für jeden Speicherprozessor.

Vorsicht Wenn die Installation von ESXi im Modus zum Starten über SAN per Skript erfolgt, sind bestimmte Schritte auszuführen, um einen unerwünschten Datenverlust zu vermeiden.

Konfigurieren eines Speicheradapters für das Starten über ein SAN

Wenn Sie Ihren Host zum Starten über ein SAN einrichten, aktivieren Sie den Startadapter im BIOS des Hosts. Sie können den Startadapter zum Initiieren einer einfachen Verbindung mit der Ziel-Start-LUN konfigurieren.

Voraussetzungen

Bestimmen Sie den WWPN für den Speicheradapter.

Verfahren

- Konfigurieren Sie den Speicheradapter für das Starten über ein SAN.

  Da die Konfiguration von Startadaptern anbieterabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Anbieters.

Einrichten des Systems zum Starten vom Installationsmedium

Wenn Sie Ihren Host zum Starten vom SAN einrichten, starten Sie den Host zuerst vom VMware-Installationsmedium. Um vom Installationsmedium aus zu starten, ändern Sie die Startreihenfolge in den BIOS-Einstellungen des Systems.

Lesen Sie die entsprechenden Anweisungen in der Herstellerdokumentation, da das Ändern der Startsequenz im BIOS herstellerspezifisch ist. Der folgende Vorgang erläutert, wie Sie die Startsequenz auf einem IBM-Host ändern können.

Verfahren

1. Schalten Sie das System ein und starten Sie das BIOS-Konfigurationsprogramm.
2. Wählen Sie **Startup Options** und drücken Sie die Eingabetaste.
3. Wählen Sie **Startup Sequence Options** und drücken Sie die Eingabetaste.
4. Setzen Sie die Option von **First Startup Device** auf **[CD-ROM]**.

Ergebnisse

Sie können ESXi jetzt installieren.

Konfigurieren des Emulex HBAs für das Starten über ein SAN

Die Konfiguration des Emulex-BA-IOS zum Starten von einem SAN beinhaltet die Aktivierung der BIOS-Einstellung zur Startauswahl und die Aktivierung des BIOS.

Verfahren

1 Aktivieren der BIOS-Einstellung zur Startauswahl

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie die BIOS-Einstellung zur Startauswahl aktivieren.

2 Aktivieren des BIOS

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie das BIOS aktivieren.

Aktivieren der BIOS-Einstellung zur Startauswahl

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie die BIOS-Einstellung zur Startauswahl aktivieren.

Verfahren

1 Führen Sie `lputil` aus.

2 Wählen Sie **3. Firmware Maintenance**.

3 Wählen Sie einen Adapter.

4 Wählen Sie **6. Boot BIOS Maintenance**.

5 Wählen Sie **1. Enable Boot BIOS**.

Aktivieren des BIOS

Wenn Sie das Emulex-HBA-BIOS zum Starten von ESXi über ein SAN konfigurieren, müssen Sie das BIOS aktivieren.

Verfahren

1 Starten Sie den Host neu.

2 Drücken Sie zum Konfigurieren der Adapterparameter ALT+E an der Emulex-Eingabeaufforderung und führen Sie diese Schritte aus.

a Wählen Sie einen Adapter (mit BIOS-Unterstützung).

b Wählen Sie **2. Configure This Adapter's Parameters.**

c Wählen Sie **1. Enable or Disable BIOS.**

d Wählen Sie **1**, um das BIOS zu aktivieren.

e Wählen Sie **x** zum Beenden und **Esc**, um zum Hauptmenü zurückzukehren.

3 Führen Sie zum Konfigurieren des Startgeräts diese Schritte vom Emulex-Hauptmenü aus.
   a Wählen Sie denselben Adapter.
   b Wählen Sie **1. Configure Boot Devices.**
   c Wählen Sie den Speicherort für den Starteintrag aus.
   d Geben Sie das zweistellige Startgerät ein.
   e Geben Sie die zweistellige (HEX) Start-LUN ein (z. B. **08**).
   f Wählen Sie die Start-LUN.
   g Wählen Sie **1. WWPN.** (Starten Sie dieses Gerät mit WWPN, nicht DID).
   h Wählen Sie **x** zum Beenden und **Y**, um neu zu starten.
4 Starten Sie im System-BIOS, und entfernen Sie zunächst Emulex aus der Start-Controller-Reihenfolge.
5 Führen Sie einen Neustart und die Installation auf einer SAN-LUN durch.

Konfigurieren des QLogic-HBAs für das Starten über ein SAN

Mit diesem Beispiel wird erläutert, wie der QLogic-HBA für das Starten von ESXi über ein SAN konfiguriert wird. Die Prozedur umfasst die Aktivierung des QLogic-HBA-BIOS, die Aktivierung der Startauswahloption sowie die Auswahl der Start-LUN.

Verfahren

1 Drücken Sie beim Starten des Servers **STRG+Q**, um das Fast!UTIL-Konfigurationsdienstprogramm zu starten.
2 Führen Sie, abhängig von der Anzahl an HBAs, die entsprechende Aktion aus.

Option	Beschreibung
Ein HBA	Wenn Sie über nur einen HBA verfügen, wird die Seite „Fast!UTIL-Optionen“ angezeigt. Wechseln Sie zu Schritt 3.
Mehrere HBAs	Wenn mehr als ein HBA vorhanden ist, wählen Sie den HBA manuell aus. a Verwenden Sie auf der Seite „Select Host Adapter“ die Pfeiltasten, um den Zeiger auf dem gewünschten HBA zu positionieren. b Drücken Sie die **Eingabetaste**.

3 Wählen Sie auf der Seite mit den Fast!UTIL-Optionen **Konfigurationseinstellungen** und drücken Sie die **Eingabetaste**.
4 Wählen Sie auf der Seite mit den Konfigurationseinstellungen die Option **Adaptereinstellungen** und drücken Sie die **Eingabetaste**.

5 Stellen Sie das BIOS so ein, dass eine Suche nach SCSI-Geräten ausgeführt wird.

   a Wählen Sie auf der Seite mit den Hostadaptereinstellungen die Option **Host Adapter BIOS**.

   b Drücken Sie die **Eingabetaste**, um den Wert auf **Aktiviert** zu setzen.

   c Drücken Sie zum Beenden die **Esc**-Taste.

6 Aktivieren Sie die Startauswahl.

   a Wählen Sie **Startauswahleinstellung** aus und drücken Sie die **Eingabetaste**.

   b Wählen Sie auf der Seite für das auswählbare Starten die Option **Startauswahl**.

   c Drücken Sie die **Eingabetaste**, um den Wert auf **Aktiviert** zu setzen.

7 Wählen Sie den BPN (Boot Port Name)-Eintrag in der Liste der Speicherprozessoren (SPs) aus und drücken Sie die **Eingabetaste**.

   Die Seite „Fibre-Channel-Gerät auswählen“ wird geöffnet.

8 Wählen Sie den gewünschten Speicherprozessor aus und drücken Sie die **Eingabetaste**.

   Bei Verwendung eines Aktiv-Passiv-Speicher-Arrays muss sich der ausgewählte Speicherprozessor auf dem bevorzugten (aktiven) Pfad zur Start-LUN befinden. Wenn Sie nicht sicher sind, welcher Speicherprozessor sich auf dem aktiven Pfad befindet, können Sie diesen mithilfe der Speicher-Array-Verwaltungssoftware ermitteln. Die Ziel-IDs werden vom BIOS erstellt und können sich bei jedem Neustart ändern.

9 Führen Sie, abhängig von der Anzahl der dem Speicherprozessor zugeordneten HBAs, die entsprechende Aktion aus.

Option	Beschreibung
Eine LUN	Die LUN ist als Start-LUN ausgewählt. Sie müssen auf der Seite für die Auswahl der LUN keine Auswahl treffen.
Mehrere LUNs	Die Seite „LUN auswählen“ wird geöffnet. Wählen Sie über den Zeiger die Start-LUN aus und drücken Sie die **Eingabetaste**.

10 Sollten weitere Speicherprozessoren in der Liste angezeigt werden, drücken Sie **C**, um die Daten zu löschen.

11 Drücken Sie **ESC** zwei Mal, um den Bildschirm zu verlassen, und drücken Sie die **Eingabetaste**, um die Einstellung zu speichern.

Starten von ESXi mit Software FCoE

8

ESXi unterstützt das Starten von FCoE-fähigen Netzwerkadaptern.

Nur Netzwerkkarten mit teilweisem FCoE-Offload unterstützen die Startfunktionen mit der Software FCoE. Wenn Sie die Netzwerkkarten ohne FCoE-Offload verwenden, wird der Software-FCoE-Start nicht unterstützt.

Wenn Sie ESXi von einem FCoE LUN installieren und starten, kann der Host einen VMware-Software FCoE-Adapter und einen Netzwerkadapter mit FCoE-Funktionen verwenden. Der Host benötigt keinen dedizierten FCoE HBA.

Sie führen die meisten Konfigurationen über den Parameter `option ROM` Ihres Netzwerkadapters aus. Die Netzwerkadapter müssen eines der folgenden Formate unterstützen, die die Parameter über ein FCoE-Startgerät an VMkernel kommunizieren.

- FCoE Boot Firmware Table (FBFT). FBFT ist Eigentum von Intel.
- FCoE Boot Parameter Table (FBPT). FBPT wird von VMware für Drittanbieter definiert, um Software FCoE Boot zu implementieren.

Die Konfigurationsparameter sind im Parameter `option ROM` Ihres Adapters festgelegt. Während einer ESXi-Installation oder einem nachfolgenden Startvorgang werden diese Parameter entweder im FBFT-Format oder im FBPT-Format in den Systemspeicher exportiert. Der VMkernel kann die Konfigurationseinstellungen lesen und diese zum Zugriff auf das Start-LUN verwenden.

Dieses Kapitel enthält die folgenden Themen:

Anforderungen und Überlegungen für das Starten mit Software FCoE

Wenn Sie den ESXi-Host aus SAN mit Software FCoE starten, gelten bestimmte Anforderungen und Überlegungen.

Anforderungen

- Verwenden Sie eine kompatible ESXi-Version.
- Der Netzwerkadapter muss folgende Fähigkeiten aufweisen:
  - Er muss FCoE-fähig sein.
  - Er muss ESXi Open FCoE Stack unterstützen.
  - Er muss FCoE-Start-Firmware enthalten, die Startinformationen im FBFT-Format oder FBPT-Format exportieren kann.

Überlegungen

- Sie können die Software FCoE-Startkonfiguration aus ESXi nicht ändern.
- Coredump wird auf keinen Software FCoE LUNs unterstützt, einschließlich der Start-LUN.
- Mehrfachpfade werden vor dem Start nicht unterstützt.
- Start-LUN kann mit anderen Hosts auch bei gemeinsam genutztem Speicher nicht gemeinsam genutzt werden. Stellen Sie sicher, dass der Host Zugriff auf die gesamte Start-LUN hat.

Einrichten des Startens mit Software FCoE

Ihr ESXi-Host kann von einer FCoE LUN mit dem Software FCoE-Adapter und einem Netzwerkadapter starten.

Wenn Sie Ihren Host für einen Software-FCoE-Start konfigurieren, führen Sie eine Reihe von Aufgaben aus.

Voraussetzungen

Der Netzwerkadapter hat folgende Fähigkeiten:

- Unterstützt teilweise FCoE Offloads (Software FCoE).
- Enthält eine FCoE Boot Firmware Table (FBFT) oder eine FCoE Boot Parameter Table (FBPT).

Informationen über Netzwerkadapter, die Software FCoE-Starts unterstützen, finden Sie unter *VMware-Kompatibilitätshandbuch*.

Verfahren

1 Konfigurieren der Parameter für das Starten mit Software FCoE

  Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte FCoE-Start-Firmware verfügen, um einen Software-FCoE-Startvorgang zu unterstützen. Wenn Sie die Firmware konfigurieren, aktivieren Sie den Adapter für den Software-FCoE-Start und geben Sie die Start-LUN-Parameter an.

2 Installieren und Starten von ESXi von Software FCoE LUN

Wenn Sie ein System einrichten, das von einer Software FCoE LUN startet, installieren Sie das ESXi-Image auf der Ziel-LUN. Sie können dann Ihren Host von dieser LUN starten.

Konfigurieren der Parameter für das Starten mit Software FCoE

Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte FCoE-Start-Firmware verfügen, um einen Software-FCoE-Startvorgang zu unterstützen. Wenn Sie die Firmware konfigurieren, aktivieren Sie den Adapter für den Software-FCoE-Start und geben Sie die Start-LUN-Parameter an.

Verfahren

- Geben Sie in der Option ROM des Netzwerkadapters die Software-FCoE-Start-Parameter an.

  Diese Parameter enthalten ein Startziel, eine Start-LUN, eine VLAN-ID usw.

  Da die Konfiguration des Netzwerkadapters anbieterabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Anbieters.

Installieren und Starten von ESXi von Software FCoE LUN

Wenn Sie ein System einrichten, das von einer Software FCoE LUN startet, installieren Sie das ESXi-Image auf der Ziel-LUN. Sie können dann Ihren Host von dieser LUN starten.

Voraussetzungen

- Konfigurieren Sie den `option ROM` des Netzwerkadapters, sodass er auf eine Ziel-Start-LUN verweist. Achten Sie darauf, dass Sie die Informationen über die hochfahrbare LUN haben.
- Ändern Sie die BIOS-Startsequenz im System-BIOS auf die folgende Sequenz:
  a Netzwerkadapter, den Sie für das Starten mit Software FCoE benutzen.
  b ESXi-Installationsmedien.

  Weitere Informationen hierzu finden Sie in der Anbieterdokumentation für Ihr System.

Verfahren

1 Starten Sie eine interaktive Installation von den ESXi-Installationsmedien.

  Das ESXi-Installationsprogramm überprüft, dass das Starten mit FCoE im BIOS aktiviert ist, und erstellt erforderlichenfalls einen virtuellen Standard-Switch für den FCoE-fähigen Netzwerkadapter. Der Name des vSwitch ist VMware_FCoE_vSwitch. Das Installationsprogramm verwendet dann vorkonfigurierte FCoE-Startparameter zum Erkennen und Anzeigen aller verfügbaren FCoE LUNs.

2 Wählen Sie auf der Seite **Festplatte auswählen** die Software-FCoE-LUN aus, die Sie in der Startparametereinstellung angegeben haben.

  Wenn die Start-LUN in diesem Menü nicht erscheint, vergewissern Sie sich, dass Sie die Startparameter im `option ROM` des Netzwerkadapters richtig konfiguriert haben.

3 Schließen Sie die Installation ab, indem Sie die folgenden Schritte durchführen.

4 Starten Sie den Host neu.

5 Ändern Sie die Startreihenfolge im System-BIOS, sodass die FCoE-Boot-LUN das erste startbare Gerät ist.

   ESXi setzt das Starten von der Software FCoE LUN fort, bis die Betriebsbereitschaft hergestellt ist.

Nächste Schritte

Erforderlichenfalls können Sie den VMware_FCoE_vSwitch umbenennen und ändern, den das Installationsprogramm automatisch erstellt hat. Achten Sie darauf, dass der Cisco Discovery Protocol-Modus (CDP) auf „Überwachen“ oder „Beide“ eingestellt ist.

Problembehebung beim Starten über Software-FCoE für einen ESXi-Host

Wenn die Installation oder das Starten von ESXi über eine FCoE-LUN fehlschlägt, können Sie mehrere Fehlerbehebungsmethoden verwenden.

Problem

Wenn Sie ESXi über einen FCoE-Speicher installieren oder starten, schlägt entweder die Installation oder der Start fehl. Das von Ihnen verwendete FCoE-Setup enthält einen VMware-Software-FCoE-Adapter und einen Netzwerkadapter mit Teilfunktionen für FCoE-Offload.

Lösung

- Stellen Sie sicher, dass Sie die Startparameter im Option-ROM des FCoE-Netzwerkadapters richtig konfiguriert haben.
- Überwachen Sie während der Installation das BIOS des FCoE-Netzwerkadapters auf etwaige Fehler.
- Überprüfen Sie das VMkernel-Protokoll auf Fehler, falls dies möglich ist.
- Verwenden Sie den Befehl `esxcli`, um sich zu vergewissern, dass die Start-LUN vorhanden ist.

```
esxcli conn_options hardware bootdevice list
```

Best Practices für Fibre-Channel-Speicher

9

Beachten Sie die Empfehlung zur Vermeidung von Leistungsproblemen, wenn Sie ESXi mit Fibre-Channel-SAN verwenden.

Der vSphere Client bietet umfangreiche Funktionen zur Erfassung von Leistungsdaten. Die Informationen werden grafisch angezeigt und ständig aktualisiert.

Zudem können Sie das `resxtop`- oder das `esxtop`-Befehlszeilenprogramm verwenden. Die Dienstprogramme liefern detaillierte Informationen darüber, wie ESXi Ressourcen verwendet. Weitere Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Erkundigen Sie sich bei Ihrem Speicheranbieter, ob Ihr Speichersystem die Hardwarebeschleunigungsfunktionen der Storage-APIs für die Array-Integration unterstützt. Wenn ja, lesen Sie in der Dokumentation Ihres Anbieters nach, um die Unterstützung für die Hardwarebeschleunigung auf dem Speichersystem zu aktivieren. Weitere Informationen finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.

Dieses Kapitel enthält die folgenden Themen:

Vermeiden von Fibre-Channel-SAN-Problemen

Bei Verwendung von ESXi mit einem Fibre-Channel-SAN müssen Sie bestimmte Richtlinien befolgen, um SAN-Probleme zu vermeiden.

Beachten Sie folgende Tipps, um Probleme mit der SAN-Konfiguration zu vermeiden:

- Platzieren Sie nur einen einzigen VMFS-Datenspeicher in jeder LUN.
- Ändern Sie die vom System festgelegte Pfadrichtlinie nur, wenn Sie die Auswirkungen dieser Änderung kennen und verstehen.
- Erstellen Sie eine ausführliche Dokumentation. Notieren Sie Informationen zu Zoning, Zugriffssteuerung, Speicher, Switch, Server und FC-HBA-Konfiguration, Software- und Firmware-Versionen sowie zum Speicherkabelplan.

- Erstellen Sie einen Notfallplan bei Ausfällen:
  - Kopieren Sie Ihre Topologiezuordnungen mehrfach. Ermitteln Sie für jedes Element, welche Auswirkungen ein Ausfall dieses Elements auf das SAN hat.
  - Überprüfen Sie alle Verbindungen, Switches, HBAs und anderen Elemente, um sicherzugehen, dass Sie keine wichtige Fehlerstelle in Ihrem Design übersehen haben.
- Stellen Sie sicher, dass die FC-HBAs an den geeigneten Steckplätzen des Hosts installiert sind (basierend auf Steckplatz- und Busgeschwindigkeit). Richten Sie einen PCI-Bus-Lastausgleich für alle Busse des Servers ein.
- Machen Sie sich mit den verschiedenen Überwachungspunkten in Ihrem Speichernetzwerk an allen Sichtbarkeitspunkten vertraut (einschließlich Leistungsdiagrammen für Hosts sowie Statistiken zu FC-Switches und Speicherleistung).
- Seien Sie beim Ändern der IDs der LUNs vorsichtig, die über von Ihrem ESXi-Host verwendete VMFS-Datenspeicher verfügen. Wenn Sie die ID ändern, wird der Datenspeicher inaktiv und seine virtuellen Maschinen fallen aus. Signieren Sie den Datenspeicher neu, um ihn wieder zu aktivieren. Weitere Informationen hierzu finden Sie unter Verwalten von duplizierten VMFS-Datenspeichern.

  Nachdem Sie die ID der LUN geändert haben, prüfen Sie zum Zurücksetzen der ID auf dem Host den Speicher erneut. Weitere Informationen über das erneute Prüfen finden Sie unter Vorgänge zum erneuten Prüfen des Speichers.

Deaktivieren der automatischen Registrierung von ESXi-Hosts

Für bestimmte Speicher-Arrays ist die Registrierung der ESXi-Hosts bei den Arrays erforderlich. ESXi führt die Hostregistrierung automatisch aus, indem es den Namen und die IP-Adresse des Hosts an das Array sendet. Schalten Sie die ESXi-Funktion für die automatische Registrierung aus, wenn Sie es vorziehen, die Registrierung manuell mithilfe von Speicherverwaltungssoftware durchzuführen.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Wählen Sie unter „Erweiterte Systemeinstellungen“ den Parameter **Disk.EnableNaviReg** aus und klicken Sie auf das Symbol **Bearbeiten**.
5. Ändern Sie den Wert in 0.

Ergebnisse

Mit diesem Vorgang wird die standardmäßig aktivierte automatische Hostregistrierung deaktiviert.

Optimieren der Fibre-Channel-SAN-Speicherleistung

Bei der Optimierung einer typischen SAN-Umgebung müssen verschiedene Faktoren berücksichtigt werden.

Wenn die Umgebung ordnungsgemäß konfiguriert ist, leisten die SAN-Fabric-Komponenten (insbesondere die SAN-Switches) aufgrund ihrer geringen Latenz im Vergleich zu Servern und Speicher-Arrays lediglich einen geringen Beitrag. Stellen Sie sicher, dass die Pfade durch das Switch-Fabric nicht ausgelastet sind, d. h. das Switch-Fabric wird mit dem höchsten Durchsatz ausgeführt.

Speicher-Array-Leistung

Einer der wichtigsten Faktoren für die Optimierung einer kompletten SAN-Umgebung ist die Speicher-Array-Leistung.

Bei Problemen mit der Speicher-Array-Leistung ziehen Sie die entsprechende Dokumentation des Speicher-Array-Herstellers zu Rate.

Befolgen Sie die folgenden allgemeinen Richtlinien, um die Array-Leistung in der vSphere-Umgebung zu erhöhen:

- Bedenken Sie beim Zuweisen von LUNs, dass möglicherweise mehrere Hosts auf die LUN zugreifen und auf jedem Host mehrere virtuelle Maschinen ausgeführt werden können. Auf einer LUN, die von einem Host verwendet wird, sind E/A-Vorgänge von einer Vielzahl von unterschiedlichen Anwendungen möglich, die unter verschiedenen Betriebssystemen ausgeführt werden. Aufgrund dieser unterschiedlichen Arbeitslast enthält die RAID-Gruppe mit den ESXi-LUNs in der Regel keine LUNs, die von anderen Servern verwendet werden, auf denen ESXi nicht ausgeführt wird.
- Stellen Sie sicher, dass der Lese-/Schreibcache verfügbar ist.
- SAN-Speicher-Arrays müssen kontinuierlich neu ausgelegt und optimiert werden, um sicherzustellen, dass die E/A-Last auf alle Speicher-Array-Pfade verteilt ist. Um diese Anforderung zu erfüllen, verteilen Sie die Pfade zu den LUNs auf alle Speicherprozessoren. Das Ergebnis ist ein optimaler Lastausgleich. Eine sorgfältige Überwachung zeigt an, wann die LUN-Verteilung ausgeglichen werden muss.

  Bei der Optimierung von Speicher-Arrays mit statischem Lastausgleich ist die Überwachung der spezifischen Leistungsstatistiken, z. B. E/A-Vorgänge pro Sekunde, Blocks pro Sekunde und Reaktionszeit, von größter Bedeutung. Das Verteilen der LUN-Arbeitslast auf alle Speicherprozessoren ist ebenfalls wichtig.

  Hinweis Der dynamische Lastausgleich wird mit ESXi zurzeit nicht unterstützt.

Serverleistung mit Fibre-Channel

Um eine optimale Serverleistung sicherzustellen, sind verschiedene Faktoren zu berücksichtigen.

Der Zugriff jeder Serveranwendung auf den integrierten Speicher muss mit den folgenden Bedingungen gewährleistet sein:

- Hohe E/A-Rate (Anzahl an E/A-Vorgängen pro Sekunde)
- Hoher Durchsatz (MB pro Sekunde)
- Minimale Latenz (Reaktionszeiten)

Da für jede Anwendung andere Anforderungen gelten, können Sie diese Ziele erreichen, indem Sie eine geeignete RAID-Gruppe für das Speicher-Array wählen.

Zum Erreichen von Leistungszielen halten Sie sich an die folgenden Richtlinien:

- Platzieren Sie jede LUN in einer RAID-Gruppe, die die erforderlichen Leistungsebenen bietet. Überwachen Sie die Aktivitäten und Ressourcennutzung anderer LUNs in der zugewiesenen RAID-Gruppe. Mit einer hochleistungsfähigen RAID-Gruppe mit zu vielen Anwendungen, die eine E/A-Last verursachen, können die Leistungsziele möglicherweise nicht erreicht werden, die für eine Anwendung auf dem ESXi-Host erforderlich sind.
- Stellen Sie sicher, dass jeder Host über ausreichend HBAs verfügt, um für die Anwendungen auf dem Host den Durchsatz in der Spitzenzeit zu erhöhen. Bei Verteilung der E/A-Last auf mehrere HBAs wird ein höherer Durchsatz und eine geringere Latenz für jede Anwendung erreicht.
- Um Redundanz für einen potenziellen HBA-Ausfall zu gewährleisten, stellen Sie sicher, dass der Host mit einem redundanten Dual-Fabric verbunden ist.
- Beachten Sie, dass beim Zuweisen von LUNs oder RAID-Gruppen für ESXi-Systeme diese Ressourcen durch mehrere Betriebssysteme gemeinsam verwendet werden. Die vom ESXi-Host erforderliche LUN-Leistung könnte viel höher als die Leistung sein, die normale physische Maschinen benötigen. Wenn Sie z. B. die Ausführung von vier E/A-intensiven Anwendungen planen, weisen Sie für die ESXi-LUNs die vierfache Leistungskapazität zu.
- Wenn Sie mehrere ESXi-Systeme mit vCenter Server verwenden, erhöhen sich die Leistungsanforderungen für das Speichersubsystem entsprechend.
- Die Anzahl an ausstehenden E/A-Vorgängen von Anwendungen, die auf dem ESXi-System ausgeführt werden, muss mit der Anzahl an E/A-Vorgängen übereinstimmen, die der HBA und das Speicher-Array verarbeiten können.

Verwenden von ESXi mit iSCSI-SAN

10

ESXi kann mit dem Internet SCSI (iSCSI)-Protokoll eine Verbindung zu einem externen SAN-Speicher herstellen. Zusätzlich zum herkömmlichen iSCSI-Protokoll unterstützt ESXi auch iSCSI-Erweiterungen für RDMA (iSER).

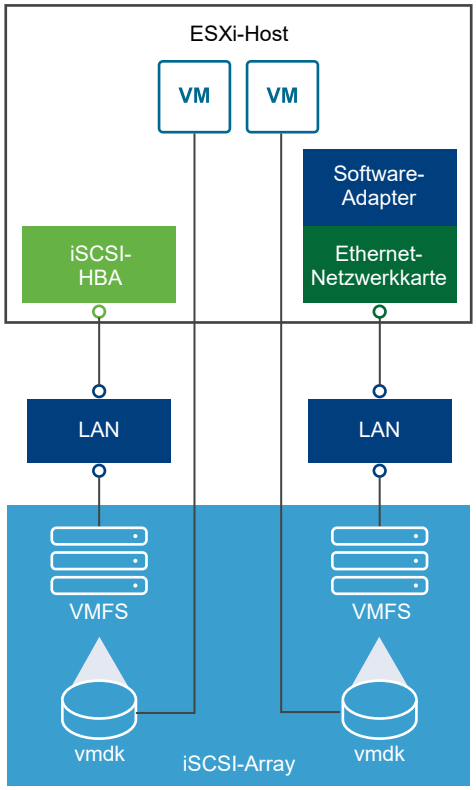
Wenn das iSER-Protokoll aktiviert ist, kann der Host dasselbe iSCSI-Framework verwenden, ersetzt dabei aber den TCP/IP-Transport durch den Remote Direct Memory Access (RDMA)-Transport.

Dieses Kapitel enthält die folgenden Themen:

Informationen zu iSCSI-SAN

iSCSI-SANs verwenden Ethernetverbindungen für die Datenübertragung zwischen Hosts und Hochleistungsspeicher-Subsystemen.

Auf der Hostseite enthalten die iSCSI-SAN-Komponenten iSCSI-Hostbusadapter (HBAs) oder Netzwerkkarten (NICs). Das iSCSI-Netzwerk umfasst zudem Switches und Router, die den Speicherdatenverkehr weiterleiten, Verkabelung, Speicherprozessoren (SPs) und Speicherfestplattensysteme.



Das iSCSI-SAN verwendet eine Client-Server-Architektur.

Der Client, der so genannte iSCSI-Initiator, ist auf Ihrem ESXi-Host installiert. Er startet iSCSI-Sitzungen, indem er SCSI-Befehle ausgibt und diese im iSCSI-Protokoll gekapselt an einen iSCSI-Server überträgt. Der Server ist als iSCSI-Ziel bekannt. Dieses iSCSI-Ziel repräsentiert in der Regel ein physisches Speichersystem im Netzwerk.

Das Ziel kann ebenfalls ein virtuelles iSCSI-SAN sein, z. B. ein in einer virtuellen Maschine ausgeführter iSCSI-Zielemulator. Das iSCSI-Ziel reagiert auf die Befehle des Initiators, indem es die erforderlichen iSCSI-Daten überträgt.

iSCSI-Multipathing

Bei der Datenübertragung zwischen dem Hostserver und dem Speicher nutzt das SAN eine Technik, die als Multipathing bezeichnet wird. Mit Multipathing kann Ihr ESXi-Host über mehrere physische Pfade zu einer LUN in einem Speichersystem verfügen.

In der Regel besteht ein einzelner Pfad von einem Host zu einer LUN aus einem iSCSI-Adapter oder der Netzwerkkarte, Switch-Ports, Verbindungskabeln und dem Speicher-Controller-Port. Falls eine Komponente des Pfads ausfällt, wählt der Host für E/A-Vorgänge einen anderen verfügbaren Pfad. Der Prozess der Erkennung eines ausgefallenen Pfads und des Wechsels auf einen anderen Pfad wird als Pfad-Failover bezeichnet.

Weitere Informationen zum Multipathing finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.

Knoten und Ports im iSCSI-SAN

Ein einzelnes erkennbares Element eines iSCSI-SAN, z. B. ein Initiator oder ein Ziel, stellt einen iSCSI-Knoten dar.

Jeder Knoten hat einen Knotennamen. ESXi verwendet verschiedene Methoden zur Identifizierung eines Knotens.

IP-Adresse

Jeder iSCSI-Knoten kann über eine eigene IP-Adresse verfügen, sodass Router und Switches im Netzwerk eine Verbindung zwischen dem Host und dem Speicher aufbauen können. Diese Adresse ist mit der IP-Adresse vergleichbar, die Sie Ihrem Computer zuweisen, um auf das Unternehmensnetzwerk oder das Internet zugreifen zu können.

iSCSI-Name

Ein weltweit eindeutiger Name zum Identifizieren des Knotens. iSCSI verwendet die Formate IQN (iSCSI Qualified Name) und EUI (Extended Unique Identifier).

ESXi generiert standardmäßig eindeutige iSCSI-Namen für Ihre iSCSI-Initiatoren, zum Beispiel `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Der Standardname muss daher in der Regel nicht geändert werden. Wenn Sie ihn dennoch ändern, stellen Sie sicher, dass der neue iSCSI-Name weltweit eindeutig ist.

iSCSI-Alias

Ein besser verwaltbarer Name für ein iSCSI-Gerät oder einen iSCSI-Port, der anstelle des iSCSI-Namens verwendet wird. iSCSI-Aliase sind nicht eindeutig und werden zur benutzerfreundlichen Benennung von Ports verwendet.

Jeder Knoten besitzt mindestens einen Port, der mit dem SAN verbunden wird. iSCSI-Ports sind Endpunkte einer iSCSI-Sitzung.

iSCSI-Benennungskonventionen

iSCSI verwendet einen speziellen, eindeutigen Bezeichner zum Identifizieren eines iSCSI-Knotens, sei es ein Ziel oder ein Initiator.

iSCSI-Namen können zwei verschiedene Formate aufweisen. Das geläufigste Format ist IQN.

Weitere Informationen zu iSCSI-Benennungskonventionen und Zeichenfolgenprofilen finden Sie unter RFC 3721 und RFC 3722 auf der IETF-Website.

iSCSI Qualified Name-Format

Das IQN-Format (iSCSI Qualified Name) hat die Form `iqn.yyyy-mm.naming-authority:unique`, wobei:

- *yyyy-mm* das Jahr und den Monat angibt, in dem die Stelle für die Namensvergabe (Naming Authority) eingerichtet wurde.

- *Namensvergabestelle* in der Regel die Syntax des Internetdomänennames der Namensvergabestelle in umgekehrter Reihenfolge angibt. Die `iscsi.vmware.com`-Namensvergabestelle kann das IQN-Format (iSCSI Qualified Name) `iqn.1998-01.com.vmware.iscsi` aufweisen. Der Name gibt an, dass der Domänenname `vmware.com` im Januar 1998 registriert wurde und `iscsi` eine von `vmware.com` verwaltete Unterdomäne ist.
- *eindeutiger_Name* steht für einen beliebigen Namen, z. B. den Namen des Hosts. Die Namensvergabestelle muss sicherstellen, dass alle zugewiesenen Namen nach dem Doppelpunkt eindeutig sind, z. B.:
  - `iqn.1998-01.com.vmware.iscsi:name1`
  - `iqn.1998-01.com.vmware.iscsi:name2`
  - `iqn.1998-01.com.vmware.iscsi:name999`

Enterprise Unique Identifier-Format

Das EUI-Format (Enterprise Unique Identifier) hat die Form `eui.16_hex_digits`.

Beispiel: `eui.0123456789ABCDEF`.

Bei den 16 Hexadezimalstellen handelt es sich um die Textdarstellung einer 64-Bit-Zahl eines IEEE-EUI-Schemas (Extended Unique Identifier). Die oberen 24 Bit identifizieren die Unternehmens-ID, die das IEEE einem bestimmten Unternehmen zuordnet. Die restlichen 40 Bit werden durch die Entität zugewiesen, der diese Unternehmens-ID zugeordnet ist, und müssen eindeutig sein.

iSCSI-Initiatoren

Für den Zugriff auf iSCSI-Ziele verwendet Ihr ESXi-Host iSCSI-Initiatoren.

Der Initiator ist eine auf Ihrem ESXi-Host installierte Software oder Hardware. Der iSCSI-Initiator stellt die Kommunikation zwischen Ihrem Host und einem externen iSCSI-Speichersystem her und sendet Daten an das Speichersystem.

In der ESXi-Umgebung übernehmen die auf Ihrem Host konfigurierten iSCSI-Adapter die Initiatorrolle. ESXi unterstützt verschiedene iSCSI-Adaptertypen.

Weitere Informationen zum Konfigurieren und Verwenden der iSCSI-Adapter finden Sie unter Kapitel 11 Konfigurieren von iSCSI- und iSER-Adapter und -Speicher.

Software-iSCSI-Adapter

Ein Software-iSCSI-Adapter ist ein im VMkernel integrierter VMware-Code. Wenn Sie den Software-iSCSI-Adapter verwenden, kann Ihr Host über Standardnetzwerkadapter eine Verbindung zum iSCSI-Speichergerät herstellen. Der Software iSCSI-Adapter dient der iSCSI-Verarbeitung und kommuniziert gleichzeitig mit dem Netzwerkadapter. Mit dem Software iSCSI-Adapter können Sie die iSCSI-Technologie verwenden, ohne besondere Hardware erwerben zu müssen.

Hardware iSCSI-Adapter

Bei einem Hardware-iSCSI-Adapter handelt es sich um einen Adapter eines Drittanbieters, der die gesamte iSCSI- und Netzwerkverarbeitung von Ihrem Host auslagert. Hardware-iSCSI-Adapter werden in Kategorien unterteilt.

Abhängige Hardware-iSCSI-Adapter

Hängt vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen ab, die von VMware zur Verfügung gestellt werden.

Bei diesem Adaptertyp kann es sich um eine Karte handeln, die einen Standard-Netzwerkadapter und die iSCSI-Offload-Funktion für denselben Port bietet. Die iSCSI-Offload-Funktion ist hinsichtlich des Abrufens der IP- und der MAC-Adresse sowie anderer Parameter für iSCSI-Sitzungen von der Netzwerkkonfiguration des Hosts abhängig. Ein Beispiel für einen abhängigen Adapter ist die iSCSI-lizenzierte Broadcom 5709-Netzwerkkarte.

Unabhängige Hardware-iSCSI-Adapter

Implementiert ein eigenes Netzwerk und eigene iSCSI-Konfigurations- und -Verwaltungsschnittstellen.

In der Regel handelt es sich bei einem unabhängigen Hardware-iSCSI-Adapter um eine Karte, die entweder nur die iSCSI-Offload-Funktion oder die iSCSI-Offload-Funktion und die standardmäßige Netzwerkkartenfunktion bietet. Die iSCSI-Offload-Funktion besitzt eine unabhängige Konfigurationsverwaltung, die die IP- und die MAC-Adresse sowie andere Parameter für die iSCSI-Sitzungen zuweist. Ein Beispiel für einen unabhängigen Adapter ist der QLogic QLA4052-Adapter.

Hardware-iSCSI-Adapter müssen möglicherweise lizenziert werden. Anderenfalls werden sie im Client oder in vSphere-CLI möglicherweise nicht angezeigt. Fragen Sie Ihren Anbieter nach Lizenzierungsinformationen.

Verwenden des iSER-Protokolls mit ESXi

Zusätzlich zum herkömmlichen iSCSI.Protokoll unterstützt ESXi auch die iSCSI-Erweiterungen für RDMA (kurz iSER-Protokoll genannt). Wenn das iSER-Protokoll aktiviert ist, kann das iSCSI-Framework auf dem ESXi-Host RDMA (Remote Direct Memory Access) anstelle von TCP/IP für den Transport verwenden.

Das herkömmliche iSCSI-Protokoll überträgt SCSI-Befehle über ein TCP/IP-Netzwerk zwischen einem iSCSI-Initiator auf einem Host und einem iSCSI-Ziel auf einem Speichergerät. Das iSCSI-Protokoll kapselt die Befehle und stellt diese Daten in Paketen für die TCP/IP-Schicht zusammen. Wenn die Daten beim Ziel eintreffen, disassembliert das iSCSI-Protokoll die TCP/IP-Pakete, sodass die SCSI-Befehle identifiziert und an das Speichergerät übergeben werden können.

iSER unterscheidet sich vom herkömmlichen iSCSI-Protokoll dadurch, dass es das TCP/IP-Datenübertragungsmodell durch den RDMA-Transport (Remote Direct Memory Access) ersetzt. Mithilfe der direkten Datenplatzierungstechnologie von RDMA kann das iSER-Protokoll Daten direkt zwischen den Arbeitsspeicher-Puffern des ESXi-Hosts und den Speichergeräten übertragen. Diese Methode vermeidet unnötige TCP/IP-Verarbeitung und unnötiges Kopieren von Daten und kann zudem die Latenzzeit und die CPU-Last auf dem Speichergerät reduzieren.

In der iSER-Umgebung arbeitet iSCSI genauso wie bisher, verwendet jedoch anstelle der TCP/IP-basierten Schnittstelle eine zugrunde liegende RDMA-Fabric-Schnittstelle.

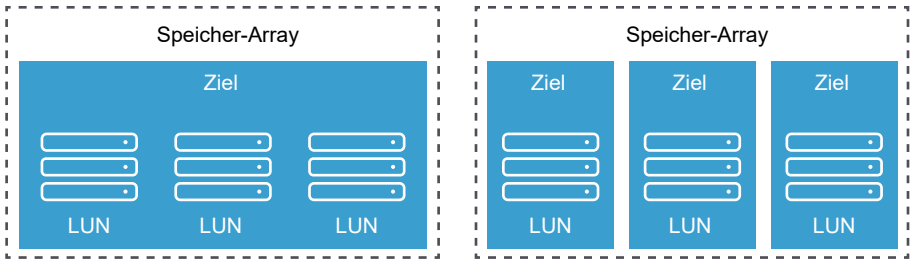
Da das iSER-Protokoll die Kompatibilität mit der iSCSI-Infrastruktur bewahrt, ähnelt der Prozess der Aktivierung von iSER auf dem ESXi-Host dem entsprechenden iSCSI-Prozess. Weitere Informationen hierzu finden Sie unter Konfigurieren von iSER-Adaptern mit ESXi.

Herstellen von iSCSI-Verbindungen

Im ESXi-Kontext beschreibt der Begriff „Ziel“ eine einzelne Speichereinheit, auf die Ihr Host zugreifen kann. Die Begriffe „Speichergerät“ und „LUN“ beschreiben ein logisches Volume, das Speicherplatz auf einem Ziel darstellt. In der Regel stehen die Begriffe „Gerät“ und „LUN“ im ESXi-Kontext für ein SCSI-Volume, das Ihrem Host von einem Speicherziel angeboten wird und formatiert werden kann.

Verschiedene iSCSI-Speicheranbieter verwenden unterschiedliche Methoden, um Speicher für Hosts bereitzustellen. Einige Anbieter stellen mehrere LUNs auf einem einzigen Ziel dar, während andere Anbieter mehrere Ziele mit je einer LUN verknüpfen.

Abbildung 10-1. Ziel im Vergleich zu LUN-Darstellungen



In diesen Beispielen stehen für jede dieser Konfigurationen drei LUNs zur Auswahl. Im ersten Fall erkennt der Host ein Ziel, obwohl in diesem Ziel drei LUNs vorhanden sind, die verwendet werden können. Jede LUN steht für ein einzelnes Speichervolume. Im zweiten Fall werden dem Host drei unterschiedliche Ziele mit je einer LUN angezeigt.

Hostbasierte iSCSI-Initiatoren richten nur Verbindungen zu jedem Ziel ein. Das bedeutet, dass sich der LUN-Datenverkehr bei Speichersystemen mit einem Ziel, das mehrere LUNs umfasst, auf diese eine Verbindung konzentriert. Sind in einem System drei Ziele mit je einer LUN vorhanden, bestehen drei Verbindungen zwischen dem Host und den drei verfügbaren LUNs.

Diese Informationen sind nützlich, wenn Sie versuchen, Speicherdatenverkehr für mehrere Verbindungen vom Host mit mehreren iSCSI-Adaptern zusammenzufassen. Sie können den Datenverkehr für ein Ziel auf einen bestimmten Adapter festlegen und einen anderen Adapter für den Datenverkehr an ein anderes Ziel verwenden.

iSCSI-Speichersystemtypen

ESXi unterstützt verschiedene Speichersysteme und Arrays.

Zu den Speichertypen, die Ihr Host unterstützt, gehören Aktiv-Aktiv, Aktiv-Passiv und ALUA-konform.

Aktiv-Aktiv-Speichersystem

Unterstützt den gleichzeitigen Zugriff auf die LUNs über alle Speicherports, die ohne wesentlichen Leistungsabfall verfügbar sind. Alle Pfade sind immer aktiviert, es sei denn, ein Pfad schlägt fehl.

Aktiv-Passiv-Speichersystem

Ein System, in dem ein Speicherprozessor aktiv den Zugriff auf eine vorhandene LUN ermöglicht. Die anderen Prozessoren fungieren als Sicherung für die LUN und können den Zugriff auf andere LUN-E/A-Vorgänge aktiv bereitstellen. E/A-Daten können ausschließlich an einen aktiven Port gesendet werden. Falls der Zugriff über den aktiven Speicherport fehlschlägt, kann einer der passiven Speicherprozessoren durch die Server, die auf ihn zugreifen, aktiviert werden.

Asymmetrisches Speichersystem

Unterstützt Asymmetric Logical Unit Access (ALUA). ALUA-konforme Speichersysteme bieten verschiedene Zugriffsebenen für einzelne Ports. Mit ALUA können Hosts die Zustände von Zielports bestimmen und Pfade priorisieren. Der Host verwendet einige der aktiven Pfade als primäre Pfade und andere als sekundäre Pfade.

Speichersystem mit virtuellem Port

Unterstützt den Zugriff auf alle verfügbaren LUNs über einen einzigen virtuellen Port. Speichersysteme mit virtuellen Ports sind Aktiv/Aktiv-Speichergeräte, die jedoch die Vielzahl der Verbindungen über einen einzigen Port verdecken. ESXi-Multipathing stellt nicht standardmäßig mehrere Verbindungen von einem bestimmten Port zum Speichersystem her. Einige Speicheranbieter bieten Sitzungs-Manager an, um mehrere Verbindungen zu den von ihnen vertriebenen Speichersystemen herzustellen und zu verwalten. Port-Failover und der Verbindungsausgleich werden von diesen Speichersystemen transparent verarbeitet. Diese Funktion wird häufig als transparentes Failover bezeichnet.

Erkennung, Authentifizierung und Zugriffssteuerung

Sie können mehrere Mechanismen verwenden, um Ihren Speicher zu erkennen und den Zugriff darauf zu beschränken.

Damit die Richtlinie für die Speicherzugriffssteuerung unterstützt wird, müssen Sie den Host und das iSCSI-Speichersystem konfigurieren.

Erkennung

Eine Erkennungssitzung ist Teil des iSCSI-Protokolls und gibt die auf einem iSCSI-Speichersystem verfügbaren Ziele zurück. ESXi bietet zwei verschiedene Erkennungsmethoden: dynamisch und statisch. Bei der dynamische Erkennung wird eine Liste der zugänglichen Ziele vom iSCSI-Speichersystem abgerufen. Bei der statischen Erkennung kann nur auf ein bestimmtes Ziel über den Zielnamen und die Adresse zugegriffen werden.

Weitere Informationen finden Sie unter Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host.

Authentifizierung

Die Authentifizierung durch iSCSI-Speichersysteme erfolgt nach Name und Schlüsselpaar. ESXi unterstützt das CHAP-Authentifizierungsprotokoll. Sowohl für den ESXi-Host als auch für das iSCSI-Speichersystem muss das CHAP-Protokoll aktiviert sein und beide müssen die gleichen Anmeldeinformationen verwenden, um die CHAP-Authentifizierung verwenden zu können.

Informationen zum Aktivieren von CHAP finden Sie unter Konfigurieren von CHAP-Parametern für iSCSI- oder iSER-Speicheradapter..

Zugriffssteuerung

Zugriffssteuerung ist eine auf dem iSCSI-Speichersystem eingerichtete Richtlinie. Eine Vielzahl der Implementierungen unterstützen mindestens eine der drei folgenden Arten der Zugriffssteuerung:

- Nach Initiatorname
- Nach IP-Adresse
- Nach dem CHAP-Protokoll

Nur Initiatoren, die alle Richtlinien einhalten, können auf das iSCSI-Volume zugreifen.

Die ausschließliche Verwendung von CHAP für die Zugriffssteuerung kann zu einer Verlangsamung von erneuten Prüfungen führen, da ESXi zwar alle Ziele ermitteln kann, aber bei der Authentifizierung fehlschlägt. iSCSI kann schneller neu prüfen, wenn der Host nur die Ziele erkennt, die er authentifizieren kann.

Zugriff auf Daten in einem iSCSI-SAN durch virtuelle Maschinen

ESXi speichert Festplattendateien einer virtuellen Maschine in einem VMFS-Datenspeicher, der sich auf einem SAN-Speichergerät befindet. Sobald Gastbetriebssysteme der virtuellen Maschine SCSI-Befehle an die virtuellen Festplatten senden, übersetzt die SCSI-Virtualisierungsebene diese Befehle in VMFS-Dateivorgänge.

Wenn eine virtuelle Maschine mit seinen auf einem SAN gespeicherten virtuellen Festplatten interagiert, finden die folgenden Prozesse statt:

1 Wenn das Gastbetriebssystem in einer virtuellen Maschine zum Lesen oder Schreiben auf eine SCSI-Festplatte zugreifen muss, sendet dieses SCSI-Befehle an die virtuelle Festplatte.

2 Gerätetreiber im Betriebssystem der virtuellen Maschine kommunizieren mit den virtuellen SCSI-Controllern.

3 Der virtuelle SCSI-Controller leitet die Befehle an den VMkernel weiter.

4 Der VMkernel führt die folgenden Aufgaben aus.

   a sucht im VMFS-Volume nach einer entsprechenden virtuellen Festplattendatei.

   b ordnet die Anforderungen für die Blöcke auf der virtuellen Festplatte den Blöcken auf dem entsprechenden physischen Gerät zu.

   c sendet die geänderte E/A-Anforderung vom Gerätetreiber im VMkernel an den iSCSI-Initiator (Hardware oder Software).

5 Handelt es sich bei dem iSCSI-Initiator um einen Hardware-iSCSI-Adapter (unabhängig oder abhängig), führt der Adapter die folgenden Aufgaben aus.

   a kapselt die E/A-Anforderungen in iSCSI-PDUs (Protocol Data Units).

   b kapselt iSCSI-PDUs in TCP/IP-Pakete.

   c sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.

6 Handelt es sich bei dem iSCSI-Initiator um einen Software-iSCSI-Adapter, findet der folgende Prozess statt.

   a Der iSCSI-Initiator kapselt E/A-Anforderungen in iSCSI-PDUs.

   b Der Initiator sendet SCSI-PDUs über TCP/IP-Verbindungen.

   c Der VMkernel-TCP/IP-Stack gibt TCP/IP-Pakete an eine physische Netzwerkkarte weiter.

   d Die physische Netzwerkkarte sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.

7 Ethernet-Switches und -Router im Netzwerk leiten die Anforderung an das entsprechende Speichergerät weiter.

Fehlerkorrektur

Um die Integrität von iSCSI-Headern und -Daten zu schützen, legt das iSCSI-Protokoll Methoden zur Fehlerkorrektur fest, die als Header- und Daten-Digests bezeichnet werden.

Beide Parameter sind standardmäßig deaktiviert, können aber von Benutzern aktiviert werden. Diese Digests beziehen sich auf den Header bzw. die SCSI-Daten, die zwischen iSCSI-Initiatoren und -Zielen in beiden Richtungen übertragen werden.

Header- und Daten-Digests überprüfen die Integrität unverschlüsselter Daten. Diese Prüfung geht über die Integritätsprüfungen hinaus, die andere Netzwerkebenen bereitstellen (z. B. TCP und Ethernet). Die Digests prüfen den gesamten Kommunikationspfad mit allen Elementen, die den Datenverkehr auf Netzwerkebene ändern können, wie Router, Switches und Proxys.

Die Bereitstellung und Art dieser Digests wird verhandelt, sobald eine iSCSI-Verbindung aufgebaut wird. Wenn der Initiator und das Ziel einer Digest-Konfiguration zustimmen, muss dieses Digest für den gesamten Datenverkehr zwischen diesem Initiator und dem Ziel verwendet werden.

Die Aktivierung von Header- und Daten-Digests erfordert eine zusätzliche Verarbeitung durch den Initiator und das Ziel, was zu einer Beeinträchtigung des Durchsatzes und der CPU-Leistung führen kann.

Hinweis Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen aus und reduzieren damit die Auswirkungen auf die Leistung.

Weitere Informationen zum Aktivieren von Header-Digests und Daten-Digests finden Sie unter Konfigurieren erweiterter Parameter für iSCSI.

Konfigurieren von iSCSI- und iSER-Adapter und -Speicher

11

Bevor ESXi mit iSCSI-SAN arbeiten kann, müssen Sie Ihre iSCSI-Umgebung einrichten.

Die Vorbereitung Ihrer iSCSI-Umgebung umfasst die folgenden Schritte:

Schritt	Details
Einrichten des iSCSI-Speichers	Informationen dazu finden Sie in der Dokumentation Ihres Speicheranbieters. Halten Sie sich darüber hinaus an diese Empfehlungen: ■ ESXi und iSCSI-SAN – Empfehlungen und Einschränkungen ■ Kapitel 13 Best Practices für iSCSI-Speicher
Konfigurieren von iSCSI/iSER-Adaptern	Verwenden Sie für die Adapterkonfiguration einen geeigneten Workflow: ■ Einrichten von unabhängigen Hardware-iSCSI-Adaptern ■ Konfigurieren von abhängigen Hardware-iSCSI-Adaptern ■ Konfigurieren des Software-iSCSI-Adapters ■ Konfigurieren von iSER-Adaptern mit ESXi
Erstellen eines Datenspeichers im iSCSI-Speicher	Erstellen von Datenspeichern

Dieses Kapitel enthält die folgenden Themen:

- ESXi und iSCSI-SAN – Empfehlungen und Einschränkungen
- Konfigurieren von iSCSI-Parametern für Adapter
- Einrichten von unabhängigen Hardware-iSCSI-Adaptern
- Konfigurieren von abhängigen Hardware-iSCSI-Adaptern
- Konfigurieren des Software-iSCSI-Adapters
- Konfigurieren von iSER-Adaptern mit ESXi
- Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter
- Einrichten eines Netzwerks für iSCSI und iSER
- Verwenden von Jumbo-Frames mit iSCSI und iSER
- Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host
- Entfernen dynamischer oder statischer iSCSI-Ziele
- Konfigurieren von CHAP-Parametern für iSCSI- oder iSER-Speicheradapter.

- Konfigurieren erweiterter Parameter für iSCSI
- iSCSI-Sitzungsverwaltung

ESXi und iSCSI-SAN – Empfehlungen und Einschränkungen

Um mit iSCSI-SAN ordnungsgemäß arbeiten zu können, muss Ihre ESXi-Umgebung bestimmte Empfehlungen befolgen. Darüber hinaus sind bei der Verwendung von ESXi mit iSCSI-SAN einige Einschränkungen zu beachten.

Empfehlungen für die Verwendung von iSCSI-Speicher

- Stellen Sie sicher, dass Ihr ESXi-Host die iSCSI-SAN-Speicherhardware und -firmware unterstützt. Eine aktuelle Liste finden Sie unter *VMware-Kompatibilitätshandbuch*.
- Damit der Host die LUNs beim Start erkennt, müssen alle iSCSI-Speicherziele so konfiguriert werden, dass Ihr Host darauf zugreifen und sie verwenden kann. Zudem sollten Sie Ihren Host so konfigurieren, dass er alle verfügbaren iSCSI-Ziele erkennen kann.
- Sofern Sie keine festplattenlosen Server einsetzen, richten Sie eine Diagnosepartition auf einem lokalen Speicher ein. Wenn Sie über festplattenlose Server verfügen, die von einem iSCSI-SAN gestartet werden, finden Sie weitere Informationen über Diagnosepartitionen mit iSCSI unter Allgemeine Empfehlungen für das Starten von iSCSI-SAN.
- Installieren Sie den SCSI Controller-Treiber im Gastbetriebssystem, damit Sie eine ausreichende Größe der Warteschlange festlegen können.
- Erhöhen Sie auf virtuellen Maschinen unter Microsoft Windows den Wert des SCSI-Parameters `TimeoutValue`. Mit dieser Parametereinstellung können Windows-VMs E/A-Verzögerungen besser tolerieren, die aus einem Pfad-Failover resultieren. Weitere Informationen hierzu finden Sie unter Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen.
- Konfigurieren Sie Ihre Umgebung so, dass für jede LUN nur ein VMFS-Datenspeicher konfiguriert ist.

Einschränkungen bezüglich der Verwendung von iSCSI-Speicher

- ESXi unterstützt keine über iSCSI verbundenen Bandlaufwerke.
- Sie können keine Multipathing-Software für virtuelle Maschinen verwenden, um einen E/A-Lastausgleich für eine einzelne physische LUN durchzuführen.
- ESXi unterstützt kein Multipathing, wenn Sie unabhängige Hardwareadapter mit Software- oder abhängigen Hardwareadaptern kombinieren.

Konfigurieren von iSCSI-Parametern für Adapter

Bevor Ihr ESXi-Host iSCSI-Speicher erkennen kann, müssen Sie Ihre iSCSI-Adapter konfigurieren. Wenn Sie die Adapter konfigurieren, legen Sie mehrere iSCSI-Parameter fest.

iSCSI-Netzwerk

Für bestimmte iSCSI-Adaptertypen müssen Sie VMkernel-Netzwerke konfigurieren.

Mit dem Dienstprogramm `vmkping` können Sie die Netzwerkkonfiguration überprüfen.

Für den unabhängigen Hardware-iSCSI-Adapter sind keine VMkernel-Netzwerke erforderlich. Sie können Netzwerkparameter, wie z. B. eine IP-Adresse, eine Subnetzmaske und ein Standard-Gateway, auf dem unabhängigen Hardware-iSCSI-Adapter konfigurieren.

Alle iSCSI-Adaptertypen unterstützen IPv4- und IPv6-Protokolle.

iSCSI-Adapter (vmhba)	Beschreibung	VMkernel-Netzwerk	Adapternetzwerkeinstellungen
Unabhängige Hardware-iSCSI-Adapter	Adapter eines Drittanbieters, der die iSCSI- und Netzwerk-Verarbeitung und -Verwaltung von Ihrem Host auslagert.	Nicht erforderlich.	Weitere Informationen hierzu finden Sie unter Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI.
Software-iSCSI-Adapter	Verwendet Standardnetzwerkkarten, um Ihren Host mit einem Remote-iSCSI-Ziel auf dem IP-Netzwerk zu verbinden.	Erforderlich. Weitere Informationen hierzu finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.	n.v.
Abhängige Hardware-iSCSI-Adapter	Adapter eines Drittanbieters, der vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen abhängt.	Erforderlich Weitere Informationen hierzu finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.	Nicht verfügbar
VMware-iSER-Adapter	Verwendet einen RDMA-fähigen Netzwerkadapter, um Ihren Host mit einem Remote-iSCSI-Ziel zu verbinden.	Erforderlich Weitere Informationen hierzu finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.	Nicht verfügbar

Erkennungsmethoden

Für alle iSCSI-Adaptertypen müssen Sie die dynamische Erkennungsadresse oder die statische Erkennungsadresse festlegen. Darüber hinaus müssen Sie einen Zielnamen des Speichersystems angeben. Für Software-iSCSI und abhängiges Hardware-iSCSI muss die Adresse mithilfe von `vmkping` angepingt werden können.

Weitere Informationen hierzu finden Sie unter Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host.

CHAP-Authentifizierung

Aktivieren Sie den CHAP-Parameter auf dem Initiator und der Speichersystemseite. Nach der Aktivierung der Authentifizierung wird er auf alle Ziele angewendet, die noch nicht erkannt wurden. Er wird nicht auf Ziele angewendet, die bereits erkannt wurden.

Weitere Informationen hierzu finden Sie unter Konfigurieren von CHAP-Parametern für iSCSI- oder iSER-Speicheradapter..

Einrichten von unabhängigen Hardware-iSCSI-Adaptern

Ein unabhängiger Hardware-iSCSI-Adapter ist ein spezielle Adapter von Drittanbietern, die über TCP/IP auf iSCSI-Speicher zugreifen kann. Dieser iSCSI-Adapter steuert die gesamte iSCSI- und Netzwerk-Verarbeitung und -Verwaltung für das ESXi-System.

Voraussetzungen

- Überprüfen Sie, ob der Adapter lizenziert werden muss.
- Installieren Sie den Adapter auf Ihrem ESXi-Host.

Informationen zur Lizenzierung, Installation sowie zu Firmware-Updates finden Sie in der Herstellerdokumentation.

Das Einrichten des unabhängigen Hardware-iSCSI-Adapters umfasst die folgenden Schritte.

Schritt	Beschreibung
Anzeigen abhängiger Hardware-iSCSI-Adapter	Zeigen Sie einen unabhängigen Hardware-iSCSI-Adapter an und überprüfen Sie, ob er korrekt installiert und konfigurationsbereit ist.
Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter	Falls erforderlich, können Sie den Standard-iSCSI-Namen und den Alias ändern, die Ihren iSCSI-Adaptern zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.
Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI	Ändern Sie die Standardnetzwerkeinstellungen, sodass der Adapter für das iSCSI-SAN ordnungsgemäß konfiguriert ist.
Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host	Richten Sie die dynamische Erkennung ein. Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.
Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter	Wenn Ihre iSCSI-Umgebung das Challenge Handshake Authentication Protocol (CHAP) verwendet, konfigurieren Sie es für Ihren Netzwerkadapter.
Aktivieren von Jumbo-Frames für unabhängige Hardware-iSCSI	Wenn Ihre Umgebung iSCSI Jumbo-Frames unterstützt, aktivieren Sie diese für den Adapter.

Anzeigen abhängiger Hardware-iSCSI-Adapter

Zeigen Sie auf dem ESXi-Host einen unabhängigen Hardware-iSCSI-Adapter an und stellen Sie sicher, das dieser installiert und konfigurationsbereit ist.

Nachdem Sie einen unabhängigen Hardware-iSCSI-Adapter auf dem Host installiert haben, wird er in der Liste der Speicheradapter angezeigt, die zum Konfigurieren zur Verfügung stehen. Seine Eigenschaften können angezeigt werden.

Voraussetzungen

Erforderliche Berechtigung:**Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter**.

Falls installiert, sollte der Hardware-iSCSI-Adapter in der Liste der Speicheradapter angezeigt werden.

4 Wählen Sie die anzuzeigenden Adapter aus.

Die standardmäßigen Detailinformationen zu dem Adapter werden angezeigt.

Adapterinformationen	Beschreibung
Modell	Adaptermodell.
iSCSI-Name	Ein in Übereinstimmung mit den iSCSI-Standards erstellter eindeutiger Name, der den FC-Adapter eindeutig identifiziert. Sie können den iSCSI-Namen bearbeiten.
iSCSI-Alias	Ein benutzerfreundlicher Name, der anstelle des iSCSI-Namens verwendet wird. Sie können das iSCSI-Alias bearbeiten.
IP-Adresse	Eine dem iSCSI-HBA zugewiesene Adresse.
Ziele	Die Anzahl der Ziele, auf die über den Adapter zugegriffen wurde.
Geräte	Alle Speichergeräte oder LUNs, auf die der Adapter zugreifen kann.
Pfade	Alle vom Adapter zum Zugreifen auf Speichergeräte verwendeten Pfade.

Bearbeiten der Netzwerkeinstellungen für Hardware-iSCSI

Nach der Installation eines unabhängigen Hardware-iSCSI-Adapters auf einem ESXi-Host müssen Sie möglicherweise die Standardnetzwerkeinstellungen ändern, damit der Adapter ordnungsgemäß für das iSCSI-SAN konfiguriert ist.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.

4 Klicken Sie auf die Registerkarte **Netzwerkeinstellungen** und anschließend auf **Bearbeiten**.

5 Deaktivieren Sie „IPv6“ im Abschnitt „IPv4-Einstellungen“ oder wählen Sie die Methode zum Abrufen von IP-Adressen aus.

Hinweis Die automatische DHCP-Option und die statische Option schließen sich gegenseitig aus.

Option	Beschreibung
Keine IPv4-Einstellungen	Deaktivieren Sie IPv4.
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden.
Statische IPv4-Einstellungen verwenden	Geben Sie die IPv4 IP-Adresse, die Subnetzmaske und das Standard-Gateway für den iSCSI-Adapter ein.

6 Deaktivieren Sie „IPv6“ im Abschnitt „IPv6-Einstellungen“ oder wählen Sie eine geeignete Option zum Abrufen von IPv6-Adressen aus.

Hinweis Automatische Optionen und die statische Option schließen sich gegenseitig aus.

Option	Beschreibung
Keine IPv6-Einstellungen	Deaktivieren Sie IPv6.
IPv6 aktivieren	Wählen Sie eine Option zum Abrufen von IPv6-Adressen aus.
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Verbindungslokale Adresse für IPv6 überschreiben	Überschreiben Sie die Link-Local IP-Adresse durch Konfigurieren einer statischen IP-Adresse.
Statische IPv6-Adressen	a Klicken Sie auf **Hinzufügen**, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf **OK**.

7 Geben Sie im Abschnitt „DNS-Einstellungen“ IP-Adressen für einen bevorzugten DNS-Server und einen alternativen DNS-Server an.

Sie müssen beide Werte angeben.

Konfigurieren von abhängigen Hardware-iSCSI-Adaptern

Ein abhängiger Hardware-iSCSI-Adapter ist ein Drittanbieter-Adapter, der vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen abhängt, die von VMware zur Verfügung gestellt werden.

Ein Beispiel für einen abhängigen iSCSI-Adapter ist eine Broadcom 5709-Netzwerkkarte. Wenn er auf einem Host installiert ist, präsentiert er seine beiden Komponenten, einen Standard-Netzwerkadapter und eine iSCSI-Engine, demselben Port. Die iSCSI-Engine wird als iSCSI-Adapter in der Liste der Speicheradapter (vmhba) angezeigt.

Der iSCSI-Adapter ist standardmäßig aktiviert. Damit er funktionsfähig ist, müssen Sie ihn jedoch über einen virtuellen VMkernel-Adapter (vmk) mit einem ihm zugeordneten physischen Netzwerkadapter (vmnic) verbinden. Anschließend können Sie den iSCSI-Adapter konfigurieren.

Nachdem Sie den abhängigen Hardware-iSCSI-Adapter konfiguriert haben, werden die Ermittlungs- und Authentifizierungsdaten über die Netzwerkverbindung geleitet. Der iSCSI-Datenverkehr wird unter Umgehung des Netzwerks über die iSCSI-Engine geleitet.

Der gesamte Installations- und Konfigurationsprozess für die abhängigen Hardware-iSCSI-Adapter besteht aus mehreren Schritten.

Schritt	Beschreibung
Abhängige Hardware-iSCSI-Adapter anzeigen	Zeigen Sie einen abhängigen Hardware-iSCSI-Adapter an, um zu überprüfen, ob er korrekt geladen ist.
Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter	Ändern Sie ggf. den Standard-iSCSI-Namen und den Alias, die Ihrem Adapter zugewiesen wurden.
Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern	Sie müssen Netzwerkverbindungen erstellen, um abhängige iSCSI- und physische Netzwerkadapter zu binden. Um die Verbindungen ordnungsgemäß zu erstellen, ermitteln Sie den Namen der physischen Netzwerkkarte, der der abhängige Hardware-iSCSI-Adapter zugewiesen werden soll.
Konfigurieren der Port-Bindung für iSCSI oder iSER	Konfigurieren Sie Verbindungen für den Datenverkehr zwischen der iSCSI-Komponente und den physischen Netzwerkadaptern. Der Prozess der Konfiguration von diesen Verbindungen wird als Port-Bindung bezeichnet.
Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host	Richten Sie die dynamische Erkennung ein. Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.
Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter	Wenn Ihre iSCSI-Umgebung das Challenge Handshake Authentication Protocol (CHAP) verwendet, konfigurieren Sie es für Ihren Netzwerkadapter.
Einrichten von CHAP für Ziele	Sie können auch verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.
Aktivieren von Jumbo-Frames für Netzwerke	Wenn Ihre Umgebung iSCSI Jumbo-Frames unterstützt, aktivieren Sie diese für den Adapter.

Überlegungen zu abhängigen Hardware-iSCSI-Adaptern

Wenn Sie abhängige Hardware-iSCSI-Adapter für ESXi verwenden, muss Folgendes beachtet werden.

- Wenn Sie einen abhängigen Hardware-iSCSI-Adapter verwenden, zeigt der Leistungsbericht für eine dem Adapter zugewiesene Netzwerkkarte möglicherweise wenig oder keine Aktivität, selbst wenn eine große Menge an iSCSI-Datenverkehr vorhanden ist. Dieses Verhalten tritt auf, weil der iSCSI-Datenverkehr den regulären Netzwerkstack umgeht.
- Falls Sie einen virtuellen Switch eines Drittanbieters einsetzen, z. B. Cisco Nexus 1000V DVS, deaktivieren Sie das automatische Binden. Verwenden Sie stattdessen das manuelle Binden und stellen Sie dabei sicher, dass Sie einen VMkernel-Adapter (vmk) mit einer entsprechenden physischen Netzwerkkarte (vmnic) verbinden. Weitere Informationen finden Sie in der Herstellerdokumentation zu Ihrem virtuellen Switch.
- Der Broadcom iSCSI-Adapter führt eine Datenumwandlung in Hardware mit begrenztem Pufferspeicher durch. Wenn Sie den Broadcom iSCSI-Adapter in einem ausgelasteten oder überlasteten Netzwerk verwenden, aktivieren Sie die Flusssteuerung, damit die Leistung nicht beeinträchtigt wird.

  Die Flusssteuerung überwacht die Datenübertragungsrate zwischen zwei Knoten und verhindert, dass ein langsamer Empfänger von einem schnellen Sender überrannt wird. Um optimale Ergebnisse zu erzielen, aktivieren Sie die Flusssteuerung an den Endpunkten des E/A-Pfads, d. h. auf den Hosts und den iSCSI-Speichersystemen.

  Verwenden Sie den Befehl `esxcli system module parameters`, um die Flusskontrolle für den Host zu aktivieren. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1013413.
- Abhängige Hardware-Adapter unterstützen IPv4 und IPv6.

Abhängige Hardware-iSCSI-Adapter anzeigen

Zeigen Sie auf einem ESXi-Host einen abhängigen Hardware-iSCSI-Adapter an, um sicherzustellen, dass dieser korrekt geladen wurde.

Der abhängige Hardware-iSCSI-Adapter (vmhba#) wird, wenn er installiert ist, in der Liste der Speicheradapter unter Kategorien wie z. B. „Broadcom iSCSI Adapter“ angezeigt. Falls der abhängige Hardware-Adapter nicht in der Liste der Speicheradapter angezeigt wird, überprüfen Sie, ob er lizenziert werden muss. Informationen finden Sie in der Dokumentation des Anbieters.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter**.

4 Wählen Sie die anzuzeigenden Adapter (vmhba#) aus.

   Es werden die standardmäßigen Detailinformationen zu dem Adapter angezeigt, etwa iSCSI-Namen, iSCSI-Alias und Status.

Nächste Schritte

Obwohl der abhängige iSCSI-Adapter standardmäßig aktiviert ist, müssen Sie, damit er funktionsbereit ist, eine Vernetzung für den iSCSI-Datenverkehr einrichten und den Adapter an den entsprechenden VMkernel-iSCSI-Port binden. Konfigurieren Sie dann die Erkennungsadressen und die CHAP-Parameter.

Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern

Auf einem ESXi-Host verbinden Netzwerkverbindungen abhängige iSCSI und physische Netzwerkadapter. Um die Verbindungen ordnungsgemäß zu erstellen, müssen Sie den Namen der physischen Netzwerkkarte ermitteln, der der abhängige Hardware-iSCSI-Adapter zugewiesen werden soll.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter**.

4 Wählen Sie den iSCSI-Adapter (vmhba#) aus und klicken Sie unter „Adapterdetails“ auf die Registerkarte **Netzwerk-Port-Bindung**.

5 Klicken Sie auf **Hinzufügen**.

   Der Netzwerkadapter (vmnic#), der dem abhängigen iSCSI-Adapter zugeordnet ist, wird in der Spalte „Physischer Netzwerkadapter“ aufgeführt.

Nächste Schritte

Wenn die Spalte „VMkernel-Adapter“ leer ist, erstellen Sie einen VMkernel-Adapter (vmk#) für den physischen Netzwerkadapter (vmnic#) und binden Sie beide an den zugewiesenen abhängigen Hardware-iSCSI. Weitere Informationen hierzu finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.

Konfigurieren des Software-iSCSI-Adapters

Bei der softwarebasierten iSCSI-Implementierung können Sie Standard-Netzwerkkarten verwenden, um Ihren Host mit einem externen iSCSI-Ziel im IP-Netzwerk zu verbinden. Der in ESXi integrierte Software-iSCSI-Adapter ermöglicht diese Verbindung, indem er über den Netzwerkstack mit den physischen Netzwerkkarten kommuniziert.

Beachten Sie bei der Verwendung von Software-iSCSI-Adaptern die folgenden Punkte:

- Legen Sie einen separaten Netzwerkadapter für iSCSI fest. Verwenden Sie iSCSI nicht bei Adaptern mit 100 MBit/s oder weniger.
- Vermeiden Sie die harte Kodierung des Namens des Softwareadapters „vmhbaXX“ in den Skripts. Der Name kann sich von einer ESXi-Version zur nächsten ändern. Die Änderung kann zu Fehlern bei vorhandenen Skripts führen, wenn darin der alte hartkodierte Name verwendet wird. Die Namensänderung wirkt sich nicht auf das Verhalten des Software-iSCSI-Adapters aus.

Die Konfiguration des Software-iSCSI-Adapters erfolgt in mehreren Schritten.

Schritt	Beschreibung
Aktivieren und Deaktivieren des Software-iSCSI-Adapters	Aktivieren Sie Ihren Software-iSCSI-Adapter, damit er von Ihrem Host für den Zugriff auf den iSCSI-Speicher verwendet werden kann.
Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter	Ändern Sie ggf. den Standard-iSCSI-Namen und den Alias, die Ihrem Adapter zugewiesen wurden.
Konfigurieren der Port-Bindung für iSCSI oder iSER	Konfigurieren Sie Verbindungen für den Datenverkehr zwischen der iSCSI-Komponente und den physischen Netzwerkadaptern. Der Prozess der Konfiguration von diesen Verbindungen wird als Port-Bindung bezeichnet.
Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host	Richten Sie die dynamische Erkennung ein. Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSCSI-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSCSI-System liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.
Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter	Wenn Ihre iSCSI-Umgebung das Challenge Handshake Authentication Protocol (CHAP) verwendet, konfigurieren Sie es für Ihren Netzwerkadapter.
Einrichten von CHAP für Ziele	Sie können auch verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.
Aktivieren von Jumbo-Frames für Netzwerke	Wenn Ihre Umgebung iSCSI Jumbo-Frames unterstützt, aktivieren Sie diese für den Adapter.

Aktivieren und Deaktivieren des Software-iSCSI-Adapters

Sie müssen Ihren Software-iSCSI-Adapter aktivieren, damit er von Ihrem ESXi-Host für den Zugriff auf den iSCSI-Speicher verwendet werden kann. Wenn Sie den Software-iSCSI-Adapter nach der Aktivierung nicht benötigen, können Sie ihn deaktivieren.

Sie können nur einen Software-iSCSI-Adapter aktivieren.

Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Hinweis Wenn Sie von iSCSI mithilfe des Software-iSCSI-Adapters starten, wird der Adapter aktiviert und die Netzwerkkonfiguration wird beim ersten Boot-Vorgang erstellt. Wenn Sie den Adapter deaktivieren, wird er bei jedem Neustart des Hosts erneut aktiviert.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Aktiviert bzw. deaktiviert den Adapter.

Option	Beschreibung
Aktivieren des Software-iSCSI-Adapters	a Klicken Sie unter **Speicher** auf **Speicheradapter** und anschließend auf das Symbol **Hinzufügen**. b Wählen Sie **Software-iSCSI-Adapter** aus und bestätigen Sie, dass Sie den Adapter hinzufügen möchten. Der Software-iSCSI-Adapter (vmhba#) wird aktiviert und erscheint in der Liste der Speicheradapter. Nachdem Sie den Adapter aktiviert haben, weist ihm der Host den Standard-iSCSI-Namen zu. Sie können jetzt die Adapterkonfiguration abschließen.
Deaktivieren des Software-iSCSI-Adapters	a Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den Adapter (vmhba#) aus, der deaktiviert werden soll. b Klicken Sie auf die Registerkarte **Eigenschaften (Properties)**. c Klicken Sie auf **Deaktivieren** und bestätigen Sie, dass Sie den Adapter deaktivieren möchten. Der Status zeigt an, dass der Adapter deaktiviert wurde. d Starten Sie den Host neu. Nach dem Neustart wird der Adapter nicht mehr in der Liste der Speicheradapter angezeigt. Die dem Adapter zugeordneten Speichergeräte sind nicht länger zugänglich. Sie können den Adapter zu einem späteren Zeitpunkt aktivieren.

Konfigurieren von iSER-Adaptern mit ESXi

Zusätzlich zum herkömmlichen iSCSI.Protokoll unterstützt ESXi auch die iSCSI-Erweiterungen für RDMA (kurz iSER-Protokoll genannt). Wenn das iSER-Protokoll aktiviert ist, kann das iSCSI-Framework auf dem ESXi-Host RDMA (Remote Direct Memory Access) anstelle von TCP/IP für den Transport verwenden. Sie können iSER auf Ihrem ESXi-Host konfigurieren.

Weitere Informationen zum iSER-Protokoll finden Sie unter Verwenden des iSER-Protokolls mit ESXi.

Der gesamte Installations- und Konfigurationsprozess für VMware iSER umfasst mehrere Schritte.

Schritt	Beschreibung
Installieren und Anzeigen eines RDMA-fähigen Netzwerkadapters	Zum Konfigurieren von iSER mit ESXi müssen Sie zunächst einen RDMA-fähigen Netzwerkadapter installieren, wie z. B. Mellanox Technologies MT27700 Family ConnectX-4. Nachdem Sie diesen Adaptertyp installiert haben, zeigt der vSphere Client seine beiden Komponenten an: einen RDMA-Adapter und einen physischen Netzwerkadapter `vmnic#`.
Aktivieren des VMware iSER-Adapters	Um den RDMA-fähigen Adapter für iSCSI verwenden zu können, aktivieren Sie die VMware iSER-Speicherkomponente mithilfe der `esxcli`. Die Komponente wird im vSphere Client als `vmhba#`-Speicheradapter in der Kategorie „VMware iSCSI over RDMA (iSER)-Adapter“ angezeigt.
Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter	Ändern Sie bei Bedarf den Standardnamen und den Aliasnamen, der dem iSER-Speicheradapter zugeordnet ist.`vmhba#`
Konfigurieren der Port-Bindung für iSCSI oder iSER	Sie müssen Netzwerkverbindungen erstellen, um die iSER-Speicheradapter `vmhba#` und den RDMA-fähigen Netzwerkadapter `vmnic#` miteinander zu verbinden. Der Prozess der Konfiguration von diesen Verbindungen wird als Port-Bindung bezeichnet. **Hinweis** NIC-Gruppierung wird von iSER nicht unterstützt. Verwenden Sie bei der Konfiguration der Port-Bindung nur einen RDMA-Adapter pro vSwitch.
Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host	Richten Sie die dynamische oder statische Erkennung für den iSER-Speicheradapter `vmhba#` ein. Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator ein angegebenes iSER-Speichersystem kontaktiert, eine „SendTargets“-Anforderung an das System übermittelt. Das iSER-System gibt als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Bei der statischen Erkennung geben Sie die Informationen für die Ziele manuell ein.
Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter	Wenn in Ihrer Umgebung das CHAP-Protokoll (Challenge Handshake Authentication Protocol) verwendet wird, konfigurieren Sie es für den iSER-Speicheradapter `vmhba#`.
Einrichten von CHAP für Ziele	Sie können auch verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.
Aktivieren von Jumbo-Frames für Netzwerke	Wenn in Ihrer Umgebung Jumbo-Frames unterstützt werden, aktivieren Sie diese für den iSER-Speicheradapter `vmhba#`.

Installieren und Anzeigen eines RDMA-fähigen Netzwerkadapters

ESXi unterstützt RDMA-fähige Netzwerkadapter, z. B. Mellanox Technologies MT27700 Family ConnectX-4. Nachdem Sie einen solchen Adapter auf Ihrem Host installiert haben, zeigt der vSphere Client seine beiden Komponenten an, einen RDMA-Adapter und einen physischen Netzwerkadapter.

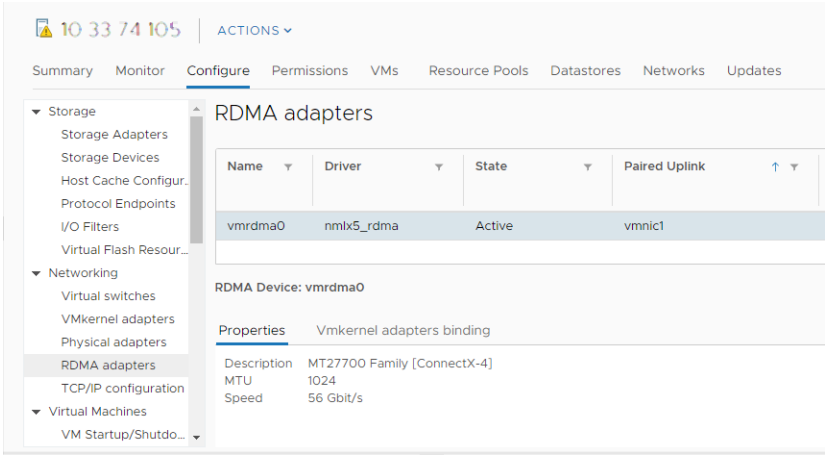
Sie können den vSphere Client verwenden, um den RDMA-Adapter und den entsprechenden Netzwerkadapter anzuzeigen.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

2 Klicken Sie unter **Netzwerk** auf **RDMA-Adapter**.

In diesem Beispiel wird der RDMA-Adapter in der Liste als `vmrdma0` angezeigt. Die Spalte **Gekoppelter Uplink** zeigt die Netzwerkkomponente als physischen Netzwerkadapter `vmnic1` an.



3 Um die Beschreibung des Adapters zu überprüfen, wählen Sie den RDMA-Adapter aus der Liste aus und klicken Sie auf die Registerkarte **Eigenschaften**.

Ergebnisse

Sie können die `vmnic#`-Netzwerkkomponente des Adapters für Speicherkonfigurationen wie iSER oder NVMe over RDMA verwenden. Informationen zu den iSER- Konfigurationsschritten finden Sie unter Konfigurieren von iSER-Adaptern mit ESXi. Informationen zu NVMe over RDMA finden Sie unter Konfigurieren von Adaptern für NVMe over RDMA (ROCE v2)-Speicher.

Aktivieren des VMware iSER-Adapters

Um den RDMA-fähigen Adapter für iSCSI verwenden zu können, aktivieren Sie die VMware iSER-Speicherkomponente mithilfe der `esxcli`. Die aktivierte Komponente wird im vSphere Client als `vmhba#`-Speicheradapter in der Kategorie „VMware iSCSI over RDMA (iSER)-Adapter“ angezeigt.

Voraussetzungen

- Stellen Sie sicher, dass Ihr iSCSI-Speicher das iSER-Protokoll unterstützt.
- Installieren Sie den RDMA-fähigen Netzwerkadapter auf Ihrem ESXi-Host. Weitere Informationen finden Sie unter Installieren und Anzeigen eines RDMA-fähigen Netzwerkadapters.
- Legen Sie für RDMA-fähige Adapter, die RoCE (RDMA over Converged Ethernet) unterstützen, die vom Adapter verwendete RoCE-Version fest.
- Verwenden Sie den RDMA-fähigen Switch.

- Aktivieren Sie die Flusssteuerung auf dem ESXi-Host. Verwenden Sie den Befehl `esxcli system module parameters`, um die Flusskontrolle für den Host zu aktivieren. Einzelheiten dazu finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1013413.
- Stellen Sie sicher, dass Sie die RDMA-Switch-Ports so konfigurieren, dass sie verlustfreie Verbindungen zwischen dem iSER-Initiator und dem Ziel herstellen.

Verfahren

1 Verwenden Sie die ESXi Shell oder vSphere-CLI, um den VMware iSER-Speicheradapter zu aktivieren und dessen RoCE-Version festzulegen.

   a Aktivieren Sie den iSER-Speicheradapter.

   ```
   esxcli rdma iser add
   ```

   b Stellen Sie sicher, dass der iSER-Adapter hinzugefügt wurde.

   ```
   esxcli iscsi adapter list
   ```

   Die Ausgabe lautet in etwa wie folgt:

   ```
   Adapter Driver State UID Description
   ------- ------ ------- ------------ -----------------------------------
   vmhba64 iser unbound iscsi.vmhba64 VMware iSCSI over RDMA (iSER) Adapter
   ```

   c Geben Sie die RoCE-Version an, die von iSER zum Herstellen einer Verbindung zum Ziel verwendet wird.

   Verwenden Sie die RoCE-Version des RDMA-fähigen Adapters. Der eingegebene Befehl lautet in etwa wie folgt:

   ```
   esxcli rdma iser params set -a vmhba64 -r 1
   ```

   Nach Abschluss des Befehls wird eine Meldung ähnlich der folgenden im VMkernel-Protokoll angezeigt.

   ```
   vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:
   Setting roce type: 1 for vmhba: vmhba64
   vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:
   Setting rdma port: 3260 for vmhba: vmhba64
   ```

   Wenn Sie die RoCE-Version nicht angeben, wird standardmäßig der Host mit der höchsten vom RDMA-fähigen Adapter unterstützten RoCE-Version verwendet.

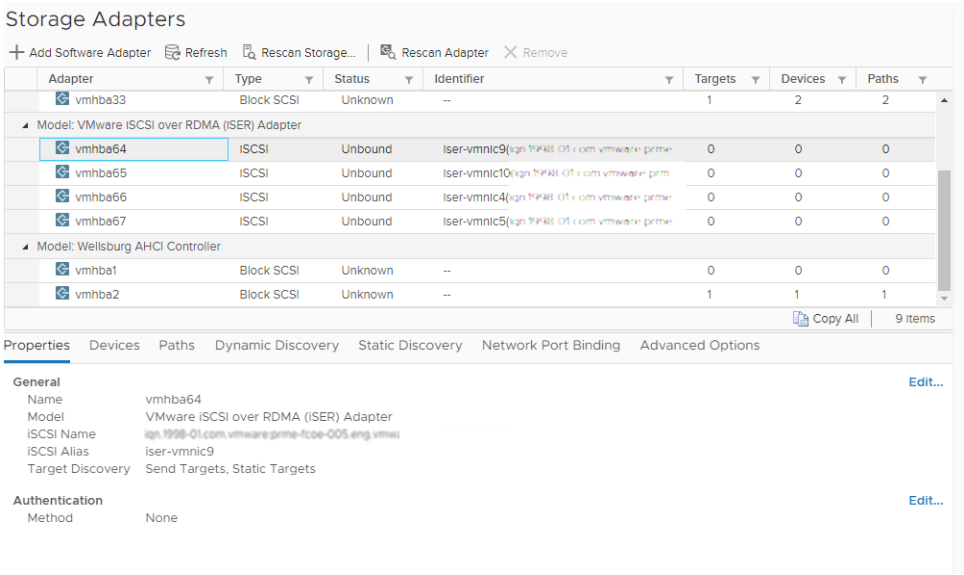
2 Verwenden Sie den vSphere Client, um den iSER-Adapter anzuzeigen.

a Navigieren Sie im vSphere Client zum ESXi-Host.

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

c Klicken Sie unter **Speicher** auf **Speicheradapter** und überprüfen Sie die Liste der Adapter.

Der aktivierte Adapter wird in der Liste unter der Kategorie „VMware iSCSI over RDMA (iSER)-Adapter“ als `vmhba#`-Speicheradapter angezeigt.



3 Wählen Sie den iSER-Speicher `vmhba#` aus, um die zugehörigen Eigenschaften zu überprüfen oder die folgenden Aufgaben durchzuführen.

Option	Bezeichnung
Konfigurieren von Port-Bindung für den iSER-Speicheradapter	Sie müssen Netzwerkverbindungen erstellen, um die iSER-Speicheradapter `vmhba#` und den RDMA-fähigen Netzwerkadapter `vmnic#` miteinander zu verbinden. Der Prozess der Konfiguration von diesen Verbindungen wird als Port-Bindung bezeichnet. Allgemeine Informationen zur Port-Bindung finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER. Informationen zum Konfigurieren von Port-Bindung für iSER finden Sie unter Konfigurieren der Port-Bindung für iSCSI oder iSER.
Einrichten dynamischer oder statischer Erkennung für den iSER-Speicheradapter	Weitere Informationen hierzu finden Sie unter Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host.
Konfigurieren des CHAP-Protokolls (Challenge Handshake Authentication Protocol) für den iSER-Speicheradapter	Weitere Informationen hierzu finden Sie unter Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter.

Nächste Schritte

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/79148.

Ändern der allgemeinen Eigenschaften für iSCSI- oder iSER-Adapter

Sie können den Standardnamen und Alias ändern, die Ihren iSCSI- oder iSER-Speicheradaptern vom ESXi-Host zugewiesen wurden. Für die unabhängigen Hardware-iSCSI-Adapter können Sie auch die Standard-IP-Einstellungen ändern.

Wichtig Wenn Sie Standardeigenschaften für Ihre Adapter ändern, müssen Sie sicherstellen, dass ihre Namen und IP-Adressen das richtige Format haben.

Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
4. Klicken Sie auf die Registerkarte **Eigenschaften** und klicken Sie im Bereich „Allgemein“ auf **Bearbeiten**.
5. (Optional) Ändern Sie die folgenden allgemeinen Eigenschaften.

Option	Beschreibung
iSCSI-Name	Ein in Übereinstimmung mit den iSCSI-Standards erstellter eindeutiger Name, der den FC-Adapter eindeutig identifiziert. Stellen Sie beim Ändern des Namens sicher, dass der Name, den Sie eingeben, weltweit eindeutig und ordnungsgemäß formatiert ist. Andernfalls können bestimmte Speichergeräte den iSCSI-Adapter möglicherweise nicht erkennen.
iSCSI-Alias	Ein benutzerfreundlicher Name, der anstelle des iSCSI-Namens verwendet wird.

Ergebnisse

Wenn Sie den iSCSI-Namen ändern, wird der angegebene Name für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst verwendet, nachdem Sie sich ab- und anschließend wieder angemeldet haben.

Nächste Schritte

Weitere Konfigurationsschritte, die Sie für die iSCSI- oder ISER-Speicheradapter durchführen können, finden Sie in den folgenden Themen:

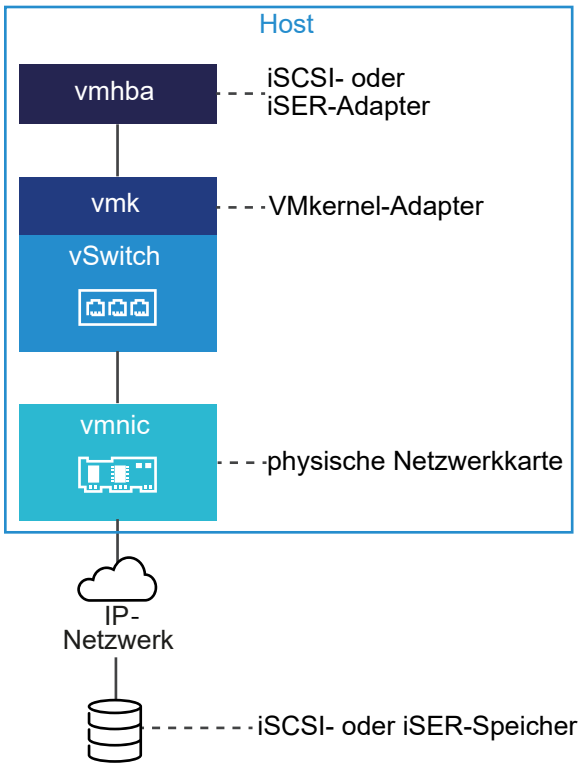
- Einrichten von unabhängigen Hardware-iSCSI-Adaptern
- Konfigurieren von abhängigen Hardware-iSCSI-Adaptern

- Konfigurieren des Software-iSCSI-Adapters
- Konfigurieren von iSER-Adaptern mit ESXi

Einrichten eines Netzwerks für iSCSI und iSER

Bestimmte iSCSI-Adaptertypen hängen vom VMkernel-Netzwerk ab. Diese Adapter umfassen den Software- oder abhängigen Hardware-iSCSI-Adapter und den VMware-iSCSI über RDMA (iSER)-Adapter. Wenn Ihre Umgebung einen dieser Adapter enthält, müssen Sie Verbindungen für den Datenverkehr zwischen der iSCSI- oder iSER-Komponente und den physischen Netzwerkadaptern konfigurieren.

Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter. Anschließend muss der VMkernel-Adapter mit einem entsprechenden iSCSI- oder iSER-Adapter verknüpft werden. Dieser Vorgang wird Port-Bindung genannt.



Befolgen Sie diese Regeln beim Konfigurieren der Port-Bindung:

- Sie können den Software-iSCSI-Adapter mit allen auf Ihrem Host verfügbaren physischen Netzwerkkarten verbinden.
- Die abhängigen iSCSI-Adapter müssen nur mit ihren eigenen physischen Netzwerkkarten verbunden sein.
- Sie dürfen den iSER-Adapter nur mit dem RDMA-fähigen Netzwerkadapter verbinden.

Spezifische Überlegungen, wann und wie Netzwerkverbindungen mit Software-iSCSI verwendet werden, finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2038869.

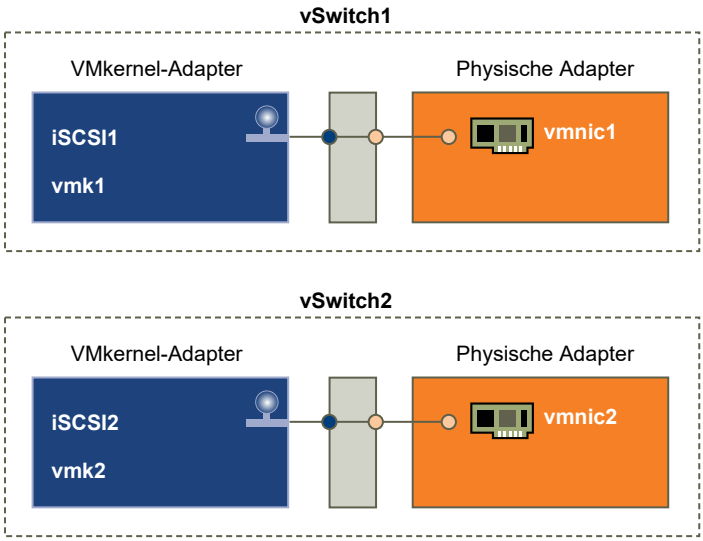
Mehrere Netzwerkadapter in der iSCSI- oder iSER-Konfiguration

Wenn Ihr Host über mehrere physische Netzwerkadapter für iSCSI oder iSER verfügt, können Sie die Adapter für das Multipathing verwenden.

Sie können mehrere physische Adapter in Konfigurationen mit einem einzelnen Switch oder mehreren Switches verwenden.

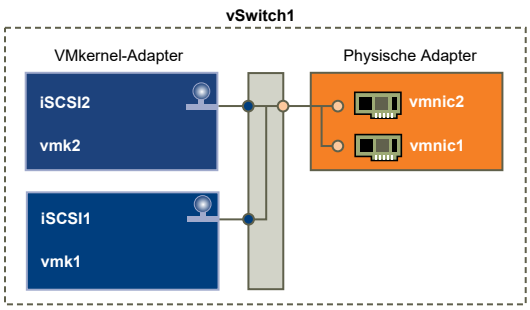
In der Konfiguration mit mehreren Switches weisen Sie für jedes V2P-Adapterpaar (Virtual-to-Physical) einen separaten vSphere-Switch zu.

Abbildung 11-1. 1:1-Adapterzuordnung auf separaten vSphere Standard-Switches



Eine Alternative besteht darin, alle Netzwerkkarten und VMkernel-Adapter zu einem einzelnen vSphere-Switch hinzuzufügen. Die Anzahl an VMkernel-Adaptern muss mit der Anzahl an physischen Adaptern auf dem vSphere Standard-Switch übereinstimmen. Die Konfiguration mit einem einzelnen Switch ist für iSER nicht geeignet, da iSER die NIC-Gruppierung nicht unterstützt.

Abbildung 11-2. 1:1-Adapterzuordnung auf einem einzelnen vSphere Standard-Switch



Für diesen Konfigurationstyp müssen Sie die Standardnetzwerkeinrichtung außer Kraft setzen und sicherstellen, dass jeder VMkernel-Adapter nur einem entsprechenden aktiven physischen Adapter zugeordnet wird, wie in der Tabelle angegeben.

VMkernel-Adapter (vmk#)	Physischer Netzwerkadapter (vmnic#)
vmk1 (iSCSI1)	**Aktive Adapter** vmnic1 **Nicht verwendete Adapter** vmnic2
vmk2 (iSCSI2)	**Aktive Adapter** vmnic2 **Nicht verwendete Adapter** vmnic1

Sie können auch Distributed Switches verwenden. Weitere Informationen zu vSphere Distributed Switches und zum Ändern der Standardnetzwerkrichtlinie finden Sie in der *vSphere-Netzwerk*-Dokumentation.

Wenn Sie mehrere physische Adapter verwenden, gelten die folgenden Bedingungen:

- Physische Netzwerkadapter müssen sich in demselben Subnetz befinden wie das Speichersystem, mit dem sie verbunden werden.
- (Gilt nur für iSCSI, nicht für iSER) Wenn Sie separate vSphere-Switches verwenden, müssen Sie sie mit unterschiedlichen IP-Subnetzen verbinden. Andernfalls können bei VMkernel-Adaptern Konnektivitätsprobleme auftreten und der Host kann keine LUNs erkennen.
- Die Konfiguration mit einem einzelnen Switch ist für iSER nicht geeignet, da iSER die NIC-Gruppierung nicht unterstützt.

Verwenden Sie die Port-Bindung nicht, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- Array-Ziel-iSCSI-Ports befinden sich in einer anderen Broadcast-Domäne und einem anderen IP-Subnetz.
- Für die iSCSI-Konnektivität verwendete VMkernel-Adapter befinden sich in verschiedenen Broadcast-Domänen und IP-Subnetzen oder verwenden verschiedene virtuelle Switches.

Hinweis In iSER-Konfigurationen können die für iSER-Konnektivität verwendeten VMkernel-Adapter nicht für konvergierten Datenverkehr verwendet werden. Die VMkernel-Adapter, die Sie erstellt haben, um die Konnektivität zwischen dem ESXi-Host mit iSER und dem iSER-Ziel zu ermöglichen, darf nur für iSER-Datenverkehr verwendet werden.

Best Practices für die Konfiguration des Netzwerks mit Software-iSCSI

Berücksichtigen Sie bei der Konfiguration des Netzwerks mit Software-iSCSI verschiedene Best Practices.

Software-iSCSI-Port-Bindung

Sie können den Software-iSCSI-Initiator auf dem ESXi-Host an einen einzelnen oder mehrere VMkernel-Ports binden, sodass der iSCSI-Datenverkehr nur über die gebundenen Ports fließt. Ungebundene Ports werden nicht für iSCSI-Datenverkehr verwendet.

Wenn die Port-Bindung konfiguriert ist, erstellt der iSCSI-Initiator iSCSI-Sitzungen von allen gebundenen Ports zu allen konfigurierten Zielportalen.

Nachfolgend finden Sie Beispiele.

VMkernel-Ports	Zielportale	iSCSI-Sitzungen
2 gebundene VMkernel-Ports	2 Zielportale	4 Sitzungen (2 x 2)
4 gebundene VMkernel-Ports	1 Zielportal	4 Sitzungen (4 x 1)
2 gebundene VMkernel-Ports	4 Zielportale	8 Sitzungen (2 x 4)

Hinweis Stellen Sie sicher, dass alle Zielportale von allen VMkernel-Ports erreicht werden können, wenn die Port-Bindung verwendet wird. Andernfalls können iSCSI-Sitzungen möglicherweise nicht erstellt werden. Infolgedessen wird für die erneute Prüfung möglicherweise mehr Zeit benötigt als erwartet.

Keine Port-Bindung

Wird keine Port-Bindung verwendet, wird auf der ESXi-Netzwerkebene der beste VMkernel-Port basierend auf seiner Routing-Tabelle ausgewählt. Der Host nutzt den Port zum Erstellen einer iSCSI-Sitzung mit dem Zielportal. Ohne die Port-Bindung wird nur eine Sitzung pro Zielportal erstellt.

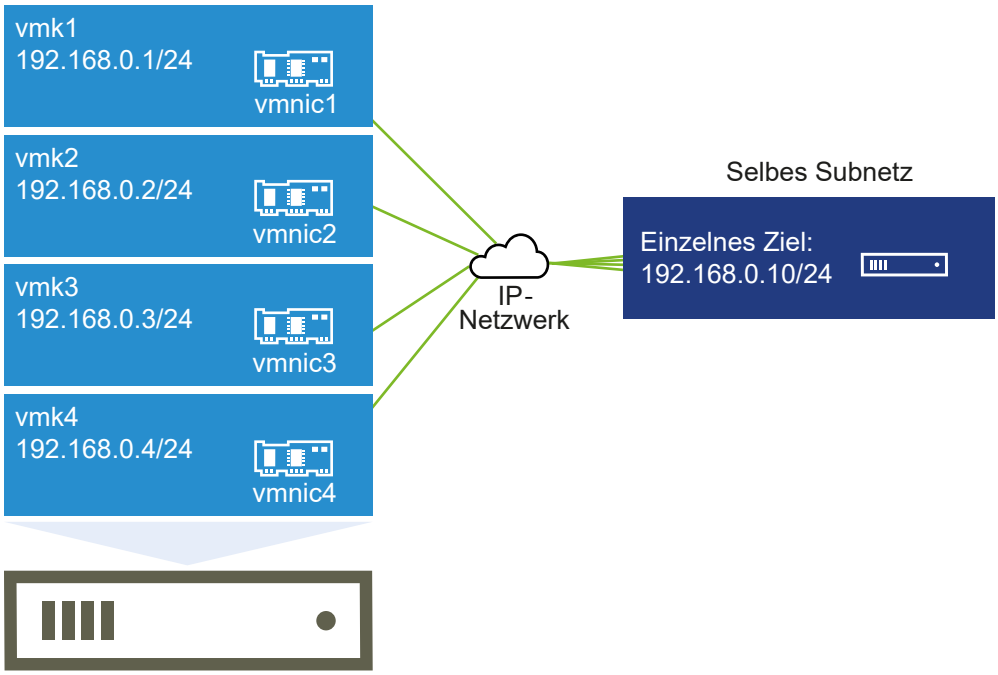
Nachfolgend finden Sie Beispiele.

VMkernel-Ports	Zielportale	iSCSI-Sitzungen
2 ungebundene VMkernel-Ports	2 Zielportale	2 Sitzungen
4 ungebundene VMkernel-Ports	1 Zielportal	1 Sitzung
2 ungebundene VMkernel-Ports	4 Zielportale	4 Sitzungen

Software-iSCSI-Multipathing

Beispiel 1: Mehrere Pfade für ein iSCSI-Ziel mit einem einzelnen Netzwerkportal

Wenn das Ziel nur über ein Netzwerkportal verfügt, können Sie mehrere Pfade zu dem Ziel erstellen, indem Sie mehrere VMkernel-Ports auf dem ESXi-Host hinzufügen und diese an den iSCSI-Initiator binden.

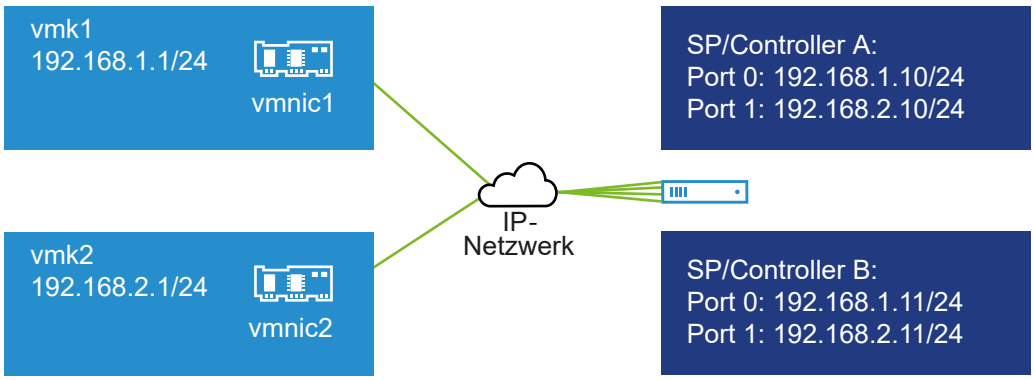


In diesem Beispiel werden alle Initiator-Ports und das Zielportal im selben Subnetz konfiguriert. Das Ziel kann über alle gebundenen Ports erreicht werden. Sie haben vier VMkernel-Ports und ein Zielportal. Es werden also insgesamt vier Pfade erstellt.

Ohne die Port-Bindung wird nur ein Pfad erstellt.

Beispiel 2: Mehrere Pfade mit VMkernel-Ports in verschiedenen Subnetzen

Sie können mehrere Pfade erstellen, indem Sie mehrere Ports und Zielportale in verschiedenen IP-Subnetzen konfigurieren. Indem Initiator- und Zielports in verschiedenen Subnetzen beibehalten werden, können Sie erzwingen, dass ESXi Pfade über bestimmte Ports erstellt. Bei dieser Konfiguration wird keine Port-Bindung verwendet, da für die Port-Bindung erforderlich ist, dass sich alle Initiator- und Zielports im selben Subnetz befinden.



ESXi wählt vmk1 aus, wenn eine Verbindung zu Port 0 von Controller A und Controller B hergestellt wird, da sich alle drei Ports im selben Subnetz befinden. Ebenso wird vmk2 ausgewählt, wenn eine Verbindung zu Port 1 von Controller A und B hergestellt wird. Bei dieser Konfiguration kann die NIC-Gruppierung verwendet werden.

Es werden insgesamt vier Pfade erstellt.

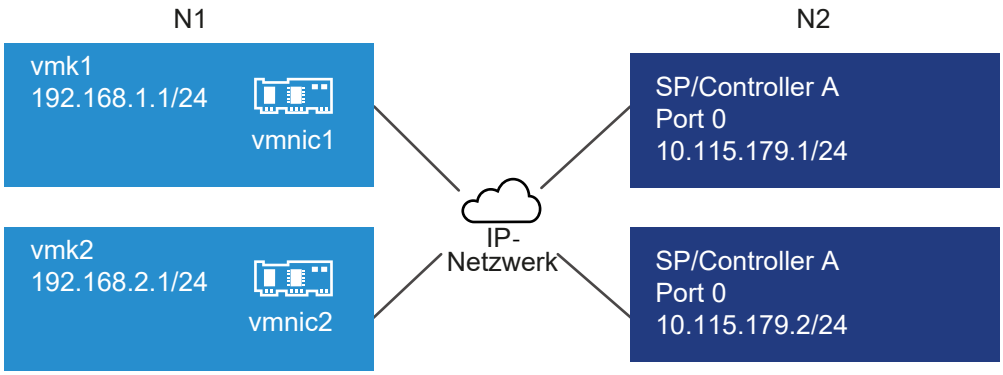
Pfade	Beschreibung
Pfad 1	vmk1 und Port 0 von Controller A
Pfad 2	vmk1 und Port 0 von Controller B
Pfad 3	vmk2 und Port 1 von Controller A
Pfad 4	vmk2 und Port 1 von Controller B

Routing mit Software-iSCSI

Mit dem Befehl `esxcli` können Sie statische Routen für Ihren iSCSI-Datenverkehr hinzufügen. Nachdem die statischen Routen konfiguriert wurden, können die Initiator- und Zielports in verschiedenen Subnetzen miteinander kommunizieren.

Beispiel 1: Verwenden von statischen Routen mit Port-Bindung

In diesem Beispiel werden alle gebundenen VMkernel-Ports in einem Subnetz (N1) beibehalten und alle Zielportale in einem anderen Subnetz (N2) konfiguriert. Sie können dann eine statische Route für das Zielsubnetz (N2) hinzufügen.

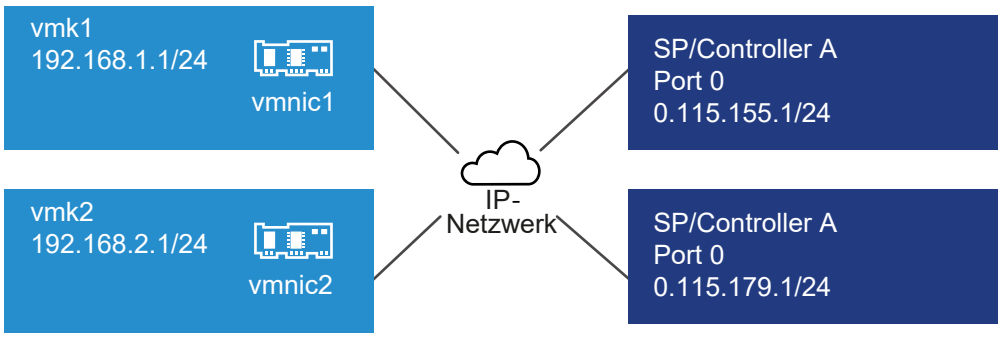


Verwenden Sie den folgenden Befehl:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Beispiel 2: Verwenden von statischen Routen, um mehrere Pfade zu erstellen

Bei dieser Konfiguration verwenden Sie statische Routen und verschiedene Subnetze. Bei dieser Konfiguration kann die Port-Bindung nicht verwendet werden.



Sie konfigurieren vmk1 und vmk2 in separaten Subnetzen: 192.168.1.0 und 192.168.2.0. Ihre Zielportale befinden sich also in separaten Subnetzen: 10.115.155.0 und 10.155.179.0.

Sie können die statische Route für 10.115.155.0 von vmk1 hinzufügen. Stellen Sie sicher, dass das Gateway von vmk1 aus erreicht werden kann.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.155.0/24
```

Anschließend fügen Sie die statische Route für 10.115.179.0 von vmk2 hinzu. Stellen Sie sicher, dass das Gateway von vmk2 aus erreicht werden kann.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network
10.115.179.0/24
```

Beim Herstellen der Verbindung mit Port 0 von Controller A wird vmk1 verwendet.

Beim Herstellen der Verbindung mit Port 0 von Controller B wird vmk2 verwendet.

Beispiel 3: Routing mit einem separaten Gateway pro vmkernel-Port

Ab vSphere 6.5 können Sie ein separates Gateway pro VMkernel-Port konfigurieren. Wenn Sie DHCP zum Abrufen der IP-Konfiguration für einen VMkernel-Port verwenden, können Gateway-Informationen ebenfalls über DHCP abgerufen werden.

Verwenden Sie den folgenden Befehl, um Gateway-Informationen pro VMkernel-Port anzuzeigen:

```
# esxcli network ip interface ipv4 address list
```

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

Bei separaten Gateways pro VMkernel-Port nutzen Sie die Port-Bindung, um Ziele in verschiedenen Subnetzen zu erreichen.

Konfigurieren der Port-Bindung für iSCSI oder iSER

Die Port-Bindung erstellt Verbindungen für den Datenverkehr zwischen bestimmte Typen von iSCSI- und iSER-Adaptern und den physischen Netzwerkadaptern.

Folgende Adaptertypen benötigen die Port-Bindung:

- Software-iSCSI-Adapter
- Abhängige Hardware-iSCSI-Adapter
- VMware iSER-Adapter (für iSCSI über RDMA)

Die folgenden Aufgaben behandeln die Netzwerkkonfiguration mit einem vSphere Standard-Switch und einem einzelnen physischen Netzwerkadapter. Wenn Sie über mehrere Netzwerkadapter verfügen, finden Sie weitere Informationen unter Mehrere Netzwerkadapter in der iSCSI- oder iSER-Konfiguration.

Hinweis NIC-Gruppierung wird von iSER nicht unterstützt. Verwenden Sie beim Konfigurieren der Port-Bindung für iSER nur einen RDMA-fähigen physischen Adapter (vmnic#) und einen VMkernel-Adapter (vmk#) pro vSwitch.

Für die Konfiguration der Port-Bindung kann jedoch auch der VMware vSphere® Distributed Switch™ oder der VMware NSX® Virtueller Switch™ verwendet werden. Weitere Informationen zu virtuellen NSX-Switches finden Sie in der Dokumentation zu *VMware NSX Data Center for vSphere*.

Wenn Sie einen vSphere Distributed Switch mit mehreren Uplink-Ports für die Port-Bindung verwenden, erstellen Sie für jede physische Netzwerkkarte eine separate verteilte Portgruppe. Legen Sie anschließend die Teamrichtlinie so fest, dass jede verteilte Portgruppe nur einen aktiven Uplink-Port besitzt. Weitere Informationen zu Distributed Switches finden Sie im Handbuch *vSphere-Netzwerk*.

Verfahren

1 Erstellen eines einzelnen VMkernel-Adapters für iSCSI oder iSER

   Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an einen physischen Netzwerkadapter auf dem ESXi-Host an. Anschließend verwenden Sie den erstellten VMkernel-Adapter in der Port-Bindungskonfiguration mit den iSCSI- oder iSER-Adaptern.

2 Binden von iSCSI- oder iSER-Adaptern an VMkernel-Adapter

   Binden Sie auf dem ESXi-Host einen iSCSI- oder iSER-Adapter an einen VMkernel-Adapter.

3 Überprüfen der Details der Portbindung auf dem ESXi-Host

   Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI- oder iSER-Adapter (vmhba) verbunden ist.

Nächste Schritte

Weitere Konfigurationsschritte, die Sie für die iSCSI- oder ISER-Speicheradapter durchführen können, finden Sie in den folgenden Themen:

- Konfigurieren von abhängigen Hardware-iSCSI-Adaptern
- Konfigurieren des Software-iSCSI-Adapters

- Konfigurieren von iSER-Adaptern mit ESXi

Erstellen eines einzelnen VMkernel-Adapters für iSCSI oder iSER

Schließen Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an einen physischen Netzwerkadapter auf dem ESXi-Host an. Anschließend verwenden Sie den erstellten VMkernel-Adapter in der Port-Bindungskonfiguration mit den iSCSI- oder iSER-Adaptern.

Folgende Adaptertypen benötigen die Port-Bindung:

- Software-iSCSI-Adapter
- Abhängige Hardware-iSCSI-Adapter
- VMware iSER-Adapter (für iSCSI über RDMA)

Voraussetzungen

- Wenn Sie einen VMkernel-Adapter für den abhängigen Hardware-iSCSI-Adapter erstellen, wählen Sie den physischen Netzwerkadapter (vmnic#) aus, der zu der iSCSI-Komponente gehört. Weitere Informationen hierzu finden Sie unter Ermitteln der Zuordnung zwischen iSCSI- und Netzwerkadaptern.
- Stellen Sie bei einem iSER-Adapter sicher, dass ein entsprechender RDMA-fähiger vmnic# verwendet wird. Weitere Informationen hierzu finden Sie unter Installieren und Anzeigen eines RDMA-fähigen Netzwerkadapters.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Wählen Sie im Kontextmenü **Netzwerk hinzufügen** aus.
3. Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
4. Wählen Sie **Neuer Standard-Switch** aus, um einen vSphere Standard-Switch zu erstellen.
5. Klicken Sie auf das Symbol **Adapter hinzufügen** und wählen Sie einen passenden Netzwerkadapter (vmnic#) aus, den Sie für iSCSI verwenden möchten.

   Stellen Sie sicher, dass die Adapter den aktiven Adaptern zugewiesen werden.
6. Geben Sie eine Netzwerkbezeichnung ein.

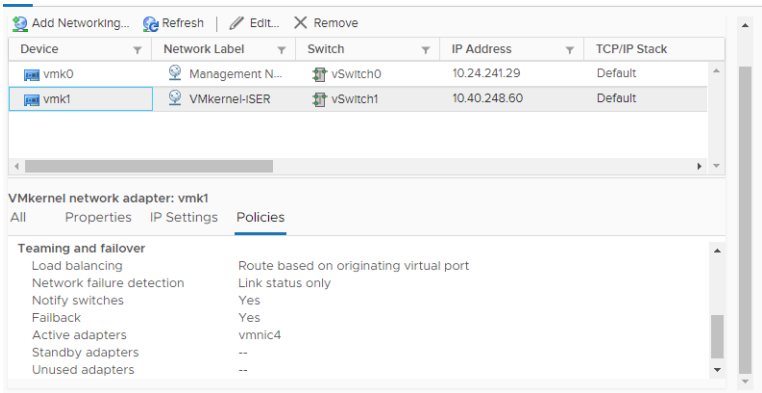
   Eine Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Adapter identifiziert, den Sie erstellen, z. B. iSCSI oder iSER.
7. Geben Sie die IP-Einstellungen an.
8. Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

   Sie haben den virtuellen VMkernel-Adapter (vmk#) für einen physischen Netzwerkadapter (vmnic#) auf Ihrem Host erstellt.

9 Verifizieren Sie die Konfiguration.

a Wählen Sie unter **Netzwerk** die Option **VMkernel-Adapter** aus und wählen Sie den VMkernel-Adapter (vmk#) aus der Liste aus.

b Klicken Sie auf die Registerkarte **Richtlinien** und stellen Sie sicher, dass der entsprechende physische Netzwerkadapter (vmnic#) als aktiver Adapter unter **Teaming und Failover** angezeigt wird.



Nächste Schritte

Wenn Ihr Host über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügt, müssen Sie den VMkernel-Adapter, den Sie erstellt haben, an den iSCSI- oder iSER-Adapter (vmhba) binden.

Wenn Sie über mehrere Netzwerkadapter verfügen, können Sie zusätzliche VMkernel-Adapter erstellen und dann die iSCSI-Bindung durchführen. Die Anzahl an virtuellen Adaptern muss mit der Anzahl an physischen Adaptern auf dem Host übereinstimmen. Weitere Informationen finden Sie unter Mehrere Netzwerkadapter in der iSCSI- oder iSER-Konfiguration.

Binden von iSCSI- oder iSER-Adaptern an VMkernel-Adapter

Binden Sie auf dem ESXi-Host einen iSCSI- oder iSER-Adapter an einen VMkernel-Adapter.

Folgende Adaptertypen benötigen die Port-Bindung:

- Software-iSCSI-Adapter
- Abhängige Hardware-iSCSI-Adapter
- VMware iSER-Adapter (für iSCSI über RDMA)

Voraussetzungen

Erstellen Sie einen virtuellen VMkernel-Adapter für jeden physischen Netzwerkadapter auf Ihrem Host. Wenn Sie mehrere VMkernel-Adapter verwenden, richten Sie die korrekte Netzwerkrichtlinie ein.

Erforderliche Berechtigung:**Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den entsprechenden iSCSI- bzw. iSER-Adapter (vmhba#) aus der Liste aus.

4 Klicken Sie auf die Registerkarte **Netzwerk-Port-Bindung** und anschließend auf das Symbol **Hinzufügen**.

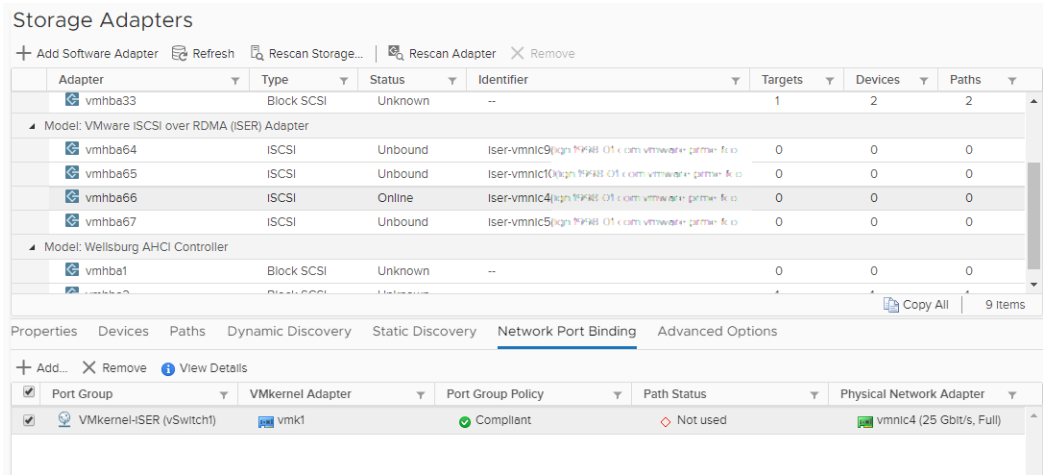
5 Wählen Sie einen VMkernel-Adapter zur Bindung mit dem iSCSI- oder iSER-Adapter aus.

Hinweis Stellen Sie sicher, dass die Netzwerkrichtlinie für den VMkernel-Adapter die Anforderungen für das Binden erfüllt.

Sie können den Software-iSCSI-Adapter an einen oder mehrere VMkernel-Adapter binden. Für einen abhängigen Hardware-iSCSI-Adapter oder den iSER-Adapter ist nur ein VMkernel-Adapter verfügbar, der mit der richtigen physischen Netzwerkkarte verknüpft ist.

6 Klicken Sie auf **OK**.

Die Netzwerkverbindung wird in der Liste der Netzwerk-Port-Bindungen für den iSCSI- oder iSER-Adapter angezeigt.



Überprüfen der Details der Portbindung auf dem ESXi-Host

Überprüfen Sie die Netzwerkdetails des VMkernel-Adapters, der mit dem iSCSI- oder iSER-Adapter (vmhba) verbunden ist.

Folgende Adaptertypen benötigen die Port-Bindung:

- Software-iSCSI-Adapter
- Abhängige Hardware-iSCSI-Adapter
- VMware iSER-Adapter (für iSCSI über RDMA)

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den entsprechenden iSCSI- bzw. iSER-Adapter aus der Liste aus.

4 Klicken Sie auf die Registerkarte **Netzwerk-Port-Bindung** und wählen Sie den VMkernel-Adapter aus der Liste aus.

5 Klicken Sie auf das Symbol **Details anzeigen**.

6 Prüfen Sie die Informationen für die VMkernel- und physischen Adapter durch das Wechseln zwischen verfügbaren Registerkarten.

Verwalten des iSCSI-Netzwerks

Besondere Berücksichtigung finden sowohl physische als auch VMkernel-Netzwerkadapter, die einem iSCSI-Adapter zugeordnet sind.

Nachdem Sie Netzwerkverbindungen für iSCSI erstellt haben, wird eine iSCSI-Kontrollanzeige im vSphere Client aktiviert. Die Kontrollanzeige zeigt, dass ein bestimmter virtueller oder physischer Netzwerkadapter iSCSI-gebunden ist. Befolgen Sie zur Vermeidung von Störungen des iSCSI-Datenverkehrs diese Richtlinien und Überlegungen bei der Verwaltung von iSCSI-gebundenen virtuellen und physischen Netzwerkadaptern:

- Stellen Sie sicher, dass den VMkernel-Netzwerkadaptern Adressen in dem Subnetz zugewiesen werden, in dem sich auch das iSCSI-Speicher-Portal befindet, zu dem sie eine Verbindung herstellen.
- iSCSI-Adapter, die VMkernel-Adapter verwenden, können keine Verbindungen zu iSCSI-Ports auf unterschiedlichen Subnetzen herstellen, selbst wenn die iSCSI-Adapter diese Ports ermitteln.
- Stellen Sie bei der Verwendung von separaten vSphere-Switches zum Verbinden von physischen Netzwerkadaptern und VMkernel-Adaptern sicher, dass die vSphere-Switches Verbindungen zu unterschiedlichen IP-Subnetzen herstellen.
- Wenn sich VMkernel-Adapter in demselben Subnetz befinden, müssen Sie mit einem einzelnen vSwitch verbunden sein.
- Wenn Sie VMkernel-Adapter auf einen anderen vSphere-Switch migrieren, verschieben Sie die zugewiesenen physischen Adapter.
- Nehmen Sie keine Änderungen an der Konfiguration von iSCSI-gebundenen VMkernel-Adaptern oder physischen Netzwerkadaptern vor.
- Nehmen Sie keine Änderungen vor, die die Zuweisungen von VMkernel-Adaptern und physischen Netzwerkadaptern aufheben könnten. Sie können die Zuweisung aufheben, wenn Sie einen der Adapter oder den vSphere-Switch, der sie verbindet, entfernen. Dieselbe Möglichkeit bietet sich auch, wenn Sie die 1:1-Netzwerkrichtlinie für die Verbindung ändern.

Fehler im iSCSI-Netzwerk beheben

Ein Warnhinweis deutet auf eine nicht übereinstimmende Portgruppenrichtlinie für einen iSCSI-gebundenen VMkernel-Adapter hin.

Problem

Die Portgruppenrichtlinie des VMkernel-Adapters wird in den folgenden Fällen als nicht übereinstimmend betrachtet:

- Der VMkernel-Adapter ist mit keinem aktiven physischen Netzwerkadapter verbunden.
- Der VMkernel-Adapter ist mit mehreren physischen Netzwerkadapter verbunden.
- Der VMkernel-Adapter ist mit mindestens einem physischen Standby-Adapter verbunden.
- Der aktive physische Adapter wurde geändert.

Lösung

Richten Sie die richtige Netzwerkrichtlinie für den iSCSI-gebundenen VMkernel-Adapter ein. Weitere Informationen hierzu finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.

Verwenden von Jumbo-Frames mit iSCSI und iSER

ESXi unterstützt die Verwendung von Jumbo-Frames mit iSCSI/iSER.

Jumbo-Frames sind Ethernet-Frames mit einer Größe, die 1500 Byte überschreitet. Der Parameter „Maximum Transmission Unit“ (MTU) wird in der Regel dazu verwendet, die Größe der Jumbo-Frames zu messen.

Wenn Sie Jumbo-Frames für den iSCSI-Datenverkehr verwenden, sollten Sie Folgendes in Betracht ziehen:

- Alle Netzwerkkomponenten müssen Jumbo-Frames unterstützen.
- Informieren Sie sich bei Ihrem Anbieter, ob Ihre physischen Netzwerkkarten und iSCSI-Adapter Jumbo-Frames unterstützen.
- Zu Fragen zum Einrichten und Überprüfen physischer Netzwerk-Switches für Jumbo-Frames konsultieren Sie Ihre Anbieterdokumentation.

Die folgende Tabelle erläutert den Grad der Unterstützung, den ESXi für Jumbo-Frames bietet.

Tabelle 11-1. Unterstützung für Jumbo-Frames

Typ des iSCSI-Adapters	Unterstützung für Jumbo-Frames
Software-iSCSI	Unterstützt
Abhängige Hardware-iSCSI	Wird unterstützt. Fragen Sie den Anbieter.
Unabhängige Hardware-iSCSI	Wird unterstützt. Fragen Sie den Anbieter.
VMware-iSER	Wird unterstützt. Fragen Sie den Anbieter.

Aktivieren von Jumbo-Frames für Netzwerke

Sie können Jumbo-Frames für ESXi-Speicheradapter aktivieren, die VMkernel-Netzwerke für den Datenverkehr verwenden. Diese Adapter umfassen Software-iSCSI-Adapter, abhängige Hardware-iSCSI-Adapter und VMware-iSER-Adapter.

Um Jumbo-Frames zu aktivieren, ändern Sie den Standardwert des MTU-Parameters (Maximum Transmission Unit, Maximale Übertragungseinheit). Sie ändern den MTU-Parameter auf dem vSphere-Switch, den Sie für iSCSI-Datenverkehr verwenden. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Netzwerk** auf **Virtuelle Switches** und wählen Sie aus der Liste den vSphere-Switch aus, den Sie ändern möchten.
4. Klicken Sie auf das Symbol **Einstellungen bearbeiten**.
5. Ändern Sie auf der Seite „Eigenschaften“ den MTU-Parameter.

   Mit diesem Schritt wird die MTU für alle physischen Netzwerkkarten auf diesem Standard-Switch festgelegt. Legen Sie als MTU-Wert die größte MTU-Größe von allen Netzwerkkarten fest, die mit dem Standard-Switch verbunden sind. ESXi unterstützt eine MTU-Größe von bis zu 9.000 Byte.

Aktivieren von Jumbo-Frames für unabhängige Hardware-iSCSI

Um Jumbo-Frames für unabhängige Hardware-iSCSI-Adapter auf dem ESXi-Host zu aktivieren, ändern Sie den Standardwert des MTU-Parameters (Maximum Transmission Unit, maximale Übertragungseinheit).

Verwenden Sie die Einstellungen unter „Erweiterte Optionen“, um den MTU-Parameter für den iSCSI-HBA zu ändern.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie in der Liste der Adapter den unabhängigen Hardware-iSCSI-Adapter aus.
4. Klicken Sie auf die Registerkarte **Erweiterte Optionen** und anschließend auf **Bearbeiten**.
5. Ändern Sie den Wert des MTU-Parameters.

   ESXi unterstützt eine MTU-Größe von bis zu 9000 Byte.

Konfigurieren der dynamischen bzw. statischen Erkennung für iSCSI und iSER auf einem ESXi-Host

Sie müssen Zielerkennungsadressen einrichten, damit der iSCSI- oder iSER-Speicheradapter erkennen kann, welche Speicherressource im Netzwerk zur Verfügung steht.

Das ESXi-System unterstützt diese Erkennungsmethoden:

Dynamische Erkennung

Wird auch als „SendTargets“-Erkennung bezeichnet. Immer wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, übermittelt der Initiator eine „SendTargets“-Anforderung an den Server. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Die Namen und IP-Adressen dieser Ziele werden auf der Registerkarte **Statische Erkennung (Static Discovery)** angezeigt. Wenn Sie ein von der dynamischen Erkennung hinzugefügtes statisches Ziel entfernen, kann das Ziel entweder bei einer erneuten Überprüfung, beim Zurücksetzen des Speicheradapters oder durch einen Neustart des Hosts erneut zur Liste hinzugefügt werden.

Hinweis Bei Software-iSCSI und davon abhängiger Hardware-iSCSI filtert ESXi die Zieladressen anhand der IP-Familie der angegebenen iSCSI-Serveradresse. Wenn die Adresse im IPv4-Format vorliegt, werden eventuelle IPv6-Adressen in der SendTargets-Antwort des iSCSI-Servers herausgefiltert. Wenn die Angabe eines iSCSI-Servers über DNS-Namen erfolgt oder die SendTargets-Antwort des iSCSI-Servers DNS-Namen aufweist, bezieht sich ESXi auf die IP-Familie des ersten aufgelösten Eintrags im DNS-Lookup.

Statische Erkennung

Neben der dynamischen Erkennungsmethode können Sie auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben. Der iSCSI- oder iSER-Adapter verwendet zur Kommunikation mit den iSCSI-Servern eine von Ihnen bereitgestellte Liste von Zielen.

Wenn Sie die statische oder dynamische Erkennung einrichten, können Sie nur neue iSCSI-Ziele hinzufügen. Sie können keine Parameter eines vorhandenen Ziels ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.

4 Konfigurieren Sie die Erkennungsmethode.

Erkennungsmethode	Beschreibung
Dynamische Erkennung	a Klicken Sie auf **Dynamische Erkennung** und klicken Sie anschließend auf **Hinzufügen**. b Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf **OK**. c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch. Nach dem Einrichten der SendTargets-Sitzung mit dem iSCSI-System füllt Ihr Host die Liste „Statische Erkennung“ mit allen neu erkannten Zielen. **Hinweis** Ein dynamisch erkanntes Ziel verbleibt auf der Liste, auch wenn es von der Array-Seite entfernt wurde.
Statische Erkennung	a Klicken Sie auf **Statische Erkennung** und klicken Sie anschließend auf **Hinzufügen**. b Geben Sie die Daten des Ziels ein, und klicken Sie auf **OK**. c Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Nächste Schritte

Weitere Konfigurationsschritte, die Sie für die iSCSI- oder ISER-Speicheradapter durchführen können, finden Sie in den folgenden Themen:

- Einrichten von unabhängigen Hardware-iSCSI-Adaptern
- Konfigurieren von abhängigen Hardware-iSCSI-Adaptern
- Konfigurieren des Software-iSCSI-Adapters
- Konfigurieren von iSER-Adaptern mit ESXi

Entfernen dynamischer oder statischer iSCSI-Ziele

Entfernen Sie mit Ihrem ESXi-Host verbundene iSCSI-Server.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu ändernden iSCSI-Adapter in der Liste aus.

4 Wechseln Sie zwischen **Dynamische Erkennung** und **Statische Erkennung**.

5 Wählen Sie einen iSCSI-Server zum Entfernen aus und klicken Sie auf **Entfernen**.

6 Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Wenn Sie ein dynamisch erkanntes statisches Ziel entfernen, müssen Sie es vor der erneuten Prüfung aus dem Speichersystem entfernen. Sonst erkennt Ihr Host das Ziel automatisch und fügt es der Liste der statischen Ziele hinzu, wenn Sie den Adapter erneut prüfen.

Konfigurieren von CHAP-Parametern für iSCSI- oder iSER-Speicheradapter.

Da die IP-Netzwerke, die von der iSCSI-Technologie zum Verbinden mit Remotezielen verwendet werden, die von ihnen übertragenen Daten nicht schützen, muss die Sicherheit der Verbindung gewährleistet werden. Eines der von iSCSI implementierten Protokolle ist das CHAP (Challenge Handshake Authentication Protocol), das die jeweiligen Berechtigungen der Initiatoren überprüft, die auf Ziele im Netzwerk zugreifen.

CHAP verwendet einen dreiteiligen Handshake-Algorithmus, um die Identität Ihres Hosts und, sofern zutreffend, des iSCSI-Ziels zu verifizieren, wenn der Host und das Ziel eine Verbindung herstellen. Die Verifizierung basiert auf einem vordefinierten privaten Wert, dem CHAP-Schlüssel, den der Initiator und das Ziel gemeinsam nutzen.

ESXi unterstützt die CHAP-Authentifizierung auf der Adapterebene. In diesem Fall erhalten alle Ziele vom iSCSI-Initiator denselben CHAP-Namen und -Schlüssel. Für Software- und abhängige Hardware-iSCSI-Adapter sowie für iSER-Adapter unterstützt ESXi auch die zielbasierte CHAP-Authentifizierung, die Ihnen ermöglicht, unterschiedliche Anmeldedaten für die einzelnen Ziele zu konfigurieren und so die Sicherheit zu erhöhen.

Auswählen der CHAP-Authentifizierungsmethode

ESXi unterstützt unidirektionales CHAP für alle Typen von iSCSI/iSER-Initiatoren und bidirektionales CHAP für Software- und abhängige Hardware-iSCSI sowie für iSER.

Überprüfen Sie vor der CHAP-Konfiguration, ob CHAP im iSCSI-Speichersystem aktiviert ist. Rufen Sie darüber hinaus die Informationen über die vom System unterstützten CHAP-Authentifizierungsmethode ab. Wenn CHAP aktiviert ist, müssen Sie es für Ihre Initiatoren konfigurieren und dabei sicherstellen, dass die Anmeldedaten für die CHAP-Authentifizierung mit den Anmeldedaten im iSCSI-Speicher übereinstimmen.

ESXi unterstützt die folgenden CHAP-Authentifizierungsmethoden:

Unidirektionales CHAP

Bei der unidirektionalen CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel.

Bidirektionales CHAP

Die bidirektionale CHAP-Authentifizierung bietet eine zusätzliche Sicherheitsstufe. Mit dieser Methode kann der Initiator auch das Ziel authentifizieren. VMware unterstützt diese Methode nur für Software- und abhängige Hardware-iSCSI-Adapter sowie für iSER-Adapter.

Für Software- und abhängige Hardware-iSCSI-Adapter sowie für iSER-Adapter können Sie unidirektionales und bidirektionales CHAP für die einzelnen Adapter oder auf der Zielebene festlegen. Unabhängige Hardware-iSCSI unterstützt CHAP nur auf der Adapterebene.

Wenn Sie die CHAP-Parameter festlegen, geben Sie eine Sicherheitsstufe für CHAP an.

Hinweis Wenn Sie die CHAP-Sicherheitsebene angeben, ist die Reaktion des Speicher-Arrays anbieterspezifisch und hängt von der CHAP-Implementierung des Arrays ab. Weitere Informationen über das Verhalten der CHAP-Authentifizierung in verschiedenen Initiator- und Zielkonfigurationen finden Sie in der Array-Dokumentation.

Tabelle 11-2. CHAP-Sicherheitsstufe

CHAP-Sicherheitsstufe	Beschreibung	Unterstützte Speicheradapter
Keine	Der Host verwendet keine CHAP-Authentifizierung. Wenn die Authentifizierung aktiviert ist, verwenden Sie diese Option, um sie zu deaktivieren.	Unabhängige Hardware-iSCSI Software-iSCSI Abhängige Hardware-iSCSI iSER
Unidirektionales CHAP verwenden, wenn vom Ziel gefordert	Der Host bevorzugt eine Nicht-CHAP-Verbindung, er kann jedoch eine CHAP-Verbindung verwenden, wenn das Ziel dies erfordert.	Software-iSCSI Abhängige Hardware-iSCSI iSER
Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es	Der Host bevorzugt CHAP, er kann jedoch Nicht-CHAP-Verbindungen verwenden, wenn das Ziel CHAP nicht unterstützt.	Unabhängige Hardware-iSCSI Software-iSCSI Abhängige Hardware-iSCSI iSER
Unidirektionales CHAP verwenden	Für den Host ist eine erfolgreiche CHAP-Authentifizierung erforderlich. Die Verbindung schlägt fehl, wenn die CHAP-Aushandlung fehlschlägt.	Unabhängige Hardware-iSCSI Software-iSCSI Abhängige Hardware-iSCSI iSER
Bidirektionales CHAP verwenden	Der Host und das Ziel unterstützen bidirektionales CHAP.	Software-iSCSI Abhängige Hardware-iSCSI iSER

Einrichten von CHAP für iSCSI- oder iSER-Speicheradapter

Wenn Sie den CHAP-Namen und -Schlüssel auf der Ebene des iSCSI/iSER-Adapters einrichten, empfangen alle Ziele dieselben Parameter vom Adapter. Standardmäßig übernehmen alle Erkennungsadressen und statischen Ziele die CHAP-Parameter, die Sie auf der Adapterebene einrichten.

Der CHAP-Name darf nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen. Einige Adapter, z. B. der QLogic-Adapter, haben möglicherweise niedrigere Grenzen: 255 für den CHAP-Namen und 100 für den CHAP-Schlüssel.

Voraussetzungen

- Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI oder abhängige Hardware-iSCSI fest, ob unidirektionales oder bidirektionales CHAP konfiguriert werden soll. Abhängige Hardware-iSCSI-Adapter unterstützen das bidirektionale CHAP nicht.
- Überprüfen Sie die auf der Speicherseite konfigurierten CHAP-Parameter. Parameter, die Sie konfigurieren, müssen zu denen auf der Speicherseite passen.
- Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1 Navigieren Sie zum iSCSI- oder iSER-Speicheradapter.
   a Navigieren Sie im vSphere Client zum ESXi-Host.
   b Klicken Sie auf die Registerkarte **Konfigurieren**.
   c Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
2 Klicken Sie auf die Registerkarte **Eigenschaften** und klicken Sie im Bereich **Authentifizierung** auf **Bearbeiten**.
3 Legen Sie die Authentifizierungsmethode fest.
   - **Keine**
   - **Unidirektionales CHAP verwenden, wenn vom Ziel gefordert**
   - **Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es**
   - **Unidirektionales CHAP verwenden**
   - **Verwenden Sie bidirektionales CHAP**. Um bidirektionales CHAP zu konfigurieren, müssen Sie diese Option auswählen.
4 Geben Sie den ausgehenden CHAP-Namen an.

   Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.
   - Wenn der CHAP-Name dem iSCSI-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden (Use initiator name)**.
   - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Textfeld **Name** ein.
5 Geben Sie einen ausgehenden CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.

6 Wenn Sie bidirektionales CHAP konfigurieren, geben Sie eingehende CHAP-Anmeldedaten an.

   Für ausgehendes und eingehendes CHAP müssen Sie verschiedene Schlüssel verwenden.

7 Klicken Sie auf **OK**.

8 Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Ergebnisse

Wenn Sie die Parameter für CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Nächste Schritte

Weitere Konfigurationsschritte, die Sie für die iSCSI- oder ISER-Speicheradapter durchführen können, finden Sie in den folgenden Themen:

- Einrichten von unabhängigen Hardware-iSCSI-Adaptern
- Konfigurieren von abhängigen Hardware-iSCSI-Adaptern
- Konfigurieren des Software-iSCSI-Adapters
- Konfigurieren von iSER-Adaptern mit ESXi

Einrichten von CHAP für Ziele

Wenn Sie Software- und abhängige Hardware-iSCSI-Adapter oder einen iSER-Speicheradapter verwenden, können Sie verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.

Der CHAP-Name darf nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen.

Voraussetzungen

- Legen Sie vor dem Einrichten von CHAP-Parametern fest, ob unidirektionales oder bidirektionales CHAP konfiguriert werden soll.
- Überprüfen Sie die auf der Speicherseite konfigurierten CHAP-Parameter. Parameter, die Sie konfigurieren, müssen zu denen auf der Speicherseite passen.
- Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1 Navigieren Sie zum iSCSI- oder iSER-Speicheradapter.

   a Navigieren Sie im vSphere Client zum ESXi-Host.

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

   c Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.

2 Klicken Sie auf **Dynamische Erkennung** oder **Statische Erkennung**.

3 Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Authentifizierung**.

4 Heben Sie die Auswahl von **Einstellungen von übergeordnetem Element übernehmen** auf und legen Sie die Authentifizierungsmethode fest.

   - **Keine**
   - **Unidirektionales CHAP verwenden, wenn vom Ziel gefordert**
   - **Unidirektionales CHAP verwenden, es sei denn, das Ziel verbietet es**
   - **Unidirektionales CHAP verwenden**
   - **Verwenden Sie bidirektionales CHAP**. Um bidirektionales CHAP zu konfigurieren, müssen Sie diese Option auswählen.

5 Geben Sie den ausgehenden CHAP-Namen an.

   Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.

   - Wenn der CHAP-Name dem iSCSI-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden (Use initiator name)**.
   - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **Initiator-Name verwenden** und geben Sie einen Namen in das Textfeld **Name** ein.

6 Geben Sie einen ausgehenden CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll. Verwenden Sie denselben Schlüssel, den Sie auf der Speicherseite eingeben.

7 Wenn Sie bidirektionales CHAP konfigurieren, geben Sie eingehende CHAP-Anmeldedaten an.

   Für ausgehendes und eingehendes CHAP müssen Sie verschiedene Schlüssel verwenden.

8 Klicken Sie auf **OK**.

9 Führen Sie eine erneute Prüfung des Speicheradapters durch.

Ergebnisse

Wenn Sie die Parameter für CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Konfigurieren erweiterter Parameter für iSCSI

Unter Umständen müssen Sie zusätzliche Parameter für iSCSI-Initiatoren auf dem ESXi-Host konfigurieren. Beispielsweise erfordern einige iSCSI-Speichersysteme eine ARP-Umleitung (Address Resolution Protocol), um iSCSI-Datenverkehr dynamisch von einem Port auf einen anderen zu verschieben. In diesem Fall müssen Sie die ARP-Umleitung auf Ihrem Host aktivieren.

In der folgenden Tabelle sind die erweiterten iSCSI-Parameter aufgelistet, die Sie mit dem vSphere Client konfigurieren können. Darüber hinaus können Sie die vSphere-CLI-Befehle verwenden, um einige der erweiterten Parameter zu konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu *Erste Schritte mit ESXCLI*.

Je nach Adaptertyp sind bestimmte Parameter möglicherweise nicht verfügbar.

Wichtig Nehmen Sie keine Änderungen an den erweiterten iSCSI-Einstellungen vor, es sei denn, dies erfolgt unter Anleitung des VMware-Supports oder des Speicheranbieters.

Tabelle 11-3. Zusätzliche Parameter für iSCSI-Initiatoren

Erweiterte Parameter	Beschreibung
Header-Digest	Erhöht die Datenintegrität. Wenn der Parameter „Header-Digest“ aktiviert ist, berechnet das System für den Header-Teil jeder iSCSI-PDU (Protocol Data Unit) eine Prüfsumme. Das System überprüft die Daten anhand des CRC32C-Algorithmus.
Daten-Digest	Erhöht die Datenintegrität. Wenn der Parameter „Daten-Digest“ aktiviert ist, berechnet das System für den Daten-Teil jeder PDU eine Prüfsumme. Das System überprüft die Daten anhand des CRC32C-Algorithmus. **Hinweis** Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen für Software-iSCSI aus. Diese Auslagerung trägt dazu bei, die Auswirkungen auf die Leistung zu reduzieren.
ErrorRecoveryLevel	Wert des iSCSI Error Recovery Level (ERL), den der iSCSI-Initiator auf dem Host bei einer Anmeldung aushandelt.
LoginRetryMax	Maximale Anzahl an Anmeldeversuchen des ESXi-iSCSI-Initiators bei einem Ziel, bevor diese eingestellt werden.
MaxOutstandingR2T	Legt fest, wie viele R2T-PDUs (Ready to Transfer) sich im Übergang befinden können, bevor eine bestätigte PDU empfangen wird.
FirstBurstLength	Legt die maximale Menge an nicht angeforderten Daten in Byte fest, die ein iSCSI-Initiator während der Ausführung eines einzelnen SCSI-Befehls an das Ziel senden kann.
MaxBurstLength	Die maximale SCSI-Datenlast in einer Data-In- oder einer angeforderten Data-Out-iSCSI-Sequenz in Byte.
MaxRecvDataSegLength	Die maximale Datensegmentlänge in Byte, die in einer iSCSI-PDU empfangen werden kann.

Tabelle 11-3. Zusätzliche Parameter für iSCSI-Initiatoren (Fortsetzung)

Erweiterte Parameter	Beschreibung
MaxCommands	Maximale Anzahl an SCSI-Befehlen, die im iSCSI-Adapter in die Warteschlange gestellt werden können.
DefaultTimeToWait	Mindestzeit in Sekunden, die nach dem unerwarteten Beendigen oder dem Zurücksetzen einer Verbindung abgewartet wird, bevor eine Abmeldung oder eine erneute Zuweisung einer aktiven Aufgabe versucht wird.
DefautTimeToRetain	Maximale Zeit in Sekunden, während der eine aktive Aufgabe nach Trennung der Verbindung oder einem Zurücksetzen noch neu zugewiesen werden kann.
LoginTimeout	Zeit in Sekunden, die ein Initiator auf das Beenden der Anmeldeantwort wartet.
LogoutTimeout	Zeit in Sekunden, die ein Initiator auf eine Antwort auf die Abmeldeanforderung PDU wartet.
RecoveryTimeout	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor eine Sitzung wiederhergestellt werden kann. Wird der angegebene Zeitraum überschritten, beendet der iSCSI-Initiator die Sitzung.
No-Op-Intervall	Gibt das Zeitintervall in Sekunden an, in dem NOP-Out-Anforderungen von Ihrem iSCSI-Initiator an ein iSCSI-Ziel gesendet werden. Mithilfe der NOP-Out-Anforderungen kann verifiziert werden, ob zwischen dem iSCSI-Initiator und dem iSCSI-Ziel eine aktive Verbindung besteht.
No-Op-Zeitüberschreitung	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor Ihr Host eine NOP-In-Meldung erhält. Das iSCSI-Ziel sendet die Meldung als Antwort auf die NOP-Out Anforderung. Wenn der Grenzwert für die No-Op-Zeitüberschreitung erreicht wurde, beendet der Initiator die aktuelle und startet eine neue Sitzung.
ARP-Weiterleitung	Wenn dieser Parameter aktiviert ist, können Speichersysteme iSCSI-Datenverkehr dynamisch von einem Port auf einen anderen verschieben. Speichersysteme, die Array-basierte Failover durchführen, benötigen den ARP-Parameter.
Verzögerte Quittierung (ACK)	Wenn dieser Parameter aktiviert ist, können Speichersysteme die Bestätigung empfangener Datenpakete verzögern.

Konfigurieren erweiterter Parameter für iSCSI auf ESXi-Host

Die erweiterten iSCSI-Einstellungen steuern Parameter wie „Header-Digest“, „Data Digest“, „ARP-Umleitung“, „Verzögerte Quittierung (ACK)“ usw.

Vorsicht Sie sollten die erweiterten iSCSI-Einstellungen nur ändern, wenn Sie eng mit dem Support-Team von VMware zusammenarbeiten oder anderweitig über umfassende Informationen zu den Werten der einzelnen Einstellungen verfügen.

Voraussetzungen

Erforderliche Berechtigung: **Host.Konfiguration.Konfiguration für Speicherpartition**

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.

4 Konfigurieren Sie die erweiterten Parameter.

Option	Beschreibung
Auf der Adapterebene	Klicken Sie auf die Registerkarte **Erweiterte Optionen** und anschließend auf **Bearbeiten**.
Auf der Zielebene	a Klicken Sie auf **Dynamische Erkennung** oder **Statische Erkennung**. b Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **Erweitert**.

5 Geben Sie die erforderlichen Werte für die erweiterten Parameter ein, die Sie ändern möchten.

iSCSI-Sitzungsverwaltung

Um miteinander zu kommunizieren, richten iSCSI-Initiatoren und -Ziele iSCSI-Sitzungen ein. Sie können iSCSI-Sitzungen mithilfe der vSphere-CLI prüfen und verwalten.

Standardmäßig starten Software-iSCSI- und abhängige Hardware-iSCSI-Initiatoren eine iSCSI-Sitzung zwischen jedem Initiatorport und jedem Zielport. Wenn Ihr iSCSI-Initiator oder -Ziel über mehrere Ports verfügt, können auf Ihrem Host mehrere Sitzungen eingerichtet sein. Die Standardanzahl an Sitzungen für jedes Ziel entspricht dem Produkt aus der Anzahl an Ports auf dem iSCSI-Adapter und der Anzahl an Zielports.

Mit vSphere CLI können Sie alle aktuellen Sitzungen anzeigen, um sie zu analysieren und zu debuggen. Wenn Sie weitere Pfade zu Speichersystemen erstellen möchten, können Sie die Standardanzahl an Sitzungen erhöhen, indem Sie die bestehenden Sitzungen zwischen dem iSCSI-Adapter und den Zielports duplizieren.

Sie können auch eine Sitzung mit einem bestimmten Zielport einrichten. Diese Funktion ist nützlich, wenn der Host eine Verbindung zu einem Einzelportspeichersystem herstellt, das dem Initiator nur einen Zielport präsentiert. Das System leitet zusätzliche Sitzungen dann an einen anderen Zielport weiter. Durch das Einrichten einer neuen Sitzung zwischen Ihrem iSCSI-Initiator und einem anderen Zielport wird ein zusätzlicher Pfad zum Speichersystem erstellt.

Für die iSCSI-Sitzungsverwaltung muss Folgendes beachtet werden:

- Einige Speichersysteme bieten keine Unterstützung für mehrere Sitzungen von demselben Initiatornamen oder Endpunkt aus. Wenn Sie mehrere Sitzungen mit solchen Zielen erstellen, kann dies zu unvorhersehbarem Verhalten Ihrer iSCSI-Umgebung führen.
- Speicheranbieter können automatische Sitzungs-Manager bereitstellen. Die Verwendung des automatischen Sitzungs-Managers zum Hinzufügen oder Löschen von Sitzungen garantiert keine nachhaltigen Ergebnisse und kann die Speicherleistung beeinträchtigen.

Überprüfen von iSCSI-Sitzungen

Verwenden Sie den vCLI-Befehl, um iSCSI-Sitzungen zwischen einem iSCSI-Adapter und einem Speichersystem anzuzeigen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um iSCSI-Sitzungen aufzulisten:

  `esxcli iscsi session list`

  Der Befehl verfügt über diese Optionen:

Option	Beschreibung
**`-A|--adapter=`*`str`*	Der Name des iSCSI-Adapters, z. B. vmhba34.
**`-s|--isid=`*`str`*	Der Bezeichner der iSCSI-Sitzung.
**`-n|--name=`*`str`*	Der Name des iSCSI-Ziels, z. B. iqn.X.

Hinzufügen von iSCSI-Sitzungen

Verwenden Sie die vCLI, um eine iSCSI-Sitzung für das von Ihnen angegebene Ziel hinzuzufügen oder um eine vorhandene Sitzung zu duplizieren. Durch das Duplizieren von Sitzungen erhöhen Sie die Standardanzahl an Sitzungen und erstellen zusätzliche Pfade zu Speichersystemen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um eine iSCSI-Sitzung hinzuzufügen oder zu duplizieren:

  `esxcli iscsi session add`

  Der Befehl verfügt über diese Optionen:

Option	Beschreibung
-A|--adapter=*str*	Der Name des iSCSI-Adapters, z. B. vmhba34. Diese Option ist erforderlich.
-s|--isid=*str*	Die ISID einer zu duplizierenden Sitzung. Sie finden diese, indem Sie alle Sitzungen auflisten.
-n|--name=*str*	Der Name des iSCSI-Ziels, z. B. iqn.X.

Nächste Schritte

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Entfernen von iSCSI-Sitzungen

Verwenden Sie den vCLI-Befehl, um eine iSCSI-Sitzung zwischen einem iSCSI-Adapter und einem Ziel zu entfernen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um eine Sitzung zu entfernen:

  `esxcli iscsi session remove`

  Der Befehl verfügt über diese Optionen:

Option	Beschreibung
**`-A|--adapter=`*`str`*	Der Name des iSCSI-Adapters, z. B. vmhba34. Diese Option ist erforderlich.
**`-s|--isid=`*`str`*	Die ISID einer zu entfernenden Sitzung. Sie finden diese, indem Sie alle Sitzungen auflisten.
**`-n|--name=`*`str`*	Der Name des iSCSI-Ziels, z. B. iqn.X.

Nächste Schritte

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Starten von einem iSCSI-SAN 12

Wenn Sie Ihren Host so einrichten, dass er von einem SAN gestartet wird, wird das Start-Image des Hosts auf einer oder mehreren LUNs im SAN-Speichersystem gespeichert. Wenn der Host startet, wird er nicht von seiner lokalen Festplatte aus, sondern von der LUN im SAN aus gestartet.

Sie können das Starten vom SAN verwenden, wenn Sie keinen lokalen Speicher warten möchten oder Hardwarekonfigurationen ohne Festplatten haben, wie z. B. Blade-Systeme.

ESXi unterstützt verschiedene Methoden zum Starten vom iSCSI-SAN.

Tabelle 12-1. Unterstützung für das Starten vom iSCSI-SAN

Unabhängige Hardware-iSCSI	Software-iSCSI
Konfigurieren Sie den iSCSI-HBA für das Starten vom SAN. Informationen zur HBA-Konfiguration finden Sie unter Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN	Verwenden Sie den Software-iSCSI-Adapter und einen Netzwerkadapter, der das iBFT-Format (iSCSI Boot Firmware Table) unterstützt. Weitere Informationen finden Sie unter *Installation und Einrichtung von VMware ESXi*.

Dieses Kapitel enthält die folgenden Themen:

- Allgemeine Empfehlungen für das Starten von iSCSI-SAN
- Vorbereiten des iSCSI-SAN
- Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN

Allgemeine Empfehlungen für das Starten von iSCSI-SAN

Wenn Sie eine iSCSI-LUN als Startgerät für Ihren Host einrichten und verwenden möchten, müssen Sie einige allgemeine Richtlinien befolgen.

Es gelten die folgenden Richtlinien für das Starten der unabhängigen Hardware-iSCSI und iBFT.

- Prüfen Sie die Herstellerempfehlungen für die Hardware, die Sie in Ihrer Startkonfiguration verwenden.
- Weitere Informationen zu Installationsvoraussetzungen und -anforderungen finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.
- Verwenden Sie statische IP-Adressen, um das Auftreten von DHCP-Konflikten zu vermeiden.

- Verwenden Sie für VMFS-Datenspeicher und Startpartitionen verschiedene LUNs.
- Konfigurieren Sie auf Ihrem Speichersystem ordnungsgemäße ACLs.
  - Die Start-LUN darf nur für den Host sichtbar sein, der die LUN verwendet. Auf diese Start-LUN dürfen andere Hosts im SAN nicht zugreifen.
  - Wenn eine LUN für einen VMFS-Datenspeicher verwendet wird, können mehrere Hosts die LUN gemeinsam nutzen.
- Konfigurieren Sie eine Diagnosepartition.
  - Nur bei unabhängiger Hardware-iSCSI können Sie die Diagnosepartition auf der Start-LUN platzieren. Wenn Sie die Diagnosepartition in der Start-LUN konfigurieren, kann diese LUN nicht von mehreren Hosts verwendet werden. Wenn eine separate LUN für eine Diagnosepartition verwendet wird, können mehrere Hosts die LUN gemeinsam nutzen.
  - Wenn Sie mithlfe von iBFT vom SAN starten, können Sie keine Diagnosepartition auf einer SAN-LUN einrichten. Verwenden Sie vSphere ESXi Dump Collector auf einem Remoteserver, um die Diagnoseinformationen Ihres Hosts zu erfassen. Informationen zu ESXi Dump Collector finden Sie unter *Installation und Einrichtung von vCenter Server* und *vSphere-Netzwerk*.

Vorbereiten des iSCSI-SAN

Bevor Sie Ihren Host zum Starten von einer iSCSI-LUN konfigurieren, müssen Sie Ihr SAN vorbereiten und konfigurieren.

Vorsicht Wenn Sie über ein SAN starten und die Installation von ESXi per Skript erfolgt, müssen Sie bestimmte Schritte ausführen, um einen unerwünschten Datenverlust zu vermeiden.

Verfahren

1. Schließen Sie die Netzwerkkabel an, wie in den Handbüchern der betreffenden Geräte beschrieben.
2. Stellen Sie die IP-Verbindung zwischen dem Speichersystem und dem Server sicher.

   Überprüfen Sie die ordnungsgemäße Konfiguration aller Router und Switches im Speichernetzwerk. Speichersysteme müssen ein Ping-Signal an die iSCSI-Adapter in den Hosts senden können.

3 Konfigurieren Sie das Speichersystem.

   a Erstellen Sie ein Volume (oder eine LUN) im Speichersystem für Ihren Host, von dem gebootet werden soll.

   b Konfigurieren Sie das Speichersystem, sodass Ihr Host auf die zugewiesene LUN zugreifen kann.

      Dieser Schritt beinhaltet möglicherweise ein Update der ACLs mit den IP-Adressen, den iSCSI-Namen und dem CHAP-Authentifizierungsparameter, den Sie auf Ihrem Host verwenden. Auf einigen Speichersystemen müssen Sie nicht nur die Zugriffsdaten für den ESXi-Host angeben, sondern auch die zugewiesene LUN ausdrücklich mit dem Host verknüpfen.

   c Stellen Sie sicher, dass die LUN dem Host ordnungsgemäß präsentiert wird.

   d Stellen Sie sicher, dass kein anderes System auf die konfigurierte LUN zugreifen kann.

   e Schreiben Sie sich den iSCSI-Namen und die IP-Adresse der Ziele auf, die dem Host zugewiesen sind.

      Sie benötigen diese Informationen für die Konfiguration Ihrer iSCSI-Adapter.

Konfigurieren eines unabhängigen Hardware-iSCSI-Adapters für das Starten von einem SAN

Wenn Ihr ESXi-Host einen unabhängigen Hardware-iSCSI-Adapter verwendet, wie z. B. einen QLogic-HBA, können Sie den Adapter so konfigurieren, dass er vom SAN startet.

Dieses Verfahren erläutert, wie der QLogic-iSCSI-HBA für das Starten vom SAN aktiviert wird. Weitere Informationen und aktuelle Einzelheiten zu den QLogic-Adapter-Konfigurationseinstellungen finden Sie auf der QLogic-Website.

Verfahren

1 Starten Sie das Installationsmedium und starten Sie den Host neu.

2 Stellen Sie im BIOS ein, dass der Host zuerst vom Installationsmedium aus gestartet wird.

3 Drücken Sie während des Server-POST die Tastenkombination Strg+q, um das QLogic-iSCSI-HBA-Konfigurationsmenü zu öffnen.

4 Wählen Sie den zu konfigurierenden E/A-Port.

   Standardmäßig ist Adapterstartmodus (Adapter Boot Mode) auf Deaktivieren (Disable) gesetzt.

5 Konfigurieren Sie den HBA.

   a Wählen Sie aus dem Menü **Fast!UTIL-Optionen (Fast!UTIL Options)** die Option **Konfigurationseinstellungen (Configuration Settings) > Host Adapter Settings (Hostadaptereinstellungen)** aus.

   b (Optional) Konfigurieren Sie die folgenden Einstellungen für Ihren Hostadapter: Initiator-IP-Adresse, Subnetzmaske, Gateway, Initiator-iSCSI-Name und CHAP.

6 Konfigurieren Sie die iSCSI-Einstellungen.

   Weitere Informationen hierzu finden Sie unter Konfigurieren der iSCSI-Starteinstellungen.

7 Speichern Sie die Änderungen, und starten Sie das System neu.

Konfigurieren der iSCSI-Starteinstellungen

Konfigurieren Sie iSCSI-Startparameter, sodass Ihr ESXi-Host von einer iSCSI-LUN starten kann.

Verfahren

1 Wählen Sie aus dem Menü **Fast!UTIL Options** die Option **Configuration Settings > iSCSI Boot Settings** aus.

2 Bevor Sie SendTargets festlegen können, müssen Sie den Adapter-Startmodus auf **Manual** festlegen.

3 Aktivieren Sie **Primary Boot Device Settings**.

   a Geben Sie **Target IP** und **Target Port** für die Zielerkennung ein.

   b Konfigurieren Sie die Parameter **Boot LUN** und **iSCSI Name** .

      - Wenn nur ein iSCSI-Ziel und eine LUN an der Zieladresse verfügbar sind, lassen Sie **Boot LUN** und **iSCSI Name** leer.

        Nachdem der Host das Zielspeichersystem erreicht, werden diese Textfelder mit entsprechenden Informationen gefüllt.

      - Wenn mehr als ein iSCSI-Ziel und eine LUN verfügbar sind, geben Sie Werte für **Start LUN** und **iSCSI Name** ein.

   c Speichern Sie die Änderungen.

4 Wählen Sie im Menü **iSCSI Boot Settings** das primäre Startgerät.

   Bei einer automatisch durchgeführten erneuten HBA-Prüfung werden neue Ziel-LUNs gefunden.

5 Wählen Sie das iSCSI-Ziel.

   Wenn mehr als eine LUN im Ziel vorhanden ist, können Sie eine bestimmte LUN-ID wählen, indem Sie nach Auswahl des iSCSI-Gerätes die **Eingabetaste** drücken.

6 Öffnen Sie das Menü **Primary Boot Device Setting**. Nach der erneuten Prüfung sind die Felder **Boot LUN** und **iSCSI Name** ausgefüllt. Ändern Sie den Wert von **Boot LUN** in die gewünschte LUN-ID.

Best Practices für iSCSI-Speicher 13

Befolgen Sie bei der Verwendung von ESXi mit iSCSI-SAN die Empfehlungen von VMware, um Probleme zu vermeiden.

Erkundigen Sie sich bei Ihrem Speicheranbieter, ob Ihr Speichersystem die Hardwarebeschleunigungsfunktionen der Storage-APIs für die Array-Integration unterstützt. Wenn ja, lesen Sie in der Dokumentation Ihres Anbieters nach, um die Unterstützung für die Hardwarebeschleunigung auf dem Speichersystem zu aktivieren. Weitere Informationen finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.

Dieses Kapitel enthält die folgenden Themen:

Vermeiden von iSCSI-SAN-Problemen

Bei Verwendung von ESXi mit einem SAN müssen Sie bestimmte Richtlinien befolgen, um SAN-Probleme zu vermeiden.

Beachten Sie die folgenden Tipps:

- Platzieren Sie nur einen einzigen VMFS-Datenspeicher in jeder LUN.
- Ändern Sie die vom System festgelegte Pfadrichtlinie nur, wenn Sie die Auswirkungen dieser Änderung kennen und verstehen.
- Erstellen Sie eine ausführliche Dokumentation. Notieren Sie Informationen zu Konfiguration, Zugriffssteuerung, Speicher, Switch, Server und iSCSI-HBA-Konfiguration, Software- und Firmware-Versionen sowie zum Speicherkabelplan.
- Erstellen Sie einen Notfallplan bei Ausfällen:
  - Kopieren Sie Ihre Topologiezuordnungen mehrfach. Ermitteln Sie für jedes Element, welche Auswirkungen ein Ausfall dieses Elements auf das SAN hat.
  - Stellen Sie mithilfe einer Liste aller Verbindungen, Switches, HBAs und anderen Elemente sicher, dass Sie keine wichtige Fehlerstelle in Ihrem Design übersehen haben.

- Stellen Sie sicher, dass die iSCSI-HBAs an den geeigneten Steckplätzen des ESXi-Hosts installiert sind (basierend auf Steckplatz- und Busgeschwindigkeit). Richten Sie einen PCI-Bus-Lastausgleich für alle Busse des Servers ein.
- Machen Sie sich mit den verschiedenen Überwachungspunkten in Ihrem Speichernetzwerk an allen Sichtbarkeitspunkten vertraut (einschließlich ESXi-Leistungsdiagramme sowie Statistiken zu Ethernet-Switches und Speicherleistung).
- Ändern Sie LUN-IDs nur, wenn der auf den LUNs bereitgestellte VMFS-Datenspeicher nicht über laufende virtuelle Maschinen verfügt. Wenn Sie die ID ändern, schlagen die auf dem VMFS-Datenspeicher ausgeführten virtuellen Maschinen möglicherweise fehl.

  Nachdem Sie die ID der LUN geändert haben, müssen Sie den Speicher erneut prüfen, um die ID auf Ihrem Host zurückzusetzen. Weitere Informationen über das erneute Prüfen finden Sie unter Vorgänge zum erneuten Prüfen des Speichers.
- Wenn Sie den standardmäßigen iSCSI-Namen Ihres iSCSI-Adapters ändern müssen, stellen Sie sicher, dass der Name, den Sie eingeben, weltweit eindeutig und ordnungsgemäß formatiert ist. Um Speicherzugriffsprobleme zu vermeiden, weisen Sie unterschiedlichen Adaptern niemals denselben iSCSI-Namen zu, auch nicht auf unterschiedlichen Hosts.

Optimieren der iSCSI-SAN-Speicherleistung

Bei der Optimierung einer typischen SAN-Umgebung müssen verschiedene Faktoren berücksichtigt werden.

Bei ordnungsgemäßer Konfiguration der Netzwerkumgebung sollten die iSCSI-Komponenten einen ausreichenden Durchsatz und eine ausreichend geringe Latenz für iSCSI-Initiatoren und -Ziele bieten. Wenn das Netzwerk überlastet und die maximale Leistung von Verbindungen, Switches oder Routern erreicht ist, ist die iSCSI-Leistung beeinträchtigt und möglicherweise nicht mehr ausreichend für ESXi-Umgebungen.

Speichersystemleistung

Einer der wichtigsten Faktoren für die Optimierung einer kompletten iSCSI-Umgebung ist die Speichersystemleistung.

Bei Problemen mit der Speichersystemleistung lesen Sie die entsprechende Dokumentation des Speichersystem-Anbieters.

Bedenken Sie beim Zuweisen von LUNs, dass über verschiedene Hosts auf jede gemeinsam genutzte LUN zugegriffen werden kann und dass auf jedem Host mehrere virtuelle Maschinen ausgeführt werden können. Auf einer LUN, die vom ESXi-Host verwendet wird, sind E/A-Vorgänge von einer Vielzahl von unterschiedlichen Anwendungen möglich, die unter verschiedenen Betriebssystemen ausgeführt werden. Aufgrund dieser unterschiedlichen Arbeitslast sollte die RAID-Gruppe mit den ESXi-LUNs keine LUNs enthalten, die von anderen Hosts verwendet werden, auf denen nicht ESXi für E/A-intensive Anwendungen ausgeführt wird.

Aktivieren Sie die Lese- und Schreibcache.

Lastenausgleich ist der Vorgang zum Verteilen von E/A-Anforderungen eines Servers auf alle verfügbaren Speicherprozessoren und die verknüpften Hostserverpfade. Das Ziel ist die Optimierung der Leistung im Hinblick auf den Durchsatz (E/A pro Sekunde, MB pro Sekunde oder Reaktionszeiten).

SAN-Speichersysteme müssen kontinuierlich neu ausgelegt und optimiert werden, um sicherzustellen, dass die E/A-Last auf alle Speichersystempfade verteilt ist. Um diese Anforderung zu erfüllen, verteilen Sie die Pfade zu den LUNs auf alle Speicherprozessoren. Das Ergebnis ist ein optimaler Lastenausgleich. Eine sorgfältige Überwachung zeigt an, wenn die LUN-Verteilung manuell angepasst werden muss.

Bei der Optimierung von Speichersystemen mit statischem Lastenausgleich ist die Überwachung der spezifischen Leistungsstatistiken (beispielsweise E/A-Vorgänge pro Sekunde, Blocks pro Sekunde und Reaktionszeit) und Verteilung der LUN-Arbeitslast auf alle Speicherprozessoren von größter Bedeutung.

Serverleistung mit iSCSI

Um eine optimale Leistung des ESXi-Hosts sicherzustellen, müssen verschiedene Faktoren berücksichtigt werden.

Der Zugriff jeder Serveranwendung auf den integrierten Speicher muss mit den folgenden Bedingungen gewährleistet sein:

- Hohe E/A-Rate (Anzahl an E/A-Vorgängen pro Sekunde)
- Hoher Durchsatz (MB pro Sekunde)
- Minimale Latenz (Reaktionszeiten)

Da für jede Anwendung andere Anforderungen gelten, können Sie diese Ziele erreichen, indem Sie eine geeignete RAID-Gruppe für das Speichersystem wählen.

Zum Erreichen von Leistungszielen halten Sie sich an die folgenden Richtlinien:

- Platzieren Sie jede LUN in einer RAID-Gruppe, die die erforderlichen Leistungsebenen bietet. Überwachen Sie die Aktivitäten und Ressourcennutzung anderer LUNs in der zugewiesenen RAID-Gruppe. Mit einer hochleistungsfähigen RAID-Gruppe mit zu vielen Anwendungen, die eine E/A-Last verursachen, können die Leistungsziele möglicherweise nicht erreicht werden, die für eine Anwendung auf dem ESXi-Host erforderlich sind.
- Um den maximalen Durchsatz für die Anwendungen auf dem Host in der Spitzenzeit zu erzielen, installieren Sie genügend Netzwerkadapter bzw. iSCSI-Hardwareadapter. Bei Verteilung der E/A-Last auf mehrere Ports wird ein höherer Durchsatz und eine geringere Latenz für jede Anwendung erreicht.
- Um für Software-iSCSI Redundanz zu bieten, verbinden Sie den Initiator mit allen Netzwerkadaptern, die für die iSCSI-Konnektivität verwendet werden.

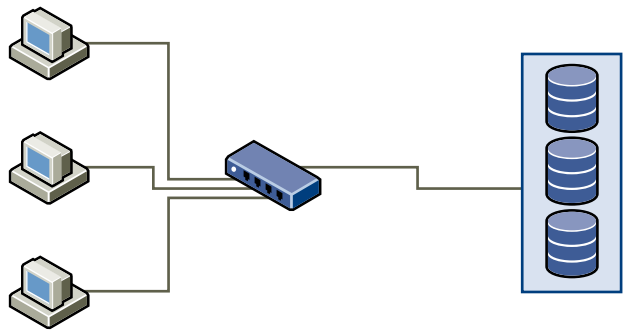
- Beachten Sie, dass beim Zuweisen von LUNs oder RAID-Gruppen für ESXi-Systeme diese Ressourcen durch mehrere Betriebssysteme gemeinsam verwendet werden. Die vom ESXi-Host erforderliche LUN-Leistung könnte viel höher als die Leistung sein, die normale physische Maschinen benötigen. Wenn Sie z. B. die Ausführung von vier E/A-intensiven Anwendungen planen, weisen Sie für die ESXi-LUNs die vierfache Leistungskapazität zu.
- Wenn Sie mehrere ESXi-Systeme mit vCenter Server verwenden, erhöhen sich die Anforderungen an die Speicherleistung.
- Die Anzahl an ausstehenden E/A-Vorgängen von Anwendungen, die auf einem ESXi-System ausgeführt werden, muss mit der Anzahl an E/A-Vorgängen übereinstimmen, die das SAN verarbeiten kann.

Netzwerkleistung

Ein typisches SAN umfasst verschiedene Computer, die über ein Netzwerk aus Switches mit verschiedenen Speichersystemen verbunden sind. Mehrere Computer greifen häufig auf denselben Speicher zu.

Die folgende Abbildung zeigt verschiedene Computersysteme, die über einen Ethernet-Switch mit einem Speichersystem verbunden sind. In dieser Konfiguration wird jedes System über eine einzige Ethernet-Verbindung mit dem Switch verbunden. Der Switch wird mit dem Speichersystem über eine einzige Ethernet-Verbindung verbunden.

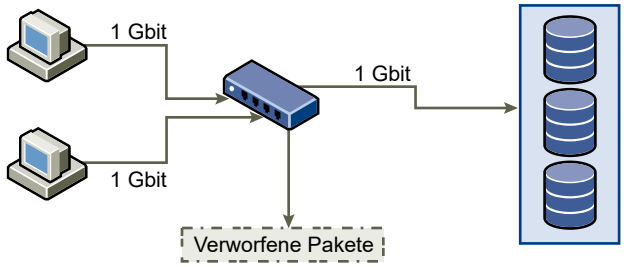
Abbildung 13-1. Eine einzige Ethernet-Verbindung mit dem Speicher



Wenn Systeme Daten aus dem Speicher lesen, reagiert der Speicher mit dem Senden von genügend Daten, um die Verbindung zwischen den Speichersystemen und dem Ethernet-Switch zu füllen. Es ist unwahrscheinlich, dass ein einziges System oder eine einzige virtuelle Maschine die Netzwerkgeschwindigkeit vollständig nutzen. Diese Situation kann jedoch eintreten, wenn viele Systeme ein Speichergerät gemeinsam nutzen.

Beim Schreiben von Daten in den Speicher versuchen möglicherweise mehrere Systeme oder virtuelle Maschinen, ihre Datenträger zu füllen. Der Switch zwischen den Systemen und dem Speichersystem kann jedoch Pakete im Netzwerk verwerfen. Das Verwerfen der Daten kann auftreten, weil der Switch mehr Datenverkehr zum Speichersystem senden muss, als ein eine einzelne Verbindung übertragen kann. Die Menge an Daten, die der Switch übertragen kann, wird durch die Geschwindigkeit der Verbindung zwischen dem Switch und dem Speichersystem begrenzt.

Abbildung 13-2. Verworfene Pakete



Das Wiederherstellen von verworfenen Netzwerkpaketen führt zu einer erheblichen Leistungsbeeinträchtigung. Neben der Zeit zur Ermittlung, dass Daten verloren gegangen sind, ist für die erneute Übermittlung Netzwerkbandbreite erforderlich, die anderenfalls für aktuelle Transaktionen verwendet werden kann.

iSCSI-Datenverkehr wird innerhalb des Netzwerks über TCP (Transmission Control Protocol) übermittelt. Bei TCP handelt es sich um ein zuverlässiges Übertragungsprotokoll, mit dem Sie sicherstellen, dass wiederholt versucht wird, verworfene Pakete zu übermitteln, bis diese ihr Ziel erreichen. TCP ist für eine Wiederherstellung und schnelle und problemlose Übermittlung von verworfenen Paketen konzipiert. Wenn der Switch jedoch regelmäßig Pakete verwirft, ist der Netzwerkdurchsatz reduziert. Das Netzwerk wird überlastet mit Anforderungen zum Senden der Daten und mit den zurückgesendeten Paketen. Es werden weniger Daten übertragen als in einem Netzwerk ohne Überlastung.

Die meisten Ethernet-Switches können Daten puffern oder speichern. Mit dieser Technik erhält jedes Gerät, das versucht, Daten zu senden, die gleiche Möglichkeit, zum Ziel zu gelangen. Die Möglichkeit zum Puffern einiger Übertragungen zusammen mit vielen Systemen, die die Anzahl ausstehender Befehle begrenzen, reduziert die Übertragungen auf kleine Spitzen. Die Spitzen von mehreren Systemen können wiederum zu einem Speichersystem gesendet werden.

Wenn die Transaktionen umfangreich sind und mehrere Server Daten über einen einzelnen Switch-Port senden, kann die Möglichkeit zum Puffern erweitert werden. In diesem Fall werden die Daten, die der Switch nicht senden kann, verworfen, und das Speichersystem muss die erneute Übermittlung des verworfenen Pakets anfordern. Wenn zum Beispiel ein Ethernet-Switch 32 KB puffern kann, der Server aber 256 KB an das Speichergerät sendet, werden einige der Daten verworfen.

Die meisten verwalteten Switches bieten Informationen zu verworfenen Paketen, die in etwa den folgenden Angaben entsprechen:

```
*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

Tabelle 13-1. Beispiel zu Switch-Informationen

Schnittstelle	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

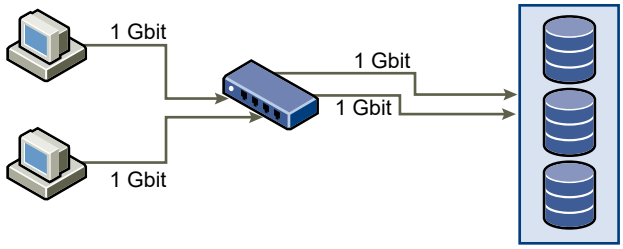
In diesem Beispiel eines Cisco-Switches lautet die verwendete Bandbreite 476303000 Bit/s, also weniger als die Hälfte der Kabelgeschwindigkeit. Der Port puffert eingehende Pakete, einige Pakete wurden jedoch verworfen. Die letzte Zeile dieser Schnittstellenübersicht zeigt, dass diese Schnittstelle bereits fast 10.000 eingehende Pakete in der IQD-Spalte verworfen hat.

Um dieses Problem zu verhindern, sind Konfigurationsänderungen erforderlich. Stellen Sie dabei sicher, dass eingehende Ethernet-Verbindungen nicht zu einer ausgehenden Verbindung zusammengefasst werden, sodass die Verbindung „überbucht“ wird. Wenn einige Verbindungen, die nahezu die gesamte Kapazität übertragen, auf eine kleinere Zahl an Verbindungen reduziert werden, kann dies zu einer Überbuchung führen.

In der Regel müssen Anwendungen oder Systeme, die viele Daten in den Speicher schreiben, die gemeinsame Nutzung von Ethernet-Verbindungen zu einem Speichergerät vermeiden. Für diese Anwendungstypen wird mit mehreren Verbindungen zu Speichergeräten eine optimale Leistung erzielt.

„Mehrere Verbindungen zwischen Switch und Speicher“ zeigt mehrere Verbindungen vom Switch zum Speicher.

Abbildung 13-3. Mehrere Verbindungen zwischen Switch und Speicher



Die Verwendung von VLANs oder VPNs ist keine geeignete Lösung für das Problem von überlasteten Verbindungen in Konfigurationen mit gemeinsam verwendeten Komponenten. VLANs und andere virtuelle Partitionierungen von Netzwerken bieten die Möglichkeit für ein logisches Netzwerkdesign. Die physischen Kapazitäten von Verbindungen und Trunks zwischen Switches werden dadurch jedoch nicht geändert. Wenn Speicherdatenverkehr und anderer Netzwerkverkehr physische Verbindungen gemeinsam nutzen, kann es zu einer Überbuchung und zu verworfenen Paketen kommen. Gleiches gilt für VLANs mit gemeinsamen Interswitch-Trunks. Für die Leistungsberechnungen in einem SAN müssen die physischen Grenzen des Netzwerks, nicht die logischen Zuordnungen berücksichtigt werden.

Überprüfen von Ethernet-Switch-Statistiken

Eine Vielzahl von Ethernet-Switches bieten verschiedene Methoden zur Überwachung des Switch-Status.

Switches mit Ports, welche die meiste Zeit einen fast maximalen Durchsatz erzielen, bieten keine optimale Leistung. Wenn Sie in Ihrem iSCSI-SAN über solche Ports verfügen, reduzieren Sie die Last. Wenn der Port mit einem ESXi-System oder iSCSI-Speicher verbunden ist, kann die Last über einen manuellen Lastenausgleich reduziert werden.

Wenn der Port mit mehreren Switches oder Routern verbunden ist, ziehen Sie die Installation zusätzlicher Verbindungen zwischen diesen Komponenten in Betracht, um eine höhere Last verarbeiten zu können. Ethernet-Switches bieten darüber hinaus meist Informationen zu Übertragungsfehlern, in der Warteschlange platzierten Paketen und verworfenen Ethernet-Paketen. Wenn ein Switch diese Bedingungen regelmäßig für Ports anzeigt, die für den iSCSI-Datenverkehr verwendet werden, bietet das iSCSI-SAN eine schlechte Leistung.

Verwalten von Speichergeräten 14

Verwalten des lokalen und vernetzten Speichergeräts, auf das Ihr ESXi-Host zugreifen kann.

Dieses Kapitel enthält die folgenden Themen:

- Eigenschaften des Speichergeräts
- Namen und Bezeichner von Speichergeräten
- Vorgänge zum erneuten Prüfen des Speichers
- Identifizieren von Problemen hinsichtlich der Gerätekonnektivität
- Aktivieren oder Deaktivieren der Locator-LEDs auf ESXi-Speichergeräten
- Löschen von Speichergeräten
- Ändern dauerhafter Reservierungseinstellungen

Eigenschaften des Speichergeräts

Wenn der ESXi-Host mit blockbasierten Speichersystemen verbunden wird, verfügt der Host über LUNs oder Speichergeräte, die ESXi unterstützen.

Nachdem die Geräte bei Ihrem Host registriert wurden, können Sie alle verfügbaren lokalen und vernetzten Geräte anzeigen und deren Informationen überprüfen. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

Hinweis Wenn ein Array impliziten Asymmetric Logical Unit Access (ALUA) unterstützt und nur über Standby-Pfade verfügt, schlägt die Registrierung des Geräts fehl. Das Gerät kann beim Host registriert werden, nachdem das Ziel einen Standby-Pfad aktiviert und es vom Host als aktiv erkannt wurde. Der erweiterte `/Disk/FailDiskRegistration`-Systemparameter steuert dieses Verhalten des Hosts.

Sie können für jeden Speicheradapter eine separate Liste von Speichergeräten anzeigen, die für diesen Adapter verfügbar sind.

In der Regel wird Ihnen beim Überprüfen von Speichergeräten Folgendes angezeigt.

Tabelle 14-1. Informationen zum Speichergerät

Informationen zum Speichergerät	Beschreibung
Name	Auch als Anzeigename bezeichnet. Es ist ein Name, den der ESXi-Host dem Gerät anhand des Speichertyps und Herstellers zuweist. Im Allgemeinen können Sie diesen Namen durch einen Namen Ihrer Wahl ersetzen. Weitere Informationen hierzu finden Sie unter Umbenennen von Speichergeräten.
Bezeichner	Eine für ein bestimmtes Gerät spezifische UUID. Weitere Informationen hierzu finden Sie unter Namen und Bezeichner von Speichergeräten.
Betriebszustand	Gibt an, ob das Gerät angeschlossen bzw. nicht angeschlossen ist. Weitere Informationen hierzu finden Sie unter Speichergeräte trennen.
LUN	Logical Unit Number (LUN) innerhalb des SCSI-Ziels. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.
Laufwerkstyp	Gibt an, ob das Gerät ein Flash-Laufwerk oder ein reguläres HDD-Laufwerk ist. Weitere Informationen zu Flash-Laufwerken und NVMe-Geräten finden Sie unter Kapitel 15 Arbeiten mit Flash-Geräten.
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet. Das Protokoll hängt vom Typ des verwendeten Speichers ab. Weitere Informationen hierzu finden Sie unter Physische Speichertypen.
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten der Pfade zum Speichergerät verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In. Weitere Informationen hierzu finden Sie unter Pluggable Storage Architecture (PSA) und Pfadverwaltung.
Hardwarebeschleunigung	Informationen dazu, ob das Speichergerät den Host bei Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten. Weitere Informationen hierzu finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.
Sektorformat	Gibt an, ob das Gerät ein herkömmliches, 512n- oder erweitertes Sektorformat wie 512e oder 4Kn verwendet. Weitere Informationen hierzu finden Sie unter Gerätesektorformate.
Speicherort	Ein Pfad zum Speichergerät im Verzeichnis `/vmfs/devices/`.
Partitionsformat	Ein Partitionsschema, das vom Speichergerät verwendet wird. Es kann sich hierbei um einen Master Boot Record (MBR) oder eine GUID-Partitionstabelle (GPT) handeln. Die GPT-Geräte unterstützen Datenspeicher größer als 2 TB. Weitere Informationen hierzu finden Sie unter Gerätesektorformate.
Partitionen	Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.
Mehrfachpfad-Richtlinien	Pfadauswahlrichtlinie und Speicher-Array-Typ-Richtlinie, die der Host für die Pfade zum Speicher verwendet. Weitere Informationen hierzu finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.
Pfade	Pfade, die zum Zugriff auf den Speicher verwendet werden, und ihr Status. Weitere Informationen hierzu finden Sie unter Deaktivieren von Speicherpfaden.

Anzeigen von Speichergeräten für einen ESXi-Host

Zeigen Sie alle für einen ESXi-Host verfügbaren Speichergeräte an. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden die durch die Plug-Ins verfügbaren Speichergeräte ebenfalls in der Liste angezeigt.

In der Ansicht „Speichergeräte“ können Sie die Speichergeräte des Hosts anzeigen, ihre Informationen analysieren und ihre Eigenschaften ändern.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speichergeräte**.

   Alle für den Host verfügbaren Speichergeräte werden in der Tabelle „Speichergeräte“ aufgeführt.
4. Wählen Sie ein Gerät in der Liste aus, um Details zu diesem Gerät anzuzeigen.
5. Verwenden Sie die Symbole, um allgemeine Speicherverwaltungsaufgaben durchzuführen.

   Die Verfügbarkeit bestimmter Symbole richtet sich nach dem Gerätetyp und der Konfiguration.

Symbol	Beschreibung
Aktualisieren	Aktualisiert die Informationen zu Speicheradaptern, zur Topologie und zu Dateisystemen.
Trennen	Trennt das ausgewählte Gerät vom Host
Anhängen	Verbindet das ausgewählte Gerät mit dem Host.
Umbenennen	Ändert den Anzeigenamen des ausgewählten Geräts.
LED einschalten	Schaltet die Locator-LED der ausgewählten Geräte ein.
LED ausschalten	Schaltet die Locator-LED der ausgewählten Geräte aus.
Als Flash-Festplatte markieren	Markiert die ausgewählten Geräte als Flash-Festplatten.
Als HDD-Festplatte markieren	Markiert die ausgewählten Geräte als HDD-Festplatten.
Als lokal markieren	Markiert die ausgewählten Geräte als lokale Geräte relativ zum Host.
Als Remote markieren	Markiert die ausgewählten Geräte als Remotegeräte relativ zum Host.
Partitionen löschen	Löscht Partitionen auf den ausgewählten Geräten.
Als dauerhaft reserviert markieren	Markieren Sie das ausgewählte Gerät als dauerhaft reserviert.
Markierung als dauerhaft reserviert aufheben	Dauerhafte Reservierung aus ausgewähltem Gerät löschen.

6 Nutzen Sie die folgenden Registerkarten, um auf zusätzliche Informationen zuzugreifen und Eigenschaften für das ausgewählte Gerät zu ändern.

Registerkarte	Beschreibung
Eigenschaften	Anzeigen von Geräteeigenschaften und -merkmalen. Anzeigen und Ändern von Multipathing-Richtlinien für das Gerät.
Pfade	Anzeigen der für das Gerät verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads.
Partitionsdetails	Zeigt Informationen zu Partitionen und ihren Formaten an.

Anzeigen von Speichergeräten für einen Adapter

Zeigen Sie eine Liste der Speichergeräte an, auf die über einen bestimmten Speicheradapter auf dem ESXi-Host zugegriffen werden kann.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter**.

Alle auf dem Host installierten Speicheradapter werden in der Tabelle „Speicheradapter“ aufgeführt.

4 Wählen Sie den Adapter in der Liste aus und klicken Sie auf die Registerkarte **Geräte**.

Die Speichergeräte, auf die der Host über den Adapter zugreifen kann, werden angezeigt.

5 Verwenden Sie die Symbole, um allgemeine Speicherverwaltungsaufgaben durchzuführen.

Die Verfügbarkeit bestimmter Symbole richtet sich nach dem Gerätetyp und der Konfiguration.

Symbol	Beschreibung
Aktualisieren	Aktualisiert die Informationen zu Speicheradaptern, zur Topologie und zu Dateisystemen.
Trennen	Trennt das ausgewählte Gerät vom Host
Anhängen	Verbindet das ausgewählte Gerät mit dem Host.
Umbenennen	Ändert den Anzeigenamen des ausgewählten Geräts.

Gerätesektorformate

ESXi unterstützt Speichergeräte mit herkömmlichen oder erweiterten Sektorformaten (so genannte Advanced Format-Geräte). Im Speicher ist ein Sektor ein Teilbereich einer Spur auf einer Speicherfestplatte oder einem Speichergerät. In jedem Sektor wird eine feste Datenmenge gespeichert.

In dieser Tabelle werden verschiedene Speichergerätformate vorgestellt, die von ESXi unterstützt werden.

Format des Speichergeräts	ESXi-Softwareemulation	Logische Sektorgröße	Physische Sektorgröße	VMFS-Datenspeicher
512n	Nicht verfügbar	512	512	VMFS5 und VMFS6 (Standard)
512e	Nicht verfügbar	512	4096	VMFS5 und VMFS56 (Standard) **Hinweis** Lokale 512e-Speichergeräte bieten keine Unterstützung für VMFS5.
4Kn	512	4096	4096	VMFS 6

Natives 512-Byte-Format

ESXi unterstützt herkömmliche 512n-Speichergeräte, die eine native 512-Byte-Sektorgröße verwenden.

512-Byte-Emulationsformat

Aufgrund der steigenden Nachfrage nach größeren Kapazitäten hat die Speicherindustrie Advanced Format-Laufwerke mit erweiterten Formaten eingeführt, wie z. B. 512-Byte-Emulation oder 512e. 512e ist das erweiterte Format, bei dem die physische Sektorgröße 4.096 Byte beträgt, der logische Sektor jedoch die 512-Byte-Sektorgröße emuliert. Speichergeräte, die das 512e-Format verwenden, können ältere Anwendungen und Gastbetriebssysteme unterstützen. Diese Geräte dienen als Zwischenschritt zu Laufwerken mit 4Kn-Sektoren.

Natives 4K-Format mit Softwareemulation

Ein anderes erweitertes Format (Advanced Format), das von ESXi unterstützt wird, ist die 4Kn-Sektortechnologie. In 4Kn-Geräten haben sowohl physische als auch logische Sektoren eine Länge von 4.096 Byte (4 KiB). Diese Geräte verfügen nicht über eine Emulationsschicht, sondern machen ihre physikalische Sektorgröße von 4Kn direkt für ESXi verfügbar.

ESXi erkennt und registriert die 4Kn-Geräte und emuliert sie automatisch als 512e-Geräte. Die Geräte werden den oberen Schichten von ESXi als 512e-Geräte präsentiert. Aus Sicht der Gastbetriebssysteme handelt es sich jedoch immer um 512n-Geräte. Bestehende VMs mit älteren Gastbetriebssystemen und Anwendungen können auf einem Host mit 4Kn-Geräten weiterhin genutzt werden.

Bei Verwendung von 4Kn-Geräten sollten Sie Folgendes beachten:

- ESXi unterstützt nur lokale 4Kn-SAS- und -SATA-Festplatten.
- ESXi unterstützt keine 4Kn-SSD- und -NVMe-Geräte oder 4Kn-Geräte als RDMs (RAW-Gerätezuordnungen).
- ESXi kann nur von einem 4Kn-Gerät mit UEFI gestartet werden.

- Mit einem 4Kn-Gerät können Sie eine Core-Dump-Partition und die Core-Dump-Datei konfigurieren.
- Nur das NMP-Plug-in kann 4Kn-Geräte beanspruchen. Sie können das HPP nicht verwenden, um diese Geräte zu beanspruchen.
- Mit vSAN können Sie nur die 4Kn-Kapazitätsfestplatten für vSAN Hybrid-Arrays verwenden. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.
- Aufgrund der Softwareemulationsschicht hängt die Leistung von 4Kn-Geräten von der Ausrichtung der E/A-Operationen ab. Um eine optimale Leistung zu erzielen, sollten Arbeitslasten mit auf 4K ausgerichteten E/A-Operationen ausgeführt werden.
- Arbeitslasten, die direkt über Scatter-Gather-E/A (SGIO) auf das emulierte 4Kn-Gerät zugreifen, müssen E/A-Operationen initiieren, die mit der 512e-Festplatte kompatibel sind.

Beispiel: Ermitteln des Geräteformats

Um festzustellen, ob ein Gerät das Format 512n, 512e oder 4Kn verwendet, führen Sie den folgenden Befehl aus.

```
esxcli storage core device capacity list
```

Das folgende Ausgabebeispiel zeigt den Formattyp.

```
Device                Physical Blocksize  Logical Blocksize  Logical Block Count
Size  Format Type
--------------------  ------------------  -----------------  -------------------
-----------  -----------
naa.5000xxxxxxxxx36f                 512                512           2344225968  1144641
MiB  512n
naa.5000xxxxxxxxx030                4096                512           3516328368  1716957
MiB  4Kn SWE
naa.5000xxxxxxxxx8df                 512                512           2344225968  1144641
MiB  512n
naa.5000xxxxxxxxx4f4                4096                512           3516328368  1716957
MiB  4Kn SWE
```

Namen und Bezeichner von Speichergeräten

In der Umgebung ESXi wird jedes Speichergerät durch mehrere Namen identifiziert.

Gerätebezeichner

Je nach Art der Speicherung verwendet der ESXi-Host unterschiedliche Algorithmen und Konventionen zum Generieren eines Bezeichners für jedes Speichergerät.

Vom Speicher bereitgestellte Bezeichner

Der ESXi-Host fragt ein Ziel-Speichergerät nach den Namen des Geräts ab. Aus den zurückgegebenen Metadaten extrahiert oder generiert der Host einen eindeutigen Bezeichner

für das Gerät. Der Bezeichner basiert auf bestimmten Speicher-Standards, ist eindeutig und einheitlich auf allen Hosts und hat einen der folgenden Formate:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Pfadbasierter Bezeichner

Stellt das Gerät keinen Bezeichner zur Verfügung, generiert der Host eine mpx.Name des *Speicherpfads*, wobei *Pfad* den ersten Pfad zu dem Gerät, z. B. `mpx.vmhba1:C0:T1:L3` darstellt. Dieser Bezeichner kann auf dieselbe Weise verwendet werden wie der vom Speicher bereitgestellte Bezeichner.

Der mpx.*path*-Bezeichner wird für lokale Geräte unter der Annahme erstellt, dass ihre Pfadnamen eindeutig sind. Dieser Bezeichner ist nicht eindeutig oder dauerhaft und kann sich nach jedem Neustart des Systems ändern.

In der Regel hat der Pfad zu dem Gerät das folgende Format:

vmhba*Adapter*:C*Kanal*:T*Ziel*:L*LUN*

- vmhba*Adapter* ist der Name des Speicheradapters. Der Name bezieht sich auf den physischen Adapter auf dem Host, nicht auf den SCSI-Controller, den die virtuellen Maschinen verwenden.
- C*Channel* ist die Nummer des Speicherkanals.

  Software-iSCSI-Adapter und abhängige Hardwareadapter verwenden die Kanalnummer, um mehrere Pfade zu demselben Ziel anzuzeigen.
- T*Ziel* ist die Zielnummer. Die Zielnummerierung wird vom Host festgelegt und kann sich ändern, wenn es eine Änderung in der Zuordnung von Zielen gibt, die für den Host sichtbar sind. Von verschiedenen Hosts gemeinsam verwendete Ziele verfügen möglicherweise nicht über dieselbe Zielnummer.
- L*LUN* ist die LUN-Nummer, die die Position der LUN innerhalb des Ziels angibt. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).

Beispielsweise repräsentiert `vmhba1:C0:T3:L1` LUN1 auf Ziel 3, auf die über den Speicheradapter vmhba1 und den Kanal 0 zugegriffen wird.

Legacy-Bezeichner

Zusätzlich zu den vom Speicher bereitgestellten Bezeichnern oder mpx.*path*-Bezeichnern generiert ESXi für jedes Gerät einen alternativen veralteten Namen. Der Bezeichner hat das folgende Format:

vml.*Nummer*

Der Legacy-Bezeichner enthält mehrere Ziffern, die für das Gerät eindeutig sind. Der Bezeichner kann teilweise aus den Metadaten, die über den Befehl SCSI INQUIRY erhalten wurden, abgeleitet werden. Für nicht lokale Geräte, die keine SCSI INQUIRY-Bezeichner bieten, wird der vml.*Nummer*-Bezeichner als einzig verfügbarer eindeutiger Bezeichner verwendet.

Beispiel: Anzeigen von Gerätenamen in der vSphere-CLI

Sie können den Befehl `esxcli storage core device list` verwenden, um alle Gerätenamen in der vSphere-CLI anzuzeigen. Die Ausgabe lautet in etwa wie folgt:

```
# esxcli storage core device list
naa.XXX
      Display Name: DGC Fibre Channel Disk(naa.XXX)
      ...
      Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

NVMe-Geräte mit NGUID-Gerätebezeichnern

Für NVMe-Geräte generiert ESXi Gerätebezeichner basierend auf den aus den Geräten abgerufenen Informationen. Allgemein unterstützen NVMe-Geräte Bezeichner in den Formaten EUI64 oder NGUID oder verwenden beide Formate. NGUID steht für „Namespace Globally Unique Identifier“ (Global eindeutiger Namespace-Bezeichner), der das 16-Byte-Kennzeichnerformat EUI64 verwendet.

Für die Geräte, die nur das NGUID-Format unterstützen, ändert sich der vom Host generierte Gerätebezeichner in Abhängigkeit von der ESXi-Version. Der ESXi-Host der Version 6.7 und früher hat den Bezeichner t10.*xxx_controller_serial_number* erstellt. Ab Version 6.7 Update 1 erstellt der Host zwei Bezeichner: eui.*xxx (NGUID)* als primären und t10.*xxx_controller_serial_number* als alternativen primären Bezeichner.

Vom Gerät unterstützte ID-Formate		Vom Host generierter Gerätebezeichner	
ID-Format EUI64	**ID-Format NGUID**	**ESXi 6.7 und früher**	**ESXi 6.7 Update 1 und höher**
Ja	Ja	t10.*xxx_EUI64*	t10.*xxx_EUI64*
Ja	Nein	t10.*xxx_EUI64*	t10.*xxx_EUI64*
Nein	Ja	t10.*xxx_controller_serial_number*	eui.*xxx (NGUID)* als primäre ID t10.*xxx_controller_serial_number* als alternative primäre ID

Hinweis Wenn Ihr Host Geräte aufweist, die ausschließlich NGUID unterstützen, und Sie ein Upgrade des Hosts von einer früheren Version auf ESXi 7.0 durchführen, ändert sich der Gerätebezeichner von t10.*xxx_controller_serial_number* in eui.*xxx (NGUID)*, und zwar in der gesamten ESXi-Umgebung. Wenn Sie den Gerätebezeichner in einem Ihrer Kundenskripte verwenden, müssen Sie diese Formatänderung berücksichtigen.

Überprüfen der Zuordnung zwischen primären und alternativen Gerätebezeichnern

Verwenden Sie den Befehl `esxcli storage core device uidmap list` zum Überprüfen der Gerätebezeichner. Die Ausgabe lautet in etwa wie folgt:

```
 esxcli storage core device uidmap list
eui.0000xyz.....
   Primary UID: eui.0000xyz.....
   Alternative Primary UIDs: t10.0000abc....
   Legacy UID: vml.0000000000766d68....
   Alternative Legacy UIDs: vml.000000000080906....
```

Upgrade auf Version 7.0 von statusfreien ESXi-Hosts mit NVMe-Geräten, die ausschließlich NGUID unterstützen.

Wenn Ihre Umgebung statusfreie ESXi-Hosts der Version 6.7 und früher enthält und NVMe-Geräte umfasst, die ausschließlich das NGUID-Format unterstützen, verwenden Sie den hier erläuterten Workflow für das Upgrade des Hosts auf Version 7.0.x.

Führen Sie beim Upgrade Ihrer statusfreien Hosts von Version 6.7 und früher auf Version 7.0.x die folgenden Schritte durch., um die Speicherkonfiguration beizubehalten. Wenn Sie das Upgrade durchführen, ohne die Anweisungen zu befolgen, kann es passieren, dass sämtliche in den Hostprofilen erfassten Speicherkonfigurationen über das Upgrade hinweg nicht erhalten bleiben. Dies kann dazu führen, dass nach dem Upgrade Übereinstimmungsfehler bei den Hostprofilen auftreten.

Voraussetzungen

- Ihre Umgebung enthält statusfreie Hosts der ESXi-Version 6.7 oder früher.

- Die Umgebung umfasst NVMe-Geräte, die ausschließlich das NGUID-Format unterstützen.

Verfahren

1 Ermitteln Sie, ob der Host NVMe-Geräte enthält, die ausschließlich NGUID unterstützen.

a Überprüfen Sie, ob der Anbieter des Geräts NVMe ist.

Beispiel eines Befehls:

```
# esxcli storage core device list -d eui.f04xxxxxxxxx0000000100000001
eui.f04xxxxxxxxx0000000100000001
Display Name: Local NVMe Disk (eui.f04xxxxxxxxx0000000100000001)
Has Settable Display Name: true
Devfs Path: /vmfs/devices/disks/eui.f04bxxxxxxxxx0000000100000001
Vendor: NVMe
```

Die Zeile `Vendor: NVMe` gibt an, dass das Gerät von NVMe ist.

b Ermitteln Sie, welcher HBA mit dem NVMe-Gerät verbunden ist.

```
# esxcli storage core adapter device list
HBA    Device UID
------ --------------------------------
vmhba2 eui.f04xxxxxxxxx0000000100000001
```

c Rufen Sie die Namespace-Informationen für das NVMe-Gerät mithilfe des HBA und der Namespace-ID ab.

```
# esxcli nvme device namespace get -A vmhba2 -n 1
Namespace Identify Info:
Namespace Size: 0xe8e088b0 Logical Blocks
Namespace Capacity: 0xe8e088b0 Logical Blocks
. . .
NVM Capacity: 0x1d1c1116000
Namespace Globally Unique Identifier: 0xf04xxxxxxxxx0000000100000001
IEEE Extended Unique Identifier: 0x0
```

Für ein NVMe-Gerät, das ausschließlich NGUID unterstützt, enthält das Feld `IEEE Extended Unique Identifier` in der Ausgabe den Wert 0 und das Feld `Namespace Globally Unique Identifier` einen Wert der nicht null ist.

2 Um die im Hostprofil erfassten Speicherkonfigurationen beizubehalten, führen Sie beim Upgrade eines statusfreien Hosts auf Version 7.0.x die folgenden Schritte durch.

   a Speichern Sie vor dem Upgrade die Datei `esx.conf` an einem persistenten Speicherort.

   Sie können die Datei `esx.conf` beispielsweise in einen VMFS-Datenspeicher kopieren.

   ```
   # cp /etc/vmware/esx.conf /vmfs/volumes/datastore1/
   ```

   b Führen Sie ein Upgrade des Hosts durch.

   Nach dem Upgrade stimmt der Host nicht mit dem Profil überein und verbleibt möglicherweise im Wartungsmodus.

   c Wenden Sie die Geräteeinstellungen für NVMe-Geräte, die ausschließlich NGUID unterstützen, unter Verwendung neuer ID-Formate an.

   Führen Sie den folgenden Befehl über den Host aus und geben Sie damit den Speicherort der Datei `esx.conf` an.

   ```
    # python ./usr/lib/vmware/nvme-nguid-support/bin/nguidApplySettings.pyc -l /vmfs/volumes/datastore1/
   ```

3 Kopieren Sie die Einstellungen vom Host und setzen Sie die Hostanpassungen zurück.

   a Klicken Sie im vSphere Client auf **Home > Richtlinien und Profile > Hostprofile** und dann auf das an den Host angehängte Profil.

   b Klicken Sie auf **Registerkarte „Konfigurieren“ > Einstellung von Host kopieren** und wählen Sie den Host aus.

   c Um die Anpassungen zurückzusetzen, navigieren Sie zu dem Host und wählen Sie im Kontextmenü **Hostprofile > Hostanpassungen zurücksetzen** aus.

4 Wählen Sie im Kontextmenü des Hosts **Hostprofile > Standardisieren** aus.

   Der Host weist nun die erforderliche Übereinstimmung auf.

5 Starten Sie den Host neu und beenden Sie den Wartungsmodus.

Beispiel: Upgrade des ESXi-Hosts ohne Beibehaltung der Speicherkonfigurationen

Wenn Sie die im Hostprofil erfassten Speicherkonfigurationen nicht beibehalten, treten möglicherweise nach dem Upgrade des Hosts Übereinstimmungsfehler auf dem Host auf. Kopieren Sie in diesem Fall die Einstellungen vom Host und setzen Sie die Hostanpassungen zurück.

Umbenennen von Speichergeräten

Der ESXi-Host weist einem Speichergerät basierend auf dem Speichertyp und dem Hersteller einen Anzeigenamen zu. Sie können den Anzeigenamen des Speichergeräts ändern.

Sie können bestimmte Arten von lokalen Geräten nicht umbenennen.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie das umzubenennende Gerät und klicken Sie auf **Umbenennen**.

5 Ändern Sie den Gerätnamen auf einen aussagekräftigen Namen.

Vorgänge zum erneuten Prüfen des Speichers

Wenn Sie Datenspeichermanagementaufgaben durchführen oder Änderungen an der SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut scannen.

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, z. B. das Erstellen eines VMFS-Datenspeichers oder RDMs, das Hinzufügen einer Erweiterung und das Vergrößern oder Löschen eines VMFS-Datenspeichers, wird Ihr Speicher von Ihrem Host oder dem vCenter Server automatisch neu geprüft und aktualisiert. Sie können die Funktion für die automatische Neuprüfung deaktivieren, indem Sie den Filter für das erneute Prüfen eines Hosts ausschalten. Weitere Informationen hierzu finden Sie unter Ausschalten von Speicherfiltern.

In bestimmten Fällen müssen Sie die erneute Prüfung manuell durchführen. Sie können alle verfügbaren Speicher Ihres Hosts oder aller Hosts in einem Ordner, Cluster oder Datencenter erneut prüfen.

Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, die über einen bestimmten Adapter verbunden sind, führen Sie eine erneute Prüfung dieses Adapters durch.

Führen Sie eine erneute manuelle Prüfung durch, wenn Sie eine der folgenden Änderungen vorgenommen haben.

- Festlegen der Zone eines neuen Festplatten-Arrays auf einem SAN.
- Erstellen von neuen LUNs in einem SAN.
- Ändern Sie die Pfadmaskierung auf einem Host.
- Erneutes Verbinden eines Kabels.
- CHAP-Einstellungen ändern (nur iSCSI).
- Hinzufügen oder Entfernen von Erkennungsadressen oder statischen Adressen (nur iSCSI).
- Hinzufügen eines einzelnen Hosts zu vCenter Server, nachdem Sie einen Datenspeicher, der von den vCenter Server-Hosts und dem einzelnen Host gemeinsam genutzt wird, bearbeitet oder vom vCenter Server entfernt haben.

Wichtig Wenn bei einer erneuten Prüfung kein Pfad verfügbar ist, entfernt der Host den Pfad aus der Liste der Pfade zu dem Gerät. Der Pfad wird erneut in der Liste angezeigt, sobald er verfügbar und wieder einsatzbereit ist.

Durchführen einer erneuten Speicherprüfung

Wenn Sie Änderungen an Ihrer SAN-Konfiguration vornehmen, müssen Sie möglicherweise den Speicher erneut prüfen. Sie können eine erneute Prüfung des für den ESXi-Host, den Cluster oder das Datencenter verfügbaren Speichers durchführen. Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, auf die über einen bestimmten Host zugegriffen wird, führen Sie die erneute Prüfung nur für diesen Host durch.

Verfahren

1. Gehen Sie im Objektnavigator des vSphere Client zu einem Host, einem Cluster, einem Datencenter oder einem Ordner, der bzw. das Hosts enthält.
2. Wählen Sie im Kontextmenü **Speicher > Speicher erneut prüfen** aus.
3. Geben Sie den Umfang der erneuten Prüfung an.

Option	Beschreibung
Auf neue Speichergeräte prüfen	Prüfen Sie alle Adapter erneut auf neu hinzugefügte Speichergeräte. Wenn neue Geräte erkannt werden, werden sie in der Geräteliste angezeigt.
Auf neue VMFS-Volumes prüfen	Prüfen Sie alle Speichergeräte neu, um neue Datenspeicher zu suchen, die seit der letzten Prüfung hinzugefügt wurden. Alle neuen Datenspeicher werden in der Datenspeicherliste angezeigt.

Durchführen einer erneuten Adapterprüfung

Wenn Sie Änderungen an Ihrer SAN-Konfiguration vornehmen und diese Änderungen auf Speicher beschränken, auf die über einen bestimmten Adapter auf einem ESXi-Host zugegriffen wird, führen Sie eine erneute Prüfung nur dieses Adapters durch.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den erneut zu prüfenden Adapter in der Liste aus.
4. Klicken Sie auf das Symbol **Adapter erneut prüfen**.

Ändern der Anzahl gescannter Speichergeräte

Der Bereich gescannter LUN-IDs für einen ESXi-Host liegt zwischen 0 und 16.383. ESXi ignoriert LUN-IDs ab 16.383. Der konfigurierbare Parameter `Disk.MaxLUN` steuert den Bereich gescannter LUN-IDs. Der Parameter hat den Standardwert 1024.

Der Parameter `Disk.MaxLUN` bestimmt außerdem, wie viele LUNs der SCSI-Scancode mithilfe einzelner INQUIRY-Befehle zu ermitteln versucht, wenn das SCSI-Ziel die direkte Erkennung mithilfe von REPORT_LUNS nicht unterstützt.

Den Parameter `Disk.MaxLUN` können Sie in Abhängigkeit von Ihren Anforderungen ändern. Wenn beispielsweise in Ihrer Umgebung wenige Speichergeräte mit LUN-IDs zwischen 1 und 100 vorhanden sind, legen Sie den Wert auf 101 fest. Folglich können Sie die Geschwindigkeit der Geräteerkennung für Ziele ohne Unterstützung von REPORT_LUNS optimieren. Durch einen niedrigeren Wert kann die Zeit zum erneuten Prüfen und Starten verkürzt werden. Die Zeit zum erneuten Prüfen der Speichergeräte hängt jedoch von verschiedenen Faktoren ab, wie beispielsweise dem Typ und der Auslastung des Speichersystems.

In anderen Situationen müssen Sie möglicherweise diesen Wert erhöhen, wenn in Ihrer Umgebung LUN-IDs über 1023 hinaus verwendet werden.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.

4 Wählen Sie in der Tabelle „Erweiterte Systemeinstellungen“ den Parameter **Disk.MaxLUN** aus und klicken Sie auf das Symbol **Bearbeiten**.

5 Ändern Sie den vorhandenen Wert in einen Wert Ihrer Wahl und klicken Sie auf **OK**.

   Der eingegebene Wert gibt die LUN-ID nach der letzten LUN an, die Sie suchen möchten.

   Wenn Sie beispielsweise nach LUN-IDs von 1 bis 100 suchen möchten, setzten Sie **Disk.MaxLUN** auf „101“.

Identifizieren von Problemen hinsichtlich der Gerätekonnektivität

Wenn bei Ihrem ESXi-Host ein Problem bei der Verbindung mit einem Speichergerät auftritt, behandelt der Host das Problem abhängig von bestimmten Faktoren als permanent oder temporär.

Verbindungsprobleme bei Speichergeräten haben verschiedene Ursachen. Obwohl ESXi die Ursache für die Nichtverfügbarkeit eines Speichergeräts oder seiner Pfade nicht immer ermitteln kann, unterscheidet der Host zwischen dem Status des permanenten Geräteverlusts (Permanent Device Loss, PDL) des Geräts und einem vorübergehenden Status „Keine Pfade verfügbar“ (All Paths Down, APD).

Permanenter Geräteverlust (Permanent Device Loss, PDL)

Dies ist ein Zustand, der eintritt, wenn ein Speichergerät dauerhaft ausfällt oder vom Administrator entfernt oder ausgeschlossen wird. Es wird nicht erwartet, dass es verfügbar wird. Wenn das Gerät dauerhaft nicht mehr verfügbar ist, erhält ESXi entsprechende Erkennungscodes oder eine Verweigerung der Anmeldung von Speicher-Arrays und erkennt einen permanenten Geräteverlust.

Keine Pfade verfügbar (All Paths Down, APD)

Ein Zustand, der eintritt, wenn ein Speichergerät für den Host nicht mehr verfügbar ist und keine Pfade zu dem Gerät verfügbar sind. ESXi behandelt dies als flüchtigen Zustand, weil in der Regel die Probleme mit dem Gerät temporär sind und anzunehmen ist, dass das Gerät wieder verfügbar wird.

Konnektivitätsprobleme und vSphere High Availability

Wenn das Gerät in den PDL- oder APD-Zustand wechselt, kann vSphere High Availability (HA) Konnektivitätsprobleme erkennen und automatische Wiederherstellung für betroffene virtuelle Maschinen auf dem ESXi-Host bereitstellen. vSphere HA verwendet VM-Komponentenschutz, um auf dem Host im vSphere HA-Cluster ausgeführte virtuelle Maschinen vor Fehlern beim Datenzugriff zu schützen. Weitere Informationen zum VM-Komponentenschutz und zum Konfigurieren von Antworten für Datenspeicher und virtuelle Maschinen bei Auftreten der APD- oder PDL-Bedingung finden Sie in der Dokumentation zu *Handbuch zur Verfügbarkeit in vSphere*.

Erkennen von PDL-Bedingungen

Einem Speichergerät wird der Zustand PDL (Permanent Device Loss, dauerhafter Geräteverlust) zugeschrieben, wenn es für den ESXi-Host dauerhaft nicht verfügbar ist.

Die PDL-Bedingung tritt typischerweise ein, wenn ein Gerät versehentlich entfernt wird, wenn seine eindeutige ID sich ändert oder wenn ein nicht behebbarer Hardwarefehler auftritt.

Wenn das Speicher-Array bestimmt, dass das Gerät dauerhaft nicht verfügbar ist, sendet es SCSI-Erkennungscodes an den ESXi-Host. Nach dem Empfang des Erkennungs-Codes erkennt Ihr Host das Gerät als fehlgeschlagen und registriert den Gerätezustand PDL. Damit das Gerät als dauerhaft verloren betrachtet wird, müssen die Erkennungs-Codes auf allen seinen Pfaden empfangen werden.

Wenn für das Gerät der Zustand PDL registriert wurde, versucht der Host nicht mehr, eine Verbindung mit dem Gerät herzustellen oder Befehle an das Gerät zu senden.

Der vSphere Client zeigt folgende Informationen für das Gerät an:

- Der Betriebszustand des Geräts wird in `Lost Communication` geändert.
- Alle Pfade werden als `Dead` angezeigt.
- Die Datenspeicher auf dem Gerät sind nicht verfügbar.

Wenn keine offenen Verbindungen zu dem Gerät vorhanden sind, oder nachdem die letzte Verbindung getrennt wurde, entfernt der Host das PDL-Gerät und alle Pfade zu dem Gerät. Sie können das automatische Entfernen von Pfaden deaktivieren, indem Sie den erweiterten Hostparameter `Disk.AutoremoveOnPDL` auf 0 festlegen.

Wenn die PDL-Bedingung für das Gerät nicht mehr vorhanden ist, kann es vom Host erkannt werden, wird aber als neues Gerät behandelt. Die Datenkonsistenz für virtuelle Maschinen auf dem wiederhergestellten Gerät ist nicht garantiert.

Hinweis Wenn ein Gerät ausfällt, ohne dass es die entsprechenden SCSI-Erkennungscodes oder die Verweigerung der iSCSI-Anmeldung sendet, kann der Host die PDL-Bedingungen nicht erkennen. In diesem Fall behandelt der Host, selbst wenn das Gerät dauerhaft ausfällt, die Geräteverbindungsprobleme weiterhin als APD.

Permanenter Geräteverlust (Permanent Device Loss, PDL) und SCSI-Erkennungscodes

Im folgenden Beispiel für ein VMkernel-Protokoll gibt ein SCSI-Erkennungscode an, dass das Gerät den Zustand PDL aufweist.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Permanenter Geräteverlust (Permanent Device Loss, PDL) und iSCSI

Bei iSCSI-Arrays mit einer einzelnen LUN pro Ziel wird der Zustand PDL daran erkannt, dass die iSCSI-Anmeldung fehlschlägt. Ein iSCSI-Speicher-Array lehnt die Versuche des Hosts zum Starten einer iSCSI-Sitzung mit dem Grund `Target Unavailable` ab. Wie bei den Erkennungs-Codes muss diese Antwort auf allen Pfaden empfangen werden, damit das Gerät als dauerhaft verloren betrachtet wird.

Permanenter Geräteverlust (Permanent Device Loss, PDL) und virtuelle Maschinen

Wenn für das Gerät der Zustand PDL registriert wurde, schließt der Host alle Eingaben/Ausgaben von virtuellen Maschinen. vSphere HA kann PDL erkennen und ausgefallene virtuelle Maschinen neu starten.

Durchführen des geplanten Entfernens von Speichergeräten

Falls ein Speichergerät nicht ordnungsgemäß funktioniert, können Sie PDL- (Permanent Device Loss, „dauerhafter Ausfall eines Geräts“) oder APD-Zustände (All Paths Down, „keine Pfade verfügbar“) vermeiden. Führen Sie eine geplante Entfernung und erneute Verbindung eines Speichergeräts durch.

Das geplante Entfernen eines Geräts ist eine beabsichtigte Trennung eines Speichergeräts. Sie können ein Gerät auch aus einem bestimmten Grund entfernen, zum Beispiel, weil Sie Ihre Hardware aktualisieren oder Ihre Speichergeräte neu konfigurieren möchten. Wenn Sie eine ordnungsgemäße Entfernung und erneute Verbindung eines Speichergeräts durchführen, führen Sie mehrere Aufgaben durch.

Aufgabe	Beschreibung
Migrieren Sie die virtuelle Maschinen von dem Gerät, das Sie trennen möchten.	*vCenter Server und Hostverwaltung*
Unmounten Sie den auf dem Gerät verwendeten Datenspeicher.	Weitere Informationen hierzu finden Sie unter Unmounten von Datenspeichern.
Trennen Sie das Speichergerät.	Weitere Informationen hierzu finden Sie unter Speichergeräte trennen.
Im Falle eines iSCSI-Geräts mit einer einzelnen LUN pro Ziel löschen Sie den Eintrag für das statische Ziel aus jedem iSCSI-HBA, der einen Pfad zum Speichergerät aufweist.	Weitere Informationen hierzu finden Sie unter Entfernen dynamischer oder statischer iSCSI-Ziele.
Über die Array-Konsole können Sie eine notwendige Neukonfiguration des Speichergeräts durchführen.	Informationen finden Sie in der Dokumentation des Anbieters.
Schließen Sie das Speichergerät erneut an.	Weitere Informationen hierzu finden Sie unter Speichergeräte anhängen.
Mounten Sie den Datenspeicher und starten Sie die virtuelle Maschinen neu.	Weitere Informationen hierzu finden Sie unter Mounten von Datenspeichern.

Speichergeräte trennen

Trennen Sie das Speichergerät sicher von Ihrem ESXi-Host.

Möglicherweise müssen Sie das Gerät trennen, um es für Ihren Host unzugänglich zu machen, wenn Sie beispielsweise ein Upgrade der Speicherhardware durchführen.

Voraussetzungen

- Das Gerät enthält keine Datenspeicher.
- Keine virtuelle Maschinen nutzen das Gerät als RDM-Festplatte.
- Das Gerät enthält keine Diagnosepartition oder Scratch-Partition.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speichergeräte**.
4. Wählen Sie das zu trennende Gerät aus und klicken Sie auf das Symbol **Trennen**.

Ergebnisse

Auf das Gerät kann nicht mehr zugegriffen werden. Der Betriebszustand des Geräts wird in „Nicht gemountet“ geändert.

Nächste Schritte

Wenn mehrere Hosts das Gerät teilen, trennen Sie das Gerät von jedem Host.

Speichergeräte anhängen

Verbinden Sie ein Speichergerät erneut, das Sie zuvor vom ESXi-Host getrennt haben.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie das getrennte Speichergerät aus und klicken Sie auf das Symbol **Anhängen**.

Ergebnisse

Das Gerät wird verfügbar.

Wiederherstellen nach PDL-Bedingungen

Ein ungeplanter permanenter Geräteverlust (Permanent Device Loss, PDL) tritt ein, wenn ein Speichergerät dauerhaft nicht mehr verfügbar ist, ohne vom ESXi-Host getrennt worden zu sein.

Die folgenden Elemente in vSphere Client zeigen an, dass sich das Gerät im PDL-Status befindet:

- Der auf dem Gerät angezeigte Datenspeicher ist nicht verfügbar.
- Der Betriebszustand des Geräts ändert sich auf „Verbindung unterbrochen".
- Alle Pfade werden als „Ausgefallen“ angezeigt.
- In der VMkernel-Protokolldatei wird in einer Warnung angezeigt, dass das Gerät dauerhaft unzugänglich ist.

Um eine Wiederherstellung nach einer ungeplanten PDL-Bedingung durchzuführen und das nicht verfügbare Gerät vom Host zu entfernen, führen Sie die folgenden Aufgaben aus.

Aufgabe	Beschreibung
Schalten Sie alle virtuellen Maschinen ab, die auf dem von der PDL-Bedingung betroffenen Datenspeicher laufen, und heben Sie ihre Registrierung auf.	Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
Unmounten Sie den Datenspeicher.	Weitere Informationen hierzu finden Sie unter Unmounten von Datenspeichern.
Führen Sie eine erneute Prüfung auf allen ESXi-Hosts durch, die Zugriff auf das Gerät hatten. **Hinweis** Wenn die erneute Prüfung nicht erfolgreich ist und der Host das Gerät weiterhin auflistet, sind vielleicht noch ausstehende E/A-Vorgänge oder aktive Verweise auf das Gerät vorhanden. Suchen Sie alle Elemente, die möglicherweise immer noch einen aktiven Verweis auf das Gerät oder den Datenspeicher haben. Die Objekte umfassen virtuelle Maschinen, Vorlagen, ISO-Images, Zuordnungen für Raw-Geräte usw.	Weitere Informationen hierzu finden Sie unter Durchführen einer erneuten Speicherprüfung.

Handhabung vorübergehender APD-Bedingungen

Ein Speichergerät befindet sich im APD-Status (All Paths Down, Keine Pfade verfügbar), wenn es für den ESXi-Host über einen unbestimmten Zeitraum nicht verfügbar ist.

Die Ursache für einen APD-Status kann beispielsweise ein ausgefallener Switch oder ein nicht angeschlossenes Speicherkabel sein.

Im Gegensatz zum Status „permanenter Geräteverlust“ (Permanent Device Loss, PDL) verarbeitet der Host den APD-Status als vorübergehend und erwartet, dass das Gerät wieder verfügbar wird.

Der Host wiederholt fortwährend die ausgegebenen Befehle, um die Verbindung mit dem Gerät wiederherzustellen. Wenn die vom Host wiederholt ausgeführte Befehlsausgabe über einen längeren Zeitraum fehlschlägt, kann es auf dem Host unter Umständen zu Leistungseinbußen kommen. Der Host und seine virtuellen Maschinen reagieren unter Umständen nicht mehr.

Um diese Probleme zu vermeiden, verfügt Ihr Host über eine Standard-APD-Behandlungsfunktion. Wenn ein Gerät in den APD-Status wechselt, aktiviert der Host einen Timer. Bei aktiviertem Timer fährt der Host für einen beschränkten Zeitraum mit der Wiederholung von Befehlen nicht virtueller Maschinen fort.

Standardmäßig wird das APD-Timeout auf 140 Sekunden festgelegt. Die meisten Geräte benötigen zur Wiederherstellung nach einem Verbindungsausfall weniger als 140 Sekunden. Wenn das Gerät während dieser Zeitspanne wieder verfügbar wird, laufen der Host und seine virtuelle Maschine ohne Probleme weiter.

Wenn das Gerät nicht wiederhergestellt wird und der festgelegte Zeitraum endet, stoppt der Host seine Neuversuche und beendet alle nicht virtuellen Maschinen-E/A-Befehle. Die virtuellen Maschinen-E/A-Befehle werden weiterhin abgesetzt. Der vSphere Client zeigt die folgenden Informationen für das Gerät, bei dem die APD-Zeitüberschreitung aufgetreten ist:

- Der Betriebszustand des Geräts wird in `Dead or Error` geändert.
- Alle Pfade werden als `Dead` angezeigt.
- Die Datenspeicher auf dem Gerät werden abgeblendet.

Obwohl das Gerät und die Datenspeicher nicht verfügbar sind, reagieren virtuelle Maschinen. Sie können die virtuellen Maschinen deaktivieren oder auf einen anderen Datenspeicher oder Host migrieren.

Wenn die Gerätepfade zu einem späteren Zeitpunkt betriebsbereit sind, kann der Host die E-/A-Ausgabe an das Gerät wiederaufnehmen und die spezielle APD-Verarbeitung beenden.

Deaktivieren der Speicher-APD-Behandlung

Die Speicher-APD-Behandlung (All Paths Down, keine Pfade verfügbar) auf dem ESXi-Host ist standardmäßig aktiviert. Wenn diese Option aktiviert ist, versucht der Host für eine begrenzte Zeit erneut, E/A-Befehle nicht virtueller Maschinen an ein Speichergerät im APD-Zustand zu senden. Wenn diese Zeit abgelaufen ist, stellt der Host diese Versuche ein und beendet alle E/A-Aktivitäten nicht virtueller Maschinen. Sie können die Funktion zur APD-Behandlung auf dem Host deaktivieren.

Wenn Sie die APD-Behandlung deaktivieren, versucht der Host immer wieder erneut, Befehle zu senden, um die Verbindung mit dem APD-Gerät wiederherzustellen. Es kann dazu führen, dass für virtuelle Maschinen auf dem Host eine interne E/A-Zeitüberschreitung eintritt, sodass sie ausfallen bzw. nicht mehr reagieren. Der Host kann vom vCenter Server getrennt werden.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.

4 Wählen Sie in der Tabelle „Erweiterte Systemeinstellungen“ den Parameter **Misc.APDHandlingEnable** aus und klicken Sie auf das Symbol `Edit`.

5 Ändern Sie den Wert in 0.

Ergebnisse

Wenn Sie die APD-Behandlung deaktiviert haben, können Sie sie erneut aktivieren und den Wert der zugehörigen Einstellung auf 1 festlegen, wenn ein Gerät in den APD-Zustand wechselt. Die Funktion zur internen APD-Behandlung wird sofort aktiviert und der Timer startet mit dem aktuellen Zeitüberschreitungswert für jedes Gerät im APD-Zustand.

Ändern der Grenzwerte für die Zeitüberschreitung für Speicher-APD

Der Parameter für die Zeitüberschreitung steuert, wie viele Sekunden der ESXi-Host im Zustand „Keine Pfade verfügbar“ (APD) wiederholt versuchen muss, E/A-Befehle auf ein Speichergerät anzuwenden. Sie können den Standardwert für die Zeitüberschreitung ändern.

Die Zeitüberschreitung beginnt sofort, nachdem das Gerät in den APD-Zustand versetzt wurde. Nach Ablauf der Zeitüberschreitung markiert der Host das APD-Gerät als nicht erreichbar. Der Host beendet die Versuche, jegliche E/A-Befehle anzuwenden, die nicht von virtuellen Maschinen kommen. Der Host sendet weiterhin E/A-Befehle virtueller Maschinen.

Der Parameter für die Zeitüberschreitung ist auf Ihrem Host standardmäßig auf 140 Sekunden festgelegt. Sie können den Zeitüberschreitungswert erhöhen, wenn beispielsweise Speichergeräte, die mit Ihrem ESXi-Host verbunden sind, länger als 140 Sekunden benötigen, um nach einem Verbindungsverlust eine neue Verbindung herzustellen.

Hinweis Falls Sie den Parameter der Zeitüberschreitung ändern, wenn das Gerät nicht mehr verfügbar ist, wird die Änderung für diesen speziellen APD-Vorfall nicht wirksam.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.

4 Wählen Sie in der Tabelle „Erweiterte Systemeinstellungen“ den Parameter **Misc.APDTimeout** aus und klicken Sie auf das Symbol `Edit`.

5 Ändern Sie den Standardwert.

Sie können einen Wert zwischen 20 und 99999 Sekunden eingeben.

Überprüfen des Verbindungsstatus eines Speichergeräts auf dem ESXi-Host

Verwenden Sie den `esxcli`-Befehl, um den Verbindungsstatus eines bestimmten Speichergeräts zu überprüfen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Führen Sie den folgenden Befehl aus: **`esxcli storage core device list -d=`*`device_ID`***.

2 Überprüfen Sie den Verbindungsstatus im Bereich `Status:`.

- `on` – Das Gerät ist verbunden.
- `dead` – Das Gerät hat den APD-Zustand. Der APD-Timer wird gestartet.
- `dead timeout` – Der APD-Timer ist abgelaufen.
- `not connected` – Das Gerät befindet sich im PDL-Zustand.

Aktivieren oder Deaktivieren der Locator-LEDs auf ESXi-Speichergeräten

Verwenden Sie die Locator-LED, um spezifische Speichergeräte zu identifizieren, damit Sie diese unter anderen Geräten finden können. Sie können die Locator-LED ein- oder ausschalten.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie aus der Liste der Speichergeräte eine oder mehrere Festplatten aus, und aktivieren bzw. deaktivieren Sie den Locator-LED-Indikator.

Option	Beschreibung
Aktivieren	Klicken Sie auf das Symbol **LED aktivieren**.
Deaktivieren	Klicken Sie auf das Symbol **LED deaktivieren**.

Löschen von Speichergeräten

Bestimmte Funktionen, wie z. B. vSAN oder virtuelle Flash-Ressource, erfordern, dass der ESXi-Host bereinigte Speichergeräte verwendet. Sie können ein HHD- oder Flash-Gerät löschen und alle vorhandenen Daten entfernen.

Voraussetzungen

- Vergewissern Sie sich, dass sich der Host im verbundenen Zustand befindet.
- Überprüfen Sie, ob die Geräte, die Sie löschen möchten, nicht in Gebrauch sind.
- Erforderliche Berechtigung: **Host.Config.Storage**

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speichergeräte**.
4. Wählen Sie mindestens ein Gerät aus und klicken Sie auf das Symbol **Partitionen löschen**.
5. Vergewissern Sie sich, dass es sich bei den Partitionsinformationen, die Sie löschen möchten, nicht um kritische Informationen handelt.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu bestätigen.

Ändern dauerhafter Reservierungseinstellungen

Sie können die dauerhafte Reservierungseinstellung auf Speichergeräten anpassen, die als physische Raw-Gerätezuordnungen (RDMs) in WSFC-Konfigurationen (Windows Server Failover Clustering) verwendet werden.

WSFC Clusterknoten, die über mehrere ESXi-Hosts verteilt sind, benötigen physische RDMs. Die RDMs werden von allen Hosts gemeinsam genutzt, auf denen Clusterknoten ausgeführt werden. Der Host mit dem aktiven Knoten weist dauerhafte SCSI-3-Reservierungen auf allen gemeinsam genutzten RDM-Geräten auf. Wenn der aktive Knoten ausgeführt wird und Geräte gesperrt sind, kann kein anderer Host auf die Geräte schreiben. Wenn ein anderer teilnehmender Host gestartet wird, während der aktive Knoten die Sperrung auf den Geräten beibehält, kann der Startvorgang ungewöhnlich viel Zeit in Anspruch nehmen, da der Host erfolglose Versuche zur Kontaktaufnahme mit den gesperrten Geräten unternimmt. Dieses Problem kann sich auch auf Vorgänge zum erneuten Prüfen auswirken.

Aktivieren Sie zur Vermeidung dieses Problems dauerhafte Reservierungen für alle Geräte auf den ESXi-Hosts, auf denen sich sekundäre WSFC-Knoten mit RDMs befinden. Mit dieser Einstellung wird der ESXi-Host über die dauerhafte SCSI-Reservierung auf den Geräten informiert, sodass der Host die Geräte während des Startvorgangs oder der erneuten Prüfung des Speichers überspringen kann.

Wenn Sie die markierten Geräte zu einem späteren Zeitpunkt erneut als VMFS-Datenspeicher verwenden, entfernen Sie die Reservierung, um unvorhersehbares Verhalten des Datenspeichers zu vermeiden.

Informationen zu WSFC-Clustern finden Sie in der Dokumentation zu *Setup für Windows Server-Failover-Clustering*.

Voraussetzungen

Stellen Sie vor der Kennzeichnung eines Geräts als dauerhaft reserviert sicher, dass das Gerät keinen VMFS-Datenspeicher enthält.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie das Gerät in der Liste der Speichergeräte aus und klicken Sie auf eines der folgenden Symbole.

Option	Beschreibung
Als dauerhaft reserviert markieren	Markieren Sie das ausgewählte Gerät als dauerhaft reserviert. **Hinweis** Wiederholen Sie den Vorgang für jedes RDM-Gerät, das am WSFC-Cluster teilnimmt.
Markierung als dauerhaft reserviert aufheben	Heben Sie die Reservierung für das Gerät auf, das zuvor markiert wurde.

Ergebnisse

Die Konfiguration wird dauerhaft mit dem ESXi-Host gespeichert und bei Neustarts beibehalten.

Beispiel

Sie können auch den Befehl `esxcli` zum Kennzeichnen der Geräte verwenden, die am WSFC-Cluster beteiligt sind.

1 Markieren Sie das Gerät als dauerhaft reserviert.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=true
```

2 Stellen Sie sicher, dass das Gerät dauerhaft reserviert ist.

```
esxcli storage core device list -d naa.id
```

Suchen Sie in der Ausgabe des Befehls `esxcli` nach dem Eintrag `Is Perennially Reserved: true`.

3 Führen Sie den folgenden Befehl aus, um das dauerhaft reservierte Flag zu entfernen.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=false
```

Arbeiten mit Flash-Geräten

15

Neben regulären Speicher-Festplattenlaufwerken (HDDs) unterstützt ESXi Flash-Speichergeräte.

Anders als die regulären Festplatten (HDDs), bei denen es sich um elektromechanische Geräte mit beweglichen Teilen handelt, verwenden Flash-Geräte Halbleiter als Speichermedium und enthalten keine beweglichen Teile. In der Regel sind Flash-Geräte widerstandsfähig und bieten schnelleren Zugriff auf Daten.

Zur Erkennung von Flash-Geräten verwendet ESXi einen Abfragemechanismus, der auf T10-Standards basiert. Erkundigen Sie sich bei Ihrem Anbieter, ob Ihr Speicher-Array die Erkennung von Flash-Geräten durch den ESXi-Mechanismus unterstützt.

Nachdem der Host die Flash-Geräte erkannt hat, können Sie diese für verschiedene Aufgaben und Funktionen verwenden.

Wenn Sie NVMe-Speicher verwenden, aktivieren Sie das Hochleistungs-Plug-In (High-Performance Plug-In, HPP), um Ihre Speicherleistung zu verbessern. Weitere Informationen hierzu finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas.

Einzelheiten zur Verwendung von NVMe-Speicher mit ESXi finden Sie unter Kapitel 16 NVMe-Speicher von VMware.

Tabelle 15-1. Verwenden von Flash-Geräten mit ESXi

Funktionalität	Beschreibung
vSAN	vSAN erfordert Flash-Geräte. Weitere Informationen finden Sie in der Dokumentation *Verwalten von VMware vSAN*.
VMFS-Datenspeicher	Erstellen Sie VMFS-Datenspeicher auf Flash-Geräten. Verwenden Sie die Datenspeicher für folgende Zwecke: ■ Speichern virtueller Maschinen. Bestimmte Gastbetriebssysteme können virtuelle Festplatten, die sich auf diesen Datenspeichern befinden, als vFlash-Festplatten identifizieren. ■ Teilen Sie Datenspeicherplatz für den ESXi-Hostauslagerungs-Cache zu. Weitere Informationen hierzu finden Sie unter Konfigurieren des Host-Caches mit VMFS-Datenspeicher.
Virtuelle Flash-Ressource (VFFS)	Soweit dies Ihr Anbieter erfordert, richten Sie eine vFlash-Ressource für E/A-Cache-Filter ein. Weitere Informationen hierzu finden Sie unter Kapitel 23 Filtern der E/A einer virtuellen Maschine.

Flash-Geräte und virtuelle Maschinen

Gastbetriebssysteme können virtuelle Festplatten, die sich auf Flash-Datenspeichern befinden, als vFlash-Festplatten identifizieren.

Gastbetriebssysteme können Standardabfragebefehle verwenden, wie z. B. SCSI VPD Page (B1h) für SCSI-Geräte und ATA IDENTIFY DEVICE (Word 217) für IDE-Geräte.

Für verknüpfte Klone, native Snapshots und Delta-Festplatten melden die Abfragebefehle den virtuellen Flash-Status der Basisfestplatte.

Betriebssysteme können eine virtuelle Festplatte unter folgenden Bedingungen als Flash-Festplatte erkennen:

- Das Erkennen von vFlash-Festplatten wird auf VMs mit der virtuellen Hardwareversion 8 oder höher unterstützt.
- Geräte, die einen gemeinsam genutzten VMFS-Datenspeicher unterstützen, müssen auf allen Hosts als „Flash“ markiert sein.
- Wenn der VMFS-Datenspeicher mehrere Geräteerweiterungen enthält, müssen alle zugrunde liegenden physischen Erweiterungen flashbasiert sein.

Dieses Kapitel enthält die folgenden Themen:

Markieren der Speichergeräte

Sie können Speichergeräte auf einem ESXi-Host als lokale Flash-Geräte kennzeichnen.

Wenn Sie vSAN konfigurieren oder eine virtuelle Flash-Ressource einrichten, muss Ihre Speicherumgebung lokale Flash-Geräte enthalten.

Es kann jedoch vorkommen, dass ESXi bestimmte Speichergeräte nicht als Flash-Geräte erkennt, wenn deren Anbieter die automatische Flash-Geräteerkennung nicht unterstützen. Es kann auch vorkommen, dass bestimmte Geräte nicht als lokal erkannt und daraufhin von ESXi als remote gekennzeichnet werden. Wenn Geräte nicht als lokale Flash-Geräte erkannt werden, werden sie aus der Liste der für vSAN oder die virtuelle Flash-Ressource angebotenen Geräte ausgeschlossen. Wenn diese Geräte als lokale Flash-Geräte markiert werden, stehen sie für vSAN und für die virtuelle Flash-Ressource zur Verfügung.

Markieren der Speichergeräte als Flash-Gerät

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

ESXi erkennt bestimmt 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.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
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 und klicken Sie auf das Symbol **Als Flash-Festplatte markieren** (F).
5. Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

Ergebnisse

Der Gerätetyp wird in „Flash“ geändert.

Nächste Schritte

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.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie aus der Liste der Speichergeräte ein oder mehrere Remotegeräte aus und klicken Sie auf das Symbol **Als lokal markieren**.

5 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

Überwachen von Flash-Geräten

Sie können bestimmte kritische Flash-Geräte-Parameter, darunter `Media Wearout Indicator`, `Temperature` und `Reallocated Sector Count`, von einem ESXi-Host aus überwachen.

Verwenden Sie den `esxcli`-Befehl, um Flash-Geräte zu überwachen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie folgenden Befehl aus, um Flash-Geräte-Statistiken anzuzeigen:

  `esxcli storage core device smart get -d=`*`flash device_ID`*

Best Practices für Flash-Geräte

Befolgen Sie diese Best Practices, wenn Sie Flash-Geräte in einer vSphere-Umgebung verwenden.

- Verwenden Sie Flash-Geräte, die vom *VMware-Kompatibilitätshandbuch* genehmigt wurden.
- Stellen Sie sicher, dass Sie mit Flash-Geräten die neueste Firmware verwenden. Erkundigen Sie sich regelmäßig bei Ihren Speicheranbietern nach Updates.
- Achten Sie sorgfältig darauf, wie intensiv Sie das Flash-Gerät nutzen, und berechnen Sie dessen geschätzte Lebensdauer. Die Lebenserwartung hängt davon ab, wie aktiv Sie das Flash-Gerät weiterhin nutzen. Weitere Informationen hierzu finden Sie unter Geschätzte Lebensdauer von Flash-Geräten.
- Wenn Sie NVMe-Geräte als Speicher verwenden, aktivieren Sie das Hochleistungs-Plug-In (High-Performance Plug-In, HPP), um Ihre Speicherleistung zu verbessern. Einzelheiten zur Verwendung der NVMe-Geräte finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas

Geschätzte Lebensdauer von Flash-Geräten

Überwachen Sie beim Arbeiten mit Flash-Geräten, wie aktiv Sie sie verwenden, und berechnen Sie ihre geschätzte Lebensdauer.

In der Regel bieten Speicheranbieter zuverlässige Schätzungen zur Lebensdauer für ein Flash-Gerät unter idealen Bedingungen. Beispielsweise garantiert ein Anbieter eine Lebensdauer von 5 Jahren unter der Bedingung, dass es 20 GB an Schreibvorgängen pro Tag gibt. Allerdings hängt die tatsächliche Lebenserwartung des Geräts davon ab, wie viele Schreibvorgänge pro Tag Ihr ESXi-Host tatsächlich generiert. Führen Sie die folgenden Schritte aus, um die Lebensdauer des Flash-Geräts zu berechnen.

Voraussetzungen

Notieren Sie die Anzahl der Tage, die seit dem letzten Neustart des ESXi-Hosts vergangen sind. Beispiel: 10 Tage.

Verfahren

1 Ermitteln Sie die Gesamtzahl der Blöcke, die seit dem letzten Neustart auf das Flash-Gerät geschrieben wurden.

   Führen Sie den folgenden Befehl aus: **`esxcli storage core device stats get -d=`*`device_ID`*** Beispiel:

```
~ # esxcli storage core device stats get -d t10.xxxxxxxxxxxxxxx
    Device: t10.xxxxxxxxxxxxxxx
    Successful Commands: xxxxxxx
    Blocks Read: xxxxxxxx
    Blocks Written: 629145600
    Read Operations: xxxxxxxx
```

   Das Element „Blocks Written“ (Geschriebene Blöcke) in der Ausgabe zeigt die Anzahl der Blöcke, die seit dem letzten Neustart auf das Gerät geschrieben wurden. In diesem Beispiel ist der Wert 629.145.600. Nach jedem Neustart wird der Zähler auf 0 zurückgesetzt.

2 Berechnen Sie die Gesamtzahl der Schreibvorgänge und wandeln Sie diese in GB um.

   Ein Block umfasst 512 Byte. Um die Gesamtzahl der Schreibvorgänge zu berechnen, multiplizieren Sie den Wert von „Blocks Written“ (Geschriebene Blöcke) mit 512. Wandeln Sie dann den Ergebniswert in GB um.

   In diesem Beispiel beträgt die Gesamtzahl der Schreibvorgänge seit dem letzten Neustart ca. 322 GB.

3 Schätzen Sie die durchschnittliche Anzahl der Schreibvorgänge pro Tag in GB.

   Dividieren Sie die Gesamtzahl der Schreibvorgänge durch die Anzahl der Tage seit dem letzten Neustart.

   Wenn der letzte Neustart vor 10 Tagen erfolgt ist, erhalten Sie 32 GB Schreibvorgänge pro Tag. Anhand dieser Anzahl können Sie den Durchschnitt über einen bestimmten Zeitraum ermitteln.

4 Schätzen Sie die Lebensdauer Ihres Geräts anhand der folgenden Formel:

Vom Anbieter angegebene Anzahl der Schreibvorgänge pro Tag mal *die vom Anbieter angegebene Lebensdauer* geteilt durch *die tatsächliche durchschnittliche Anzahl der Schreibvorgänge pro Tag*

Wenn der Anbieter beispielsweise eine Lebensdauer von 5 Jahren garantiert unter der Bedingung, dass es 20 GB an Schreibvorgängen pro Tag gibt, und die tatsächliche Anzahl an Schreibvorgängen pro Tag 30 GB ist, beträgt die Lebensdauer Ihres Flash-Geräts ungefähr 3,3 Jahre.

Informationen zu vFlash-Ressourcen

Sie können lokale Flash-Geräte auf einem ESXi-Host zu einem einzelnen virtualisierten Zwischenspeicher-Layer, der so genannten vFlash-Ressource, zusammenfassen.

Wenn Sie die vFlash-Ressource einrichten, erstellen Sie ein neues Dateisystem, das virtuelle Flash-Dateisystem (Virtual Flash File System, VFFS). Das VFFS ist eine Ableitung des VMFS, das für Flash-Geräte optimiert ist und zum Gruppieren der physischen Flash-Geräte zu einem einzelnen Zwischenspeicherressourcenpool verwendet wird. Als nicht dauerhafte Ressource kann es nicht zum Speichern von virtuellen Maschinen verwendet werden.

Nachdem Sie die virtuelle Flash-Ressource eingerichtet haben, können Sie sie für E/A-Cache-Filter verwenden. Weitere Informationen hierzu finden Sie unter Kapitel 23 Filtern der E/A einer virtuellen Maschine.

Überlegungen zu vFlash-Ressourcen

Wenn Sie eine virtuelle Flash-Ressource konfigurieren, gelten mehrere Überlegungen.

- Auf jedem ESXi-Host kann nur eine virtuelle Flash-Ressource vorhanden sein. Die virtuelle Flash-Ressource wird auf Hostebene verwaltet.
- Sie können die virtuelle Flash-Ressource nicht zum Speichern von virtuellen Maschinen verwenden. Die virtuelle Flash-Ressource ist nur eine Zwischenspeicherebene.
- Sie können nur lokale Flash-Geräte für die virtuelle Flash-Ressource verwenden.
- Sie können die virtuelle Flash-Ressource von gemischten Flash-Geräten aus verwenden. Alle Gerätetypen werden gleich behandelt, und es wird nicht zwischen SAS-, SATA- oder PCI Express-Verbindungen unterschieden. Wenn die Ressource aus gemischten Flash-Geräten erstellt wird, müssen Sie Geräte mit vergleichbarer Leistung zusammen gruppieren, um die Leistung zu maximieren.
- Sie können nicht die gleichen Flash-Geräte für die virtuelle Flash-Ressource und vSAN verwenden. Diese benötigen jeweils ein eigenes, dediziertes Flash-Gerät.

Einrichten der vFlash-Ressource

Sie können eine vFlash-Ressource einrichten oder einer vorhandenen vFlash-Ressource Kapazität hinzufügen.

Zum Einrichten einer vFlash-Ressource verwenden Sie lokale Flash-Geräte, die mit Ihrem Host oder Hostcluster verbunden sind. Wenn Sie die Kapazität der virtuellen Flash-Ressource erhöhen möchten, können Sie weitere Geräte hinzufügen. Die maximale Anzahl der Geräte ist in der Dokumentation *Maximalwerte für die Konfiguration* angegeben. Ein einzelnes Flash-Gerät muss der vFlash-Ressource exklusiv zugeteilt werden. Keine andere vSphere-Funktionalität, wie z. B. vSAN oder VMFS, kann das Gerät mit der vFlash-Ressource gemeinsam nutzen.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Virtueller Flash** auf **Virtual Flash-Ressourcenverwaltung**.

4 Klicken Sie auf eine der folgenden Optionen.

Option	Beschreibung
Kapazität hinzufügen	Wenn Sie die vFlash-Ressource auf einem einzelnen Host erstellen.
Kapazität auf Cluster hinzufügen	Wenn Sie die vFlash-Ressource auf einem Cluster erstellen.

5 Wählen Sie aus der Liste der verfügbaren Elemente eines oder mehrere zur Verwendung durch die vFlash-Ressource aus und klicken Sie auf **OK**.

Wenn Ihre Flash-Geräte nicht in der Liste angezeigt werden, finden Sie weitere Informationen unter Markieren der Speichergeräte.

Option	Beschreibung
Lokale VMware-Festplatte	Wählen Sie eine beliebige Kombination von nicht beanspruchten Flash-Geräten aus. ESXi erstellt das VFFS-Volume auf einem der Geräte und erweitert dann das Volume auf die restlichen Geräte. Das System konfiguriert die vFlash-Ressource auf dem gesamten VFFS-Volume. Wenn ein VFFS-Volume auf Ihrem Host vorhanden ist, können Sie erst dann nicht beanspruchte Geräte auswählen, nachdem Sie das vorhandene VFFS-Volume ausgewählt haben.
***Volume-ID* – Mithilfe der vorhandenen VFFS-Volume-Erweiterungen konfigurieren**	Wenn Sie zuvor ein VFFS-Volume auf einem der Flash-Geräte des Hosts mit dem Befehl `vmkfstools` erstellt haben, wird das Volume ebenfalls in der Liste der geeigneten Elemente angezeigt. Sie können nur dieses Volume für die vFlash-Ressource auswählen. Sie können es aber auch mit den nicht beanspruchten Geräten kombinieren. ESXi verwendet das vorhandene VFFS-Volume, um es über andere Geräte zu erweitern.

Ergebnisse

Die vFlash-Ressource wird erstellt. Im Bereich „Geräte-Backing“ werden alle Geräte aufgelistet, die für die virtuelle Flash-Ressource verwendet werden.

Nächste Schritte

Verwenden Sie die vFlash-Ressource für E/A-Cache-Filter, die über vSphere APIs für E/A-Filterung entwickelt wurden. Weitere Informationen finden Sie unter Verwenden von Flash-Speichergeräten mit Cache-E/A-Filtern.

Durch Hinzufügen weiterer Flash-Geräte zur virtuellen Flash-Ressource können Sie die Kapazität erhöhen.

Entfernen der vFlash-Ressource

Sie müssen möglicherweise eine virtuelle Flash-Ressource entfernen, die auf mit dem ESXi-Host verbundenen lokalen Flash-Geräten bereitgestellt wird. Durch das Entfernen der virtuellen Flash-Ressource werden die Geräte für andere Dienste freigegeben.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Flash-Ressource nicht für E/A-Filter verwendet wird.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Virtueller Flash** auf **Virtual Flash-Ressourcenverwaltung** und klicken Sie auf **Alle entfernen**.

Ergebnisse

Nachdem Sie die vFlash-Ressource entfernt und das Flash-Gerät gelöscht haben, ist das Gerät für andere Vorgänge verfügbar.

Einrichten eines Alarms für die Verwendung virtueller Flashs

Richten Sie einen Alarm ein, um anzugeben, dass die Verwendung einer virtuellen Flash-Ressource auf Ihrem ESXi-Host den angegebenen Schwellenwert überschreitet.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.

4 Wählen Sie die gewünschte Einstellung aus und klicken Sie auf **Bearbeiten**.

Parameter	Beschreibung
VFLASH.ResourceUsageThreshold	Das System löst den Alarm `Host-vFlash-Ressourcennutzung` aus, sobald die Nutzung einer virtuellen Flash-Ressource den Schwellenwert überschreitet. Der Standardschwellenwert ist 80 %. Sie können den Schwellenwert an Ihre Anforderungen anpassen. Der Alarm wird zurückgesetzt, wenn die Nutzung der virtuellen Flash-Ressource wieder unter den Schwellenwert fällt.

5 Klicken Sie auf **OK**.

Konfigurieren des Host-Caches mit VMFS-Datenspeicher

Aktivieren Sie das Auslagern des Host-Cache auf Ihrem ESXi-Host. Sie können auch die Größe des Speicherplatzes ändern, der dem Host-Cache zugeteilt ist.

Ihre ESXi-Hosts können einen Teil des Flash-gestützten Speicherelements als Auslagerungs-Cache verwenden, der von allen virtuellen Maschinen gemeinsam genutzt wird.

Der Cache auf Hostebene besteht aus Dateien auf einer niedriglatenten Festplatte, die von ESXi als Write-Back-Cache für Auslagerungsdateien der virtuellen Maschinen verwendet wird. Der Cache wird von allen virtuellen Maschinen gemeinsam verwendet, die auf dem Host ausgeführt werden. Durch das Auslagern von Seiten der virtuelle Maschinen kann der potenziell beschränkte Speicherplatz auf Flash-Geräten optimal genutzt werden.

Voraussetzungen

Erstellen Sie einen VMFS-Datenspeicher mit Flash-Geräten als Backing. Weitere Informationen hierzu finden Sie unter Erstellen eines VMFS-Datenspeichers.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Host-Cache-Konfiguration**.

4 Wählen Sie den flash-Datenspeicher aus der Liste und klicken Sie auf das Symbol **Bearbeiten**.

5 Teilen Sie dem Host-Cache ausreichend Speicherplatz zu.

6 Klicken Sie auf **OK**.

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 ESXi-Referenzhost fest.

1. Navigieren Sie im vSphere Client zu dem Host, 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. Legen Sie die folgenden Elemente fest.

Parameter	Wert
VMkernel.Boot.autoPartition	True
VMkernel.Boot.skipPartitioningSsds	True

4. Starten Sie den Host neu.

Falls Flash-Festplatten, die Sie mit der virtuellen Flash-Ressource und vSAN verwenden möchten, bereits VMFS-Datenspeicher aufweisen, entfernen Sie die Datenspeicher.

NVMe-Speicher von VMware

16

Speichergeräte mit nicht flüchtigem Arbeitsspeicher (NVM), die persistenten Arbeitsspeicher verwenden, werden in Datencentern immer beliebter. NVM Express (NVMe) ist ein standardisiertes Protokoll, das speziell für die Hochleistungskommunikation mit NVM-Geräten entwickelt wurde, wobei mehrere Warteschlangen unterstützt werden. ESXi unterstützt das NVMe-Protokoll für Verbindungen mit lokalen Geräten und Netzwerkspeichergeräten.

Dieses Kapitel enthält die folgenden Themen:

VMware NVMe-Konzepte

Bevor Sie mit der Arbeit mit NVMe-Speicher in der ESXi-Umgebung beginnen, können Sie sich mit den grundlegenden NVMe-Konzepten vertraut machen.

NVM Express (NVMe)

NVMe ist eine Methode zum Verbinden und Übertragen von Daten zwischen einem Host und einem Zielspeichersystem. NVMe ist für die Verwendung mit schnelleren Speichermedien ausgelegt, die mit nicht flüchtigem Arbeitsspeicher ausgestattet sind, z. B. Flash-Geräten. Diese Art von Speicher kann eine niedrige Latenz, eine niedrige CPU-Auslastung und eine hohe Leistung erzielen und dient in der Regel als Alternative zum SCSI-Speicher.

NVMe-Transporte

NVMe-Speicher kann über eine PCIe-Schnittstelle direkt oder über verschiedene Fabric-Transporte indirekt mit einem Host verbunden werden. VMware NVMe over Fabrics (NVMe-oF) stellt Konnektivität über Entfernungen zwischen einem Host und einem Zielspeichergerät auf einem freigegebenen Speicher-Array bereit.

Die folgenden Transporttypen für NVMe sind derzeit vorhanden. Weitere Informationen finden Sie unter Anforderungen und Einschränkungen des VMware NVMe-Speichers.

NVMe-Transport	ESXi-Unterstützung
NVMe over PCIe	Lokaler Speicher.
NVMe over RDMA	Freigegebener NVMe-oF-Speicher. Mit der ROCE v2-Technologie.
NVMe over Fibre Channel (FC-NVMe)	Freigegebener NVMe-oF-Speicher.
NVME over TCP	Freigegebener NVMe-oF-Speicher.

NVMe-Namespaces

Im NVMe-Speicher-Array ist ein Namespace ein Speichervolume, das durch eine bestimmte Menge an nicht flüchtigem Arbeitsspeicher gestützt wird. Im Kontext von ESXi ist der Namespace analog zu einem Speichergerät oder einer LUN. Nachdem Ihr ESXi-Host den NVMe-Namespace ermittelt hat, wird ein Flash-Gerät, das den Namespace repräsentiert, in der Liste der Speichergeräte im vSphere Client angezeigt. Sie können das Gerät zum Erstellen eines VMFS-Datenspeichers und zum Speichern virtueller Maschinen verwenden.

NVMe-Controller

Ein Controller ist mit einem oder mehreren NVMe-Namespaces verknüpft und bietet einen Zugriffspfad zwischen dem ESXi-Host und den Namespaces im Speicher-Array. Für den Zugriff auf den Controller kann der Host zwei Mechanismen verwenden, die Controller-Ermittlung und die Controller-Verbindung. Weitere Informationen finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

Controller-Ermittlung

Mit diesem Mechanismus kontaktiert der ESXi-Host zuerst einen Ermittlungs-Controller. Der Ermittlungs-Controller gibt eine Liste der verfügbaren Controller zurück. Nachdem Sie einen Controller ausgewählt haben, auf den Ihr Host zugreifen kann, stehen alle diesem Controller zugeordneten Namespaces für Ihren Host zur Verfügung.

Controller-Verbindung

Ihr ESXi-Host stellt eine Verbindung mit dem von Ihnen angegebenen Controller her. Alle diesem Controller zugeordneten Namespaces werden Ihrem Host zur Verfügung gestellt.

NVMe-Subsystem

Im Allgemeinen handelt es sich bei einem NVMe-Subsystem um ein Speicher-Array, das mehrere NVMe-Controller, mehrere Namespaces, ein nicht flüchtiges Speichermedium und eine Schnittstelle zwischen dem Controller und einem nicht flüchtigen Speichermedium enthalten kann. Das Subsystem wird durch einen Subsystem NVMe Qualified Name (NQN) identifiziert.

VMware-Hochleistungs-Plug-In (VMware High-Performance Plug-in, HPP)

Standardmäßig verwendet der ESXi-Host das HPP, um die NVMe-oF-Ziele zu beanspruchen. Bei der Auswahl von physischen Pfaden für E/A-Anforderungen wendet das HPP ein geeignetes Pfadauswahlschema (PSS) an. Weitere Informationen zum HPP finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas. Informationen zum Ändern des standardmäßigen Pfadauswahlmechanismus finden Sie unter Ändern der Pfadauswahl-Richtlinie.

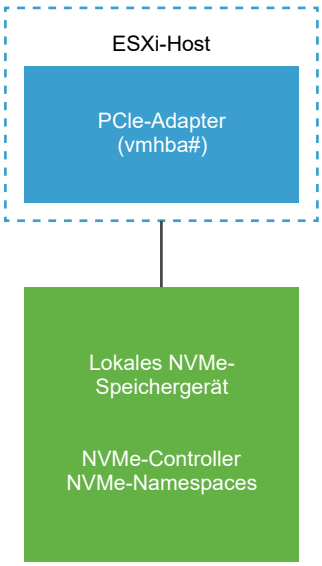
Grundlegende VMware NVMe-Architektur und -Komponenten

ESXi unterstützt lokalen NVMe over PCIe-Speicher und gemeinsam genutzten NVMe-oF-Speicher, z. B. NVMe over Fibre Channel, NVMe over RDMA (RoCE v2) und NVMe over TCP.

In NVMe-oF-Umgebungen können Ziele Namespaces entsprechend LUNs in SCSI für einen Host im aktiv/aktiven oder asymmetrischen Zugriffsmodus darstellen. ESXi ist in der Lage, in beiden Fällen dargestellte Namespaces zu erkennen und zu verwenden. ESXi emuliert NVMe-oF-Ziele intern als SCSI-Ziele und stellt sie als aktiv/aktive SCSI-Ziele oder implizite ALUA-SCSI-Ziele dar.

VMware NVMe over PCIe

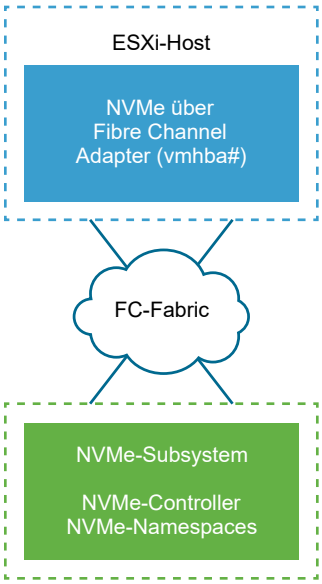
In dieser Konfiguration verwendet Ihr ESXi-Host einen PCIe-Speicheradapter für den Zugriff auf ein oder mehrere lokale NVMe-Speichergeräte. Nachdem Sie den Adapter auf dem Host installiert haben, erkennt der Host die verfügbaren NVMe-Geräte, und diese werden in der Liste der Speichergeräte im vSphere Client angezeigt.



VMware NVMe over FC

Diese Technologie ordnet NVMe dem Fibre Channel-Protokoll zu, um die Übertragung von Daten und Befehlen zwischen einem Hostcomputer und einem Zielspeichergerät zu ermöglichen. Dieser Transport kann vorhandene Fibre Channel-Infrastruktur verwenden, die zur Unterstützung von NVMe aktualisiert wurde.

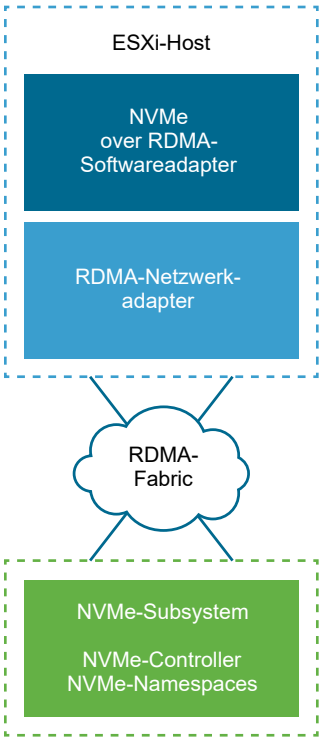
Um auf den NVMe over Fibre Channel-Speicher zuzugreifen, installieren Sie einen Fibre Channel-Speicheradapter, der NVMe auf Ihrem ESXi-Host unterstützt. Es ist kein Konfigurieren des Adapters erforderlich. Er stellt automatisch eine Verbindung zu einem geeigneten NVMe-Subsystem her und erkennt alle gemeinsam genutzten NVMe-Speichergeräte, die er erreichen kann. Sie können den Adapter später neu konfigurieren und seine Controller trennen oder andere Controller verbinden, die während des Hoststarts nicht verfügbar waren. Weitere Informationen finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.



NVMe over RDMA (RoCE v2)

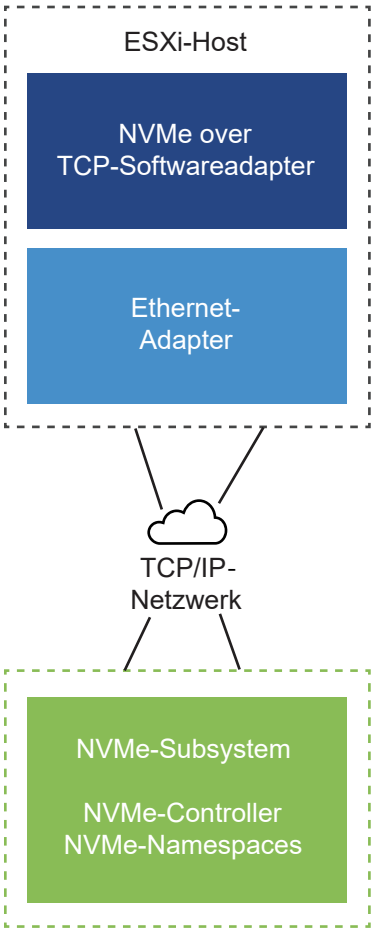
Diese Technologie verwendet einen RDMA-Transport (Remote Direct Memory Access) zwischen zwei Systemen im Netzwerk. Der Transport ermöglicht den Datenaustausch im Hauptspeicher, wobei das Betriebssystem oder der Prozessor eines der beiden Systeme umgangen werden. ESXi unterstützt RDMA over Converged Ethernet v2 (ROCE v2)-Technologie, die einen direkten Remote-Arbeitsspeicherzugriff über ein Ethernet-Netzwerk ermöglicht.

Für den Zugriff auf Speicher verwendet der ESXi-Host einen RDMA-Netzwerkadapter, der auf Ihrem Host installiert ist, und einen NVMe over RDMA-Software-Speicheradapter. Sie müssen beide Adapter so konfigurieren, dass sie für die Speichererkennung verwendet werden. Weitere Informationen finden Sie unter Konfigurieren von Adaptern für NVMe over RDMA (ROCE v2)-Speicher.



NVMe over TCP

Diese Technologie verwendet Ethernet-Verbindungen zwischen zwei Systemen. Für den Zugriff auf Speicher verwendet der ESXi-Host einen auf Ihrem Host installierten Netzwerkadapter sowie einen NVMe over TCP-Softwarespeicheradapter. Sie müssen beide Adapter so konfigurieren, dass sie für die Speichererkennung verwendet werden. Weitere Informationen finden Sie unter Konfigurieren von Adaptern für NVMe over TCP-Speicher.



Anforderungen und Einschränkungen des VMware NVMe-Speichers

Wenn Sie die NVMe-Technologie mit VMware verwenden, müssen Sie spezifische Richtlinien und Anforderungen befolgen.

Anforderungen für NVMe over PCIe

Ihre ESXi-Speicherumgebung muss über die folgenden Komponenten verfügen:

- Lokale NVMe-Speichergeräte.
- Kompatibler ESXi-Host.
- NVMe over PCIe-Hardwareadapter. Nach der Installation des Adapters erkennt Ihr ESXi-Host ihn und zeigt ihn im vSphere Client als Speicheradapter (vmhba) mit als PCIe angegebenem Protokoll an. Es ist kein Konfigurieren des Adapters erforderlich.

Anforderungen für NVMe over RDMA (ROCE v2)

- NVMe-Speicher-Array mit NVMe over RDMA (ROCE v2)-Transportunterstützung.

- Kompatibler ESXi-Host.
- Ethernet-Switches, die ein verlustfreies Netzwerk unterstützen.
- Netzwerkadapter, der RDMA over Converged Ethernet (ROCE v2) unterstützt. Informationen zur Konfiguration des Adapters finden Sie unter Anzeigen von RDMA-Netzwerkadaptern.
- NVMe over RDMA-Softwareadapter. Diese Softwarekomponente muss auf Ihrem ESXi-Host aktiviert und mit einem entsprechenden Netzwerk-RDMA-Adapter verbunden sein. Weitere Informationen finden Sie unter Aktivieren von NVMe over RDMA- oder NVMe oder TCP-Softwareadaptern.
- NVMe-Controller. Sie müssen einen Controller hinzufügen, nachdem Sie einen NVMe over RDMA-Softwareadapter konfiguriert haben. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

Anforderungen für NVMe over Fibre Channel

- Fibre Channel-Speicher-Array, das NVMe unterstützt. Weitere Informationen finden Sie unter Kapitel 4 Verwenden von ESXi mit Fibre-Channel-SAN.
- Kompatibler ESXi-Host.
- NVMe-Hardwareadapter. In der Regel handelt es sich um einen Fibre Channel-HBA, der NVMe unterstützt. Wenn Sie den Adapter installieren, erkennt der ESXi-Host ihn und zeigt ihn im vSphere Client als Fibre Channel-Standardadapter (vmhba) mit als NVMe angegebenem Speicherprotokoll an. Für den NVMe-Hardwareadapter ist keine Konfiguration erforderlich, um ihn verwenden zu können.
- NVMe-Controller. Es ist kein Konfigurieren des Controllers erforderlich. Nachdem Sie den erforderlichen NVMe-Hardwareadapter installiert haben, stellt er automatisch eine Verbindung zu allen Zielen und Controllern her, die derzeit erreichbar sind. Sie können die Controller später trennen oder andere Controller verbinden, die während des Hoststarts nicht verfügbar waren. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

Anforderungen für NVMe over TCP

- NVMe-Speicher-Array mit NVMe over TCP-Transportunterstützung.
- Kompatibler ESXi-Host.
- Ein Ethernet-Adapter.
- NVMe over TCP-Softwareadapter. Diese Softwarekomponente muss auf Ihrem ESXi-Host aktiviert und mit einem entsprechenden Netzwerkadapter verbunden sein. Weitere Informationen finden Sie unter Aktivieren von NVMe over RDMA- oder NVMe oder TCP-Softwareadaptern.
- NVMe-Controller. Sie müssen einen Controller hinzufügen, nachdem Sie einen NVMe over TCP-Softwareadapter konfiguriert haben. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

VMware NVMe over Fabric-Unterstützung für gemeinsam genutzten Speicher

In der ESXi-Umgebung werden die NVMe-Speichergeräte ähnlich wie SCSI-Speichergeräte angezeigt und können als gemeinsam genutzter Speicher verwendet werden. Befolgen Sie die folgenden Regeln bei Verwendung des NVMe-oF-Speichers.

- Mischen Sie keine Transporttypen, um auf denselben Namespace zuzugreifen.
- Stellen Sie sicher, dass dem Host aktive Pfade angezeigt werden. Die Namespaces können erst registriert werden, nachdem der aktive Pfad erkannt wurde.

Gemeinsam genutzter Speicher – Funktionalität	SCSI over Fabric-Speicher	NVMe over Fabric-Speicher
RDM	Unterstützt	Nicht unterstützt
Core-Dump	Unterstützt	Nicht unterstützt
SCSI-2-Reservierungen	Unterstützt	Nicht unterstützt
Cluster-VMDK	Unterstützt	Nicht unterstützt
Gemeinsam genutzte VMDK mit Multiwriter-Flag	Unterstützt	Unterstützt In vSphere 7.0 Update 1 und höher. Weitere Informationen finden Sie im Knowledgebase-Artikel.
Virtual Volumes	Unterstützt	Nicht unterstützt
Hardwarebeschleunigung mit VAAI-Plug-Ins	Unterstützt	Nicht unterstützt
Standard-MPP	NMP	HPP (NVMe-oF-Ziele können nicht von NMP beansprucht werden)
Grenzwerte	LUNs=1024, Pfade=4096	Namespaces=32, Pfade=128 (maximal 4 Pfade pro Namespace in einem Host)

Konfigurieren von verlustfreiem Ethernet für NVMe over RDMA

NVMe over RDMA in ESXi benötigt ein verlustfreies Ethernet-Netzwerk für effizienten Betrieb.

Zum Einrichten von verlustfreien Netzwerken können Sie eine der verfügbaren QoS-Einstellungen auswählen.

Aktivieren von Global Pause Flow Control

Stellen Sie in dieser Netzwerkkonfiguration sicher, dass Global Pause Flow Control auf dem Netzwerk-Switch-Port aktiviert ist. Stellen Sie außerdem sicher, dass RDMA-fähige Netzwerkkarten auf dem Host automatisch die richtige Flusssteuerung aushandeln.

Führen Sie die folgenden Befehle aus, um die Flusssteuerung zu überprüfen.

```
#esxcli network nic get -n vmnicX
   Pause RX: true
   Pause TX: true
```

Wenn die obigen Befehlsoptionen nicht auf „True“ festgelegt sind, führen Sie folgenden Befehl aus.

```
#esxcli network nic pauseParams set -r true -t true -n vmnicX
```

Aktivieren von Priority Flow Control

Für verlustfreien RoCE-Datenverkehr müssen Sie den PFC-Prioritätswert im physischen Switch und den Hosts auf 3 festlegen. Zum Konfigurieren der PFC im ESXi-Host stehen zwei Möglichkeiten zur Verfügung:

- Automatische Konfiguration. Ab ESXi 7.0 können Sie die DCB-PFC-Konfiguration automatisch auf der Host-RNIC anwenden, wenn der RNIC-Treiber DCB und DCBx unterstützt.

  Sie können die aktuellen DCB-Einstellungen überprüfen, indem Sie den folgenden Befehl ausführen:

  ```
  #esxcli network nic dcb status get -n vmnicX
  ```

- Manuelle Konfiguration. In bestimmten Fällen stellen die RNIC-Treiber eine Methode zur manuellen Konfiguration der DCB-PFC mithilfe von treiberspezifischen Parametern bereit. Informationen zur Verwendung dieser Methode finden Sie in der Treiberdokumentation des jeweiligen Herstellers. Im Mellanox ConnectX-4/5-Treiber können Sie den PFC-Prioritätswert beispielsweise auf 3 festlegen, indem Sie den folgenden Befehl ausführen und den Host neu starten.

  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08"
  ```

Aktivieren einer DSCP-basierten PFC

Mit einer DSCP-basierten PFC erhalten Sie eine weitere Möglichkeit zum Konfigurieren eines verlustfreien Netzwerks. Für physische Switches und Hosts müssen Sie den DSCP-Wert auf 26 festlegen. Informationen zur Verwendung dieser Option finden Sie in der Treiberdokumentation des jeweiligen Herstellers. Im Mellanox ConnectX-4/5-Treiber können Sie den DSCP-Tag-Wert beispielsweise auf 26 festlegen, indem Sie die folgenden Befehle ausführen.

- PFC- und DSCP-Vertrauensmodus aktivieren

  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08 trust_state=2"
  ```

- Wert für DSCP auf 26 festlegen

  ```
  #esxcli system module parameters set -m nmlx5_rdma -p "dscp_force=26"
  ```

- Überprüfen Sie die Parameter, um zu bestätigen, ob die Einstellungen korrekt und festgelegt sind.

  ```
  esxcli system module parameters list -m nmlx5_core | grep 'trust_state\|pfcrx\|pfctx'
  ```

- Host neu starten

Konfigurieren von Adaptern für NVMe over RDMA (ROCE v2)-Speicher

Der Adapter-Konfigurationsvorgang auf dem ESXi-Host umfasst das Einrichten der VMkernel-Bindung für einen RDMA-Netzwerkadapter und das anschließende Aktivieren eines NVMe over RDMA-Softwareadapters.

Das folgende Video führt Sie durch die Schritte zum Konfigurieren von NVMe over RDMA-Adaptern.

 (Einrichten von NVMe over RDMA-Adaptern)

Verfahren

1 Anzeigen von RDMA-Netzwerkadaptern

   Nachdem Sie einen Netzwerkadapter installiert haben, der RDMA (RoCE v2) auf Ihrem ESXi-Host unterstützt, verwenden Sie den vSphere Client zum Überprüfen des RDMA-Adapters und eines physischen Netzwerkadapters.

2 Konfigurieren der VMkernel-Bindung für den RDMA-Adapter

   Die Port-Bindung für NVMe over RDMA umfasst das Erstellen eines Switches und das Verbinden des physischen Netzwerkadapters und des VMkernel-Adapters mit dem Switch. Über diese Verbindung wird der RDMA-Adapter an den VMkernel-Adapter gebunden. In der Konfiguration können Sie einen vSphere Standard-Switch oder einen vSphere Distributed Switch verwenden.

Nächste Schritte

Nachdem Sie den NVMe over RDMA-Softwareadapter aktiviert haben, fügen Sie NVMe-Controller hinzu, damit der Host die NVMe-Ziele erkennen kann. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

Anzeigen von RDMA-Netzwerkadaptern

Nachdem Sie einen Netzwerkadapter installiert haben, der RDMA (RoCE v2) auf Ihrem ESXi-Host unterstützt, verwenden Sie den vSphere Client zum Überprüfen des RDMA-Adapters und eines physischen Netzwerkadapters.

Verfahren

1 Installieren Sie auf Ihrem ESXi-Host einen Adapter, der RDMA (ROCE v2) unterstützt, z. B. Mellanox Technologies MT27700 Family ConnectX-4.

   Der Host erkennt den Adapter und der vSphere Client zeigt seine beiden Komponenten an, einen RDMA-Adapter und einen physischen Netzwerkadapter.

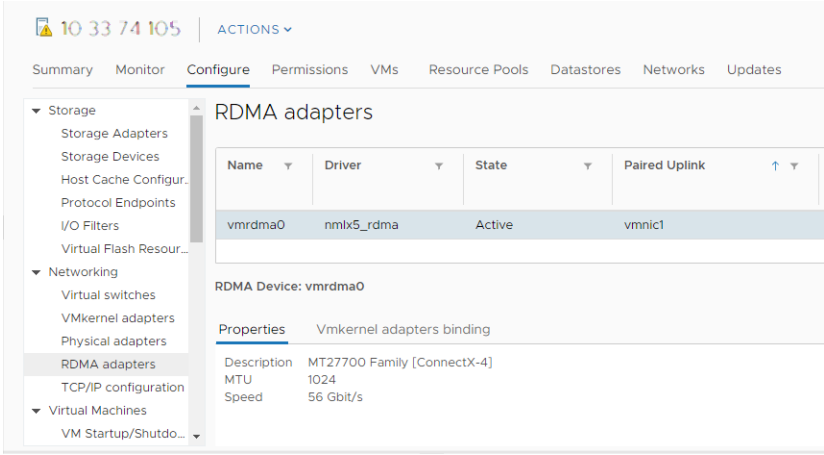
2 Stellen Sie im vSphere Client sicher, dass der RDMA-Adapter von Ihrem Host erkannt wird.

a Navigieren Sie zum Host.

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

c Klicken Sie unter **Netzwerk** auf **RDMA-Adapter**.

In diesem Beispiel wird der RDMA-Adapter in der Liste als `vmrdma0` angezeigt. Die Spalte **Gekoppelter Uplink** zeigt die Netzwerkkomponente als physischen Netzwerkadapter `vmnic1` an.



d Um die Beschreibung des Adapters zu überprüfen, wählen Sie den RDMA-Adapter aus der Liste aus und klicken Sie auf die Registerkarte **Eigenschaften**.

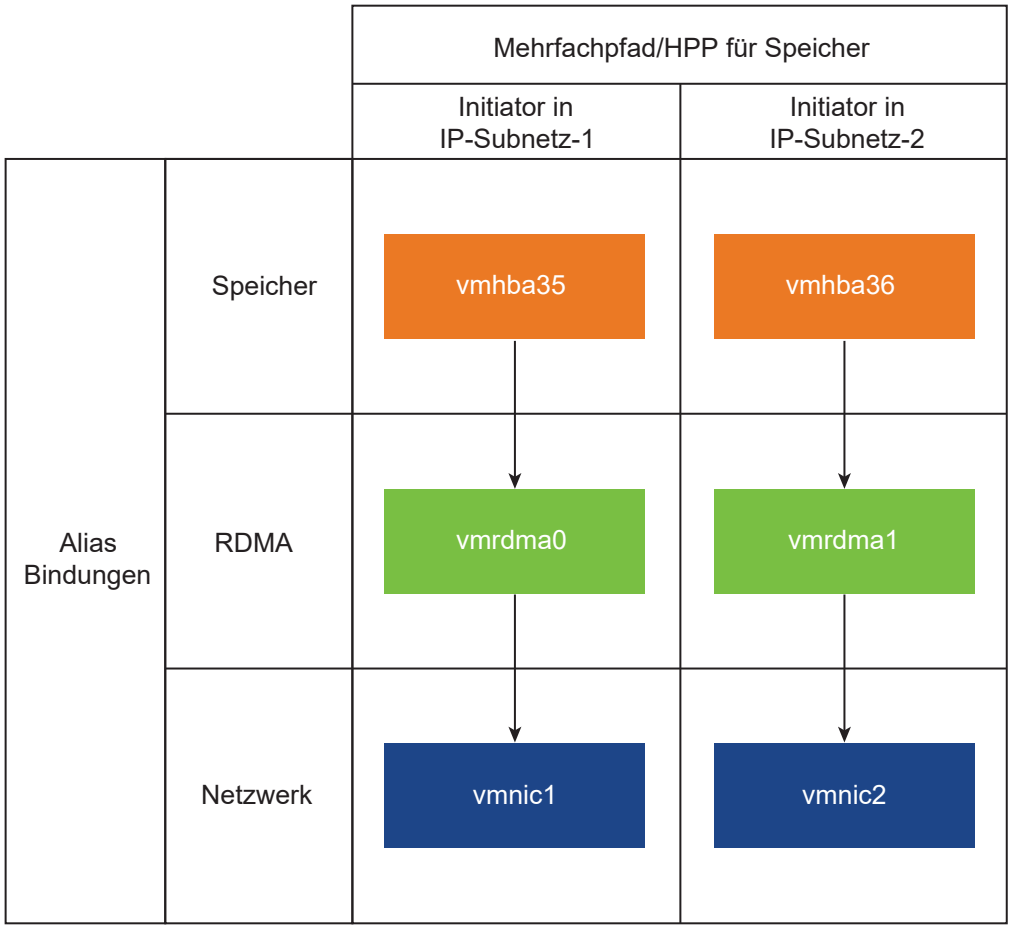
Nächste Schritte

Sie können jetzt die Software NVMe over RDMA-Adapter erstellen.

Konfigurieren der VMkernel-Bindung für den RDMA-Adapter

Die Port-Bindung für NVMe over RDMA umfasst das Erstellen eines Switches und das Verbinden des physischen Netzwerkadapters und des VMkernel-Adapters mit dem Switch. Über diese Verbindung wird der RDMA-Adapter an den VMkernel-Adapter gebunden. In der Konfiguration können Sie einen vSphere Standard-Switch oder einen vSphere Distributed Switch verwenden.

Im folgenden Diagramm wird die Port-Bindung für den NVMe over RDMA-Adapter angezeigt.

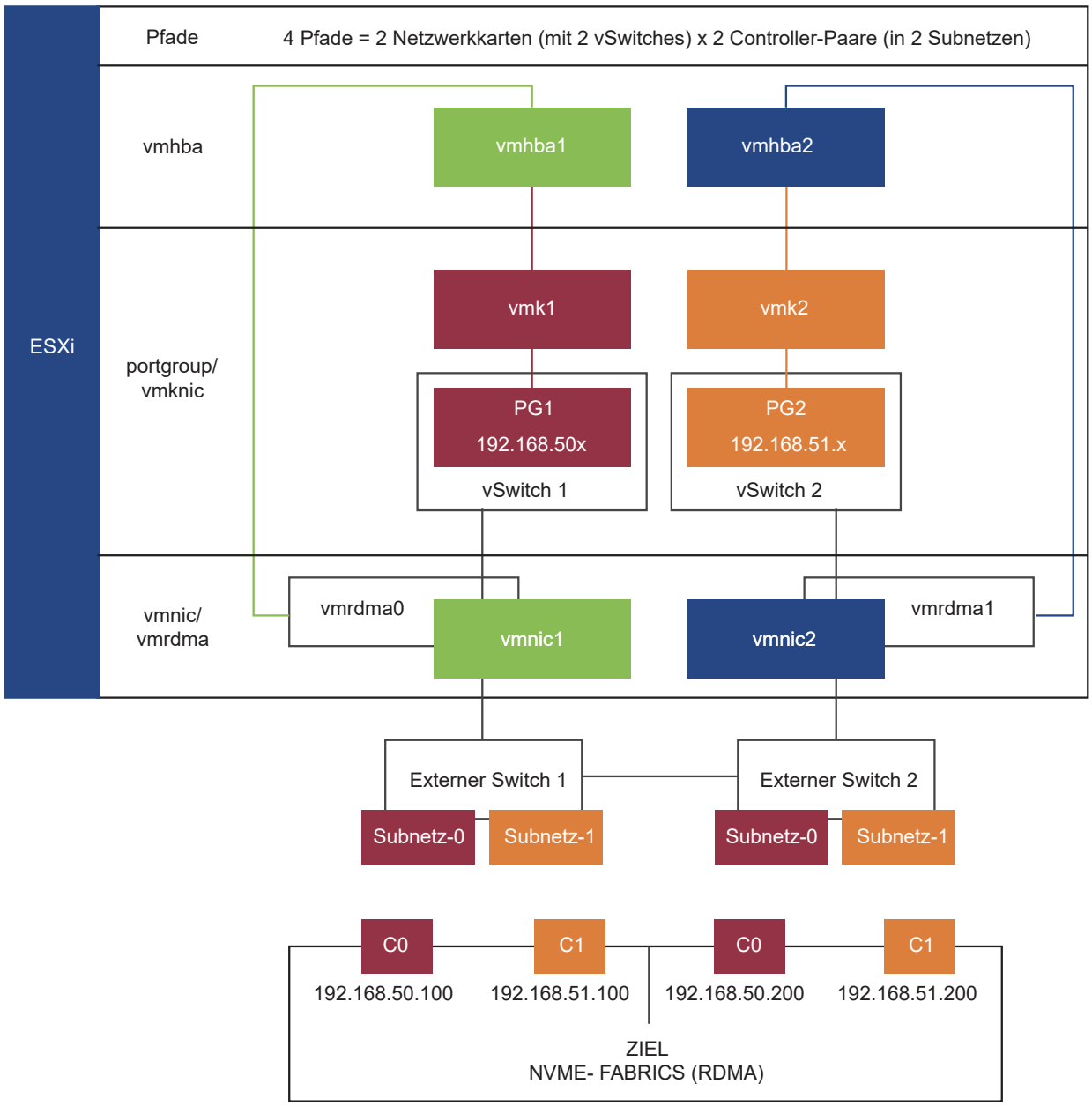


Informationen zum Erstellen von Switches finden Sie unter *vSphere Standard-Switch erstellen* oder *vSphere Distributed Switch erstellen* in der *vSphere-Netzwerk*-Dokumentation.

Beispiel einer Netzwerktopologie mit NVMe over RDMA

In diesem Beispiel stellen zwei vSphere Standard-Switches und zwei Uplinks (RDMA-fähige Netzwerkkarten) Hochverfügbarkeit bereit. Sie stellen eine Verbindung zu zwei Controller-Paaren in zwei Subnetzen her.

Hochverfügbarkeit mit mehreren vSwitches und mehreren Uplinks (RNICs)



Konfigurieren der VMkernel-Bindung mit einem vSphere Standard-Switch

Sie können eine VMkernel-Port-Bindung für den RDMA-Adapter mithilfe eines vSphere Standard-Switches und eines Uplinks pro Switch konfigurieren. Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter.

Verfahren

1 Erstellen Sie einen vSphere Standard-Switch mit einem VMkernel-Adapter und der Netzwerkkomponente.

   a Wählen Sie im vSphere Client Ihren Host aus und klicken Sie auf die Registerkarte **Netzwerke**.

   b Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.

   c Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **WEITER**.

   d Wählen Sie **Neuer Standard-Switch** und klicken Sie auf **WEITER**.

   e Klicken Sie unter **Zugewiesene Adapter** auf **+**.

   Die Liste der verfügbaren physischen Adapter wird angezeigt.

   f Wählen Sie den notwendigen physischen Adapter `vmnic` aus und klicken Sie auf **OK**.

   Hinweis Stellen Sie sicher, dass Sie den physischen Netzwerkadapter auswählen, der dem RDMA-Adapter entspricht. Zum Anzeigen der Verknüpfung zwischen dem RDMA-Adapter `vmrdma` und dem physischen Netzwerkadapter `vmnic` finden Sie Informationen unter Anzeigen von RDMA-Netzwerkadaptern.

   g Geben Sie unter **Porteinstellungen für VMkernel** die notwendigen Werte ein.

   Geben Sie bei Verwendung von VLAN für den Speicherpfad die VLAN-ID ein.

   h Geben Sie in der Liste **IP-Einstellungen** die IPv4-Einstellungen für den VMkernel ein.

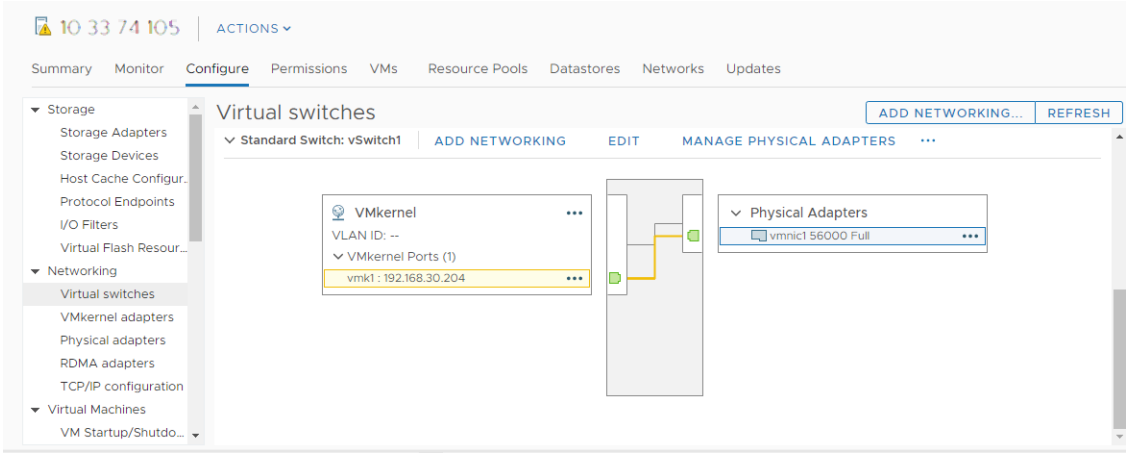
   i Wählen Sie unter „Verfügbare Dienste“ die Option **NVMe over RDMA** aus.

2 Stellen Sie sicher, dass der Switch ordnungsgemäß konfiguriert ist.

a Wählen Sie auf der Registerkarte **Konfigurieren** die Option **Virtuelle Switches** unter **Netzwerk** aus.

b Erweitern Sie den Switch und überprüfen Sie die zugehörige Konfiguration.

Die Abbildung zeigt, dass der physische Netzwerkadapter und der VMkernel-Adapter mit dem vSphere Standard-Switch verbunden sind. Über diese Verbindung ist der RDMA-Adapter an den VMkernel-Adapter gebunden.

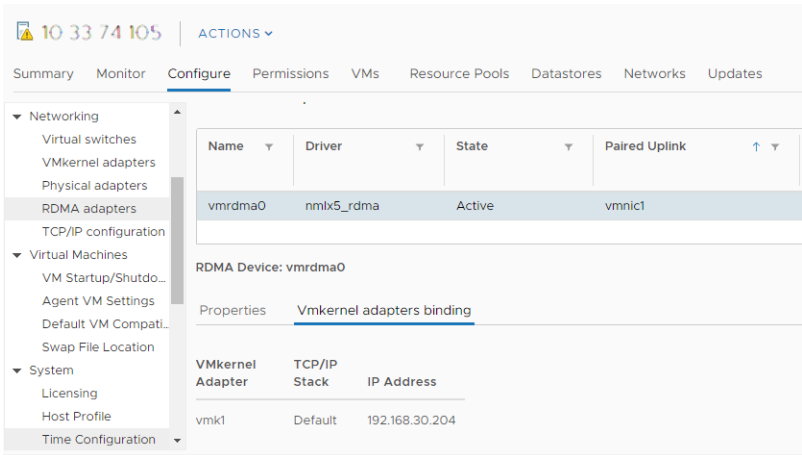


3 Überprüfen Sie die Konfiguration der VMkernel-Bindung für den RDMA-Adapter.

a Klicken Sie unter der Liste **Netzwerk** auf **RDMA-Adapter** und wählen Sie den RDMA-Adapter in der Liste aus.

b Klicken Sie auf die Registerkarte **Bindung von VMkernel-Adaptern** und stellen Sie sicher, dass der zugehörige VMkernel-Adapter auf der Seite angezeigt wird.

In diesem Beispiel wird der RDMA-Adapter `vmrdma0`mit dem Netzwerkadapter `vmnic1` gekoppelt und mit dem VMkernel-Adapter `vmk1` verbunden.



Konfigurieren der VMkernel-Bindung mit einem vSphere Standard-Switch und NIC-Gruppierung

Sie können eine VMkernel-Port-Bindung für den RDMA-Adapter konfigurieren, indem Sie einen vSphere Standard-Switch mit der NIC-Gruppierungskonfiguration verwenden. Sie können die NIC-Gruppierung verwenden, um Netzwerkredundanz zu erreichen. Sie können zwei oder mehr Netzwerkadapter (NICs) als Gruppe für Hochverfügbarkeit und Lastausgleich konfigurieren.

Verfahren

1 Erstellen Sie einen vSphere Standard-Switch mit einem VMkernel-Adapter und der Netzwerkkomponente mit der NIC-Gruppierungskonfiguration.

   a Wählen Sie im vSphere Client Ihren Host aus und klicken Sie auf die Registerkarte **Netzwerke**.

   b Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.

   c Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **WEITER**.

   d Wählen Sie **Neuer Standard-Switch** und klicken Sie auf **WEITER**.

   e Klicken Sie unter **Zugewiesene Adapter** auf **+**.

   Eine Liste der verfügbaren physischen Adapter wird angezeigt.

   f Wählen Sie den notwendigen physischen Adapter `vmnic` aus und fügen Sie ihn unter **Aktive Adapter** hinzu.

   g Wählen Sie einen anderen physischen Adapter `vmnic` aus und fügen Sie ihn unter **Nicht verwendete Adapter** hinzu.

   h Geben Sie unter **Porteinstellungen für VMkernel** die notwendigen Werte ein.

   Geben Sie bei Verwendung von VLAN für den Speicherpfad die VLAN-ID ein.

   i Geben Sie in der Liste **IP-Einstellungen** die IPv4-Einstellungen für den VMkernel an.

   j Wählen Sie unter „Verfügbare Dienste“ die Option **NVMe over RDMA** aus.

   Wiederholen Sie Schritt 1, um einen vorhandenen Standard-Switch zu konfigurieren.

2 Konfigurieren Sie Ihren Switch für die NIC-Gruppierungskonfiguration.

   a Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie die Option **Virtuelle Switches** unter **Netzwerk** aus.

   b Wählen Sie den entsprechenden VMkernel-Adapter aus.

   c Klicken Sie im Kontextmenü auf **Einstellungen bearbeiten**.

   d Wählen Sie **Teaming und Failover** aus.

   e Verschieben Sie unter **Aktive Adapter** den erforderlichen physischen Adapter `vmnic`.

   f Verschieben Sie unter **Standby-Adapter > Failover-Reihenfolge** die anderen physischen Adapter.

g Richten Sie den entsprechenden Lastausgleich und andere Eigenschaften ein.

h Wiederholen Sie die Schritte, um zusätzliche VMkernel-Adapter zu konfigurieren.

3 Wiederholen Sie die Schritte 1 und 2, um einen zusätzlichen Satz gruppierter `rnic`s hinzuzufügen und zu konfigurieren. Um sicherzustellen, dass der Adapter konfiguriert ist, klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **VMkernel-Adapter** aus.

Konfigurieren der VMkernel-Bindung mit einem vSphere Distributed Switch

Sie können eine VMkernel-Port-Bindung für den RDMA-Adapter mithilfe eines vSphere Distributed Switches und eines Uplinks pro Switch konfigurieren. Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter.

Verfahren

1 Erstellen Sie einen vSphere Distributed Switch mit einem VMkernel-Adapter und der Netzwerkkomponente.

a Wählen Sie im vSphere Client die Option **Datencenter** aus und klicken Sie auf die Registerkarte **Netzwerke**.

b Klicken Sie auf **Aktionen** und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.

c Wählen Sie einen Namen für den Switch aus.

Stellen Sie sicher, dass der Speicherort des Datencenters innerhalb Ihres Hosts vorhanden ist, und klicken Sie auf **Weiter**.

d Wählen Sie die ESXi-Version **7.0.0 und höher** aus und klicken Sie auf **Weiter**.

e Geben Sie die erforderliche Anzahl an Uplinks ein und klicken Sie auf **Beenden**.

2 Fügen Sie einen oder mehrere Hosts zu Ihrem Distributed Virtual Switch hinzu.

a Wählen Sie im vSphere Client die Option **Datencenter** aus und klicken Sie auf **Distributed Switches**.

Eine Liste der verfügbaren DSwitches wird angezeigt.

b Klicken Sie mit der rechten Maustaste auf den DSwitch und wählen Sie **Hosts hinzufügen und verwalten** aus.

c Wählen Sie **Hosts hinzufügen** aus und klicken Sie auf **Weiter**.

d Wählen Sie den Host aus und klicken Sie auf **Weiter**.

e Wählen Sie **Uplink zuweisen** aus.

f Geben Sie den relevanten Uplink ein, um die `vmnic` zuzuweisen.

g Weisen Sie einen VMkernel-Adapter zu und klicken Sie auf **Weiter**.

h Wählen Sie im vSphere Client den DSwitch aus und klicken Sie auf die Registerkarte **Ports**.

Sie können die Uplinks anzeigen, die für Ihren Switch erstellt wurden.

3 Erstellen Sie verteilte Portgruppen für den Speicherpfad „NVMe over RDMA“.

a Wählen Sie im vSphere Client den erforderlichen DSwitch aus.

b Klicken Sie auf **Aktionen** und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

c Geben Sie unter **Einstellungen konfigurieren** die allgemeinen Eigenschaften der Portgruppe ein.

Wenn ein spezielles VLAN konfiguriert wurde, fügen Sie es in der VLAN-ID hinzu.

Hinweis Netzwerkkonnektivitätsprobleme können auftreten, wenn das VLAN nicht ordnungsgemäß konfiguriert wurde.

4 Konfigurieren Sie die VMkernel-Adapter.

a Erweitern Sie im vSphere Client die Liste **DSwitch** und wählen Sie die verteilte Portgruppe aus.

b Klicken Sie auf **Aktionen > VMkernel-Adapter hinzufügen**.

c Wählen Sie im Dialogfeld **Mitglieder-Hosts auswählen** Ihren Host aus und klicken Sie auf **OK**.

d Stellen Sie im Dialogfeld **VMkernel-Adapter konfigurieren** sicher, dass die MTU mit der Switch-MTU übereinstimmt.

e Wählen Sie unter **Verfügbare Dienste** die Option **NVMe over RDMA** für das entsprechende Tagging aus.

f Klicken Sie auf **Beenden**.

g Wiederholen Sie Schritt B und Schritt C, um mehrere RDMA-fähige Netzwerkkarten hinzuzufügen.

5 Legen Sie NIC-Gruppierungsrichtlinien für die verteilten Portgruppen fest.

a Klicken Sie unter **Verteilte Portgruppe** auf **Aktionen > Einstellungen bearbeiten**.

b Klicken Sie auf **Teaming und Failover** und überprüfen Sie die aktiven Uplinks.

c Weisen Sie einen Uplink als **Aktiv** für die Portgruppe zu und den anderen Uplink als **Nicht verwendet**.

Wiederholen Sie Schritt C für jede erstellte Portgruppe.

Nächste Schritte

Klicken Sie nach Abschluss der Konfiguration auf **Konfigurieren** und stellen Sie sicher, dass auf der Registerkarte „Physischer Adapter“ Ihres Hosts der DVSwitch für die ausgewählten Netzwerkkarten aufgelistet wird.

Konfigurieren von Adaptern für NVMe over TCP-Speicher

Der Adapter-Konfigurationsvorgang auf dem ESXi-Host umfasst das Einrichten der VMkernel-Bindung für einen TCP-Netzwerkadapter und das anschließende Aktivieren eines NVMe over TCP-Softwareadapters.

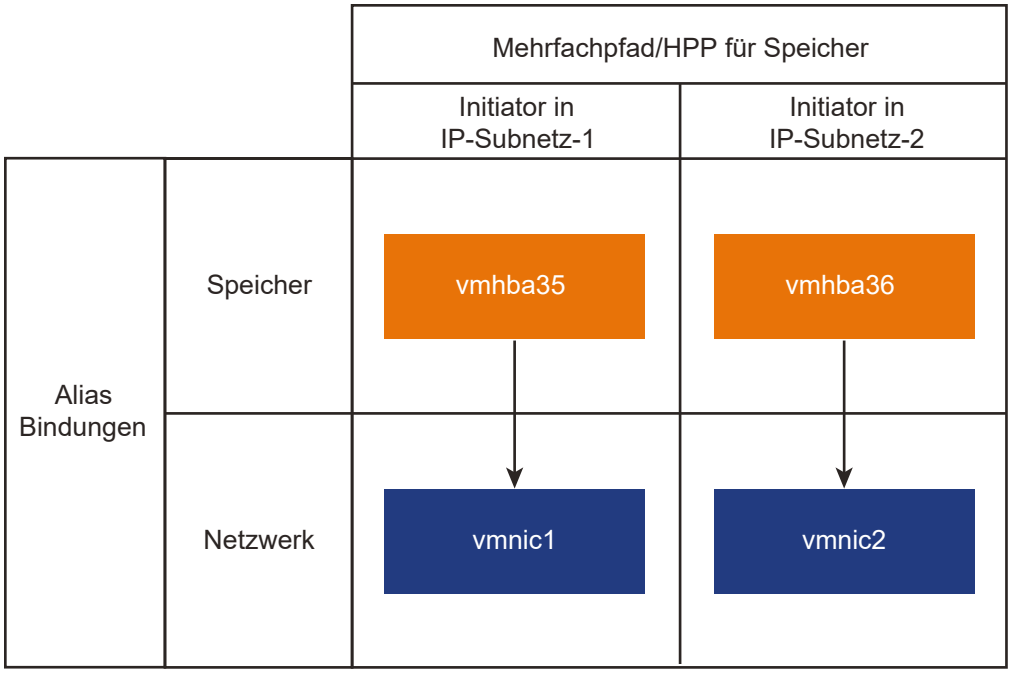
Nächste Schritte

Nachdem Sie den NVMe over TCP-Softwareadapter aktiviert haben, fügen Sie NVMe-Controller hinzu, damit der Host die NVMe-Ziele erkennen kann. Weitere Informationen finden Sie unter Hinzufügen eines Controllers für NVMe over Fabrics.

Konfigurieren der VMkernel-Bindung für den NVMe over TCP-Adapter

Die Port-Bindung für NVMe over TCP umfasst das Erstellen eines virtuellen Switches und das Verbinden des physischen Netzwerkadapters und des VMkernel-Adapters mit dem virtuellen Switch. Durch diese Verbindung wird der TCP-Adapter an den VMkernel-Adapter gebunden. In der Konfiguration können Sie einen vSphere Standard-Switch oder einen vSphere Distributed Switch verwenden.

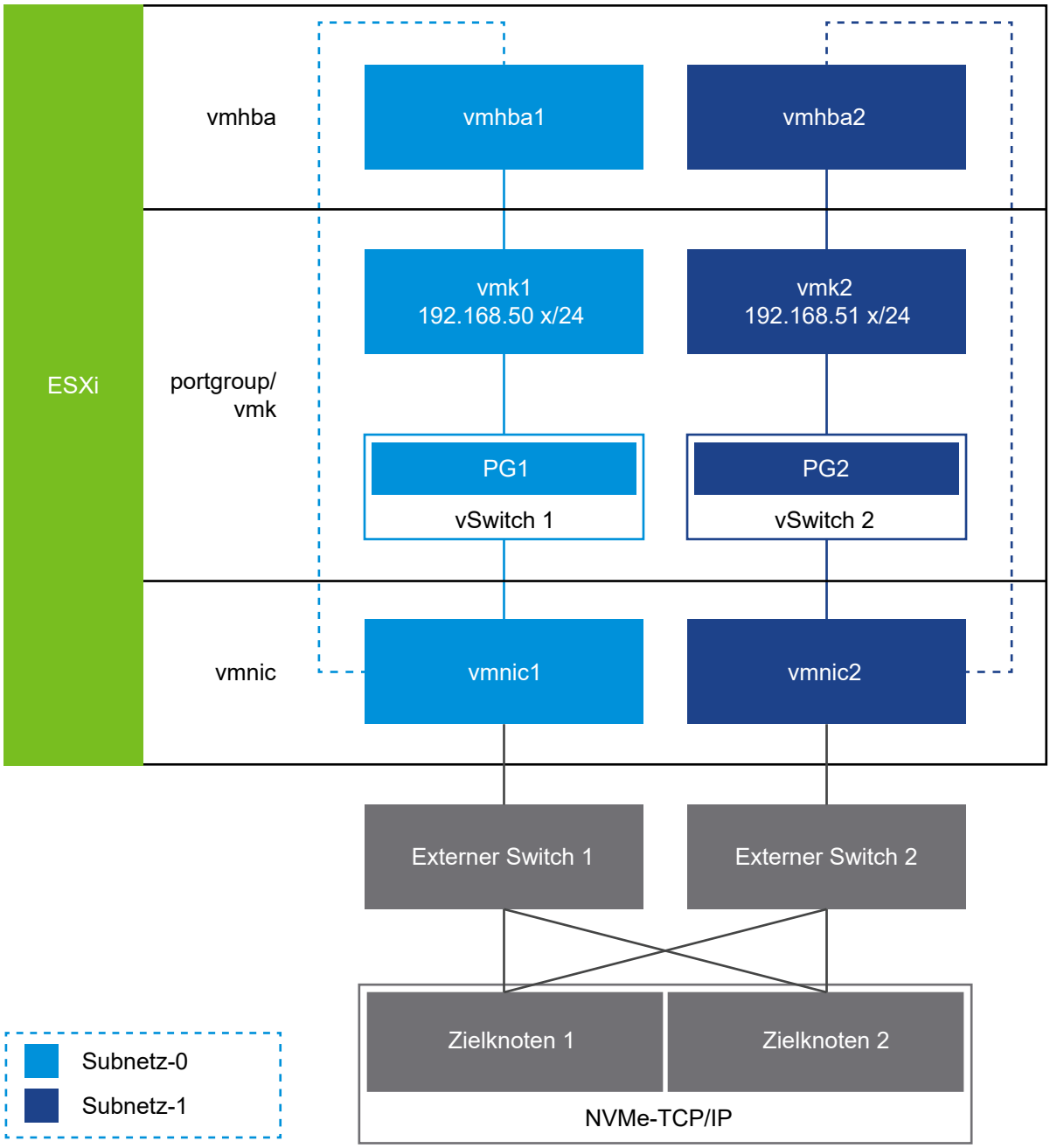
Das folgende Diagramm zeigt die Port-Bindung für den NVMe over TCP-Adapter.



Informationen zum Erstellen von Switches finden Sie unter *vSphere Standard-Switch erstellen* oder *vSphere Distributed Switch erstellen* in der *vSphere-Netzwerk*-Dokumentation.

Beispiel einer Netzwerktopologie mit NVMe over TCP

Bei diesem Beispiel sorgen zwei vSphere-Standardswitches und zwei Netzwerkadapter (vmnic) auf dem Host für Hochverfügbarkeit. Sie bauen eine Verbindung mit zwei externen Switches auf.



Konfigurieren der VMkernel-Bindung für den TCP-Adapter mit einem vSphere Standard-Switch

Sie können die VMkernel-Port-Bindung für den TCP-Adapter mit einem vSphere Standard-Switch und einem Uplink pro Switch konfigurieren. Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter.

Verfahren

1 Erstellen Sie einen vSphere Standard-Switch mit einem VMkernel-Adapter und der Netzwerkkomponente.

   a Wählen Sie im vSphere Client Ihren Host aus und klicken Sie auf die Registerkarte **Netzwerke**.

   b Klicken Sie auf **Aktionen > Netzwerk hinzufügen**.

   c Wählen Sie **VMkernel-Netzwerkadapter** aus und klicken Sie auf **WEITER**.

   d Wählen Sie **Neuer Standard-Switch** und klicken Sie auf **WEITER**.

   e Klicken Sie unter **Zugewiesene Adapter** auf **+**.

   Die Liste der verfügbaren physischen Adapter wird angezeigt.

   f Wählen Sie den notwendigen physischen Adapter `vmnic` aus und klicken Sie auf **OK**.

   Hinweis Stellen Sie sicher, dass Sie den physischen Netzwerkadapter auswählen, der dem TCP/IP-Adapter entspricht.

   g Geben Sie unter **Porteinstellungen für VMkernel** die notwendigen Werte ein.

   Geben Sie bei Verwendung von VLAN für den Speicherpfad die VLAN-ID ein.

   h Geben Sie in der Liste **IP-Einstellungen** die IPv4-Einstellungen für den VMkernel ein.

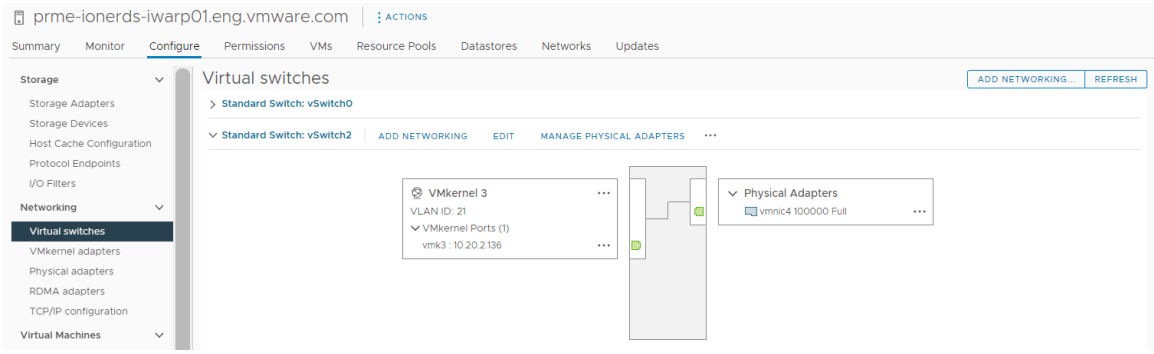
   i Wählen Sie unter **Verfügbare Dienste** die Option **NVMe over TCP** für das entsprechende Tagging aus.

2 Stellen Sie sicher, dass der Switch ordnungsgemäß konfiguriert ist.

a Wählen Sie auf der Registerkarte **Konfigurieren** die Option **Virtuelle Switches** unter **Netzwerk** aus.

b Erweitern Sie den Switch und überprüfen Sie die zugehörige Konfiguration.

Die Abbildung zeigt, dass der physische Netzwerkadapter und der VMkernel-Adapter mit dem vSphere Standard-Switch verbunden sind. Über diese Verbindung wird der TCP-Adapter an den VMkernel-Adapter gebunden.



3 Legen Sie NIC-Gruppierungsrichtlinien für vSphere Standard-Switch fest.

Hinweis Der NVMe-/TCP-Adapter unterstützt keine NIC-Gruppierungsfunktionen wie Failover und Lastausgleich. Stattdessen wird für diese Funktionen Storage Multipathing genutzt. Wenn Sie jedoch die NIC-Gruppierung für andere Netzwerkarbeitslasten auf dem Uplink konfigurieren müssen, der den NVMe-/TCP-Adapter bedient, führen Sie die folgenden Schritte aus.

a Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie die Option **Virtuelle Switches** unter **Netzwerk** aus.

b Wählen Sie den entsprechenden VMkernel-Adapter aus.

c Klicken Sie im Kontextmenü auf **Einstellungen bearbeiten**.

d Wählen Sie **Teaming und Failover** aus.

e Verschieben Sie unter **Aktive Adapter** den erforderlichen physischen Adapter `vmnic`.

f Verschieben Sie unter **Standby-Adapter > Failover-Reihenfolge** die anderen physischen Adapter.

g Richten Sie den entsprechenden Lastausgleich und andere Eigenschaften ein.

h Wiederholen Sie die Schritte, um zusätzliche VMkernel-Adapter zu konfigurieren.

Um zu überprüfen, ob der Adapter konfiguriert ist, klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **VMkernel-Adapter** aus.

Konfigurieren der VMkernel-Bindung für den TCP-Adapter mit einem vSphere Distributed Switch

Sie können die VMkernel-Port-Bindung für den TCP-Adapter mithilfe eines vSphere Distributed Switch und eines Uplinks pro Switch konfigurieren. Zum Konfigurieren der Netzwerkverbindung muss für jeden physischen Netzwerkadapter ein virtueller VMkernel-Adapter erstellt werden. Sie verwenden eine 1:1-Zuordnung zwischen jedem virtuellen und physischen Netzwerkadapter.

Verfahren

1 Erstellen Sie einen vSphere Distributed Switch mit einem VMkernel-Adapter und der Netzwerkkomponente.

   a Wählen Sie im vSphere Client die Option **Datencenter** aus und klicken Sie auf die Registerkarte **Netzwerke**.

   b Klicken Sie auf **Aktionen** und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.

   c Wählen Sie einen Namen für den Switch aus.

   Stellen Sie sicher, dass der Speicherort des Datencenters innerhalb Ihres Hosts vorhanden ist, und klicken Sie auf **Weiter**.

   d Wählen Sie die ESXi-Version **ESXi 7.0 und höher** aus und klicken Sie auf **Weiter**.

   e Geben Sie die erforderliche Anzahl an Uplinks ein und klicken Sie auf **Beenden**.

2 Fügen Sie einen oder mehrere Hosts zu Ihrem Distributed Virtual Switch hinzu.

   a Wählen Sie im vSphere Client die Option **Datencenter** aus und klicken Sie auf **Distributed Switches**.

   Eine Liste der verfügbaren DSwitches wird angezeigt.

   b Klicken Sie mit der rechten Maustaste auf den DSwitch und wählen Sie **Hosts hinzufügen und verwalten** aus.

   c Wählen Sie **Hosts hinzufügen** aus und klicken Sie auf **Weiter**.

   d Wählen Sie den Host aus und klicken Sie auf **Weiter**.

   e Wählen Sie **Uplink zuweisen** aus.

   f Geben Sie den relevanten Uplink ein, um die `vmnic` zuzuweisen.

   g Weisen Sie einen VMkernel-Adapter zu und klicken Sie auf **Weiter**.

   h Wählen Sie im vSphere Client den DSwitch aus und klicken Sie auf die Registerkarte **Ports**.

   Sie können die Uplinks anzeigen, die für Ihren Switch erstellt wurden.

3 Erstellen Sie verteilte Portgruppen für den Speicherpfad „NVMe over TCP“.

a Wählen Sie im vSphere Client den erforderlichen DSwitch aus.

b Klicken Sie auf **Aktionen** und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

c Geben Sie unter **Einstellungen konfigurieren** die allgemeinen Eigenschaften der Portgruppe ein.

Wenn ein spezielles VLAN konfiguriert wurde, fügen Sie es in der VLAN-ID hinzu.

Hinweis Netzwerkkonnektivitätsprobleme können auftreten, wenn das VLAN nicht ordnungsgemäß konfiguriert wurde.

4 Konfigurieren Sie die VMkernel-Adapter.

a Erweitern Sie im vSphere Client die Liste **DSwitch** und wählen Sie die verteilte Portgruppe aus.

b Klicken Sie auf **Aktionen > VMkernel-Adapter hinzufügen**.

c Wählen Sie im Dialogfeld **Mitglieder-Hosts auswählen** Ihren Host aus und klicken Sie auf **OK**.

d Stellen Sie im Dialogfeld **VMkernel-Adapter konfigurieren** sicher, dass die MTU mit der Switch-MTU übereinstimmt.

e Klicken Sie auf **Beenden**.

f Wiederholen Sie Schritt B und Schritt C, um mehrere TCP-fähige Netzwerkkarten hinzuzufügen.

5 Legen Sie NIC-Gruppierungsrichtlinien für die verteilten Portgruppen fest.

Hinweis Der NVMe-/TCP-Adapter unterstützt keine NIC-Gruppierungsfunktionen wie Failover und Lastausgleich. Stattdessen wird für diese Funktionen Storage Multipathing genutzt. Wenn Sie jedoch die NIC-Gruppierung für andere Netzwerkarbeitslasten auf dem Uplink konfigurieren müssen, der den NVMe-/TCP-Adapter bedient, führen Sie die folgenden Schritte aus.

a Klicken Sie unter **Verteilte Portgruppe** auf **Aktionen > Einstellungen bearbeiten**.

b Klicken Sie auf **Teaming und Failover** und überprüfen Sie die aktiven Uplinks.

c Weisen Sie einen Uplink als **Aktiv** für die Portgruppe zu und den anderen Uplink als **Nicht verwendet**.

Wiederholen Sie Schritt C für jede erstellte Portgruppe.

Nächste Schritte

Klicken Sie nach Abschluss der Konfiguration auf **Konfigurieren** und stellen Sie sicher, dass auf der Registerkarte „Physischer Adapter“ Ihres Hosts der DVSwitch für die ausgewählten Netzwerkkarten aufgelistet wird.

Aktivieren von NVMe over RDMA- oder NVMe oder TCP-Softwareadaptern

ESXi unterstützt NVMe over RDMA- und NVMe over TCP-Softwareadapter. Aktivieren Sie die Software-Speicheradapter für NVMe over RDMA und NVMe over TCP mit vSphere Client.

Voraussetzungen

- Installieren Sie auf Ihrem ESXi-Host einen Adapter, der die folgenden Speichertypen unterstützt.
  - NVMe over RDMA-Adapter. Beispiel: Mellanox Technologies MT27700 Family ConnectX-4.
  - NVMe over TCP-Adapter. Beispiel: i40en.
- Konfigurieren Sie die VMkernel-Bindung für Ihre Adapter.
  - Informationen zu NVMe over RDMA finden Sie unter Konfigurieren der VMkernel-Bindung für den RDMA-Adapter.
  - Informationen zu NVMe over TCP finden Sie unter Konfigurieren der VMkernel-Bindung für den NVMe over TCP-Adapter.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und anschließend auf das Symbol **Softwareadapter hinzufügen**.
4. Wählen Sie den Adaptertyp nach Bedarf aus.
   - **NVMe over RDMA-Adapter**
   - **NVMe over TCP-Adapter**
5. Wählen Sie je nach Ihrer Auswahl in Schritt 4 im Dropdown-Menü einen geeigneten RDMA- oder TCP-Netzwerkadapter (`vmnic`) aus.

   Hinweis Wenn Sie eine Fehlermeldung erhalten, die verhindert, dass Sie den Softwareadapter erstellen, stellen Sie sicher, dass die VMkernel-Bindung für den Adapter ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren der VMkernel-Bindung für den RDMA-Adapter und Konfigurieren der VMkernel-Bindung für den NVMe over TCP-Adapter.

Ergebnisse

Die NVMe over RDMA- und NVMe TCP-Softwareadapter werden in der Liste als `vmhba`-Speicheradapter angezeigt. Sie können die Adapter entfernen, wenn Sie den zugrunde liegenden RDMA- und TCP-Netzwerkadapter für andere Zwecke freigeben müssen.

Hinzufügen eines Controllers für NVMe over Fabrics

Verwenden Sie den vSphere Client, um einen NVMe-Controller hinzuzufügen. Nachdem Sie den Controller hinzugefügt haben, werden die dem Controller zugeordneten NVMe-Namespaces für Ihren ESXi-Host verfügbar. Die NVMe-Speichergeräte, die die Namespaces in der ESXi-Umgebung darstellen, werden in der Liste der Speichergeräte angezeigt.

Wenn Sie NVMe over RDMA (ROCE v2)-Speicher verwenden, müssen Sie einen Controller hinzufügen, nachdem Sie einen NVMe over RDMA-Softwareadapter konfiguriert haben. Wenn Sie NVMe over TCP-Speicher verwenden, müssen Sie einen Controller hinzufügen, nachdem Sie einen NVMe over TCP-Softwareadapter konfiguriert haben. Nach der Installation des erforderlichen Adapters stellt der FC-NVMe-Speicher automatisch eine Verbindung zu allen Zielen her, die zu dem Zeitpunkt erreichbar sind. Sie können den Adapter später neu konfigurieren und seine Controller trennen oder andere Controller verbinden, die während des Hoststarts nicht verfügbar waren.

Voraussetzungen

Stellen Sie sicher, dass Ihr ESXi-Host über die entsprechenden Adapter für Ihren Speichertyp verfügt. Weitere Informationen hierzu finden Sie unter Anforderungen und Einschränkungen des VMware NVMe-Speichers.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den zu konfigurierenden Adapter (vmhba#) aus.
4. Klicken Sie auf die Registerkarte **Controller** und dann auf **Controller hinzufügen**.

5 Um den Controller hinzuzufügen, wählen Sie eine der folgenden Optionen aus und klicken Sie auf **Hinzufügen**.

Option	Bezeichnung
Controller automatisch ermitteln	Diese Methode gibt an, dass Ihr Host eine Verbindung zu einem beliebigen verfügbaren Controller akzeptieren kann. a Geben Sie den folgenden Parameter für einen Ermittlungs-Controller an. ■ Für NVMe over RDMA (ROCE v2) geben Sie die IP-Adresse und die Transport-Portnummer an. ■ Für NVMe over TCP werden die IP-Adresse, die Nummer des Transportports und der Digest-Parameter verwendet. b Klicken Sie auf **Controller erkennen**. c Wählen Sie in der Liste der Controller den zu verwendenden Controller aus.
Controller-Details manuell eingeben	Mit dieser Methode fordert Ihr Host eine Verbindung zu einem bestimmten Controller mit den folgenden Parametern an: ■ NQN des Subsystems ■ Angabe des Zielports. Für NVMe over RDMA (RoCE v2) geben Sie die IP-Adresse und die Nummer des Transportports (optional) an. Für FC-NVMe geben Sie den WorldWideNodeName und den WorldWidePortName an. ■ Für NVMe over TCP werden die IP-Adresse, die Nummer des Transportports (optional) und der Digest-Parameter (optional) verwendet. ■ Größe der Verwaltungswarteschlange. Ein optionaler Parameter, der die Größe der Verwaltungswarteschlange des Controllers angibt. Der Standardwert ist 16. ■ Keep Alive-Zeitüberschreitung. Ein optionaler Parameter, der die Keep-Alive-Zeitüberschreitung in Sekunden zwischen dem Adapter und dem Controller angibt. Der Standardwert für die Zeitüberschreitung beträgt 60 Sekunden. ■ Größe und Nummer der E/A-Warteschlange. Optionale Parameter, die nur über esxcli festgelegt werden können.

Ergebnisse

Der Controller ist in der Liste der Controller aufgeführt. Ihr Host kann jetzt die NVMe-Namespaces erkennen, die dem Controller zugeordnet sind. Die NVMe-Speichergeräte, die die Namespaces in der ESXi-Umgebung darstellen, werden in der Liste der Speichergeräte auf dem vSphere Client angezeigt.

Entfernen von NVMe over RDMA- und TCP-Softwareadaptern

Verwenden Sie den vSphere Client, um NVMe over RDMA- und TCP-Softwareadapter zu entfernen. Sie können den Adapter entfernen, wenn Sie den zugrunde liegenden RDMA-Adapter oder Ethernet-Adapter für andere Zwecke freigeben müssen.

Die NVMe over PCIe- und FC-NVMe-Adapter können Sie nicht entfernen.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speicheradapter** und wählen Sie den Adapter (`vmhba#`) aus, der entfernt werden soll.

4 Entfernen Sie den NVMe-Controller, der mit dem Adapter verbunden ist.

   a Klicken Sie auf die Registerkarte **Controller**.

   b Wählen Sie den Controller aus und klicken Sie auf **Entfernen**.

   Der NVMe-Controller wird getrennt und nicht mehr in der Liste angezeigt.

5 Klicken Sie auf das Symbol **Entfernen** („Speicheradapter des Hosts entfernen“), um den NVMe over RDMA- oder NVMe over TCP-Adapter zu entfernen.

Arbeiten mit Datenspeichern 17

Datenspeicher sind besondere logische Container (analog zu Dateisystemen), bei denen Angaben zu physischen Speichern verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Datenspeicher können auch zum Speichern von ISO-Images, Vorlagen virtueller Maschinen und Disketten-Images genutzt werden.

Dieses Kapitel enthält die folgenden Themen:

Datenspeichertypen

Je nach verwendetem Speicher können die Datenspeicher unterschiedliche Typen aufweisen.

vCenter Server und ESXi unterstützen die folgenden Datenspeichertypen.

Tabelle 17-1. Datenspeichertypen

Datenspeichertyp	Beschreibung
VMFS (Version 5 und 6)	Die Datenspeicher, die Sie auf Blockspeichergeräten bereitstellen, verwenden das native VMFS-Format (vSphere Virtual Machine File System). VMFS ist ein spezielles Hochleistungs-Dateisystemformat, das für die Speicherung virtueller Maschinen optimiert ist. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen VMFS-Datenspeicher.
NFS (Version 3 und 4.1)	In ESXi integrierte NFS-Clients verwenden das Network File System-Protokoll (NFS) über TCP/IP, um auf ein ausgewähltes NFS-Volume zuzugreifen. Das Volume befindet sich auf einem NAS-Server. Der ESXi-Host mountet das Volume als NFS-Datenspeicher und verwendet es zur Erfüllung von Speicheranforderungen. ESXi unterstützt die Versionen 3 und 4.1 des NFS-Protokolls. Siehe Informationen zu NFS-Datenspeichern.
vSAN	vSAN fasst alle verfügbaren lokalen Kapazitätsgeräte auf den Hosts zu einem einzelnen, von allen Hosts im vSAN-Cluster gemeinsam genutzten Datenspeicher zusammen. Informationen finden Sie in der Dokumentation *Verwalten von VMware vSAN*.
vVol	Ein Virtual Volumes-Datenspeicher stellt einen Speichercontainer im vCenter Server und im vSphere Client dar. Weitere Informationen hierzu finden Sie unter Kapitel 22 Arbeiten mit VMware vSphere Virtual Volumes.

In Abhängigkeit von Ihrem Speichertyp sind einige der folgenden Aufgaben für die Datenspeicher verfügbar.

- Erstellen von Datenspeichern. Sie können den vSphere Client verwenden, um bestimmte Datenspeichertypen zu erstellen.
- Führen Sie Verwaltungsvorgänge für die Datenspeicher aus. Bestimmte Vorgänge, wie zum Beispiel das Umbenennen eines Datenspeichers, stehen für alle Datenspeichertypen zur Verfügung. Andere beziehen sich auf bestimmte Typen von Datenspeichern.
- Organisieren der Datenspeicher. Sie können beispielsweise eine Gruppierung in Ordnern nach Geschäftsmethoden vornehmen. Nachdem die Datenspeicher gruppiert wurden, können Sie allen Datenspeichern einer Gruppe im gleichen Vorgang dieselben Berechtigungen und Alarme zuzuweisen.
- Hinzufügen der Datenspeicher zu Datenspeicher-Clustern. Ein Datenspeicher-Cluster ist eine Sammlung von Datenspeichern mit gemeinsam genutzten Ressourcen und einer gemeinsamen Verwaltungsoberfläche. Beim Erstellen des Datenspeicher-Clusters können Sie Storage DRS zum Verwalten von Ressourcen verwenden. Weitere Informationen zu Datenspeicher-Clustern finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*

Grundlegende Informationen VMFS-Datenspeicher

Zum Speichern von virtuellen Festplatten verwendet ESXi Datenspeicher. Bei den Datenspeichern handelt es sich um logische Container, bei denen Angaben zum physischen Speicher der virtuellen Maschinen verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Die Datenspeicher, die Sie auf Blockspeichergeräten bereitstellen, verwenden das native VMFS-Format (vSphere Virtual Machine File System). Es handelt sich dabei um ein spezielles Hochleistungs-Dateisystemformat, das für die Speicherung virtueller Maschinen optimiert ist.

Mit dem vSphere Client können Sie den VMFS-Datenspeicher im Voraus auf einem blockbasierten Speichergerät einrichten, das Ihr ESXi-Host erkennt. Der VMFS-Datenspeicher kann über mehrere physische Speichergeräte ausgedehnt werden, die SAN LUNs und lokalen Speicher umfassen. Diese Funktion ermöglicht Ihnen die Zusammenfassung von Speicher und gibt Ihnen bei der Erstellung des für die virtuelle Maschine erforderlichen Datenspeichers die notwendige Flexibilität.

Die Kapazität des Datenspeichers kann während der Ausführung von virtuellen Maschinen im Datenspeicher erhöht werden. Auf diese Weise lässt sich entsprechend den aktuellen Anforderungen der virtuellen Maschine stets neuer Speicherplatz zu VMFS-Volumes hinzufügen. VMFS wurde für den gleichzeitigen Zugriff mehrerer physischer Maschinen konzipiert und erzwingt eine geeignete Zugriffsteuerung für die VM-Dateien.

Versionen von VMFS-Datenspeichern

Seit der Einführung wurden mehrere Versionen des VMFS-Dateisystems veröffentlicht. Zurzeit unterstützt ESXi VMFS5 und VMFS6.

Für alle unterstützen VMFS-Versionen bietet ESXi vollständige Unterstützung von Lese- und Schreibvorgängen. In den unterstützten VMFS-Datenspeichern können Sie virtuelle Maschinen erstellen und einschalten.

Tabelle 17-2. Hostzugriff auf VMFS-Versionen

VMFS	ESXi
VMFS 6	Lesen und schreiben
VMFS5	Lesen und schreiben

In der folgenden Tabelle werden die Hauptmerkmale von VMFS5 und VMFS6 verglichen. Weitere Informationen finden Sie unter *Maximalwerte für die Konfiguration*.

Tabelle 17-3. Vergleich von VMFS5 und VMFS6

Features und Funktionen	VMFS5	VMFS 6
Zugriff für ESXi-Hosts, Version 6.5 und neuere Versionen	Ja	Ja
Zugriff für ESXi-Hosts, Version 6.0 und früher	Ja	Nein
Datenspeicher pro Host	512	512

Tabelle 17-3. Vergleich von VMFS5 und VMFS6 (Fortsetzung)

Features und Funktionen	VMFS5	VMFS 6
512n-Speichergeräte	Ja	Ja (Standard)
512e-Speichergeräte	Ja. Nicht unterstützt auf lokalen 512e-Geräten.	Ja (Standard)
4Kn-Speichergeräte	Nein	Ja
Automatische Speicherplatzrückforderung	Nein	Ja
Manuelle Speicherplatzrückforderung über den esxcli-Befehl. Weitere Informationen hierzu finden Sie unter Manuelles Rückfordern von angesammeltem Speicherplatz.	Ja	Ja
Speicherplatzrückforderung vom Gastbetriebssystem	Eingeschränkt	Ja
Partitionierung des GPT-Speichergeräts	Ja	Ja
Partitionierung des MBR-Speichergeräts	Ja Für einen VMFS5-Datenspeicher, der zuvor von VMFS3 aktualisiert wurde.	Nein
Speichergeräte mit einer Kapazität von mehr als 2 TB für jede VMFS-Erweiterung	Ja	Ja
Unterstützung von virtuellen Maschinen mit virtuellen Festplatten mit hoher Kapazität oder von Festplatten mit mehr als 2 TB	Ja	Ja
Unterstützung von kleinen Dateien mit 1 KB	Ja	Ja
Standardmäßige Verwendung von Nur-ATS-Sperrmechanismen auf Speichergeräten mit ATS-Unterstützung. Weitere Informationen hierzu finden Sie unter VMFS-Sperrmechanismen.	Ja	Ja
Blockgröße	Standard 1 MB	Standard 1 MB
Standard-Snapshots	VMFSsparse für virtuelle Festplatten mit einer Kapazität von weniger als 2 TB. SEsparse für virtuelle Festplatten mit einer Kapazität von mehr als 2 TB.	SEsparse
Emulationstyp für virtuelle Festplatten	512n	512n
vMotion	Ja	Ja
Storage vMotion zwischen verschiedenen Datenspeichertypen	Ja	Ja

Tabelle 17-3. Vergleich von VMFS5 und VMFS6 (Fortsetzung)

Features und Funktionen	VMFS5	VMFS 6
Hochverfügbarkeit und Fault Tolerance	Ja	Ja
DRS und Storage DRS	Ja	Ja
RDM	Ja	Ja

Beachten Sie beim Arbeiten mit VMFS-Datenspeichern folgende Punkte:

- Datenspeichererweiterungen. Ein übergreifender VMFS-Datenspeicher darf nur homogene Speichergeräte nutzen (entweder 512n, 512e oder 4Kn). Der übergreifende Datenspeicher kann nicht über Geräte mit verschiedenen Formaten hinweg erweitert werden.
- Blockgröße. Die Blockgröße in einem VMFS-Datenspeicher bestimmt die maximale Dateigröße und den Speicherplatz, den eine Datei einnimmt. VMFS5- und VMFS6-Datenspeicher unterstützen die Blockgröße 1 MB.
- Storage vMotion. Storage vMotion unterstützt die Migration zwischen VMFS-, vSAN- und Virtual Volumes-Datenspeichern. vCenter Server führt Kompatibilitätsprüfungen durch, um Storage vMotion für verschiedene Arten von Datenspeichern zu validieren.
- Storage DRS: VMFS5 und VMFS6 können parallel im selben Datenspeicher-Cluster vorhanden sein. Jedoch müssen alle Datenspeicher im Cluster homogene Speichergeräte verwenden. Kombinieren Sie keine Geräte mit unterschiedlichen Formaten im selben Datenspeicher-Cluster.
- Gerätepartitionsformate: Jeder neue VMFS5- oder VMFS6-Datenspeicher nutzt die GUID-Partitionstabelle (GPT) zur Formatierung des Speichergeräts. Das GPT-Format ermöglicht Ihnen das Erstellen von Datenspeichern mit einer Kapazität von mehr als 2 TB. Falls Ihr VMFS5-Datenspeicher zuvor von VMFS3 aktualisiert wurde, verwendet er weiterhin das MBR-Partitionsformat (Master-Boot-Datensatz, Master Boot Record), das charakteristisch für VMFS3 ist. Die Konvertierung in GPT erfolgt erst, nachdem Sie den Datenspeicher auf über 2 TB erweitert haben.

VMFS-Datenspeicher als Repositorys

ESXi kann SCSI-basierte Speichergeräte wie VMFS-Datenspeicher formatieren. VMFS-Datenspeicher dienen hauptsächlich als Ablagen für virtuelle Maschinen.

Hinweis Ordnen Sie jeder LUN stets nur einen VMFS-Datenspeicher zu.

Sie können mehrere virtuelle Maschinen auf demselben VMFS-Datenspeicher speichern. Jede virtuelle Maschine ist in einem Satz Dateien gekapselt und belegt ein eigenes Verzeichnis. Für das Betriebssystem innerhalb der virtuellen Maschine behält VMFS die interne Dateisystemsemantik bei. Dadurch wird das ordnungsgemäße Verhalten von Anwendungen und die Datensicherheit für Anwendungen gewährleistet, die in virtuelle Maschinen ausgeführt werden.

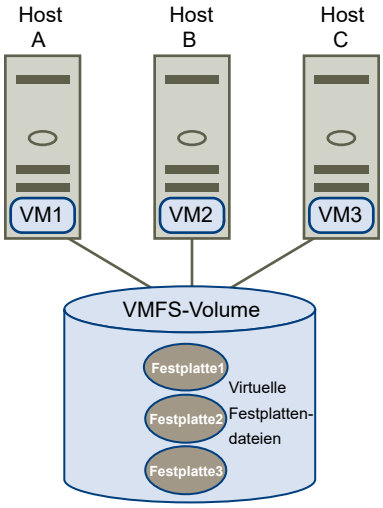
Wenn mehrere virtuelle Maschinen ausgeführt werden, stellt VMFS spezifische Sperrmechanismen für die Dateien virtueller Maschinen zur Verfügung. Infolgedessen können die virtuellen Maschinen sicher in einer SAN-Umgebung betrieben werden, in der mehrere ESXi-Hosts denselben VMFS-Datenspeicher nutzen.

Neben den virtuellen Maschinen können in VMFS-Datenspeichern auch andere Dateien, beispielsweise Vorlagen für virtuelle Maschinen und ISO-Images gespeichert werden.

Gemeinsames Nutzen eines VMFS-Datenspeichers durch mehrere Hosts

Als Clusterdateisystem ermöglicht VMFS mehreren ESXi-Hosts, parallel auf denselben VMFS-Datenspeicher zuzugreifen.

Abbildung 17-1. Gemeinsames Nutzen eines VMFS-Datenspeichers durch mehrere Hosts



Informationen zur maximal zulässigen Anzahl von Hosts, die eine Verbindung mit einem einzelnen VMFS-Datenspeicher herstellen können, finden Sie im Dokument *Maximalwerte für die Konfiguration*.

Um sicherzustellen, dass nicht mehrere Hosts gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine festplatteninterne Sperrung.

Die gemeinsame Nutzung des VMFS-Volumes durch mehrere Hosts bietet beispielsweise folgende Vorteile:

- Sie können vSphere Distributed Resource Scheduling (DRS) und VMware High Availability (HA) verwenden.

  Sie können virtuelle Maschinen auf mehrere physische Server verteilen. Sie können also auf jedem Server eine Kombination virtueller Maschinen ausführen, sodass nicht alle zur selben Zeit im selben Bereich einer hohen Nachfrage unterliegen. Falls ein Server ausfällt, können Sie die virtuellen Maschinen auf einem anderen physischen Server neu starten. Bei einem Störfall

wird die festplatteninterne Sperre für die einzelnen virtuellen Maschinen aufgehoben. Weitere Informationen zu VMware DRS finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*. Informationen zu VMware HA finden Sie in der Dokumentation *Handbuch zur Verfügbarkeit in vSphere*.

- Mit vMotion können Sie virtuelle Maschinen bei laufendem Betrieb von einem physischen Server auf einen anderen migrieren. Informationen zur Migration von virtuellen Maschinen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Um einen freigegebenen Datenspeicher zu erstellen, mounten Sie den Datenspeicher auf den ESXi-Hosts, die Zugriff auf den Datenspeicher benötigen. Weitere Informationen hierzu finden Sie unter Mounten von Datenspeichern.

Updates von VMFS-Metadaten

Ein VMFS-Datenspeicher enthält u. a. Dateien virtueller Maschinen, Verzeichnisse, symbolische Links und RDM-Deskriptordateien. Der Datenspeicher stellt außerdem eine einheitliche Ansicht aller Zuordnungsdaten für diese Objekte zur Verfügung. Diese Zuordnungsdaten werden als Metadaten bezeichnet.

Metadaten werden immer dann aktualisiert, wenn Sie Verwaltungsvorgänge für Datenspeicher oder virtuelle Maschinen durchführen. Bei folgenden Vorgängen sind u. a. Aktualisierungen von Metadaten erforderlich:

- Erstellen, Vergrößern oder Sperren einer Datei einer virtuellen Maschine
- Ändern der Attribute einer Datei
- Ein- oder Ausschalten einer virtuellen Maschine
- Erstellen oder Löschen eines VMFS-Datenspeichers
- Erweitern eines VMFS-Datenspeichers
- Erstellen einer Vorlage
- Bereitstellen einer virtuellen Maschine anhand einer Vorlage
- Migrieren einer virtuellen Maschine mit vMotion

Wenn in einer Umgebung mit gemeinsam genutztem Speicher Änderungen an Metadaten vorgenommen werden, verwendet VMFS einen speziellen Sperrmechanismus, um seine Daten zu schützen und zu verhindern, dass mehrere Hosts gleichzeitig in die Metadaten schreiben.

VMFS-Sperrmechanismen

In Umgebungen mit gemeinsam genutztem Speicher, bei denen mehrere Hosts auf denselben VMFS-Datenspeicher zugreifen, werden bestimmte Sperrmechanismen eingesetzt. Diese Sperrmechanismen verhindern den gleichzeitigen Schreibzugriff mehrerer Hosts auf die Metadaten und stellen sicher, dass keine Daten beschädigt werden.

Je nach seiner Konfiguration und dem Typ des zugrunde liegenden Speichers kann ein VMFS-Datenspeicher verschiedene Arten von Sperrmechanismen nutzen. Er kann den Atomic Test and Set-Sperrmechanismus exklusiv (Nur ATS) oder eine Kombination von ATS und SCSI-Reservierungen (ATS+SCSI) verwenden.

Mechanismus „Nur ATS“

Bei Speichergeräten, die die auf dem T10-Standard basierten VAAI-Spezifikationen unterstützen, bietet VMFS ATS-Sperrung, auch als hardwaregestütztes Sperren bezeichnet. Der ATS-Algorithmus unterstützt ein differenziertes Sperren von Festplatten auf Sektorbasis. Alle neu formatierten VMFS5- und VMFS6-Datenspeicher verwenden den Mechanismus „Nur ATS“, wenn er vom zugrunde liegenden Speicher unterstützt wird, und verwenden nie SCSI-Reservierungen.

Wenn Sie einen Datenspeicher mit mehreren Erweiterungen erstellen, in dem ATS verwendet wird, filtert vCenter Server Nicht-ATS-Geräte heraus. Dieses Filtern ermöglicht Ihnen, nur solche Geräte zu verwenden, die das ATS-Primitiv unterstützen.

In bestimmten Fällen müssen Sie möglicherweise für VMFS5- oder VMFS6-Datenspeicher den Standardsperrmechanismus deaktivieren. Weitere Informationen hierzu finden Sie unter Ändern des Sperrmechanismus zu ATS+SCSI.

Hinweis Wenn Sie eine VMware vSAN-Umgebung ausführen oder über „Nur ATS“-VMFS-Volumes verfügen, deaktivieren Sie ATS nicht. Die Deaktivierung von ATS kann zu einem Ausfall führen, da kein Sperrmechanismus verfügbar ist. Weitere Informationen finden Sie in einem VMware-Knowledgebase-Artikel.

Mechanismus „ATS+SCSI“

Ein VMFS-Datenspeicher, der den Mechanismus „ATS+SCSI“ unterstützt, ist für die Verwendung von ATS konfiguriert und versucht, es zu verwenden, sofern möglich. Wenn ATS fehlschlägt, kehrt der VMFS-Datenspeicher zu SCSI-Reservierungen zurück. Im Gegensatz zur ATS-Sperrung wird bei der SCSI-Reservierung ein Speichergerät vollständig gesperrt, während ein Vorgang durchgeführt wird, der den Schutz von Metadaten erfordert. Nach dem Abschluss des Vorgangs hebt VMFS die Reservierung auf, und andere Vorgänge können fortgesetzt werden.

Zu den Datenspeichern, die den Mechanismus „ATS+SCSI“ verwenden, gehören VMFS5-Datenspeicher, die von VMFS3 aktualisiert wurden. Außerdem verwenden neue VMFS5- oder VMFS6-Datenspeicher auf Speichergeräten, die ATS nicht unterstützen, den Mechanismus „ATS+SCSI“.

Wenn der VMFS-Datenspeicher zu SCSI-Reservierungen zurückkehrt, bemerken Sie möglicherweise einen Leistungsabfall, der durch übermäßige SCSI-Reservierungen verursacht wird.

Anzeigen von Informationen zu VMFS-Sperren

Verwenden Sie den `esxcli`-Befehl zum Abrufen von Informationen zu dem Sperrmechanismus, den ein VMFS-Datenspeicher verwendet.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Zum Anzeigen von Informationen in Bezug auf VMFS-Sperrmechanismen führen Sie den folgenden Befehl aus:

  `esxcli storage vmfs lockmode list`

Ergebnisse

Die Tabelle enthält Elemente, die bei der Ausgabe des Befehls enthalten sein können.

Tabelle 17-4. Informationen zu VMFS-Sperren

Felder	Werte	Beschreibungen
Sperrmodi		Zeigt die Sperrkonfiguration des Datenspeichers an.
	`ATS`	Der Datenspeicher ist für die Verwendung des Sperrmodus „Nur ATS“ konfiguriert.
	`ATS+SCSI`	Der Datenspeicher ist für die Verwendung des ATS-Modus konfiguriert. Wenn ATS ausfällt oder nicht unterstützt wird, kann der Datenspeicher auf SCSI zurückgreifen.
	`ATS upgrade pending`	Beim Datenspeicher wird gerade ein Online-Upgrade auf den Modus „Nur ATS“ ausgeführt.
	`ATS downgrade pending`	Beim Datenspeicher wird gerade ein Online-Downgrade auf den Modus „ATS+SCSI“ ausgeführt.
ATS-kompatibel		Zeigt an, ob der Datenspeicher für den Modus „Nur ATS“ konfiguriert werden kann.
ATS-Upgrade-Modi		Zeigt die Art des Upgrades an, das der Datenspeicher unterstützt.
	`None`	Der Datenspeicher ist nicht zu „Nur ATS“ kompatibel.
	`Online`	Der Datenspeicher kann während des Upgrades auf den Modus „Nur ATS“ verwendet werden.

Tabelle 17-4. Informationen zu VMFS-Sperren (Fortsetzung)

Felder	Werte	Beschreibungen
	`Offline`	Der Datenspeicher kann während des Upgrades auf den Modus „Nur ATS“ nicht verwendet werden.
Grund für ATS-Inkompatibilität		Wenn der Datenspeicher nicht mit „Nur ATS“ kompatibel ist, gibt dieses Element den Grund für die Inkompatibilität an.

Ändern von VMFS-Sperren in „Nur ATS“

Wenn Ihr VMFS-Datenspeicher mit dem Sperrmechanismus ATS+SCSI arbeitet, können Sie den Sperrmechanismus auf „Nur ATS“ setzen.

VMFS5-Datenspeicher, die zuvor von VMFS3 aktualisiert wurden, verwenden üblicherweise weiterhin den Sperrmechanismus ATS+SCSI. Wenn diese Datenspeicher auf ATS-aktivierter Hardware bereitgestellt werden, ist ein Upgrade auf die Nur-ATS-Sperrung möglich. Abhängig von Ihrer vSphere-Umgebung können Sie einen der folgenden Upgrademodi verwenden:

- Das Online-Upgrade auf den Mechanismus Nur-ATS ist für die meisten VMFS5-Datenspeicher mit nur einer Erweiterung verfügbar. Während des Online-Upgrades eines Ihrer Hosts können andere Hosts den Datenspeicher weiter verwenden.
- Bei VMFS5-Datenspeichern mit mehreren physischen Erweiterungen muss ein Offline-Upgrade auf Nur-ATS durchgeführt werden. Für Datenspeicher mit mehreren physischen Erweiterungen ist das Online-Upgrade nicht verfügbar. Der Grund ist, dass bei diesen Datenspeichern während des Upgrades keine Hosts mit ihnen verbunden sein dürfen.

Verfahren

1 Vorbereiten eines Upgrades auf „Nur ATS“-Sperre

   Sie müssen mehrere Schritte durchführen, um Ihre Umgebung auf ein Online- oder Offline-Upgrade auf „Nur ATS“-Sperre vorzubereiten.

2 Upgrade des Sperrmechanismus auf den Typ „Nur ATS“

   Bei Nur-ATS-kompatiblen VMFS-Datenspeichern können Sie den Sperrmechanismus von ATS+SCSI auf Nur ATS aktualisieren.

Vorbereiten eines Upgrades auf „Nur ATS“-Sperre

Sie müssen mehrere Schritte durchführen, um Ihre Umgebung auf ein Online- oder Offline-Upgrade auf „Nur ATS“-Sperre vorzubereiten.

Verfahren

1 Führen Sie ein Upgrade für alle Hosts, die auf den VMFS5-Datenspeicher zugreifen, auf die neueste vSphere-Version durch.

2 Bestimmen Sie, ob der Datenspeicher sich für ein Upgrade seines aktuellen Sperrmechanismus eignet, indem Sie den Befehl `esxcli storage vmfs lockmode list` ausführen.

Die Ausgabe des folgenden Beispiels zeigt an, dass der Datenspeicher für ein Upgrade geeignet ist. Gezeigt werden auch der aktuelle Sperrmechanismus und der verfügbare Upgrade-Modus für den Datenspeicher.

```
Locking Mode  ATS Compatible  ATS Upgrade Modes
------------  --------------  -----------------
ATS+SCSI           true       Online or Offline
```

3 Je nach dem für den Datenspeicher verfügbaren Upgrade-Modus führen Sie eine der folgenden Aktionen durch:

Upgrade-Modus	Aktion
Online	Überprüfen Sie, dass alle Hosts konsistente Speicherverbindung zum VMFS-Datenspeicher aufweisen.
Offline	Überprüfen Sie, dass keine Hosts den Datenspeicher aktiv nutzen.

Upgrade des Sperrmechanismus auf den Typ „Nur ATS“

Bei Nur-ATS-kompatiblen VMFS-Datenspeichern können Sie den Sperrmechanismus von ATS+SCSI auf Nur ATS aktualisieren.

Bei den meisten Datenspeichern, die sich nicht über mehrere Erweiterungen erstrecken, sind Online-Upgrades möglich. Während des Online-Upgrades eines Ihrer ESXi-Hosts können andere Hosts den Datenspeicher weiter verwenden. Der Online-Upgrade wird erst dann abgeschlossen, wenn alle Hosts den Datenspeicher geschlossen haben.

Voraussetzungen

Wenn Sie das Upgrade des Sperrmechanismus abschließen möchten, indem Sie den Datenspeicher in den Wartungsmodus versetzen, deaktivieren Sie Storage DRS. Dies bezieht sich nur auf Online-Upgrades.

Verfahren

1 Führen Sie das Upgrade des Sperrmechanismus mit dem folgenden Befehl durch:

`esxcli storage vmfs lockmode set -a|--ats -l|--volume-label=` *VMFS-Bezeichnung* `-u|--volume-uuid=` *VMFS-UUID*.

2 Beim Online-Upgrade sind weitere Schritte notwendig.

   a Schließen Sie den Datenspeicher auf allen Hosts, die Zugriff darauf haben, sodass der Host die Änderung erkennen kann.

   Dazu können Sie eine der folgenden Methoden verwenden:

   - Unmounten Sie den Datenspeicher und mounten Sie ihn erneut.
   - Versetzen Sie den Datenspeicher in den Wartungsmodus und verlassen Sie den Wartungsmodus.

   b Prüfen Sie, dass der Sperrungsstatus des Datenspeichers zu „Nur ATS“ geändert wurde, indem Sie folgenden Befehl ausführen:

   ```
   esxcli storage vmfs lockmode list
   ```

   c Wenn der Sperrungsmodus irgendein einen anderen Status aufweist, etwa ATS UPGRADE PENDING, sehen Sie nach, welcher Host das Upgrade noch nicht durchgeführt hat. Verwenden Sie dazu folgenden Befehl:

   ```
   esxcli storage vmfs host list
   ```

Ändern des Sperrmechanismus zu ATS+SCSI

Wenn Sie einen VMFS5-Datenspeicher auf einem Gerät erstellen, das die ATS (Atomic Test and Set)-Sperrung unterstützt, verwendet der Datenspeicher den „Nur ATS“-Sperrmechanismus. Unter bestimmten Umständen müssen Sie möglicherweise ein Downgrade vom Sperrmodus „Nur ATS“ auf „ATS+SCSI“ ausführen.

Möglicherweise müssen Sie zum Sperrmechanismus „ATS+SCSI“ wechseln, wenn beispielsweise ein Downgrade auf Ihrem Speichergerät durchgeführt wird. Oder wenn Firmware-Updates fehlschlagen und das Gerät ATS nicht mehr unterstützt.

Der Downgrade-Vorgang verläuft ähnlich wie das Upgrade auf „Nur ATS“. Wie beim Upgrade können Sie je nach Ihrer Speicherkonfiguration das Downgrade im Online- oder Offline-Modus durchführen.

Hinweis Wenn Sie eine VMware vSAN-Umgebung ausführen oder über „Nur ATS“-VMFS-Volumes verfügen, deaktivieren Sie ATS nicht. Die Deaktivierung von ATS kann zu einem Ausfall führen, da kein Sperrmechanismus verfügbar ist. Weitere Informationen finden Sie in einem VMware-Knowledgebase-Artikel.

Verfahren

1 Ändern Sie den Sperrmechanismus auf „ATS+SCSI“ durch Ausführen des folgenden Befehls:

   `esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label=` *VMFS-Bezeichnung* `-u|--volume-uuid=` *VMFS-UUID*.

2 Schließen Sie beim Online-Modus den Datenspeicher auf allen Hosts, die auf den Datenspeicher zugreifen können, damit die Hosts die Änderung erkennen können.

Snapshot-Formate in VMFS

Beim Erstellen eines Snapshots wird der Status der virtuellen Festplatte beibehalten, wodurch sie vom Gastbetriebssystem nicht mehr beschrieben werden kann. Eine Delta- oder untergeordnete Festplatte wird erstellt. Das Delta stellt den Unterschied zwischen dem aktuellen Status der VM-Festplatte und dem Status zum Zeitpunkt der Aufnahme des vorherigen Snapshots dar. Im VMFS-Datenspeicher ist die Delta-Festplatte eine Festplatte mit geringer Datendichte.

Festplatten mit geringer Datendichte verwenden den COW-Mechanismus (Copy-on-Write), bei dem die virtuelle Festplatte so lange keine Daten enthält, bis diese durch einen Schreibvorgang auf die Festplatte kopiert werden. Diese Optimierung spart Speicherplatz.

Je nach Typ des Datenspeichers nutzen Delta-Festplatten unterschiedliche Formate mit geringer Datendichte.

Snapshot-Formate	VMFS5	VMFS 6
VMFSsparse	Für virtuelle Festplatten mit einer Kapazität von weniger als 2 TB.	n.v.
SEsparse	Für virtuelle Festplatten mit einer Kapazität von mehr als 2 TB.	Für alle Festplatten.

VMFSsparse

VMFS5 verwendet das VMFSsparse-Format für virtuelle Festplatten mit einer Kapazität von weniger als 2 TB.

VMFSsparse wird auf VMFS implementiert. Die VMFSsparse-Schicht verarbeitet die E/A-Vorgänge eines VM-Snapshots. Eigentlich ist VMFSsparse ein Wiederholen-Protokoll, das unmittelbar nach der Erfassung eines VM-Snapshots leer beginnt. Das Wiederholen-Protokoll wächst bis auf die Größe seiner vmdk-Basisdatei an, wenn die gesamte vmdk-Datei nach der Erstellung des VM-Snapshots mit neuen Daten neu erstellt wird. Dieses Wiederholen-Protokoll ist eine Datei im VMFS-Datenspeicher. Beim Erstellen des Snapshots wird die an die VM angefügte vmdk-Basisdatei in die neu erstellte vmdk-Datei mit geringer Datendichte geändert.

SEsparse

SEsparse ist ein Standardformat für alle Delta-Festplatten in den VMFS6-Datenspeichern. In VMFS5 wird SEsparse für virtuelle Festplatten mit einer Kapazität von 2 TB und mehr verwendet.

SEsparse ist ein VMFSsparse ähnliches Format mit einigen Verbesserungen. Das Format ist speichereffizient und unterstützt die Speicherplatzrückforderungstechnik. Bei der Speicherplatzrückforderung werden die vom Gastbetriebssystem gelöschten Blöcke markiert. Das System sendet Befehle an die SEsparse-Schicht im Hypervisor, um die Zuordnung dieser Blöcke aufzuheben. Dieses Aufheben der Zuordnung ist hilfreich bei der Rückforderung von Speicherplatz, der von SEsparse zugeteilt wurde, sobald diese Daten vom Gastbetriebssystem gelöscht wurden. Weitere Informationen zur Speicherplatzrückforderung finden Sie unter Speicherplatzrückforderung.

Snapshot-Migration

VMs mit Snapshots können zwischen verschiedenen Datenspeichern migriert werden. Folgendes ist zu beachten:

- Wenn Sie eine VM mit dem VMFSsparse-Snapshot zu VMFS6 migrieren, wird das Snapshot-Format in SEsparse geändert.
- Wird eine VM mit einer vmdk-Datei mit weniger als 2 TB zu VMFS5 migriert, wird das Snapshot-Format in VMFSsparse geändert.
- VMFSsparse-Wiederholen-Protokolle können nicht mit SEsparse-Wiederholen-Protokollen in derselben Hierarchie kombiniert werden.

Upgrade von VMFS-Datenspeichern

ESXi verwendet verschiedene Ansätze für VMFS5- und VMFS3-Upgrades.

VMFS5-Datenspeicher

Ein Upgrade eines VMFS5-Datenspeichers auf VMFS6 ist nicht möglich. Wenn Sie über einen VMFS5-Datenspeicher in Ihrer Umgebung verfügen, erstellen Sie einen VMFS6-Datenspeicher und migrieren Sie virtuelle Maschinen vom VMFS5-Datenspeicher auf VMFS6.

VMFS3-Datenspeicher

VMFS3-Datenspeicher werden von ESXi nicht mehr unterstützt. Beim Mounten der vorhandenen Datenspeicher führt der ESXi-Host automatisch ein Upgrade von VMFS3 auf VMFS5 durch. Der Host führt das Upgrade in folgenden Fällen durch:

- Beim ersten Start nach dem Upgrade auf ESXi 7.0 oder höher, wenn der Host alle erkannten VMFS3-Datenspeicher mountet.
- Wenn Sie die nach dem Start erkannten VMFS3-Datenspeicher manuell mounten oder dauerhaft nicht gemountete Datenspeicher mounten.

Informationen zu NFS-Datenspeichern

In ESXi integrierte NFS-Clients verwenden das Network File System-Protokoll (NFS) über TCP/IP, um auf ein ausgewähltes NFS-Volume auf einem NAS-Server zuzugreifen. Der ESXi-Host kann das Volume mounten und für seine Speicherzwecke nutzen. vSphere unterstützt die Versionen 3 und 4.1 des NFS-Protokolls.

Das NFS-Volume bzw. NFS-Verzeichnis wird von einem Speicheradministrator erstellt und vom NFS-Server exportiert. Das NFS-Volume muss nicht mit einem lokalen Dateisystem wie VMFS formatiert werden. Stattdessen mounten Sie das Volume direkt auf den ESXi-Hosts und verwenden es auf die gleiche Weise zum Speichern und Starten der virtuellen Maschinen wie die VMFS-Datenspeicher.

Neben der Speicherung von virtuellen Festplatten in NFS-Datenspeichern können Sie NFS als zentrales Repository für ISO-Images, VM-Vorlagen usw. nutzen. Wenn Sie den Datenspeicher für die ISO-Images verwenden möchten, können Sie das CD-ROM-Laufwerk der virtuellen Maschine mit einer ISO-Datei auf dem Datenspeicher verbinden. Anschließend können Sie ein Gastbetriebssystem von der ISO-Datei installieren.

NFS-Protokolle und ESXi

ESXi unterstützt NFS-Protokolle der Versionen 3 und 4.1. Zur Unterstützung beider Versionen verwendet ESXi zwei verschiedene NFS-Clients.

Vergleich der Versionen der NFS-Clients

In der folgenden Tabelle sind die Funktionen aufgeführt, die von den NFS-Versionen 3 und 4.1 unterstützt werden.

Merkmale	NFS Version 3	NFS-Version 4.1
Sicherheitsmechanismen	AUTH_SYS	AUTH_SYS und Kerberos (krb5 und krb5i)
Verschlüsselungsalgorithmen mit Kerberos	Nicht verfügbar	AES256-CTS-HMAC-SHA1-96 und AES128-CTS-HMAC-SHA1-96
Multipathing	Nicht unterstützt	Unterstützt durch Session Trunking
Sperrmechanismen	Proprietäre clientseitige Sperren	Serverseitige Sperren
Hardwarebeschleunigung	Unterstützt	Unterstützt
Virtuelle Festplatten im Thick-Format	Unterstützt	Unterstützt
IPv6	Unterstützt	Unterstützt für AUTH_SYS und Kerberos
ISO-Images, die virtuellen Maschinen als CD-ROMs angezeigt werden	Unterstützt	Unterstützt
Snapshots einer virtuellen Maschine	Unterstützt	Unterstützt
Virtuelle Maschinen mit virtuellen Festplatten mit mehr als 2 TB	Unterstützt	Unterstützt

NFS-Protokolle und vSphere-Lösungen

In der folgenden Tabelle sind die vSphere-Hauptlösungen aufgeführt, die von NFS-Versionen unterstützt werden.

vSphere-Funktionen	NFS Version 3	NFS-Version 4.1
vMotion und Storage vMotion	Ja	Ja
High Availability (HA)	Ja	Ja
Fault Tolerance (FT)	Ja	Ja

vSphere-Funktionen	NFS Version 3	NFS-Version 4.1
Distributed Resource Scheduler (DRS)	Ja	Ja
Hostprofile	Ja	Ja
Storage DRS	Ja	Nein
Storage I/O Control	Ja	Nein
Site Recovery Manager	Ja	Site Recovery Manager unterstützt keine NFS 4.1-Datenspeicher für die Array-basierte Replizierung und die Virtual Volumes-Replizierung. Sie können Site Recovery Manager NFS v 4.1-Datenspeichern für die vSphere-Replizierung verwenden.
Virtual Volumes	Ja	Ja
vSphere Replication	Ja	Ja
vRealize Operations Manager	Ja	Ja

NFS 4.1 und Fault Tolerance

Virtuelle Maschinen auf NFS 4.1 unterstützen den neuen Fault Tolerance-Mechanismus, der in vSphere 6.0 eingeführt wurde. Der Mechanismus kann symmetrische Multiprozessor-V Maschinen (SMP) mit bis zu vier vCPUs aufnehmen.

NFS 4.1-VMs unterstützen den Fault Tolerance-Legacy-Mechanismus nicht.

NFS-Upgrades

Wenn Sie ein Upgrade von einer früheren ESXi-Version als 6.5 durchführen, beginnen bestehende NFS 4.1-Datenspeicher automatisch mit der Unterstützung der Funktionen, die in der vorherigen ESXi-Version nicht verfügbar waren. Zu diesen Funktionen zählen u. a. Virtual Volumes und Hardwarebeschleunigung.

ESXi bietet keine Unterstützung für automatische Datenspeicherkonvertierungen von NFS 3 zu NFS 4.1.

Wenn Sie Ihren Datenspeicher aus NFS 3 aktualisieren möchten, haben Sie folgende Möglichkeiten:

- Erstellen Sie den NFS 4.1-Datenspeicher und führen Sie anschließend mithilfe von Storage vMotion die Migration der virtuellen Maschinen vom alten zum neuen Datenspeicher durch.
- Verwenden Sie die von Ihrem NFS-Speicheranbieter vorgesehenen Konvertierungsmethoden. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

- Unmounten Sie den NFS 3-Datenspeicher und mounten Sie ihn dann als NFS 4.1-Datenspeicher.

  Vorsicht Wenn Sie so vorgehen, achten Sie darauf, dass Sie den Datenspeicher von allen Hosts unmounten, die Zugriff auf den Datenspeicher haben. Ein Datenspeicher kann niemals mit zwei Protokollen gleichzeitig gemountet werden.

Richtlinien und Anforderungen für NFS-Speicher

Bei Verwendung des NFS-Speichers müssen Sie spezifische Richtlinien zur NFS-Serverkonfiguration, zum Netzwerk, zu NFS-Datenspeichern usw. befolgen.

- NFS-Serverkonfiguration

  Befolgen Sie beim Konfigurieren des NFS-Servers für die Nutzung von ESXi die Empfehlungen des Speicheranbieters. Beachten Sie neben diesen allgemeinen Empfehlungen die speziellen Richtlinien, die sich auf NFS in einer vSphere-Umgebung beziehen.

- NFS-Netzwerk

  Ein ESXi-Host verwendet eine TCP/IP-Netzwerkverbindung für den Zugriff auf einen Remote-NAS-Server. Für die Konfiguration des Netzwerks bei Verwendung eines NFS-Speichers sind bestimmte Richtlinien und Best Practices zu beachten.

- NFS-Dateisperrung

  Mithilfe von Dateisperrmechanismen wird der Zugriff auf Daten, die auf einem Server gespeichert sind, auf nur jeweils einen einzigen Benutzer oder Prozess zur gleichen Zeit beschränkt. Die Sperrmechanismen der beiden NFS-Versionen sind nicht kompatibel. NFS 3 verwendet proprietäre Sperren und NFS 4.1 verwendet über natives Protokoll angegebene Sperren.

- NFS-Sicherheit

  Bei Verwendung von NFS 3 und NFS 4.1 unterstützt ESXi die AUTH_SYS-Sicherheit. Darüber hinaus wird für NFS 4.1 der Kerberos-Sicherheitsmechanismus unterstützt.

- NFS-Multipathing

  NFS 4.1 unterstützt Multipathing gemäß Protokollspezifikationen. Für NFS 3 ist Multipathing nicht anwendbar.

- NFS und Hardwarebeschleunigung

  In NFS-Datenspeichern erstellte virtuelle Festplatten sind standardmäßig per Thin Provisioning bereitgestellt. Um per Thick Provisioning bereitgestellte virtuelle Festplatten zu erstellen, müssen Sie die Hardwarebeschleunigung verwenden, die den Vorgang „Speicherplatz reservieren“ unterstützt.

- NFS-Datenspeicher

  Beim Erstellen eines NFS-Datenspeichers müssen bestimmte Richtlinien befolgt werden.

NFS-Serverkonfiguration

Befolgen Sie beim Konfigurieren des NFS-Servers für die Nutzung von ESXi die Empfehlungen des Speicheranbieters. Beachten Sie neben diesen allgemeinen Empfehlungen die speziellen Richtlinien, die sich auf NFS in einer vSphere-Umgebung beziehen.

Es sollten u. a. folgende Richtlinien beachtet werden.

- Vergewissern Sie sich, dass die verwendeten NAS-Server in der *VMware HCL* aufgelistet sind. Achten Sie auf die korrekte Version der Server-Firmware.
- Exportieren Sie das NFS-Volume mithilfe von NFS über TCP.
- Vergewissern Sie sich, dass eine Freigabe vom NAS-Server entweder als NFS 3 oder als NFS 4.1 exportiert wird. Der NAS-Server darf nicht beide Protokollversionen für dieselbe Freigabe bereitstellen. Diese Richtlinie muss vom NAS-Server durchgesetzt werden, da ESXi das Mounten derselben Freigabe über unterschiedliche NFS-Versionen nicht verhindert.
- NFS 3 und NFS 4.1 ohne Kerberos (AUTH_SYS) bieten keine Unterstützung für delegierte Benutzer, über die der Zugriff auf NFS-Volumes mit Nicht-Root-Anmeldedaten möglich wäre. Wenn Sie NFS 3 oder NFS 4.1 ohne Kerberos verwenden, stellen Sie sicher, dass alle Hosts Rootzugriff auf das Volume besitzen. Diese Funktion wird bei verschiedenen Speicheranbietern unterschiedlich aktiviert. NAS-Server verwenden üblicherweise die Option `no_root_squash`. Wenn der NAS-Server keinen Rootzugriff zulässt, können Sie den NFS-Datenspeicher weiterhin auf dem Host mounten. Sie können jedoch keine virtuellen Maschinen im Datenspeicher erstellen.
- Falls das zugrunde liegende NFS-Volume schreibgeschützt ist, müssen Sie sicherstellen, dass es vom NFS-Server als schreibgeschützte Freigabe exportiert wird. Sie können das Volume jedoch auch als schreibgeschützten Datenspeicher auf dem ESXi-Host mounten. Anderenfalls betrachtet der Host den Datenspeicher als beschreibbar und öffnet die Dateien möglicherweise nicht.

NFS-Netzwerk

Ein ESXi-Host verwendet eine TCP/IP-Netzwerkverbindung für den Zugriff auf einen Remote-NAS-Server. Für die Konfiguration des Netzwerks bei Verwendung eines NFS-Speichers sind bestimmte Richtlinien und Best Practices zu beachten.

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

- Verwenden Sie für die Netzwerkverbindung einen standardmäßigen Netzwerkadapter in Ihrem ESXi-Host.
- ESXi unterstützt Layer-2- und Layer-3-Netzwerk-Switches. Bei Layer-3-Switches müssen sich ESXi-Hosts und NFS-Speicherarrays in unterschiedlichen Subnetzen befinden und die Routing-Informationen müssen vom Netzwerk-Switch verarbeitet werden.

- Konfigurieren Sie für den NFS-Speicher eine VMkernel-Portgruppe. Die VMkernel-Portgruppe für IP-Speicher kann auf einem bereits vorhandenen virtuellen Switch (vSwitch) oder einem neuen vSwitch erstellt werden. Beim vSwitch kann es sich um einen vSphere Standard Switch (VSS) oder einen vSphere Distributed Switch (VDS) handeln.
- Bei Verwendung mehrerer Ports für den NFS-Datenverkehr müssen Sie sicherstellen, dass alle virtuellen und physischen Switches korrekt konfiguriert sind.
- NFS 3 und NFS 4.1 unterstützen IPv6.

NFS-Dateisperrung

Mithilfe von Dateisperrmechanismen wird der Zugriff auf Daten, die auf einem Server gespeichert sind, auf nur jeweils einen einzigen Benutzer oder Prozess zur gleichen Zeit beschränkt.
Die Sperrmechanismen der beiden NFS-Versionen sind nicht kompatibel. NFS 3 verwendet proprietäre Sperren und NFS 4.1 verwendet über natives Protokoll angegebene Sperren.

Die NFS-3-Sperrung in ESXi verwendet nicht das Protokoll Network Lock Manager (NLM). Stattdessen liefert VMware ein eigenes Sperrprotokoll. NFS-3-Sperrungen werden durch Sperrdateien auf dem NFS-Server erzielt. Diese tragen den Namen `.lck-`*`file_id`*`..`

NFS 4.1 verwendet Freigabereservierungen als Sperrmechanismus.

Da NFS 3- und NFS 4.1-Clients nicht das gleiche Sperrprotokoll verwenden, können Sie denselben Datenspeicher nicht mit verschiedenen NFS-Versionen auf mehreren Hosts mounten. Der Zugriff auf dieselbe virtuelle Festplatte über zwei nicht kompatible Clients kann zu unvorhersehbarem Verhalten und Datenbeschädigung führen.

NFS-Sicherheit

Bei Verwendung von NFS 3 und NFS 4.1 unterstützt ESXi die AUTH_SYS-Sicherheit. Darüber hinaus wird für NFS 4.1 der Kerberos-Sicherheitsmechanismus unterstützt.

NFS 3 unterstützt den AUTH_SYS-Sicherheitsmechanismus. Mit diesem Mechanismus wird Speicherdatenverkehr in einem unverschlüsseltem Format über das LAN übertragen. Aufgrund dieser Einschränkungen bei der Sicherheit sollten Sie die NFS-Speicherung ausschließlich in vertrauenswürdigen Netzwerken einsetzen und den Datenverkehr in getrennten physischen Switches isolieren. Sie können auch ein privates VLAN verwenden.

NFS 4.1 unterstützt das Authentifizierungsprotokoll Kerberos zur sicheren Kommunikation mit dem NFS-Server. Nicht-Root-Benutzer können auf Dateien zugreifen, wenn Kerberos verwendet wird. Weitere Informationen finden Sie unter Verwenden von Kerberos für NFS 4.1.

Neben Kerberos unterstützt NFS 4.1 herkömmliche Nicht-Kerberos-Bereitstellungen durch die AUTH_SYS-Sicherheit. Halten Sie sich dabei an die Richtlinien für den Root-Zugriff für NFS-Version 3.

Hinweis Es ist nicht möglich, zwei Sicherheitsmechanismen (AUTH_SYS und Kerberos) für denselben NFS 4.1-Datenspeicher zu verwenden, der von mehreren Hosts gemeinsam genutzt wird.

NFS-Multipathing

NFS 4.1 unterstützt Multipathing gemäß Protokollspezifikationen. Für NFS 3 ist Multipathing nicht anwendbar.

NFS 3 nutzt für E/A-Vorgänge eine einzige TCP-Verbindung. Aus diesem Grund unterstützt ESXi die E/A-Vorgänge für den NFS-Server nur für eine IP-Adresse oder einen Hostnamen und bietet keine Unterstützung für mehrere Pfade. Je nach Netzwerkinfrastruktur und -konfiguration können Sie mithilfe der Netzwerk-Stacks mehrere Verbindungen mit den Speicherzielen konfigurieren. Dazu müssen Sie mehrere Datenspeicher betreiben, von denen jeder eine eigene Netzwerkverbindung zwischen Host und Speicher verwendet.

NFS 4.1 stellt mehrere Pfade für Server mit unterstütztem Session Trunking zur Verfügung. Wenn Trunking verfügbar ist, können Sie über mehrere IP-Adressen auf dasselbe NFS-Volume zugreifen. Client-ID-Trunking wird nicht unterstützt.

NFS und Hardwarebeschleunigung

In NFS-Datenspeichern erstellte virtuelle Festplatten sind standardmäßig per Thin Provisioning bereitgestellt. Um per Thick Provisioning bereitgestellte virtuelle Festplatten zu erstellen, müssen Sie die Hardwarebeschleunigung verwenden, die den Vorgang „Speicherplatz reservieren“ unterstützt.

NFS 3 und NFS 4.1 unterstützen die Hardwarebeschleunigung, über die der Host mit NAS-Geräten vernetzt wird und mehrere vom NAS-Speicher bereitgestellte Hardwarevorgänge nutzen kann. Weitere Informationen finden Sie unter Hardwarebeschleunigung auf NAS-Geräten.

NFS-Datenspeicher

Beim Erstellen eines NFS-Datenspeichers müssen bestimmte Richtlinien befolgt werden.

Folgende Richtlinien und Best Practices für den NFS-Datenspeicher müssen u. a. beachtet werden:

- Das Mounten desselben Datenspeichers mit unterschiedlichen NFS-Versionen auf verschiedenen Hosts ist nicht möglich. NFS 3- und NFS 4.1-Clients sind nicht kompatibel und arbeiten mit unterschiedlichen Sperrprotokollen. Das bedeutet, dass es beim Zugriff auf dieselbe virtuelle Festplatte über zwei nicht kompatible Clients zu unvorhersehbarem Verhalten und Datenbeschädigung kommen kann.
- NFS-3- und NFS-4.1-Datenspeicher können nebeneinander auf demselben Host existieren.
- ESXi kann NFS 3 nicht automatisch auf Version 4.1 aktualisieren. Sie können jedoch andere Konvertierungsmethoden verwenden. Weitere Informationen hierzu finden Sie unter NFS-Protokolle und ESXi.

- Wenn Sie dasselbe NFS-3-Volume auf verschiedenen Hosts mounten, müssen Sie sicherstellen, dass Server- und Ordnernamen auf allen Hosts identisch sind. Wenn die Namen nicht übereinstimmen, betrachten die Hosts das NFS-3-Volume als zwei separate Datenspeicher. Bei Funktionen wie vMotion kann dies zu einem Fehler führen. Ein Beispiel für eine solche Diskrepanz wäre `filer` als Servernamen auf einem Host und `filer.domain.com` auf dem anderen. Diese Richtlinie gilt nicht für NFS Version 4.1.
- Wenn Sie beim Benennen von Datenspeichern und virtuellen Maschinen Nicht-ASCII-Zeichen verwenden, stellen Sie sicher, dass der zugrunde liegende NFS-Server die Internationalisierung unterstützt. Wenn der Server keine Sonderzeichen unterstützt, verwenden Sie nur die Standard-ASCII-Zeichen, da andernfalls unvorhersehbare Fehler auftreten können.

Firewall-Konfigurationen für NFS-Speicher

ESXi enthält eine Firewall zwischen der Verwaltungsschnittstelle und dem Netzwerk. Die Firewall ist standardmäßig aktiviert. Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme der Standarddienste wie NFS der eingehende und ausgehende Datenverkehr blockiert wird.

Unterstützte Dienste, einschließlich NFS, sind in einer Regelsatzkonfigurationsdatei im ESXi-Firewallverzeichnis `/etc/vmware/firewall/` beschrieben. Die Datei enthält Firewallregeln und Informationen über deren Beziehungen zu Ports und Protokollen.

Das Verhalten des NFS-Client-Regelsatzes (`nfsClient`) unterscheidet sich von dem Verhalten anderer Regelsätze.

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

NFS-Client-Firewallverhalten

Der NFS-Client-Firewallregelsatz weist ein anderes Verhalten als andere ESXi-Firewallregelsätze auf. ESXi konfiguriert NFS-Client-Einstellungen, wenn Sie einen NFS-Datenspeicher mounten oder unmounten. Das Verhalten unterscheidet sich je nach NFS-Version.

Beim Hinzufügen, Mounten und Unmounten eines NFS-Datenspeichers hängt das Verhalten von der NFS-Version ab.

Firewallverhalten in NFS v3

Wenn Sie einen NFS-v3-Datenspeicher hinzufügen oder mounten, überprüft ESXi den Status des NFS-Client-Firewallregelsatzes (`nfsClient`).

- Wenn der Regelsatz `nfsClient` deaktiviert ist, aktiviert ihn ESXi und deaktiviert die Richtlinie „Alle IP-Adressen zulassen“, indem das Flag `allowedAll` auf `FALSE` gesetzt wird. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.

- Wenn `nfsClient` aktiviert ist, bleiben der Status des Regelsatzes und die Richtlinien der zugelassenen IP-Adressen unverändert. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.

Hinweis Wenn Sie vor oder nach dem Hinzufügen eines NFS-v3-Datenspeichers zum System den Regelsatz `nfsClient` manuell aktivieren oder die Richtlinie „Alle IP-Adressen zulassen“ manuell festlegen, werden Ihre Einstellungen nach dem Unmounten des letzten NFS-v3-Datenspeichers überschrieben. Der Regelsatz `nfsClient` wird nach dem Unmounten aller NFS-v3-Datenspeicher deaktiviert.

Beim Entfernen oder Unmounten eines NFS-v3-Datenspeichers führt ESXi eine der folgenden Aktionen aus.

- Wenn keiner der verbleibenden NFS-v3-Datenspeicher von dem Server gemountet werden, auf dem der ungemountete Datenspeicher angesiedelt ist, entfernt ESXi die IP-Adresse des Servers aus der Liste der ausgehenden IP-Adressen.
- Wenn nach dem Unmounten keine gemounteten NFS-v3-Datenspeicher mehr übrig bleiben, deaktiviert ESXi den Firewallregelsatz `nfsClient`.

Firewallverhalten in NFS v4.1

Beim Mounten des ersten NFS-v4.1-Datenspeichers aktiviert ESXi den Regelsatz `nfs41client` und setzt das Flag `allowedAll` auf TRUE. Dabei wird Port 2049 für alle IP-Adressen geöffnet. Das Unmounten eines NFS-v4.1-Datenspeichers hat keine Auswirkungen auf den Status der Firewall. Das heißt, dass durch den ersten gemounteten NFS-v4.1-Datenspeicher Port 2049 geöffnet wird und dieser so lange geöffnet bleibt, bis Sie ihn explizit schließen.

Überprüfen der Firewall-Ports für NFS-Clients

Um den Zugriff auf NFS-Speicher zu ermöglichen, öffnet ESXi automatisch Firewall-Ports für die NFS-Clients, wenn Sie einen NFS-Datenspeicher mounten. Zu Zwecken der Fehlerbehebung müssen Sie möglicherweise überprüfen, ob die Ports geöffnet sind.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Firewall** und anschließend auf **Bearbeiten**.
4. Führen Sie einen Bildlauf nach unten zu einer passenden NFS-Version durch, um sicherzustellen, dass der Port geöffnet ist.

Geroutete Schicht 3-Verbindungen für Zugriff auf NFS-Speicher verwenden

Wenn Sie geroutete Schicht 3 (L3)-Verbindungen für den Zugriff auf NFS-Speicher verwenden, müssen Sie bestimmte Anforderungen und Beschränkungen beachten.

Ihre Umgebung muss die folgenden Anforderungen erfüllen:

- Das HSRP-Protokoll von Cisco (Hot Standby Router Protocol) wird im IP-Router verwendet. Falls Sie einen anderen Router als den von Cisco verwenden, verwenden Sie stattdessen das VRRP-Protokoll (Virtual Router Redundancy Protocol).
- Für die Priorisierung des NFS L3-Datenverkehrs auf Netzwerken mit begrenzter Bandbreite oder auf überlasteten Netzwerken verwenden Sie QoS (Quality of Service). Weitere Informationen hierzu finden Sie in der Dokumentation des Routers.
- Befolgen Sie die Empfehlungen zu geroutetem NFS L3 des Speicheranbieters. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.
- Deaktivieren der Netzwerk-E/A-Ressourcenverwaltung (NetIORM).
- Falls Sie vorhaben, Systeme mit Top-of-Rack-Switches oder der Switch-abhängigen E/A-Gerätepartitionierung einzusetzen, wenden Sie sich bezüglich Kompatibilität und Unterstützung an Ihren Systemanbieter.

In einer L3-Umgebung gelten die folgenden Beschränkungen:

- Die Umgebung unterstützt VMware Site Recovery Manager nicht.
- Die Umgebung unterstützt nur das NFS-Protokoll. Verwenden Sie keine anderen Speicherprotokolle, wie z. B. FCoE, in demselben physischen Netzwerk.
- Der NFS-Datenverkehr in dieser Umgebung unterstützt IPv6 nicht.
- Der NFS-Datenverkehr in dieser Umgebung kann nur über ein LAN geleitet werden. Andere Umgebungen, wie z. B. WAN, werden nicht unterstützt.

Verwenden von Kerberos für NFS 4.1

Mit NFS-Version 4.1 unterstützt ESXi den Kerberos-Authentifizierungsmechanismus.

Beim RPCSEC_GSS-Kerberos-Mechanismus handelt es sich um einen Authentifizierungsdienst. Mit diesem Dienst kann ein auf ESXi installierter NFS 4.1-Client vor dem Mounten einer NFS-Freigabe seine Identität bei einem NFS-Server nachweisen. Die Kerberos-Sicherheit verwendet Verschlüsselung beim Einsatz in einer ungesicherten Netzwerkverbindung.

Die ESXi-Implementierung von Kerberos für NFS 4.1 weist die beiden Sicherheitsmodelle krb5 und krb5i auf, die ein unterschiedliches Sicherheitsniveau bieten.

- Kerberos nur für Authentifizierung (krb5) unterstützt die Identitätsprüfung.
- Kerberos für Authentifizierung und Datenintegrität (krb5i) bietet neben der Identitätsprüfung auch Datenintegritätsdienste. Mit diesen Diensten kann NFS-Datenverkehr vor Manipulation geschützt werden, indem Datenpakete auf potenzielle Modifikationen überprüft werden.

Kerberos unterstützt Verschlüsselungsalgorithmen, die nicht autorisierte Benutzer daran hindern, auf NFS-Datenverkehr zuzugreifen. Der NFS 4.1-Client in ESXi versucht, mithilfe des Algorithmus AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf eine Freigabe auf dem NAS-Server zuzugreifen. Stellen Sie vor der Verwendung Ihrer NFS 4.1-Datenspeicher sicher, dass AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf dem NAS-Server aktiviert ist.

In der folgenden Tabelle werden die von ESXi unterstützten Kerberos-Sicherheitsstufen verglichen.

Tabelle 17-5. Kerberos-Sicherheitstypen

		ESXi 6.0	ESXi 6.5 und höher
Kerberos nur für Authentifizierung (krb5)	Integritätsprüfsumme für RPC-Header	Ja mit DES	Ja mit AES
	Integritätsprüfsumme für RPC-Daten	Nein	Nein
Kerberos für Authentifizierung und Datenintegrität (krb5i)	Integritätsprüfsumme für RPC-Header	Kein krb5i	Ja mit AES
	Integritätsprüfsumme für RPC-Daten		Ja mit AES

Wenn Sie die Kerberos-Authentifizierung verwenden, ist Folgendes zu beachten:

- ESXi verwendet Kerberos zusammen mit der Active Directory-Domäne.
- Als vSphere-Administrator geben Sie Active Directory-Anmeldedaten an, um einem NFS-Benutzer Zugriff auf NFS 4.1-Kerberos-Datenspeicher zu erteilen. Ein einzelner Anmeldedatensatz wird zum Zugriff auf alle Kerberos-Datenspeicher, die auf diesem Host gemountet sind, verwendet.
- Wenn mehrere ESXi-Hosts den NFS 4.1-Datenspeicher gemeinsam nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Um den Zuweisungsvorgang zu automatisieren, legen Sie den Benutzer in Hostprofilen fest und wenden das Profil auf alle ESXi-Hosts an.
- Es ist nicht möglich, zwei Sicherheitsmechanismen (AUTH_SYS und Kerberos) für denselben NFS 4.1-Datenspeicher zu verwenden, der von mehreren Hosts gemeinsam genutzt wird.

Einrichten der NFS-Speicherumgebung

Es sind einige Konfigurationsschritte erforderlich, bevor ein NFS-Datenspeicher in vSphere gemountet werden kann.

Voraussetzungen

- Machen Sie sich mit den Richtlinien in Richtlinien und Anforderungen für NFS-Speicher vertraut.

- Details zum Konfigurieren des NFS-Speichers erhalten Sie in der Dokumentation Ihres Speicheranbieters.
- Stellen Sie bei Verwendung von Kerberos sicher, dass AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf dem NAS-Server aktiviert ist.

Verfahren

1. Konfigurieren Sie auf dem NFS-Server ein NFS-Volume und exportieren Sie es, damit es auf den ESXi-Hosts gemountet werden kann.
   a. Notieren Sie sich die IP-Adresse oder den DNS-Namen des NFS-Servers und den vollständigen Pfad oder Ordnernamen der NFS-Freigabe.

      Bei NFS 4.1 können Sie mehrere IP-Adressen oder DNS-Namen erfassen, um die Mehrfachpfadfunktion in NFS-4.1-Datenspeichern zu nutzen.

   b. Wenn Sie NFS 4.1 mit Kerberos-Authentifizierung ausstatten möchten, geben Sie die Kerberos-Anmeldedaten ein, die von ESXi zur Authentifizierung verwendet werden sollen.
2. Konfigurieren Sie auf allen ESXi Hosts einen VMkernel-Netzwerkport für den NFS-Datenverkehr.

   Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.
3. Wenn Sie den NFS-4.1-Datenspeicher mit Kerberos-Authentifizierung ausstatten möchten, konfigurieren Sie die ESXi-Hosts für die Authentifizierung mit Kerberos.

   Weitere Informationen hierzu finden Sie unter Konfigurieren der Kerberos-Authentifizierung für ESXi-Hosts.

Nächste Schritte

Jetzt können Sie einen NFS-Datenspeicher auf den ESXi-Hosts erstellen.

Konfigurieren der Kerberos-Authentifizierung für ESXi-Hosts

Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie verschiedene Aufgaben zum Einrichten Ihrer Hosts für Kerberos-Authentifizierung ausführen.

Wenn mehrere ESXi-Hosts den NFS 4.1-Datenspeicher gemeinsam nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Sie können den Zuweisungsvorgang durch Festlegen des Benutzers in Hostprofilen und Anwenden des Profils auf alle ESXi-Hosts automatisieren.

Voraussetzungen

- Stellen Sie sicher, dass Microsoft Active Directory (AD) und NFS-Server für die Verwendung von Kerberos konfiguriert sind.
- Aktivieren Sie den Verschlüsselungsmodus AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 in AD. Der NFS 4.1-Client unterstützt den Verschlüsselungsmodus DES-CBC-MD5 nicht.

- Stellen Sie sicher, dass die NFS-Server-Exporte so konfiguriert sind, dass Vollzugriff auf den Kerberos-Benutzer gewährt wird.

Verfahren

1 Konfigurieren von DNS für NFS 4.1 mit Kerberos

   Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie die DNS-Einstellungen auf ESXi-Hosts ändern. Die Einstellungen müssen auf den DNS-Server verweisen, der dafür konfiguriert wurde, DNS-Datensätze für das Kerberos Key Distribution Center (KDC) auszugeben. Verwenden Sie zum Beispiel die Active Directory-Serveradresse, wenn AD als DNS-Server verwendet wird.

2 Konfigurieren von NTP (Network Time Protocol) für NFS 4.1 mit Kerberos

   Wenn Sie NFS 4.1 mit Kerberos verwenden, muss die Uhrzeit für ESXi-Hosts, den NFS-Server und den aktiven Domänenserver synchronisiert sein. In der Regel wird der aktive Domänenserver im Setup als NTP-Server (Network Time Protocol) verwendet.

3 Aktivieren der Kerberos-Authentifizierung in Active Directory

   Bei Verwendung des NFS-4.1-Speichers mit Kerberos müssen Sie jedem ESXi-Host eine Active Directory-Domäne hinzufügen und die Kerberos-Authentifizierung aktivieren. Kerberos wird in Active Directory integriert und ermöglicht Single Sign-On sowie eine zusätzliche Schutzebene für unsichere Netzwerkverbindungen.

Nächste Schritte

Nach dem Konfigurieren Ihres Hosts für Kerberos können Sie einen NFS 4.1-Datenspeicher erstellen, in dem Kerberos aktiviert ist.

Konfigurieren von DNS für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, müssen Sie die DNS-Einstellungen auf ESXi-Hosts ändern. Die Einstellungen müssen auf den DNS-Server verweisen, der dafür konfiguriert wurde, DNS-Datensätze für das Kerberos Key Distribution Center (KDC) auszugeben. Verwenden Sie zum Beispiel die Active Directory-Serveradresse, wenn AD als DNS-Server verwendet wird.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Netzwerk** auf **TCP/IP-Konfiguration**.

4 Wählen Sie **Standard** aus und klicken Sie auf das Symbol **Bearbeiten**.

5 Geben Sie die DNS-Einstellungen manuell ein.

Option	Beschreibung
Domäne	*AD-Domänenname*
Bevorzugter DNS-Server	*AD-Server-IP*
Domänen durchsuchen	*AD-Domänenname*

Konfigurieren von NTP (Network Time Protocol) für NFS 4.1 mit Kerberos

Wenn Sie NFS 4.1 mit Kerberos verwenden, muss die Uhrzeit für ESXi-Hosts, den NFS-Server und den aktiven Domänenserver synchronisiert sein. In der Regel wird der aktive Domänenserver im Setup als NTP-Server (Network Time Protocol) verwendet.

Die folgende Aufgabe beschreibt, wie der ESXi-Host mit dem NTP-Server synchronisiert wird.

Es empfiehlt sich, den Active Domain-Server als NTP-Server zu verwenden.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Wählen Sie unter **System** die Option **Uhrzeitkonfiguration** aus.

4 Klicken Sie auf **Bearbeiten** und richten Sie den NTP-Server ein.

   a Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.

   b Geben Sie für die Synchronisierung mit dem NTP-Server dessen IP-Adressen ein.

   c Wählen Sie **NTP-Dienst starten**.

   d Legen Sie die Startrichtlinie für den NTP-Dienst fest.

5 Klicken Sie auf **OK**.

   Der Host wird mit dem NTP-Server synchronisiert.

Aktivieren der Kerberos-Authentifizierung in Active Directory

Bei Verwendung des NFS-4.1-Speichers mit Kerberos müssen Sie jedem ESXi-Host eine Active Directory-Domäne hinzufügen und die Kerberos-Authentifizierung aktivieren. Kerberos wird in Active Directory integriert und ermöglicht Single Sign-On sowie eine zusätzliche Schutzebene für unsichere Netzwerkverbindungen.

Voraussetzungen

Richten Sie eine AD-Domäne und ein Domänenadministratorkonto mit Berechtigungen zum Hinzufügen von Hosts zur Domäne ein.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **System** auf **Authentifizierungsdienste**.

4 Fügen Sie den ESXi-Host zu einer Active Directory-Domäne hinzu.

   a Klicken Sie im Bereich „Authentifizierungsdienste“ auf **Domäne beitreten**.

   b Geben Sie die Domäneneinstellungen an und klicken Sie auf **OK**.

   Der Verzeichnisdiensttyp wird zu Active Directory geändert.

5 Konfigurieren oder bearbeiten Sie die Anmeldedaten eines NFS-Kerberos-Benutzers.

   a Klicken Sie im Bereich „NFS-Kerberos-Anmeldedaten“ auf **Bearbeiten**.

   b Geben Sie einen Benutzernamen und ein Kennwort ein.

      Der Zugriff auf die in allen Kerberos-Datenspeichern gespeicherten Dateien erfolgt über diese Anmeldedaten.

   Der Status der NFS-Kerberos-Anmeldedaten ändert sich zu „Aktiviert“.

Erfassen statistischer Informationen für den NFS-Speicher

Sie können das `nfsStats`-Tool in Ihrem ESXi-Host verwenden, um statistische Informationen zu NFS-Aufrufen und Remoteprozeduraufrufen (RPC) anzuzeigen. Der Befehl zeigt statistische Informationen für NFS 3- und NFS 4.1-Mounts auf dem ESXi-Host an.

Im Allgemeinen führt das `nfsStats`-Tool die folgenden Aufgaben aus.

- Erfasst NFS-Statistiken, um Probleme bei der Bereitstellung einer neuen Konfiguration, z. B. eines neuen NFS-Servers oder Netzwerks, in der NFS-Umgebung zu untersuchen.
- Liefert Statistiken zum Erfolg und Fehlschlag von NFS-Vorgängen.
- Veröffentlicht Latenzstatistiken über den Erfolg und Fehler von NFS-Vorgängen.
- Behebt NFS-Leistungsprobleme.

Die Befehlssyntax ist `nfsStats` *Optionen*.

Die folgenden Befehlsoptionen sind verfügbar.

Tabelle 17-6. `nfsStats`**-Befehle**

Befehlsoption	Beschreibung
`No option`	Rufen Sie nfs-Statistiken und RPC-Statistiken für alle NFS-Datenspeicher ab.
`-3`	Zeigen Sie nur NFS 3-Statistiken an.
`-4`	Zeigen Sie nur NFS 4.1-Statistiken an.
`-n`	Zeigen Sie nur NFS 3- und NFS 4.1-Statistiken an.
`-r`	Zeigen Sie RPC-Statistiken an.

Tabelle 17-6. `nfsStats`-Befehle (Fortsetzung)

Befehlsoption	Beschreibung
`-i` *Intervall*	Zeigen Sie NFS- und RPC-Statistiken in einem Intervall an, das dem angegebenen Wert in Sekunden entspricht. Wenn der Wert beispielsweise 10 ist, wird die Statistik alle 10 Sekunden aktualisiert.
`-v` *DSNAME1, DSNAME2 ...*	Zeigen Sie NFS- und RPC-Statistiken für die angegebenen NFS-Datenspeicher an. Verwenden Sie diese Option in Verbindung mit dem NFS-Datenspeichertyp, z. B. -3 oder -4.
`-j`	Zeigen Sie Statistiken im JSON-Format an.

Erstellen von Datenspeichern

Mit dem Assistenten für neue Datenspeicher erstellen Sie die Datenspeicher. Je nach Typ des verwendeten Speichers und Ihren Speicheranforderungen können Sie einen VMFS-, NFS- oder Virtual Volumes-Datenspeicher erstellen.

Ein vSAN-Datenspeicher wird automatisch erstellt, wenn Sie vSAN aktivieren. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.

Sie können auch den Assistenten für neue Datenspeicher verwenden, um VMFS-Datenspeicherkopien zu verwalten.

- Erstellen eines VMFS-Datenspeichers

  VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte.
- Erstellen eines NFS-Datenspeichers

  Sie können ein NFS-Volume mit dem **Assistenten für neue Datenspeicher** mounten.
- Erstellen eines Virtual Volumes-Datenspeichers

  Virtual Volumes-Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

Erstellen eines VMFS-Datenspeichers

VMFS-Datenspeicher dienen als Repositorys für virtuelle Maschinen. Sie können VMFS-Datenspeicher auf allen SCSI-basierenden Speichergeräten einrichten, die der Host erkennt, einschließlich Fibre-Channel, iSCSI und lokaler Speichergeräte.

Voraussetzungen

1 Installieren und konfigurieren Sie alle Adapter, die vom Speicher benötigt werden.

2 Führen Sie eine erneute Prüfung durch, um neu hinzugefügte Speichergeräte zu ermitteln. Weitere Informationen hierzu finden Sie unter Vorgänge zum erneuten Prüfen des Speichers.

3 Überprüfen Sie, ob die Speichergeräte, die Sie für Ihre Datenspeicher verwenden möchten, verfügbar sind. Weitere Informationen hierzu finden Sie unter Eigenschaften des Speichergeräts.

Verfahren

1 Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.

2 Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.

3 Wählen Sie „VMFS“ als Datenspeichertyp aus.

4 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.

   Das System setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.

5 Wählen Sie das Gerät aus, das für den Datenspeicher verwendet werden soll.

   Wichtig Für das Gerät, das Sie auswählen, dürfen keine Werte in der Spalte „Snapshot-Volume“ angezeigt werden. Wenn ein Wert vorhanden ist, enthält das Gerät eine Kopie des vorhandenen VMFS-Datenspeichers. Weitere Informationen zur Verwaltung von Datenspeicherkopien finden Sie unter Verwalten von duplizierten VMFS-Datenspeichern.

6 Geben Sie die Version des Datenspeichers an.

Option	Beschreibung
VMFS 6	Standardformat auf allen Hosts, die VMFS6 unterstützen. Die ESXi-Hosts der Version 6.0 oder früher können den VMFS6-Datenspeicher nicht erkennen.
VMFS5	Der VMFS5-Datenspeicher unterstützt den Zugriff durch die ESXi-Hosts der Version 6.7 oder früher.

7 Definieren Sie die Konfigurationsdaten für den Datenspeicher.

Hinweis Die erforderliche Mindestgröße für einen VMFS6-Datenspeicher beträgt 2 GB.

a Legen Sie die Konfiguration der Partition fest.

Option	Beschreibung
Alle verfügbaren Partitionen verwenden	Weist einem einzelnen VMFS-Datenspeicher die gesamte Festplatte zu. Bei Auswahl dieser Option werden die momentan auf diesem Gerät gespeicherten Dateisysteme und Daten dauerhaft gelöscht.
Freien Speicherplatz verwenden	Stellt einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereit.

b Wenn der für den Datenspeicher zugeteilte Speicherplatz für Ihre Zwecke zu groß ist, passen Sie die Kapazitätswerte im Feld „Größe des Datenspeichers“ an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zugeteilt.

c Geben Sie für VMFS6 die Blockgröße an und definieren Sie die Parameter für die Speicherplatzrückforderung. Weitere Informationen hierzu finden Sie unter Anforderungen zur Speicherplatzrückforderung von VMFS-Datenspeichern.

8 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **Beenden**.

Ergebnisse

Der Datenspeicher auf dem SCSI-basierten Gerät wird erstellt. Er ist für alle Hosts verfügbar, die auf das Gerät Zugriff haben.

Nächste Schritte

Nachdem Sie den VMFS-Datenspeicher erstellt haben, können Sie die folgenden Aufgaben durchführen:

- Die Kapazität des Datenspeichers ändern. Weitere Informationen hierzu finden Sie unter Erhöhen der VMFS-Datenspeicherkapazität.
- Einstellungen für die Speicherplatzrückforderung bearbeiten. Weitere Informationen hierzu finden Sie unter Ändern der Einstellungen für die Speicherplatzrückforderung.
- Gemeinsam genutzte VMDK-Unterstützung aktivieren. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren der Unterstützung für geclusterte virtuelle Festplatten im VMFS6-Datenspeicher.

Erstellen eines NFS-Datenspeichers

Sie können ein NFS-Volume mit dem **Assistenten für neue Datenspeicher** mounten.

Voraussetzungen

- Richten Sie die NFS-Speicherumgebung ein.

- Wenn Sie die Kerberos-Authentifizierung mit dem NFS 4.1-Datenspeicher verwenden möchten, müssen Sie für die ESXi-Hosts die Kerberos-Authentifizierung konfigurieren.

Verfahren

1 Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.

2 Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.

3 Wählen Sie „NFS“ als Datenspeichertyp aus und geben Sie eine NFS-Version an.

   - NFS 3
   - NFS 4.1

   Wichtig Wenn mehrere Hosts auf denselben Datenspeicher zugreifen, müssen Sie dasselbe Protokoll auf allen Hosts verwenden.

4 Geben Sie die Datenspeicher-Parameter ein.

Option	Beschreibung
Datenspeichername	Das System setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.
Ordner	Der Name des Mount-Punkt-Ordners.
Server	Der Servername oder die IP-Adresse. Sie können das Format IPv6 oder IPv4 verwenden. Bei NFS 4.1 können Sie mehrere IP-Adressen oder Servernamen hinzufügen, wenn der NFS-Server Trunking unterstützt. Der ESXi-Host verwendet diese Werte, um Multipathing für den Mount-Punkt dieses NFS-Servers zu ermöglichen.

5 Wählen Sie **NFS schreibgeschützt mounten**, wenn das Laufwerk vom NFS-Server als schreibgeschützt exportiert wurde.

6 Um Kerberos-Sicherheit mit NFS 4.1 zu verwenden, aktivieren Sie Kerberos und wählen ein geeignetes Kerberos-Modell aus.

Option	Beschreibung
Kerberos nur für Authentifizierung verwenden (krb5)	Unterstützt die Identitätsüberprüfung
Kerberos für Authentifizierung und Datenintegrität verwenden (krb5i)	Stellt neben der Integritätsüberprüfung Datenintegritätsdienste zur Verfügung. Mit diesen Diensten kann NFS-Datenverkehr vor Manipulation geschützt werden, indem Datenpakete auf potenzielle Modifikationen überprüft werden.

   Wenn Sie Kerberos nicht aktivieren, nutzt der Datenspeicher die standardmäßige AUTH_SYS-Sicherheit.

7 Wenn Sie einen Datenspeicher auf Datencenter- oder Cluster-Ebene erstellen, wählen Sie Hosts aus, die den Datenspeicher mounten.

8 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

Erstellen eines Virtual Volumes-Datenspeichers

Virtual Volumes-Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

Verfahren

1 Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.

2 Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.

3 Wählen Sie **vVol** als Datenspeichertyp aus.

4 Geben Sie den Namen des Datenspeichers ein und wählen Sie aus der Liste der Speichercontainer einen Backing-Speichercontainer aus.

   Achten Sie darauf, für jeden Datenspeicher in Ihrer Datenspeicherumgebung einen eindeutigen Namen zu vergeben.

   Beim Mounten eines Virtual Volumes-Datenspeichers auf mehreren Hosts muss der Datenspeichername auf allen Hosts gleich sein.

5 Wählen Sie die Hosts aus, die Zugriff auf den Datenspeicher benötigen.

6 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

Nächste Schritte

Nach der Erstellung des Virtual Volumes-Datenspeichers können Sie ihn umbenennen, Datenspeicherdateien durchsuchen, den Datenspeicher unmounten und weitere Datenspeicheraktionen ausführen.

Sie können den Virtual Volumes-Datenspeicher nicht einem Datenspeicher-Cluster hinzufügen.

Verwalten von duplizierten VMFS-Datenspeichern

Wenn ein Speichergerät eine Kopie eines VMFS-Datenspeichers enthält, können Sie den Datenspeicher mit der vorhandenen Signatur mounten oder eine neue Signatur zuweisen.

Jeder in einem Speichergerät erstellte VMFS-Datenspeicher besitzt eine eindeutige Signatur, die auch als UUID bezeichnet wird und im Superblock des Dateisystems gespeichert ist. Wenn das Speichergerät repliziert oder ein Snapshot von ihm auf der Array-Seite erstellt wird, ist die dabei entstehende Gerätekopie Byte für Byte mit dem ursprünglichen Gerät identisch. Wenn zum Beispiel das ursprüngliche Speichergerät einen VMFS-Datenspeicher mit UUIDX enthält, scheint die Kopie eine Datenspeicherkopie mit demselben UUIDX zu enthalten.

Neben LUN-Snapshots und Replizierungen erstellen bestimmte Gerätevorgänge, wie zum Beispiel LUN-ID-Änderungen, eine Kopie des ursprünglichen Datenspeichers.

ESXi kann die VMFS-Datenspeicherkopie erkennen. Sie können die Datenspeicherkopie mit ihrer ursprünglichen UUID mounten oder die UUID ändern. Der Prozess der Änderung der UUID wird als Neusignierung des Datenspeichers bezeichnet.

Ob Sie die Neusignierung oder das Mounten ohne Neusignierung wählen, hängt davon ab, wie die LUNs in der Speicherumgebung maskiert werden. Wenn Ihre Hosts beide Kopien der LUN sehen können, ist die Neusignierung die optimale Methode.

Beibehalten der vorhandenen Datenspeichersignatur

Wenn Sie eine Kopie eines VMFS-Datenspeichers nicht neu signieren müssen, können Sie sie mounten, ohne ihre Signatur zu ändern.

Sie können die Signatur beispielsweise beibehalten, wenn Sie synchronisierte Kopien von virtuellen Maschinen als Teil eines Notfallplans auf einer sekundären Site unterhalten. Bei einem Notfall an der primären Site mounten Sie die Datenspeicherkopie und schalten die virtuelle Maschinen der sekundären Site ein.

Neusignieren einer VMFS-Datenspeicherkopie

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten.

Beim Neusignieren einer VMFS-Kopie weist ESXi der Kopie eine neue Signatur (UUID) zu und mountet die Kopie als einen vom Original unabhängigen Datenspeicher. Alle Referenzen der Originalsignatur in den Konfigurationsdateien der virtuellen Maschine werden aktualisiert.

Beachten Sie bei der Datenspeicher-Neusignierung Folgendes:

- Die Datenspeicher-Neusignierung kann nicht rückgängig gemacht werden.
- Nach der Neusignierung wird die Speichergerätereplik, die die VMFS-Kopie enthalten hat, nicht mehr als Replik behandelt.
- Ein übergreifender Datenspeicher kann nur neu signiert werden, wenn all seine Erweiterungen online sind.
- Der Neusignierungsprozess ist fehlertolerant. Wenn der Prozess unterbrochen wird, können Sie ihn später fortsetzen.
- Sie können den neuen VMFS-Datenspeicher mounten, ohne dass das Risiko besteht, dass seine UUID mit UUIDs anderer Datenspeicher in einer Hierarchie von LUN-Snapshots in Konflikt steht.

Mounten einer VMFS-Datenspeicherkopie

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten. Wenn Sie die Kopie des VMFS-Datenspeichers nicht neu signieren müssen, können Sie sie mounten, ohne ihre Signatur zu ändern.

Voraussetzungen

- Führen Sie eine erneute Speicherprüfung auf Ihrem Host durch, um die Ansicht der Speichergeräte auf dem Host zu aktualisieren.

- Unmounten Sie den Original-VMFS-Datenspeicher, der dieselbe UUID hat wie die Kopie, die Sie mounten möchten. Sie können die VMFS-Datenspeicherkopie nur mounten, wenn sie nicht mit dem Original-VMFS-Datenspeicher kollidiert.

Verfahren

1 Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.

2 Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.

3 Wählen Sie „VMFS“ als Datenspeichertyp aus.

4 Geben Sie den Namen des Datenspeichers ein und wählen Sie, falls erforderlich, den Speicherplatz für den Datenspeicher aus.

5 Wählen Sie aus der Liste der Speichergeräte das Gerät aus, dessen Wert in der Spalte „Snapshot-Volume“ angezeigt wird.

   Der in der Spalte „Snapshot-Volume“ vorhandene Name gibt an, dass das Gerät eine Kopie ist, die eine Kopie eines vorhandenen VMFS-Datenspeichers enthält.

6 Mounten Sie den Datenspeicher.

Option	Beschreibung
Mounten mit Neusignierung	Wählen Sie unter **Optionen für das Mounten** die Option **Neue Signatur zuweisen** und klicken Sie auf **Weiter**.
Mounten ohne Neusignierung	Wählen Sie unter „Optionen für das Mounten“ die Option **Vorhandene Signatur beibehalten** aus.

7 Überprüfen Sie die Konfigurationsinformationen für den Datenspeicher, und klicken Sie auf **Beenden (Finish)**.

Erhöhen der VMFS-Datenspeicherkapazität

Sie können die Kapazität eines VMFS-Datenspeichers erhöhen. Zusätzliche Kapazität ist unter Umständen erforderlich, wenn Sie virtuelle Maschinen zum Datenspeicher hinzufügen oder wenn die auf dem Datenspeicher ausgeführten virtuellen Maschinen mehr Speicherplatz benötigen.

Wenn ein gemeinsam genutzter Datenspeicher eingeschaltete virtuelle Maschinen aufweist und seine Kapazität zu 100 % ausgeschöpft ist, können Sie die Kapazität des Datenspeichers erhöhen. Sie können diese Aktion nur von dem Host aus durchführen, bei dem die eingeschalteten virtuellen Maschinen registriert sind.

Je nach Ihrer Speicherkonfiguration können Sie eine der folgenden Methoden verwenden, um die Kapazität des Datenspeichers zu erhöhen. Sie müssen virtuelle Maschinen nicht ausschalten, wenn eine der beiden Methoden zum Erhöhen der Kapazität des Datenspeichers eingesetzt wird.

Vorhandenen Datenspeicher erweitern

Erhöhen Sie die Größe eines erweiterbaren VMFS-Datenspeichers. Der Datenspeicher wird als vergrößerbar angesehen, wenn das Backing-Speichergerät unmittelbar hinter der Erweiterung über freien Speicherplatz verfügt.

Eine Erweiterung hinzufügen

Erhöhen Sie die Kapazität eines vorhandenen VMFS-Datenspeichers durch Hinzufügen von neuen Speichergeräten zum Datenspeicher. Der Datenspeicher kann sich über mehrere Erweiterungen erstrecken und wird dennoch als einzelnes Volume angezeigt.

Der übergreifende VMFS-Datenspeicher kann jederzeit jede einzelne oder alle seiner Erweiterungen verwenden. Es ist nicht notwendig, dass eine bestimmte Erweiterung aufgefüllt wird, bevor die nächste Erweiterung verwendet werden kann.

Hinweis Datenspeicher, die nur hardwaregestützte Sperren unterstützen, die auch als Atomic Test and Set-Mechanismus (ATS) bezeichnet werden, können sich nicht über Nicht-ATS-Geräte erstrecken. Weitere Informationen finden Sie unter VMFS-Sperrmechanismen.

Voraussetzungen

Sie können die Kapazität des Datenspeichers erhöhen, wenn der Hostspeicher eine der folgenden Bedingungen erfüllt:

- Das Backing-Gerät für den vorhandenen Datenspeicher verfügt über ausreichend Speicherplatz.
- Sie haben neue Speichergeräte zum Host hinzugefügt.

Verfahren

1. Navigieren Sie im vSphere Client zum Datenspeicher.
2. Wählen Sie im Kontextmenü für den Datenspeicher die Option **Datenspeicherkapazität erhöhen** aus.
3. Wählen Sie ein Gerät aus der Liste der Speichergeräte aus.

   Die Auswahlmöglichkeiten hängen davon ab, ob ein erweiterbares Speichergerät verfügbar ist.

Option	Beschreibung
So vergrößern Sie eine vorhandene Datenspeichererweiterung	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Ja“ hat.
So fügen Sie eine Erweiterung hinzu	Wählen Sie das Gerät aus, das in der Spalte „Erweiterbar“ den Eintrag „Nein“ hat.

4. Überprüfen Sie das **Partitionslayout**, um die verfügbaren Konfigurationen anzuzeigen.

5 Wählen Sie eine Konfigurationsoption im unteren Fenster aus.

Die angezeigten Menübefehle variieren abhängig vom aktuellen Festplattenlayout und Ihrer vorherigen Auswahl.

Menüelement	Beschreibung
Freien Speicherplatz verwenden, um den Datenspeicher zu erweitern	Vergrößert eine vorhandene Erweiterung auf die erforderliche Kapazität.
Freien Speicherplatz verwenden	Stellt eine Erweiterung im verbleibenden freien Speicherplatz auf der Festplatte bereit. Dieser Menübefehl ist nur verfügbar, wenn Sie eine Erweiterung hinzufügen.
Alle verfügbaren Partitionen verwenden	Weist einer einzelnen Erweiterung die gesamte Festplatte zu. Dieser Menübefehl ist nur verfügbar, wenn Sie eine Erweiterung hinzufügen und die zu formatierende Festplatte nicht leer ist. Die Festplatte wird neu formatiert und dabei werden alle darauf enthaltenen Datenspeicher und Daten gelöscht.

6 Geben Sie die Kapazität der Erweiterung an.

Die Mindesterweiterungsgröße ist 1,3 GB. Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

7 Klicken Sie auf **Weiter**.

8 Überprüfen Sie das vorgeschlagene Layout und die neue Konfiguration des Datenspeichers, und klicken Sie anschließend auf **Beenden**.

Aktivieren oder Deaktivieren der Unterstützung für geclusterte virtuelle Festplatten im VMFS6-Datenspeicher

Wenn Sie beabsichtigen, eine virtuelle Festplatte in WSFC-Konfigurationen (Windows Server Failover Clustering) zu verwenden, muss Ihr VMFS6-Datenspeicher geclusterte virtuelle Festplatten unterstützen. Verwenden Sie den vSphere Client, um die Unterstützung von geclusterten Festplatten zu aktivieren.

Informationen zur Verwendung von geclusterten virtuellen Festplatten in VM-Clustern finden Sie in der *Setup für Windows Server-Failover-Clustering*-Dokumentation.

Voraussetzungen

Befolgen Sie die folgenden Richtlinien, wenn Sie einen Datenspeicher für geclusterte virtuelle Festplatten verwenden:

- Das Speicher-Array muss den Reservierungstyp ATS, Write Exclusive – All Registrant (WEAR) SCSI-3 unterstützen.
- ESXi unterstützt nur Fibre Channel-Arrays für diese Art von Konfigurationen.
- Nur VMFS6-Datenspeicher unterstützen geclusterte Festplatten. Die verwendeten Datenspeicher können nicht erweitert werden oder mehrere Erweiterungen umfassen.

- Speichergeräte müssen vom NMP beansprucht werden. ESXi unterstützt keine Drittanbieter-Plug-Ins (MPPs) in den Konfigurationen mit geclusterten virtuellen Festplatten.
- Stellen Sie sicher, dass die virtuellen Festplatten, die Sie für das Clustering verwenden, im Format Thick Provision Eager-Zeroed vorliegen.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Allgemein**.

3 Klicken Sie unter **Datenspeicherfunktionen** auf eine der folgenden Optionen neben dem Element **Cluster-VMDK**.

Option	Bezeichnung
Aktivieren	So aktivieren Sie die Unterstützung für geclusterte virtuelle Festplatten im Datenspeicher. Nachdem Sie die Unterstützung aktiviert haben, können Sie die geclusterten virtuellen Festplatten in diesem VMFS-Datenspeicher ablegen.
Deaktivieren	Zum Deaktivieren der Unterstützung. Stellen Sie vor dem Deaktivieren sicher, dass alle virtuellen Maschinen mit den geclusterten virtuellen Festplatten ausgeschaltet werden.

4 Bestätigen Sie die Konfiguration.

Verwaltungsvorgänge für Datenspeicher

Nach dem Erstellen von Datenspeichern können Sie mehrere Verwaltungsvorgänge für die Datenspeicher durchführen. Bestimmte Vorgänge wie das Umbenennen eines Datenspeichers stehen für alle Datenspeichertypen zur Verfügung. Andere beziehen sich auf bestimmte Typen von Datenspeichern.

- Ändern des Datenspeichernamens

  Verwenden Sie den vSphere Client, um den Namen eines vorhandenen Datenspeichers ändern. Sie können ohne negative Auswirkungen den Datenspeicher umbenennen, auf dem virtuelle Maschinen ausgeführt werden.

- Unmounten von Datenspeichern

  Wenn Sie einen Datenspeicher unmounten, bleibt dieser intakt, er wird jedoch von den von Ihnen angegebenen Hosts nicht mehr angezeigt. Der Datenspeicher wird weiterhin auf anderen Hosts angezeigt, auf denen er gemountet bleibt.

- Mounten von Datenspeichern

  Sie können einen zuvor ungemounteten Datenspeicher mounten. Sie können einen Datenspeicher auch auf weiteren Hosts mounten. Dadurch wird dieser zu einem gemeinsam genutzten Datenspeicher.

- Entfernen von VMFS-Datenspeichern

  Sie können jede Art von VMFS-Datenspeicher löschen, einschließlich Kopien, die Sie gemountet haben, ohne sie neu zu signieren. Beim Löschen eines Datenspeichers wird er zerstört und auf keinem Host mehr angezeigt, der davor Zugriff auf ihn hatte.

- Verwenden des Datenspeicherbrowsers

  Verwenden Sie den Datenspeicherbrowser zum Verwalten des Inhalts Ihrer Datenspeicher. Sie können Ordner und Dateien durchsuchen, die im Datenspeicher gespeichert sind. Im Browser können Sie auch Dateien hochladen und Verwaltungsaufgaben für Ihre Dateien und Ordner durchführen.

- Ausschalten von Speicherfiltern

  Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, verwendet vCenter Server Standardspeicherschutzfilter. Die Filter helfen Ihnen Speicherschäden zu vermeiden, indem nur die Speichergeräte abgerufen werden, die für einen bestimmten Vorgang verwendet werden können. Ungeeignete Geräte werden nicht zur Auswahl angezeigt. Sie können die Filter deaktivieren, um alle Geräte anzuzeigen.

Ändern des Datenspeichernamens

Verwenden Sie den vSphere Client, um den Namen eines vorhandenen Datenspeichers ändern. Sie können ohne negative Auswirkungen den Datenspeicher umbenennen, auf dem virtuelle Maschinen ausgeführt werden.

Hinweis Wenn der Host von vCenter Server verwaltet wird, können Sie den Datenspeicher nicht umbenennen, indem Sie direkt über den VMware Host Client auf den Datenspeicher zugreifen. Sie müssen den Datenspeicher über vCenter Server umbenennen.

Verfahren

1. Navigieren Sie im vSphere Client zum Datenspeicher.
2. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, den Sie umbenennen möchten, und wählen Sie **Umbenennen** aus.
3. Geben Sie einen neuen Datenspeichernamen ein.

   Das System setzt eine Längenbeschränkung von 42 Zeichen für den Datenspeichernamen voraus.

Ergebnisse

Der neue Name erscheint auf allen Hosts, die Zugriff auf den Datenspeicher haben.

Unmounten von Datenspeichern

Wenn Sie einen Datenspeicher unmounten, bleibt dieser intakt, er wird jedoch von den von Ihnen angegebenen Hosts nicht mehr angezeigt. Der Datenspeicher wird weiterhin auf anderen Hosts angezeigt, auf denen er gemountet bleibt.

Führen Sie keine Konfigurationsvorgänge durch, die zu E/A des Datenspeichers führen können, während das Unmounten ausgeführt wird.

Hinweis Stellen Sie sicher, dass der Datenspeicher nicht für vSphere HA-Taktsignale verwendet wird. vSphere HA-Taktsignale verhindern das Unmounten des Datenspeichers nicht. Wenn jedoch der Datenspeicher für das Taktsignal verwendet wird, kann das Unmounten des Datenspeichers dazu führen, dass der Host ausfällt und eine aktive virtuelle Maschine neu gestartet wird.

Voraussetzungen

Stellen ggf. Sie vor dem Unmounten von Datenspeichern sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Es dürfen sich keine virtuelle Maschinen im Datenspeicher befinden.
- Speicher-DRS verwaltet den Datenspeicher nicht.
- Storage I/O Control ist für diesen Datenspeicher deaktiviert.

Verfahren

1. Navigieren Sie im vSphere Client zum Datenspeicher.
2. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Datenspeicher unmounten** aus.
3. Wenn der Datenspeicher gemeinsam genutzt wird, wählen Sie die Hosts aus, von denen der Datenspeicher abgetrennt werden soll.
4. Bestätigen Sie, dass Sie den Datenspeicher unmounten möchten.

Ergebnisse

Nachdem Sie einen VMFS-Datenspeicher von allen Hosts ungemountet haben, wird der Datenspeicher als inaktiv markiert. Wenn Sie einen NFS- oder Virtual Volumes-Datenspeicher von allen Hosts unmounten, wird er in der Bestandsliste nicht mehr angezeigt. Sie können den VMFS-Datenspeicher, der ungemountet wurde, wieder mounten. Zum Mounten eines NFS- oder Virtual Volumes-Datenspeichers, der aus der Bestandsliste entfernt wurde, verwenden Sie den Assistenten „Neuer Datenspeicher“.

Nächste Schritte

Wenn Sie den VMFS-Datenspeicher im Zuge eines Verfahrens zum Entfernen eines Speichergeräts unmounten, können Sie jetzt das zugrunde liegende Speichergerät trennen. Weitere Informationen hierzu finden Sie unter Speichergeräte trennen.

Mounten von Datenspeichern

Sie können einen zuvor ungemounteten Datenspeicher mounten. Sie können einen Datenspeicher auch auf weiteren Hosts mounten. Dadurch wird dieser zu einem gemeinsam genutzten Datenspeicher.

Ein VMFS-Datenspeicher, der auf allen Hosts ungemountet wurde, verbleibt zwar in der Bestandsliste, wird aber als unzugänglich markiert. Weitere Informationen finden Sie unter Unmounten von Datenspeichern.

Sie können diese Aufgabe zum Mounten des VMFS-Datenspeichers auf einem bestimmten Host oder mehreren Hosts verwenden.

Wenn Sie einen NFS- oder Virtual Volumes-Datenspeicher von allen Hosts unmounten, wird der Datenspeicher in der Bestandsliste nicht mehr angezeigt. Zum Mounten eines NFS- oder Virtual Volumes-Datenspeichers, der aus der Bestandsliste entfernt wurde, verwenden Sie den Assistenten „Neuer Datenspeicher“.

Ein beliebiger Datenspeicher, der auf einigen Hosts ungemountet wird, während er auf anderen gemountet ist, wird in der Bestandsliste als aktiv angezeigt.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher, der gemountet werden soll, und wählen Sie eine der folgenden Optionen aus:

- **Datenspeicher mounten**
- **Datenspeicher auf zusätzlichen Hosts mounten**

Von der Art des verwendeten Datenspeichers hängt ab, welche Optionen verfügbar sind.

3 Wählen Sie die Hosts, die auf den Datenspeicher zugreifen sollen, und klicken Sie auf **OK**.

4 Um alle Hosts aufzulisten, die den Datenspeicher gemeinsam nutzen, navigieren Sie zu dem Datenspeicher und klicken Sie auf die Registerkarte **Hosts**.

Entfernen von VMFS-Datenspeichern

Sie können jede Art von VMFS-Datenspeicher löschen, einschließlich Kopien, die Sie gemountet haben, ohne sie neu zu signieren. Beim Löschen eines Datenspeichers wird er zerstört und auf keinem Host mehr angezeigt, der davor Zugriff auf ihn hatte.

Hinweis Beim Löschvorgang für den Datenspeicher werden alle Dateien, die virtuellen Maschinen auf dem Datenspeicher zugeordnet sind, endgültig gelöscht. Obwohl Sie den Datenspeicher ohne Unmounten löschen können, empfiehlt es sich, zuerst den Datenspeicher zu unmounten.

Voraussetzungen

- Entfernen oder migrieren Sie alle virtuellen Maschinen aus dem Datenspeicher.
- Unmounten Sie den Datenspeicher aus allen Hosts.
- Deaktivieren Sie Speicher-DRS für den Datenspeicher.
- Deaktivieren Sie Storage I/O Control für den Datenspeicher.
- Stellen Sie sicher, dass der Datenspeicher nicht für vSphere HA-Taktsignale verwendet wird.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

2 Klicken Sie mit der rechten Maustaste auf den Datenspeicher, der entfernt werden soll, und wählen Sie dann **Datenspeicher löschen** aus.

3 Bestätigen Sie, dass Sie den Datenspeicher entfernen möchten.

Verwenden des Datenspeicherbrowsers

Verwenden Sie den Datenspeicherbrowser zum Verwalten des Inhalts Ihrer Datenspeicher. Sie können Ordner und Dateien durchsuchen, die im Datenspeicher gespeichert sind. Im Browser können Sie auch Dateien hochladen und Verwaltungsaufgaben für Ihre Dateien und Ordner durchführen.

Verfahren

1 Öffnen Sie den Datenspeicherbrowser.

   a Zeigen Sie den Datenspeicher in der Bestandsliste an.

   b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.

2 Untersuchen Sie den Inhalt des Datenspeichers, indem Sie zu vorhandenen Ordnern und Dateien navigieren.

3 Führen Sie Verwaltungsaufgaben mithilfe der entsprechenden Symbole und Optionen durch.

Symbole und Optionen	Beschreibungen
Dateien hochladen	Lädt eine Datei in den Datenspeicher hoch.
Ordner hochladen (nur im vSphere Client verfügbar)	Lädt einen Ordner in den Datenspeicher hoch.
Herunterladen	Lädt eine Datei aus dem Datenspeicher herunter.
Neuer Ordner	Erstellt einen Ordner im Datenspeicher.
Kopieren nach	Kopiert ausgewählte Ordner oder Dateien an einen neuen Speicherort, entweder im selben oder in einem anderen Datenspeicher.
Verschieben nach	Verschiebt ausgewählte Ordner oder Dateien an einen neuen Speicherort, entweder im selben oder in einem anderen Datenspeicher.
Umbenennen in	Benennt ausgewählte Dateien um.
Löschen	Löscht ausgewählte Dateien oder Ordner.
Vergrößern	Konvertiert eine ausgewählte virtuelle Festplatte vom Thin-Format in das Thick-Format. Diese Option gilt nur für per Thin Provisioning bereitgestellte Festplatten.

Hochladen von Dateien oder Ordnern in Datenspeicher

Verwenden Sie den Datenspeicher-Dateibrowser zum Hochladen von Dateien in Datenspeicher auf dem ESXi-Host. Wenn Sie vSphere Client verwenden, können Sie auch Ordner hochladen.

Zusätzlich zur herkömmlichen Verwendung als Speicher für VM-Dateien können zu virtuellen Maschinen gehörende Daten oder Dateien in Datenspeichern gespeichert werden. Beispiel: Sie können ISO-Images von Betriebssystemen von einem lokalen Computer in einen Datenspeicher auf dem Host hochladen. Anschließend können Sie diese Images zum Installieren von Gastbetriebssystemen auf den neuen virtuellen Maschinen verwenden.

Hinweis Sie können keine Dateien direkt in die Virtual Volumes-Datenspeicher hochladen. Sie müssen zuerst einen Ordner im Virtual Volumes-Datenspeicher erstellen und dann die Dateien in den Ordner hochladen. Die erstellten Ordner in Virtual Volumes-Datenspeichern für Blockspeicher haben eine begrenzte Speicherkapazität von 4 GB. Virtual Volumes-Datenspeicher unterstützen direktes Hochladen von Ordnern.

Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1 Öffnen Sie den Datenspeicherbrowser.
   a Zeigen Sie den Datenspeicher in der Bestandsliste an.
   b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.
2 (Optional) Erstellen Sie einen Ordner zum Speichern der Datei oder des Ordners.
3 Laden Sie die Datei oder den Ordner hoch.

Option	Beschreibung
Datei hochladen	a Wählen Sie den Zielordner aus und klicken Sie auf **Dateien hochladen**. b Suchen Sie das Element zum Hochladen auf dem lokalen Computer und klicken Sie auf **Öffnen**.
Hochladen eines Ordners (nur in vSphere Client verfügbar)	a Wählen Sie den Datenspeicher oder den Zielordner aus und klicken Sie auf **Ordner hochladen**. b Suchen Sie das Element zum Hochladen auf dem lokalen Computer und klicken Sie auf **OK**.

4 Aktualisieren Sie den Dateibrowser des Datenspeichers, damit die hochgeladenen Dateien oder Ordner in der Liste angezeigt werden.

Nächste Schritte

Möglicherweise treten Probleme auf, wenn Sie eine OVF-Vorlage bereitstellen, die Sie zuvor exportiert und dann in einen Datenspeicher hochgeladen haben. Einzelheiten dazu und eine Problemumgehung finden Sie im VMware-Knowledgebase-Artikel 2117310.

Herunterladen von Dateien aus Datenspeichern

Laden Sie mit dem Datenspeicherbrowser Dateien aus dem verfügbaren Datenspeicher auf den ESXi-Host auf den lokalen Computer herunter.

Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Öffnen Sie den Datenspeicherbrowser.
   a. Zeigen Sie den Datenspeicher in der Bestandsliste an.
   b. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.
2. Navigieren Sie zu der Datei, die Sie herunterladen möchten, und klicken Sie auf **Herunterladen**.
3. Befolgen Sie die Anweisungen zum Speichern der Datei auf dem lokalen Computer.

Verschieben oder Kopieren von Datenspeicherordnern oder -dateien

Verwenden Sie den Datenspeicherbrowser, um Ordner oder Dateien an einen neuen Speicherort im selben oder einem anderen Datenspeicher zu verschieben oder zu kopieren.

Hinweis Virtuelle Festplattendateien werden ohne Formatkonvertierung verschoben oder kopiert. Wenn Sie eine virtuelle Festplatte in einen Datenspeicher verschieben, der zu einem anderen Host als dem Quellhost gehört, müssen Sie die virtuelle Festplatte möglicherweise konvertieren. Andernfalls können Sie die Festplatte möglicherweise nicht verwenden.

VM-Dateien können nicht zwischen vCenter Server-Systemen kopiert werden.

Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1. Öffnen Sie den Datenspeicherbrowser.
   a. Zeigen Sie den Datenspeicher in der Bestandsliste an.
   b. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.
2. Navigieren Sie zu einem Objekt, das Sie verschieben oder kopieren möchten, entweder ein Ordner oder eine Datei.
3. Wählen Sie das Objekt aus und klicken Sie auf **Verschieben nach** oder **Kopieren nach**.
4. Geben Sie den Zielort an.

5 (Optional) Wählen Sie **Überschreiben von Dateien und Ordnern mit passenden Namen am Zielort** aus.

6 Klicken Sie auf **OK**.

Umbenennen von Datenspeicherdateien

Verwenden Sie den Datenspeicherbrowser, um Dateien umzubenennen.

Voraussetzungen

Erforderliche Berechtigung: **Datenspeicher.Datenspeicher durchsuchen**

Verfahren

1 Öffnen Sie den Datenspeicherbrowser.

   a Zeigen Sie den Datenspeicher in der Bestandsliste an.

   b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.

2 Navigieren Sie zu einer Datei, die Sie umbenennen möchten.

3 Wählen Sie die Datei aus und klicken Sie auf **Umbenennen in**.

4 Geben Sie den neuen Namen an und klicken Sie auf **OK**.

Vergrößern virtueller Thin-Festplatten

Virtuelle Festplatten, die Sie im Thin-Format erstellt haben, können in das Thick-Format konvertiert werden.

Sie können mit dem Datenspeicherbrowser die virtuelle Festplatte im Thin-Format vergrößern.

Voraussetzungen

- Stellen Sie sicher, dass der Datenspeicher, in dem sich die virtuelle Maschine befindet, über ausreichend Speicherplatz verfügt.
- Stellen Sie zudem sicher, dass die virtuelle Festplatte das Thin-Format aufweist.
- Entfernen Sie Snapshots.
- Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie im vSphere Client zum Ordner der virtuellen Festplatte, die Sie vergrößern möchten.

   a Navigieren Sie zu der virtuellen Maschine.

   b Klicken Sie auf die Registerkarte **Datenspeicher**.

   Der Datenspeicher, in dem die Dateien der virtuellen Maschine gespeichert sind, wird angezeigt.

   c Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.

   Der Datenspeicherbrowser zeigt den Inhalt des Datenspeichers an.

2 Erweitern Sie den Ordner der virtuellen Maschine und navigieren Sie zu der Datei der virtuellen Festplatte, die Sie konvertieren möchten.

   Die Datei hat die Erweiterung `.vmdk` und ist durch das Symbol für virtuelle Festplatten () gekennzeichnet.

3 Wählen Sie die virtuelle Festplattendatei aus und klicken Sie auf **Vergrößern**.

   Hinweis Die Option ist möglicherweise nicht verfügbar, wenn die virtuelle Festplatte das Thick-Format aufweist oder wenn die virtuelle Maschine ausgeführt wird.

Ergebnisse

Die vergrößerte virtuelle Festplatte belegt den ganzen Datenspeicherplatz, der ursprünglich für sie bereitgestellt wurde.

Ausschalten von Speicherfiltern

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, verwendet vCenter Server Standardspeicherschutzfilter. Die Filter helfen Ihnen Speicherschäden zu vermeiden, indem nur die Speichergeräte abgerufen werden, die für einen bestimmten Vorgang verwendet werden können. Ungeeignete Geräte werden nicht zur Auswahl angezeigt. Sie können die Filter deaktivieren, um alle Geräte anzuzeigen.

Voraussetzungen

Wenden Sie sich an den VMware Support, bevor Sie die Gerätefilter ändern.

Verfahren

1 Navigieren Sie zur vCenter Server-Instanz.

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

3 Klicken Sie unter **Einstellungen** auf **Erweiterte Einstellungen** und dann auf **EINSTELLUNGEN BEARBEITEN**.

4 Geben Sie den Filter an, der deaktiviert werden soll.

Geben Sie in den Textfeldern **Name** und **Wert** am unteren Rand der Seite entsprechende Informationen ein.

Name	Wert
config.vpxd.filter.vmfsFilter	Falsch
config.vpxd.filter.rdmFilter	Falsch
config.vpxd.filter.sameHostsAndTransportsFilter	Falsch
config.vpxd.filter.hostRescanFilter	Falsch **Hinweis** Wenn Sie diesen Filter deaktivieren, führen Ihre Hosts weiterhin eine erneute Prüfung durch, sobald Sie für einen Host oder Cluster eine neue LUN bereitstellen.

5 Klicken Sie auf **HINZUFÜGEN** und dann auf **SPEICHERN**, um Ihre Änderungen zu speichern.

Es ist nicht erforderlich, dass Sie das vCenter Server-System neu starten.

Speicherfilterung

vCenter Server stellt Speicherfilter zur Verfügung, um eine Beschädigung von Speichergeräten oder Beeinträchtigung der Leistung zu vermeiden, die durch eine nicht unterstützte Nutzung von Speichergeräten verursacht werden kann. Diese Filter sind standardmäßig verfügbar.

Tabelle 17-7. Speicherfilter

Filtername	Beschreibung
config.vpxd.filter.vmfsFilter (VMFS-Filter)	Filtert Speichergeräte oder LUNs heraus, die bereits von einem VMFS-Datenspeicher auf einem von vCenter Server verwalteten Host verwendet werden. Die LUNs werden nicht als Kandidaten angezeigt, die mit einem anderen VMFS-Datenspeicher formatiert oder als RDM verwendet werden sollen.
config.vpxd.filter.rdmFilter (RDM-Filter)	Filtert LUNs heraus, auf die bereits von einer RDM-Datei auf einem von vCenter Server verwalteten Host verwiesen wird. Die LUNs werden nicht als Kandidaten angezeigt, die mit VMFS formatiert oder von einer anderen RDM-Datei verwendet werden sollen. Damit Ihre virtuellen Maschinen auf dieselbe LUN zugreifen können, müssen die virtuellen Maschinen dieselbe RDM-Zuordnungsdatei nutzen. Informationen über diesen Konfigurationstyp finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Tabelle 17-7. Speicherfilter (Fortsetzung)

Filtername	Beschreibung
config.vpxd.filter.sameHostsAndTransportsFilter (Filter für dieselben Hosts und Transporte)	Filtert LUNs heraus, die aufgrund einer Inkompatibilität des Hosts oder des Speichertyps nicht zur Verwendung als VMFS-Datenspeichererweiterungen geeignet sind. Verhindert, dass Sie die folgenden LUNs als Erweiterungen hinzufügen: ■ LUNs, die nicht für alle Hosts verfügbar gemacht werden, die den ursprünglichen VMFS-Datenspeicher gemeinsam nutzen. ■ LUNs, die einen Speichertyp nutzen, der von demjenigen abweicht, den der ursprüngliche VMFS-Datenspeicher verwendet. Sie können beispielsweise keine Fibre Channel-Erweiterung zu einem VMFS-Datenspeicher auf einem lokalen Speichergerät hinzufügen.
config.vpxd.filter.hostRescanFilter (Filter für das erneute Prüfen eines Hosts)	Führt eine automatische erneute Prüfung und Aktualisierung von VMFS-Datenspeichern durch, nachdem Sie Vorgänge zur Verwaltung von Datenspeichern durchgeführt haben. Der Filter hilft bei der Bereitstellung einer einheitlichen Ansicht aller VMFS-Datenspeicher auf allen von vCenter Server verwalteten Hosts. **Hinweis** Wenn Sie eine neue LUN für einen Host oder Cluster bereitstellen, führt der Host automatisch eine erneute Prüfung durch, unabhängig davon, ob der Filter zum erneuten Prüfen des Hosts aktiviert oder deaktiviert ist.

Dynamische Festplattenspiegelung einrichten

In der Regel können Sie LUN Manager-Software nicht auf virtuellen Maschinen zum Spiegeln von virtuellen Festplatten verwenden. Wenn Ihre virtuellen Microsoft Windows-Maschinen jedoch Unterstützung für dynamische Festplatten bieten, können Sie Festplatten über zwei SAN LUNs hinweg spiegeln. Das Spiegeln hilft Ihnen, virtuelle Maschinen vor einem ungeplanten Speichergeräteausfall zu schützen.

Voraussetzungen

- Verwenden Sie eine virtuelle Windows-Maschine, die dynamische Festplatten unterstützt.
- Notwendige Berechtigung: **Virtuelle Maschine. Konfiguration. Einstellungen**.

Verfahren

1. Erstellen Sie eine virtuelle Maschine mit zwei virtuellen Festplatten.

   Platzieren Sie die Festplatten auf verschiedene Datenspeicher.
2. Melden Sie sich an Ihre virtuelle Maschine an und konfigurieren Sie die Festplatten als dynamisch gespiegelte Festplatten.

   Weitere Informationen finden Sie in der Microsoft-Dokumentation.
3. Schalten Sie die virtuelle Maschine nach der Synchronisierung der Festplatten aus.

4 Ändern Sie die Einstellungen für die virtuelle Maschine, um die Verwendung der dynamischen Festplattenspiegelung zu aktivieren.

a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

b Klicken Sie auf die Registerkarte **VM-Optionen**, und erweitern Sie das Menü **Erweitert**.

c Klicken Sie auf **Konfiguration bearbeiten** neben den Konfigurationsparametern.

d Klicken Sie auf **Konfigurationsparameter hinzufügen** und fügen Sie folgende Parameter hinzu:

Name	Wert
`scsi#.returnNoConnectDuringAPD`	True
`scsi#.returnBusyOnNoConnectStatus`	Falsch

e Wenn Sie ESXi-Version 6.7 oder höher verwenden, fügen Sie einen zusätzlichen Parameter für jede virtuelle Festplatte hinzu, die Teil der Software-RAID-1-Konfiguration ist.

Der Parameter verhindert E/A-Fehler bei Gastbetriebssystemen, wenn ein Speichergerät ausfällt.

Name	Wert
`scsi#:1.passthruTransientErrors`	True
`scsi#:2.passthruTransientErrors`	True

f Klicken Sie auf **OK**.

Erfassen von Diagnoseinformationen für ESXi-Hosts auf einem VMFS-Datenspeicher

Während eines Hostfehlers muss ESXi in der Lage sein, Diagnoseinformationen an einem vorkonfigurierten Speicherort zur Diagnose und für technischen Support zu speichern.

In der Regel wird eine Partition zum Erfassen von Diagnoseinformationen, auch als Core-Dump bezeichnet, auf einem lokalen Speichergerät während der ESXi-Installation erstellt. Sie können ESXi Dump Collector auch für das Beibehalten von Core-Dumps auf einem Netzwerkserver konfigurieren. Informationen zum Einrichten von ESXi Dump Collector finden Sie in der Dokumentation *Installation und Einrichtung von VMware ESXi*.

Eine weitere Möglichkeit besteht darin, eine Datei in einem VMFS-Datenspeicher zu verwenden, um die Diagnoseinformationen zu erfassen.

- Einrichten einer Datei als Core-Dump-Speicherort

  Wenn Ihre verfügbare Core-Dump-Partition nicht groß genug ist, können Sie ESXi so konfigurieren, dass eine Datei auf einem VMFS-Datenspeicher für Diagnoseinformationen verwendet wird.

- Deaktivieren und Löschen einer Core-Dump-Datei

  Deaktivieren Sie eine konfigurierte Core-Dump-Datei und entfernen Sie sie bei Bedarf aus dem VMFS-Datenspeicher.

Einrichten einer Datei als Core-Dump-Speicherort

Wenn Ihre verfügbare Core-Dump-Partition nicht groß genug ist, können Sie ESXi so konfigurieren, dass eine Datei auf einem VMFS-Datenspeicher für Diagnoseinformationen verwendet wird.

Hinweis VMFS-Datenspeicher auf Software-iSCSI unterstützen keine Core-Dump-Dateien.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Erstellen Sie eine Core-Dump-Datei eines VMFS-Datenspeichers durch Ausführen des folgenden Befehls:

`esxcli system coredump file add`

Der Befehl verfügt über die folgenden Optionen, die jedoch nicht erforderlich sind und ausgelassen werden können:

Option	Beschreibung
`--auto | -a`	Erstellt automatisch eine Datei, wenn keine gefunden wurde.
`--datastore | -d` ***`Datenspeicher_UUID oder Datenspeichername`***	Gibt den Datenspeicher für die Dump-Datei an. Wenn Sie keine Angabe machen, wird ein Datenspeicher mit ausreichender Größe ausgewählt.
`--enable | -e`	Aktiviert die Diagnosedatei nach der Erstellung.
`--file | -f` ***`Dateiname`***	Gibt den Dateinamen der Dump-Datei an. Wenn Sie keine Angabe machen, wird ein eindeutiger Name für die Datei erstellt.
`--size |-s` ***`Dateigröße_MB`***	Legt die Größe der Dump-Datei in MB fest. Wenn Sie keine Angabe machen, wird eine Datei mit einer Größe erstellt, die dem im Host vorhandenen Arbeitsspeicher entspricht.

2 Stellen Sie sicher, dass die Datei erstellt wurde:

`esxcli system coredump file list`

Es wird eine Ausgabe ähnlich der folgenden angezeigt:

```
Path                                          Active Configured Size
--------------------------------------------- ------ ---------- ---------
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile false  false      104857600
```

3 Aktivieren Sie die Core-Dump-Datei für den Host:

esxcli system coredump file set

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
--enable |-e	Aktiviert oder deaktiviert die Dump-Datei. Diese Option kann beim Aufheben der Konfiguration der Dump-Datei nicht angegeben werden.
--path | -p	Der Pfad der zu verwendenden Core-Dump-Datei. Die Datei muss vorab zugeteilt sein.
--smart | -s	Dieses Flag kann nur zusammen mit **--enable | -e=true** verwendet werden. Es bewirkt, dass die Datei mithilfe des intelligenten Auswahlalgorithmus ausgewählt wird. Beispiel: **esxcli system coredump file set --smart --enable true**
--unconfigure | -u	Hebt die Konfiguration der aktuellen VMFS-Dump-Datei auf.

4 Stellen Sie sicher, dass die Core-Dump-Datei aktiv und konfiguriert ist:

esxcli system coredump file list

Eine Ausgabe ähnlich der Folgenden zeigt an, dass die Core-Dump-Datei aktiv und konfiguriert ist:

```
Path                                            Active Configured Size
----------------------------------------------- ------ ---------- ---------
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile True   True       104857600
```

Nächste Schritte

Informationen zu anderen Befehlen, die Sie zum Verwalten der Core-Dump-Dateien verwenden können, finden Sie in der Dokumentation *ESXCLI – Referenz*.

Deaktivieren und Löschen einer Core-Dump-Datei

Deaktivieren Sie eine konfigurierte Core-Dump-Datei und entfernen Sie sie bei Bedarf aus dem VMFS-Datenspeicher.

Sie können die Core-Dump-Datei temporär deaktivieren. Wenn Sie nicht beabsichtigen, die deaktivierte Datei zu verwenden, können Sie sie aus dem VMFS-Datenspeicher entfernen. Zum Entfernen der nicht aktivierten Datei können Sie den Befehl `esxcli system coredump file remove` mit dem Parameter `--force | -F` verwenden.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Auflisten der Core-Dump-Dateien:

```
esxcli system coredump file list
```

2 Deaktivieren Sie die Core-Dump-Datei durch Ausführen des folgenden Befehls:

```
esxcli system coredump file set --unconfigure | -u
```

3 Entfernen Sie die Datei aus dem VMFS-Datenspeicher:

```
esxcli system coredump file remove --file | -f file_name
```

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
`--file | -f`	Gibt den Namen der zu entfernenden Dump-Datei an. Wenn Sie den Dateinamen nicht eingeben, entfernt der Befehl die konfigurierte Core-Dump-Datei.
`--force | -F`	Deaktiviert die zu entfernende Dump-Datei und hebt deren Konfiguration auf. Diese Option ist erforderlich, wenn die Datei nicht zuvor deaktiviert wurde und aktiv ist.

Ergebnisse

Die Core-Dump-Datei wird deaktiviert und aus dem VMFS-Datenspeicher entfernt.

Überprüfen der Metadatenkonsistenz mit VOMA

Verwenden Sie vSphere On-disk Metadata Analyzer (VOMA), um Metadatenbeschädigungen zu identifizieren und zu beheben, 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
("<Datastore_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 logische Volumes, die VMFS-Datenspeicher stützen, überprüft und behoben werden.

Mit VOMA können die folgenden Elemente überprüft und korrigiert werden.

Tabelle 17-8. VOMA-Funktionen

VOMA-Funktionen	Beschreibung
Metadatenprüfung und -korrektur	Beispiele für Metadatenprüfung und -korrektur umfassen unter anderem die folgenden: ■ Validierung des VMFS-Volume-Headers für grundlegende Metadatenkonsistenz. ■ Überprüfen der Konsistenz der VMFS-Ressourcendateien (Systemdatei). ■ Überprüfen des Pfadnamens und der Konnektivität aller Dateien.
Affinitäts-Metadatenprüfung und -korrektur	Um die Affinitätsüberprüfung für VMFS6 zu aktivieren, verwenden Sie die Option `-a|--affinityChk`. Nachfolgend sind einige Beispiele für die Affinitäts-Metadatenprüfung und -korrektur aufgeführt: ■ Affinitäts-Flags in Ressourcentypen und FS3_ResFileMetadata. ■ Validierung der Affinität-Flags in SFB RC Meta (FS3_ResourceClusterMDVMFS6). ■ Validierung aller Einträge in den affinityInfo-Einträgen in rcMeta von RC, einschließlich des Überlaufschlüssels, um sicherzustellen, dass keine ungültigen Einträge vorhanden sind. Fehlende Einträge werden gesucht.
Verzeichnisvalidierung	Mit VOMA können die folgenden Fehler erkannt und behoben werden: ■ Beschädigung des Verzeichnis-Hash-Blocks. ■ Beschädigung der Alloc-Zuordnung. ■ Beschädigungen der Link-Blöcke. ■ Beschädigungen der Verzeichniseintragsblöcke. Je nach Art der Beschädigung kann VOMA entweder nur die beschädigten Einträge korrigieren oder den Hash-Block, Alloc-Zuordnungsblöcke und Link-Blöcke vollständig rekonstruieren.
lost+found-Dateien	Während einer Dateisystemprüfung kann VOMA Dateien finden, die an keiner Stelle im Dateisystem referenziert werden. Diese verwaisten Dateien sind gültig und vollständig, verfügen aber über keinen Namen oder Verzeichniseintrag im System. Wenn VOMA während des Scanvorgangs verwaiste Dateien feststellt, erstellt es ein Verzeichnis mit dem Namen „lost+found“ im Stammverzeichnis des Volumes, um die verwaisten Dateien zu speichern. Die Namen der Dateien verwenden das `Dateiformat` *`Sequence-number`*.

Für das VOMA-Tool gibt es die folgenden Befehlsoptionen.

Tabelle 17-9. 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 die VMFS-Dateisysteme sowie die Dateisysteme überprüfen, die virtuelle Flash-Ressourcen unterstützen. Wenn Sie dieses Modul angeben, werden zudem Minimalüberprüfungen für LVM durchgeführt.
	`lvm`	Überprüft logische Volumes, die die VMFS-Datenspeicher unterstützen.
	`ptbl`	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.
	`fix`	Sucht und behebt Fehler.
	`dump`	Erfasst das Metadaten-Speicherabbild.
`-a|--affinityChk`	Enthält eine affinitätsbezogene Prüfung und Korrektur für VMFS6.	
`-d|--device`	Gibt das Gerät oder die Festplatte an, das bzw. die überprüft werden soll. Stellen Sie sicher, dass Sie den absoluten Pfad zur Gerätepartition angeben, die den VMFS-Datenspeicher stützt. Wenn sich der Datenspeicher über mehrere Geräte erstreckt, geben Sie die UUID des Head-Extent an. Beispielsweise `voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x` Wenn Sie den Befehl `-x|--extractDump` verwenden, geben Sie mehrere durch Kommata getrennte Gerätepfade mit einem Partitionsbezeichner ein. Die Anzahl der Gerätepfade, die Sie eingeben, entspricht der Anzahl der überspannten Geräte.	
`-b|--blockSize`	Geben Sie die Blockgröße der Festplatte an.	
`-s|--logfile`	Geben Sie den Pfad zur Protokolldatei für die Ausgabe der Ergebnisse an.	
`-x|--extractDump`	Extrahiert das erfasste Speicherabbild mithilfe von VOMA.	
`-D|--dumpfile`	Geben Sie die Speicherabbilddatei zum Speichern des erfassten Metadaten-Speicherabbilds an.	

Tabelle 17-9. VOMA-Befehlsoptionen (Fortsetzung)

Befehlsoption	Beschreibung
`-v|--version`	Zeigt die VOMA-Version an.
`-h|--help`	Zeigt einen Hilfetext zum VOMA-Befehl an.
`-Y`	Geben Sie an, dass Sie VOMA ausführen, ohne PE-Tabellen für die Adressauflösung zu verwenden.
`-Z| --file`	Geben Sie an, dass Sie VOMA auf extrahierten Gerätedateien ausführen.

Beispiel

Erfassen Sie das Metadaten-Speicherabbild von einem übergreifenden Volume:

voma -m vmfs -f dump -d *head_extent* -D *dump_filename*

Extrahiert das erfassten Speicherabbild zurück auf die Geräte eines übergreifenden Volumes:

voma -x *dump_filename* -d *head_extent,extent_2,extent_3...extent_n*

Verwenden von VOMA zum Überprüfen der Metadatenkonsistenz

Die folgende Aufgabe veranschaulicht die Überprüfung der VMFS-Metadatenkonsistenz mithilfe von VOMA. Mit VOMA können geringfügige Inkonsistenzprobleme für einen VMFS-Datenspeicher oder eine vFlash-Ressource überprüft und behoben werden. Führen Sie VOMA an der CLI eines ESXi-Hosts aus.

Voraussetzungen

Schalten Sie alle ausgeführten virtuellen Maschinen aus oder migrieren Sie sie in einen anderen Datenspeicher.

Verfahren

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

#esxcli storage vmfs extent list

Der Gerätename und die Partitionsspalten in der Ausgabe geben das Gerät an. Beispiel:

```
Volume Name  .....  Device Name                              Partition
1TB_VMFS6    .....  naa.xxxx                                    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.xxxx:x

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

```
XXXXXXXXXXXXXXXXXXXXXXX
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
```

Konfigurieren des Cachespeichers für VMFS-Zeigerblöcke

Zeigerblöcke, auch Dereferenzierungsblöcke genannt, sind Dateisystemressourcen, die Adressen für VMFS-Dateiblöcke enthalten. Wenn Sie eine `vmdk`-Datei auf einem ESXi-Host öffnen, werden die mit dieser Datei verbundenen Zeigerblöcke im Zeigerblock-Cache gespeichert. Die Größe des Zeigerblock-Caches ist ein konfigurierbarer Parameter.

Der Zeigerblock-Cache ist ein VMFS-unabhängiger Cache für den gesamten Host. Der Cache wird über alle Datenspeicher, die von demselben ESXi-Host genutzt werden, hinweg gemeinsam genutzt.

Die Größe des Zeigerblock-Caches wird durch `/VMFS3/MinAddressableSpaceTB` und `/VMFS3/MaxAddressableSpaceTB` kontrolliert. Sie können die minimale und maximale Größe auf jedem ESXi-Host konfigurieren.

/VMFS3/MinAddressableSpaceTB

Der Mindestwert ist die Mindestgröße des Arbeitsspeichers, die dem Zeigerblock-Cache vom System garantiert wird. So benötigt zum Beispiel 1 TB Speicherplatz für geöffnete Dateien etwa 4 MB Arbeitsspeicher. Der Standardwert ist 10 TB.

/VMFS3/MaxAddressableSpaceTB

Der Parameter definiert die Höchstmenge von Zeigerblöcken, die im Arbeitsspeicher gespeichert werden können. Der Standardwert ist 32 TB. Der Höchstwert ist 128 TB. In der Regel ist der Standardwert des Parameters `/VMFS3/MaxAddressableSpaceTB` ausreichend.

Mit zunehmender Größe der geöffneten VMDK-Dateien steigt allerdings auch die Anzahl der mit diesen Dateien verbundenen Zeigerblöcke. Verursacht dieser Anstieg Leistungsbeeinträchtigungen, so können Sie einfach den Höchstwert für den Parameter so festlegen, dass mehr Speicherplatz für den Zeigerblock-Cache bereitgestellt wird. Bestimmen Sie die maximale Größe des Zeigerblock-Caches anhand des Arbeitssatzes oder der erforderlichen Anzahl aktiver Zeigerblöcke.

Zeigerblock-Bereinigung

Der `/VMFS3/MaxAddressableSpaceTB`-Parameter steuert auch das Wachstum des Zeigerblock-Caches. Nähert sich die Größe des Zeigerblock-Caches der konfigurierten Maximalgröße an, wird ein Zeigerblock-Bereinigungsprozess eingeleitet. Der Mechanismus belässt aktive Zeigerblöcke, entfernt jedoch inaktive oder weniger ausgelastete Blöcke aus dem Cache, damit der Speicherplatz wiederverwendet werden kann.

Um die Werte für den Zeigerblock-Cache zu ändern, verwenden Sie das Dialogfeld **Erweiterte Systemeinstellungen** des vSphere Client oder den Befehl `esxcli system settings advanced set -o`.

Mit dem Befehl `esxcli storage vmfs pbcache` können Sie Informationen über die Größe des Zeigerblock-Cachespeichers und andere Statistiken erhalten. Diese Informationen helfen Ihnen dabei, die minimale und maximale Größe des Zeigerblock-Cachespeichers anzupassen, um maximale Leistung zu erzielen.

Abrufen von Informationen für den Cachespeicher für VMFS-Zeigerblöcke

Sie können Informationen über die Nutzung des Cachespeichers für VMFS-Zeigerblöcke abrufen. Dadurch erfahren Sie, wie viel Speicherplatz der Zeigerblock-Cachespeicher verbraucht. Zudem können Sie ermitteln, ob Sie die Mindest- oder Höchstgröße des Zeigerblock-Cachespeichers anpassen müssen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Mit dem folgenden Befehl können Sie Statistiken zum Zeigerblock-Cachespeicher abrufen oder zurücksetzen:

  ```
  esxcli storage vmfs pbcache
  ```

Option	Beschreibung
get	Ruft die Statistik des Cachespeichers für VMFS-Zeigerblöcke ab.
reset	Setzt die Statistik des Cachespeichers für VMFS-Zeigerblöcke zurück.

Beispiel: Abrufen von Statistiken für den Zeigerblock-Cachespeicher

```
#esxcli storage vmfs pbcache get
   Cache Capacity Miss Ratio: 0 %
   Cache Size: 0 MiB
   Cache Size Max: 132 MiB
   Cache Usage: 0 %
   Cache Working Set: 0 TiB
```

```
   Cache Working Set Max: 32 TiB
   Vmfs Heap Overhead: 0 KiB
   Vmfs Heap Size: 23 MiB
   Vmfs Heap Size Max: 256 MiB
```

Ändern der Größe des Zeigerblock-Cache

Sie können die Mindest- und Höchstgröße des Zeigerblock-Caches anpassen.

Vorsicht Das Ändern der erweiterten Optionen wird nicht unterstützt. In der Regel werden mit den Standardeinstellungen bereits beste Ergebnisse erzielt. Ändern Sie die erweiterten Optionen nur dann, wenn Sie spezifische Anweisungen hierzu vom technischen Support von VMware erhalten oder einem Knowledgebase-Artikel entnehmen.

Verfahren

1. Navigieren Sie zum Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Wählen Sie unter „Erweiterte Systemeinstellungen“ den entsprechenden Eintrag.

Option	Beschreibung
VMFS3.MinAddressableSpaceTB	Von VMFS-Cache garantiert unterstützte minimale Größe aller geöffneten Dateien.
VMFS3.MaxAddressableSpaceTB	Von VMFS-Cache unterstützte maximale Größe aller geöffneten Dateien, bevor die Bereinigung startet.

5. Klicken Sie auf **Bearbeiten** und ändern Sie den Wert.
6. Klicken Sie auf **OK**.

Beispiel: Verwenden des Befehls „Esxcli“ zum Ändern des Zeigerblock-Caches

Sie können die Größe des Zeigerblock-Caches auch mithilfe von `esxcli system settings advanced set -o` ändern. Das folgende Beispiel beschreibt, wie Sie die Größe auf den Maximalwert von 128 TB festlegen können.

1. Um den Wert von `/VMFS3/MaxAddressableSpaceTB` auf 128 TB zu erhöhen, geben Sie den folgenden Befehl ein:

   ```
   # esxcli system settings advanced set -i 128 -o /VMFS3/
   MaxAddressableSpaceTB
   ```

2. Um zu bestätigen, dass der Wert korrekt festgelegt wurde, geben Sie diesen Befehl ein:

   ```
   # esxcli system settings advanced list -o /VMFS3/MaxAddressableSpaceTB
   ```

Grundlegende Informationen zu Multipathing und Failover

18

ESXi unterstützt Multipathing, um eine dauerhafte Verbindung zwischen einem Host und seinem Speicher aufrechtzuerhalten. Mithilfe von Multipathing können Sie mehrere physische Pfade zur Übertragung von Daten zwischen dem Host und einem externen Speichergerät verwenden.

Beim Ausfall eines Elements im SAN-Netzwerk, z. B. eines Adaptera, Switches oder Kabels, kann ESXi ein Failover auf einen anderen funktionsfähigen physischen Pfad durchführen. Der Prozess des Wechselns zu einem anderen Pfad, um fehlgeschlagene Komponenten zu vermeiden, wird als Pfad-Failover bezeichnet.

Neben dem Pfad-Failover bietet Multipathing Lastausgleich. Lastausgleich ist der Vorgang zum Aufteilen der E/A-Lasten auf mehrere physische Pfade. Mit diesem Verfahren können potenzielle Engpässe reduziert oder vermieden werden.

Hinweis Während eines Failovers kann es bei virtuellen Maschinen zu einer E/A-Verzögerung von bis zu 60 Sekunden kommen. Mit diesen Verzögerungen kann das SAN nach Topologieänderungen seine Konfiguration stabilisieren. Die E/A-Verzögerungen sind möglicherweise auf Aktiv/Passiv-Arrays länger und auf Aktiv-Aktiv-Arrays kürzer.

Dieses Kapitel enthält die folgenden Themen:

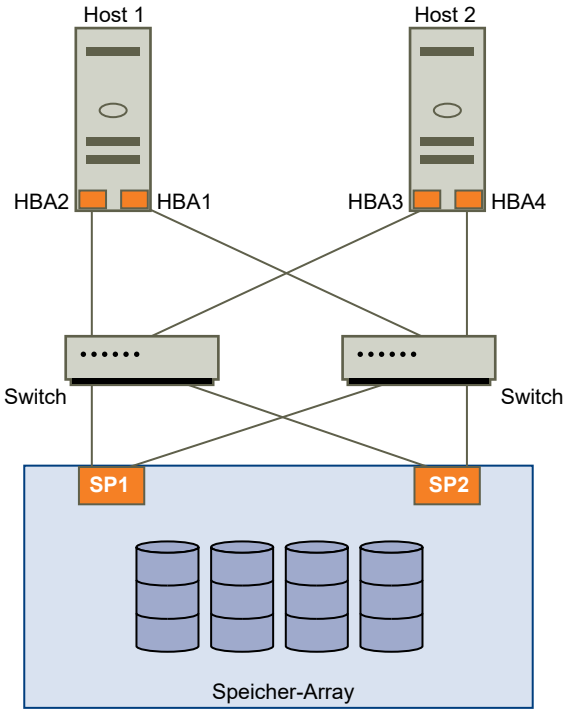
Failover mit Fibre-Channel

Zur Unterstützung von Multipathing verfügt Ihr Host normalerweise über zwei oder mehrere HBAs. Diese Konfiguration ergänzt die SAN-Multipathing-Konfiguration. In der Regel stellt SAN-

Multipathing mindestens einen Switch im SAN-Fabric und mindestens einen Speicherprozessor im Speicher-Array-Gerät selbst bereit.

In der folgenden Abbildung wird dargestellt, wie jeder Server über mehrere physische Pfade mit dem Speichergerät verbunden ist. Wenn zum Beispiel HBA1 oder die Verbindung zwischen HBA1 und dem FC-Switch ausfällt, übernimmt HBA2 und stellt die Verbindung zur Verfügung. Der Prozess, in dem ein HBA für einen anderen HBA einspringt, wird als HBA-Failover bezeichnet.

Abbildung 18-1. Multipathing und Failover mit Fibre-Channel



Wenn SP1 oder die Verbindung zwischen SP1 und den Switches ausfällt, übernimmt SP2. SP2 stellt die Verbindung zwischen dem Switch und dem Speichergerät bereit. Dieser Vorgang wird SP-Failover genannt. VMware ESXi unterstützt sowohl HBA- als auch SP-Failover.

Hostbasiertes Failover mit iSCSI

Wenn Sie Ihren ESXi-Host für Multipathing und Failover einrichten, können Sie mehrere iSCSI-HBAs verwenden oder mehrere Netzwerkkarten mit dem Software-iSCSI-Adapter kombinieren.

Weitere Informationen über verschiedene iSCSI-Adaptertypen finden Sie unter iSCSI-Initiatoren.

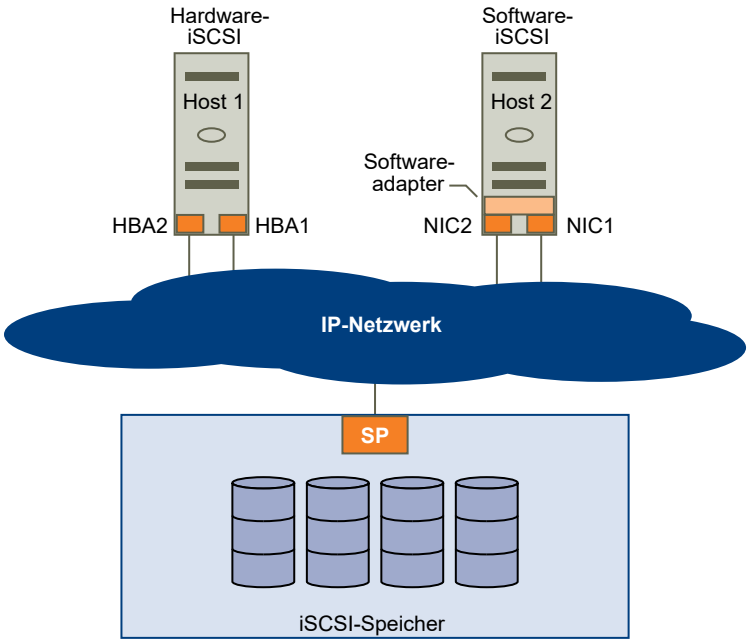
Bei der Verwendung von Multipathing muss Folgendes beachtet werden.

- ESXi unterstützt kein Multipathing, wenn Sie einen unabhängigen Hardwareadapter auf demselben Host mit Software-iSCSI- oder abhängigen iSCSI-Adaptern kombinieren.
- Multipathing zwischen Software- und abhängigen Adaptern auf demselben Host wird unterstützt.

- Sie können auf unterschiedlichen Hosts sowohl abhängige als auch unabhängige Adapter kombinieren.

Die folgende Abbildung zeigt Multipathing-Setups, die mit verschiedenen Typen von iSCSI-Initiatoren möglich sind.

Abbildung 18-2. Hostbasiertes Pfad-Failover



Hardware-iSCSI und Failover

Mit der Hardware-iSCSI sind auf dem Host in der Regel zwei oder mehr Hardware-iSCSI-Adapter vorhanden. Der Host verwendet die Adapter, um das Speichersystem über einen oder mehrere Switches zu erreichen. Alternativ könnte das Setup auch einen Adapter und zwei Speicherprozessoren umfassen, sodass der Adapter andere Pfade verwenden kann, um das Speichersystem zu erreichen.

In der Abbildung hat Host1 zwei Hardware-iSCSI-Adapter, HBA1 und HBA2, die zwei physische Pfade zum Speichersystem zur Verfügung stellen. Multipathing-Plug-Ins auf Ihrem Host (egal ob VMkernel NMP oder Drittanbieter-MPPs) haben standardmäßig Zugriff auf die Pfade. Die Plug-Ins können den Systemzustand der einzelnen physischen Pfade überwachen. Wenn beispielsweise HBA1 oder die Verknüpfung zwischen HBA1 und dem Netzwerk fehlschlägt, können Mehrfachpfad-Plug-Ins den Pfad auf HBA2 wechseln.

Software-iSCSI und Failover

Mit Software-iSCSI können Sie, wie bei Host 2 der Abbildung dargestellt, mehrere Netzwerkkarten verwenden, die Failover- und Lastausgleichsfunktionen für iSCSI-Verbindungen bereitstellen.

Multipathing-Plug-Ins haben keinen direkten Zugriff auf die physischen Netzwerkkarten auf Ihrem Host. Für dieses Setup müssen Sie daher jede einzelne physische Netzwerkkarte mit einem separaten VMkernel-Port verbinden. Danach verbinden Sie mithilfe einer Port-Bindungstechnik alle VMkernel-Ports mit dem Software-iSCSI-Initiator. Jeder VMkernel-Port, der mit einer separaten NIC verbunden ist, erhält einen anderen Pfad, der vom iSCSI-Speicherstapel und dessen speicherfähigen Multipathing-Plug-Ins verwendet werden kann.

Informationen zur Konfiguration von Multipathing für Software-iSCSI finden Sie unter Einrichten eines Netzwerks für iSCSI und iSER.

Array-basiertes Failover mit iSCSI

Einige iSCSI-Speichersysteme verwalten die Pfadnutzung ihrer Ports automatisch und für ESXi transparent.

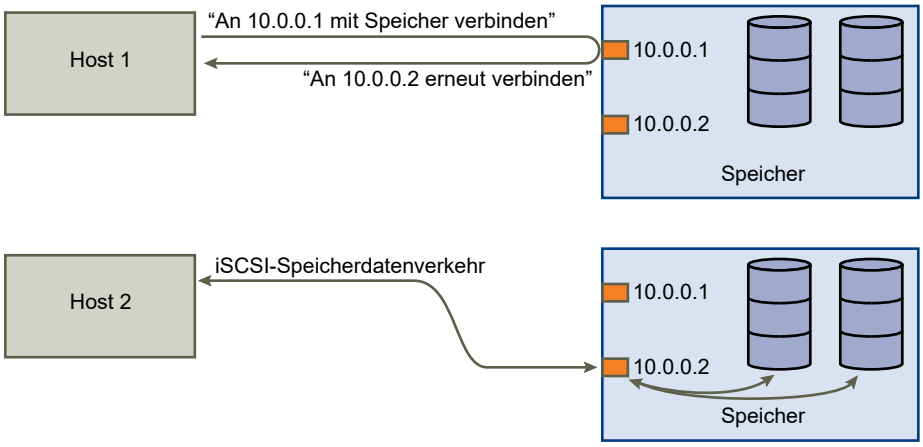
Wenn eines dieser Speichersysteme verwendet wird, erkennt der Host mehrere Ports im Speicher nicht und kann den Speicherport, mit dem er verbunden wird, nicht selbst wählen. Diese Systeme verfügen über eine einzelne virtuelle Portadresse, die der Host für die Anfangskommunikation nutzt. Während dieser Anfangskommunikation kann das Speichersystem den Host weiterleiten, sodass er mit einem anderen Port im Speichersystem kommuniziert. Die iSCSI-Initiatoren im Host befolgen diese Anforderung einer erneuten Verbindung und stellen dann eine Verbindung mit einem anderen Port im System her. Das Speichersystem nutzt diese Technik, um die Datenlast auf mehrere verfügbare Ports zu verteilen.

Falls der ESXi-Host die Verbindung zu einem dieser Ports verliert, versucht er automatisch, wieder eine Verbindung mit dem virtuellen Port des Speichersystems herzustellen und sollte an einen aktiven, nutzbaren Port weitergeleitet werden. Dieses Wiederverbinden und Umleiten erfolgt schnell und führt in der Regel nicht zu einer Unterbrechung bei der Ausführung der virtuellen Maschinen. Diese Speichersysteme können auch anfordern, dass iSCSI-Initiatoren wieder mit dem System verbunden werden, um den Speicherport zu ändern, mit dem sie verbunden sind. Dadurch wird eine möglichst effektive Nutzung mehrerer Ports gewährleistet.

Die Abbildung „Portweiterleitung“ zeigt ein Beispiel für die Portweiterleitung. Der Host versucht, eine Verbindung zum virtuellen Port 10.0.0.1 herzustellen. Das Speichersystem leitet diese Anforderung an den Port 10.0.0.2 weiter. Der Host stellt eine Verbindung mit dem Port 10.0.0.2 her und verwendet diesen Port für die E/A-Kommunikation.

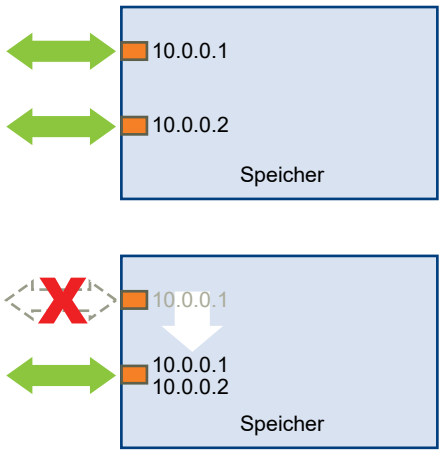
Hinweis Das Speichersystem leitet Verbindungen nicht immer weiter. Der Port 10.0.0.1 kann auch für Datenverkehr verwendet werden.

Abbildung 18-3. Portweiterleitung



Falls der Port im Speichersystem, der als virtueller Port fungiert, nicht mehr verfügbar ist, weist das Speichersystem die Adresse des virtuellen Ports einem anderen Port im System zu. Die Abbildung „Erneute Portzuweisung“ zeigt ein Beispiel für diese Art der erneuten Zuweisung von Ports. In diesem Fall ist der virtuelle Port 10.0.0.1 nicht mehr verfügbar, und das Speichersystem weist die IP-Adresse des virtuellen Ports einem anderen Port zu. Der zweite Port antwortet an beiden Adressen.

Abbildung 18-4. Erneute Portzuweisung



Bei dieser Art von Array-basiertem Failover sind nur dann mehrere Pfade zum Speicher möglich, wenn mehrere Ports im ESXi-Host verwendet werden. Dies sind Pfade vom Typ „Aktiv/Aktiv“. Weitere Informationen finden Sie unter iSCSI-Sitzungsverwaltung.

Pfad-Failover und virtuelle Maschinen

Ein Pfad-Failover erfolgt, wenn der aktive Pfad einer LUN geändert wurde. In der Regel tritt das Pfad-Failover infolge des Ausfalls einer SAN-Komponente im aktuellen Pfad auf.

Wenn ein Pfad ausfällt, wird Storage I/O für 30 bis 60 Sekunden angehalten, bis Ihr Host ermittelt hat, dass der Link nicht verfügbar ist, und das Failover durchführt. Beim Versuch, den Host, seine Speichergeräte oder seine Adapter anzuzeigen, hat es möglicherweise den Anschein, als sei der Vorgang angehalten worden. Es scheint, als ob virtuelle Maschinen mit ihren auf dem SAN installierten Festplatten nicht mehr reagieren. Nach dem Failover wird die Ein-/Ausgabe normal fortgesetzt und die virtuellen Maschinen laufen wieder weiter.

Wenn Failover sehr lange dauern, unterbricht eine virtuelle Windows-Maschine möglicherweise die Ein-/Ausgabe. Um dies zu verhindern, setzen Sie den Datenträger-Zeitüberschreitungswert für die virtuelle Windows-Maschine auf mindestens 60 Sekunden.

Festlegen der Zeitüberschreitung bei Windows-Gastbetriebssystemen

Um Unterbrechungen während eines Pfad-Failovers zu vermeiden, erhöhen Sie den Standard-Zeitüberschreitungswert für Festplatten auf einem Windows-Gastbetriebssystem.

Dieses Verfahren erläutert, wie der Zeitüberschreitungswert mithilfe der Windows-Registrierung geändert wird.

Voraussetzungen

Sichern Sie die Windows-Registrierung.

Verfahren

1. Wählen Sie**Start > Ausführen**.
2. Geben Sie **`regedit.exe`** ein und klicken Sie auf **OK**.
3. Doppelklicken Sie in der Hierarchieansicht auf der linken Seite auf **HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > Disk**.
4. Doppelklicken Sie auf **TimeOutValue**.
5. Setzen Sie den Datenwert auf 0x3c (hexadezimal) oder 60 (dezimal) und klicken Sie auf **OK**.

   Nach dem Durchführen dieser Änderung wartet Windows mindestens 60 Sekunden darauf, dass die verzögerten Festplattenoperationen abgeschlossen werden, bevor ein Fehler generiert wird.
6. Starten Sie das Gastbetriebssystem neu, damit die Änderung wirksam wird.

Pluggable Storage Architecture (PSA) und Pfadverwaltung

Dieses Thema dient als Einführung der Schlüsselkonzepte hinter dem ESXi-Speicher-Multipathing.

Pluggable Storage Architecture (PSA)

Zur Verwaltung von Multipathing verwendet ESXi eine spezielle VMkernel-Schicht: die Architektur des im laufenden Betrieb austauschbaren Speichers (Pluggable Storage Architecture, PSA). PSA ist ein offenes und modulares Framework, das verschiedene

für Multipathing-Vorgänge verantwortliche Softwaremodule koordiniert. Diese Module umfassen von VMware bereitgestellte generische Multipathing-Module (NMP und HPP) sowie Drittanbieter-MPPs.

Natives Multipathing-Plug-In (NMP)

Das NMP ist das VMkernel-Multipathing-Modul, das ESXi standardmäßig bereitstellt. Das NMP verbindet physische Pfade mit einem bestimmten Speichergerät und bietet einen standardmäßigen Pfadauswahlalgorithmus basierend auf dem Array-Typ. Das NMP ist erweiterbar und verwaltet zusätzliche Untermodule, die als Pfadauswahlrichtlinien (Path Selection Policies, PSPs) und Speicher-Array-Typ-Richtlinien (Storage Array Type Policies, SATPs) bezeichnet werden. PSPs und SATPs können von VMware oder von einem Drittanbieter bereitgestellt werden.

Pfadauswahl-Plug-Ins (Path Selection Plug-ins, PSPs)

Die PSPs sind Untermodule von VMware NMP. PSPs sind verantwortlich für die Auswahl eines physischen Pfads für E/A-Anforderungen.

Speicher-Array-Typ-Plug-Ins (Storage Array Type Plug-ins, SATPs)

Die SATPs sind Untermodule von VMware NMP. SATPs sind verantwortlich für Array-spezifische Vorgänge. Das SATP kann den Status eines bestimmten Array-spezifischen Pfads ermitteln, eine Pfadaktivierung durchführen und Pfadfehler erkennen.

Multipathing-Plug-Ins (MPPs)

Die PSA bietet eine Sammlung von VMkernel-APIs, die Drittanbieter zum Erstellen ihrer eigenen Multipathing-Plug-Ins (MPPs) verwenden können. Die Module bieten spezifische Lastausgleichs- und Failover-Funktionen für ein bestimmtes Speicher-Array. Die MPPs können auf dem ESXi-Host installiert werden. Sie können zusätzlich zu den nativen VMware-Modulen bzw. als deren Ersatz ausgeführt werden.

VMware-Hochleistungs-Plug-In (VMware High-Performance Plug-in, HPP)

Das HPP ersetzt das NMP für Hochgeschwindigkeitsgeräte, wie z. B. NVMe. Das HPP kann die Leistung von Ultra-Fast-Flash-Geräten verbessern, die lokal auf Ihrem ESXi-Host installiert sind, und ist das Standard-Plug-In, das NVMe-Ziele beansprucht.
Zur Unterstützung von Multipathing verwendet das HPP die Pfadauswahlschemas (PSS). Ein bestimmtes PSS ist für die Auswahl physischer Pfade für E/A-Anforderungen verantwortlich.

Weitere Informationen finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas.

Beanspruchungsregeln

Die PSA verwendet Beanspruchungsregeln, um zu bestimmen, welches Plug-In die Pfade zu einem bestimmten Speichergerät besitzt.

Tabelle 18-1. Multipathing-Akronyme

Akronym	Definition
PSA	Architektur des im Betrieb austauschbaren Speichers
NMP	Natives Multipathing-Plug-In. Generisches VMware Multipathing-Modul, das von SCSI-Speichergeräten verwendet wird.
PSP	Pfadauswahl-Plug-In (Path Selection Plug-in). Verarbeitet die Pfadauswahl für ein SCSI-Speichergerät.
SATP	Speicher-Array-Typ-Plug-In (Storage Array Type Plug-in). Verarbeitet Pfad-Failover für ein bestimmtes SCSI-Speicher-Array.
MPP (Drittanbieter)	Multipathing-Plug-In. Ein von einem Drittanbieter entwickeltes und bereitgestelltes Multipathing-Modul.
HPP	Natives von VMware bereitgestelltes Hochleistungs-Plug-In. Es wird mit ultra-schnellen lokalen und vernetzten Flash-Geräten wie z. B. NVMe verwendet.
PSS	Pfadauswahlschema (Path Selection Scheme). Verarbeitet Multipathing für NVMe-Speichergeräte.

Grundlegendes zur Architektur des im Betrieb austauschbaren Speichers

Die Architektur des im Betrieb austauschbaren Speichers (Pluggable Storage Architecture, PSA) stellt ein offenes und modulares Framework dar, das die verschiedenen Softwaremodule koordiniert, die für Multipathing-Vorgänge verantwortlich sind.

VMware stellt generische native Multipathing-Module zur Verfügung, die als VMware NMP und VMware HPP bezeichnet werden. Darüber hinaus bietet die PSA eine Sammlung von VMkernel-APIs, die von Drittanbieter-Entwicklern genutzt werden können. Die Softwareentwickler können eigene Lastausgleichs- und Failover-Module für ein bestimmtes Speicher-Array erstellen. Diese Multipathing-Module (MPPs) von Drittanbietern können auf dem ESXi-Host installiert und zusätzlich zu den nativen VMware-Module oder als deren Ersatz ausgeführt werden.

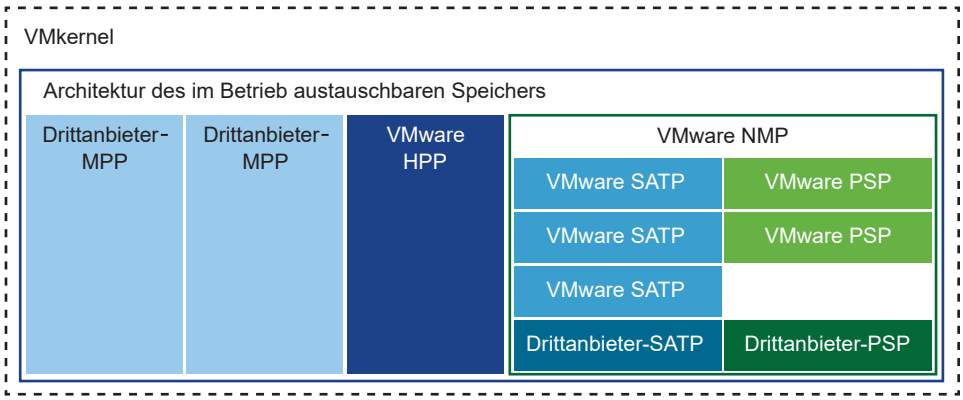
Bei der Koordination der nativen VMware-Module und ggf. installierter Drittanbieter-MPPs führt die PSA die folgenden Aufgaben aus:

- Laden und Entladen von Multipathing-Plug-Ins.
- Verbergen von Angaben zur virtuellen Maschine vor einem bestimmten Plug-In.
- Weiterleiten von E/A-Anforderungen für ein bestimmtes logisches Gerät an das MPP, das das Gerät verwaltet.
- Verarbeiten der E/A-Warteschlangen für logische Geräte.
- Implementieren der gemeinsamen Nutzung der Bandbreite für logische Geräte durch virtuelle Maschinen.
- Verarbeiten der E/A-Warteschlangen für physische Speicher-HBAs.
- Verarbeiten der Erkennung und Entfernung physischer Pfade.

- Bereitstellen von E/A-Statistiken für logische Geräte und physische Pfade.

Wie in der Abbildung der Architektur des im Betrieb austauschbaren Speichers dargestellt, können mehrere Drittanbieter-MPPs parallel zum VMware NMP oder VMware HPP ausgeführt werden. Wenn sie installiert sind, können die Drittanbieter-MPPs das Verhalten der nativen Module ersetzen. Die MPPs können die Steuerung des Pfad-Failovers und der Lastausgleichs-Vorgänge für die angegebenen Speichergeräte übernehmen.

Abbildung 18-5. Architektur des im Betrieb austauschbaren Speichers



Natives Multipathing-Plug-In von VMware

Standardmäßig bietet ESXi ein erweiterbares Multipathing-Modul, das als NMP (Natives Multipathing-Plug-In) bezeichnet wird.

Das VMware NMP unterstützt normalerweise alle in der VMware Speicher-HCL aufgeführten Speicher-Arrays und bietet einen auf dem Array-Typ basierenden Pfadauswahl-Algorithmus. Das NMP weist einem bestimmten Speichergerät oder einer bestimmten LUN mehrere physische Pfade zu.

Für zusätzliche Multipathing-Vorgänge verwendet das NMP Untermodule, die als SATPs und PSPs bezeichnet werden. Das NMP delegiert die spezifischen Details für die Abwicklung des Pfad-Failovers für das Gerät an das SATP. Das PSP verarbeitet die Pfadauswahl für das Gerät.

In der Regel führt das NMP die folgenden Vorgänge aus:

- Verwalten der Beanspruchung und Freigabe von physischen Pfaden.
- Registrieren und Aufheben der Registrierung von logischen Geräten.
- Zuordnen physischer Pfade zu logischen Geräten.
- Unterstützung der Erkennung und Behebung von nicht verfügbaren Pfaden.
- Verarbeiten von E/A-Anforderungen an logische Geräte:
  - Auswählen eines optimalen physischen Pfades für die Anforderung.
  - Ausführen von notwendigen Maßnahmen zur Behebung von Pfadfehlern und Wiederholungsversuchen für E/A-Befehle.

- Unterstützen von Verwaltungsaufgaben, wie z. B. dem Zurücksetzen von logischen Geräten.

ESXi installiert automatisch ein geeignetes SATP für ein von Ihnen verwendetes Array. Sie müssen keine SATPs beschaffen oder herunterladen.

NMP-E/A-Ablauf von VMware

Wenn eine virtuelle Maschine eine E/A-Anforderung an ein vom NMP verwaltetes Speichergerät ausgibt, läuft der folgende Prozess ab.

1 Das NMP ruft das PSP auf, das diesem Speichergerät zugewiesen ist.

2 Das PSP wählt einen entsprechenden physischen Pfad für die zu sendende E/A.

3 Das NMP gibt die E/A-Anforderung auf dem vom PSP gewählten Pfad aus.

4 Wenn der E/A-Vorgang erfolgreich ist, meldet das NMP dessen Abschluss.

5 Wenn der E/A-Vorgang einen Fehler meldet, ruft das NMP das entsprechende SATP auf.

6 Das SATP interpretiert die E/A-Fehlercodes und aktiviert ggf. die inaktiven Pfade.

7 Das PSP wird aufgerufen, um einen neuen Pfad für das Senden der E/A zu wählen.

Anzeigen von Multipathing-Modulen

Verwenden Sie den `esxcli`-Befehl, um alle im System geladenen Mutipathing-Module aufzulisten. Multipathing-Module verwalten physische Pfade, die Ihren Host mit Speicher verbinden. Die Module enthalten native NMP und HPP von VMware sowie alle Drittanbieter-MPPs.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um die Mutipathing-Module aufzulisten:

  `esxcli storage core plugin list --plugin-class=MP`

Ergebnisse

Mit diesem Befehl werden in der Regel das NMP und, falls geladen, das HPP sowie das Attribut „MASK_PATH“ angezeigt. Wenn Drittanbieter-MPPs geladen wurden, werden diese ebenfalls aufgelistet.

```
Plugin name  Plugin class
-----------  ------------
NMP          MP
```

Weitere Informationen zu diesem Befehl finden Sie in der Dokumentation *ESXCLI – Konzepte und Beispiele* und *ESXCLI – Referenz*.

Anzeigen von NMP-Speichergeräten

Verwenden Sie den `esxcli`-Befehl, um alle von VMware NMP gesteuerten Speichergeräte aufzulisten und mit diesen Geräten verbundene SATP- und PSP-Informationen anzuzeigen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um alle Speichergeräte aufzulisten:

  `esxcli storage nmp device list`

  Verwenden Sie den Parameter **`--device | -d=`*`Geräte-ID`***, um die Ausgabe dieses Befehls zu filtern, so dass ein einzelnes Gerät angezeigt wird.

Beispiel: Anzeigen von NMP-Speichergeräten

```
# esxcli storage nmp device list
mpx.vmhba1:C0:T2:L0
   Device Display Name: Local VMware Disk (mpx.vmhba1:C0:T2:L0)
   Storage Array Type: VMW_SATP_LOCAL
   Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device
configuration.
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba1:C0:T2:L0;current=vmhba1:C0:T2:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba1:C0:T2:L0
   Is USB: false

......

eui.6238666462643332
   Device Display Name: SCST_BIO iSCSI Disk (eui.6238666462643332)
   Storage Array Type: VMW_SATP_DEFAULT_AA
   Storage Array Type Device Config: {action_OnRetryErrors=off}
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba65:C0:T0:L0;current=vmhba65:C0:T0:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba65:C0:T0:L0
   Is USB: false
```

Weitere Informationen zu diesem Befehl finden Sie in der Dokumentation *ESXCLI – Konzepte und Beispiele* und *ESXCLI – Referenz*.

Pfadauswahl-Plug-Ins und Richtlinien

VMware Pfadauswahl-Plug-Ins (Path Selection Plug-ins, PSPs) sind verantwortlich für die Auswahl eines physischen Pfads für E/A-Anforderungen.

Die Plug-Ins sind Untermodule von VMware NMP. Das NMP weist ein Standard-PSP für jedes logische Gerät basierend auf den Gerätetyp zu. Sie können das Standard-PSP außer Kraft setzen. Weitere Informationen finden Sie unter Ändern der Pfadauswahl-Richtlinie.

Jedes PSP aktiviert und erzwingt eine entsprechende Pfadauswahl-Richtlinie.

VMW_PSP_MRU – Zuletzt verwendet (VMware)

Die Richtlinie „Zuletzt verwendet (VMware)“ wird durch VMW_PSP_MRU erzwungen. Dabei wird der erste funktionierende Pfad ausgewählt, der beim Systemstart ermittelt wird. Ist der Pfad nicht mehr verfügbar, wählt der Host einen alternativen Pfad aus. Der Host wird nicht auf den ursprünglichen Pfad zurückgesetzt, wenn dieser verfügbar ist. Die Richtlinie „Zuletzt verwendet“ verwendet nicht die Einstellung „Bevorzugter Pfad“. Diese Richtlinie ist die Standardrichtlinie für die meisten Aktiv/Passiv-Speichergeräte.

Das VMW_PSP_MRU unterstützt die Pfadrangfolge. Um den Rang einzelner Pfade festzulegen, verwenden Sie den Befehl `esxcli storage nmp psp generic pathconfig set`. Weitere Informationen hierzu finden Sie im VMware Knowledgebase-Artikel unter http://kb.vmware.com/kb/2003468 und in der *ESXCLI – Referenz*-Dokumentation.

VMW_PSP_FIXED – Fest (VMware)

Die Richtlinie „Fest (VMware)“ wird von VMW_PSP_FIXED implementiert. Die Richtlinie verwendet den festgelegten bevorzugten Pfad. Wenn der bevorzugte Pfad nicht zugewiesen ist, wählt die Richtlinie den ersten funktionierenden Pfad aus, der beim Systemstart ermittelt wird. Ist der bevorzugte Pfad nicht mehr verfügbar, wählt der Host einen alternativen verfügbaren Pfad aus. Der Host kehrt zum zuvor definierten bevorzugten Pfad zurück, wenn dieser wieder verfügbar ist.

Die Standardrichtlinie für die meisten Aktiv/Aktiv-Speichergeräte ist „Fest“.

VMW_PSP_RR – Round-Robin (VMware)

VMW_PSP_RR aktiviert die Richtlinie „Round-Robin (VMware)“. „Round-Robin“ ist die Standardrichtlinie für viele Arrays. Sie verwendet einen Algorithmus zur automatischen Pfadauswahl, der die konfigurierten Pfade durchgehend rotiert.

Sowohl die Aktiv/Aktiv- als auch Aktiv/Passiv-Arrays verwenden die Richtlinie, um den Lastausgleich zwischen Pfaden für verschiedene LUNs zu implementieren. Mit Aktiv/Passiv-Arrays verwendet die Richtlinie die aktiven Pfade. Mit Aktiv/Aktiv-Arrays verwendet die Richtlinie alle verfügbaren Pfade.

Der Latenz-Mechanismus, der standardmäßig für die Richtlinie aktiviert ist, sorgt für eine größere Anpassungsfähigkeit. Um bessere Ergebnisse beim Lastausgleich zu erzielen, wählt der Mechanismus dynamisch einen optimalen Pfad unter Berücksichtigung der folgenden Pfadmerkmale aus:

- E/A-Bandbreite
- Pfadlatenz

Anleitungen zum Ändern der Standardparameter für die adaptive Latenz-Round-Robin-Richtlinie oder zum Deaktivieren des Latenzmechanismus finden Sie in Ändern der Standardparameter für Latenz-Round-Robin.

Um andere konfigurierbaren Parameter für VMW_PSP_RR festzulegen, verwenden Sie den Befehl `esxcli storage nmp psp roundrobin`. Weitere Informationen finden Sie in der Dokumentation *ESXCLI – Referenz*.

VMware SATPs

Speicher-Array-Typ-Plug-Ins (SATPs) sind für Array-spezifische Vorgänge zuständig. Die SATPs sind Submodule des VMware NMP.

ESXi bietet ein SATP für jeden von VMware unterstützten Array-Typ. ESXi bietet auch Standard-SATPs, die nicht spezifische Aktiv-Aktiv-, Aktiv-Passiv-, ALUA- und lokale Geräte unterstützen.

Jedes SATP ist für spezifische Merkmale einer bestimmten Klasse von Speicher-Arrays geeignet. Das SATP kann die zum Ermitteln des Pfadzustands und zum Aktivieren eines inaktiven Pfads erforderlichen Array-spezifischen Vorgänge durchführen. Daher kann das NMP-Modul selbst mit mehreren Speicher-Arrays arbeiten, ohne die Besonderheiten der Speichergeräte kennen zu müssen.

In der Regel bestimmt das NMP, welches SATP für ein bestimmtes Speichergerät verwendet werden soll, und verknüpft das SATP mit den physischen Pfaden für dieses Speichergerät. Das SATP implementiert die folgenden Aufgaben:

- Überwachung der Integrität der einzelnen physischen Pfade.
- Melden von Zustandsänderungen der einzelnen physischen Pfade.
- Ausführen von für das Speicher-Failover erforderlichen Array-spezifischen Aktionen. Beispielsweise kann es für Aktiv-Passiv-Geräte passive Pfade aktivieren.

ESXi umfasst verschiedene generische SATP-Module für Speicher-Arrays.

VMW_SATP_LOCAL

SATP für lokale direkt angeschlossene Geräte.

Ab der Version vSphere 6.5 Update 2 bietet VMW_SATP_LOCAL Multipathing-Unterstützung für die lokalen Geräte mit Ausnahme von Geräten im nativen 4K-Format. Um mehrere Pfade zu den lokalen Geräten zu beanspruchen, ist das Verwenden anderer SATPs als der in früheren vSphere-Versionen verwendeten SATPs nicht mehr erforderlich.

VMW_SATP_LOCAL unterstützt die Pfadauswahl-Plug-Ins VMW_PSP_MRU und VMW_PSP_FIXED, unterstützt jedoch nicht VMW_PSP_RR.

VMW_SATP_DEFAULT_AA

Generisches SATP für Aktiv-Aktiv-Arrays.

VMW_SATP_DEFAULT_AP

Generisches SATP für Aktiv-Passiv-Arrays.

VMW_SATP_ALUA

SATP für ALUA-konforme Arrays.

Weitere Informationen finden Sie in den Dokumenten *VMware-Kompatibilitätshandbuch* und *ESXCLI – Referenz*.

Anzeigen von SATPs für den Host

Verwenden Sie den `esxcli`-Befehl, um in das System geladene VMware NMP SATPs aufzulisten. Zeigen Sie Informationen über die SATPs an.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus, um VMware SATPs aufzulisten:

  `esxcli storage nmp satp list`

Ergebnisse

Für jedes SATP zeigt die Ausgabe Informationen zum Typ des Speicher-Arrays oder Systems, das das SATP unterstützt. Die Ausgabe zeigt zudem das Standard-PSP für alle LUNs an, die dieses SATP verwenden. `Placeholder (plugin not loaded)` gibt in der Spalte „Beschreibung“ an, dass das SATP nicht geladen ist.

Beispiel: Anzeigen von SATPs für den Host

```
# esxcli storage nmp satp list
Name                 Default PSP    Description
VMW_SATP_MSA         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_ALUA        VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AP  VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_SVC         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EQL         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_INV         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EVA         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_ALUA_CX     VMW_PSP_RR     Placeholder (plugin not loaded)
VMW_SATP_SYMM        VMW_PSP_RR     Placeholder (plugin not loaded)
VMW_SATP_CX          VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_LSI         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AA  VMW_PSP_FIXED  Supports non-specific active/active arrays
VMW_SATP_LOCAL       VMW_PSP_FIXED  Supports direct attached devices
```

Weitere Informationen zu diesem Befehl finden Sie in der Dokumentation *ESXCLI – Konzepte und Beispiele* und *ESXCLI – Referenz*.

VMware High Performance-Plug-In und Pfadauswahlschemas

VMware stellt das High Performance Plug-In (HPP, Hochleistungs-Plug-In) bereit, um die Leistung von Speichergeräten auf Ihrem ESXi-Host zu verbessern.

Das HPP ersetzt das NMP für Hochgeschwindigkeitsgeräte, wie z. B. NVMe. Das HPP ist das Standard-Plug-In, das NVMe-oF-Ziele beansprucht. Innerhalb von ESXi werden die NVMe-oF-Ziele emuliert und den Benutzern als SCSI-Ziele präsentiert. Das HPP unterstützt nur aktiv/aktive und implizite ALUA-Ziele.

In vSphere Version 7.0 Update 1 und früher bleibt NMP das Standard-Plug-In für lokale NVMe-Geräte. Sie können es jedoch durch HPP ersetzen. Ab vSphere 7.0 Update 2 wird HPP das Standard-Plug-In für lokale NVMe- und SCSI-Geräte. Sie können es jedoch durch NMP ersetzen.

HPP-Unterstützung	vSphere 7.0 Update 1	vSphere 7.0 Update 2 und Update 3
Speichergeräte	Lokale NVMe PCIe Gemeinsam genutzte NVMe-oF (nur aktiv/aktive und implizite ALUA-Ziele)	Lokales NVMe und SCSI Gemeinsam genutzte NVMe-oF (nur aktiv/aktive und implizite ALUA-Ziele)
Multipathing	Ja	Ja
Plug-Ins auf zweiter Ebene	Nein Pfadauswahlschemas (Path Selection Schemes, PSS)	Nein
Dauerhafte SCSI-3-Reservierungen	Nein	Nein
4Kn-Geräte mit Software-Emulation	Nein	Ja

Pfadauswahlschemas (Path Selection Schemes)

Zur Unterstützung von Multipathing verwendet das HPP die Pfadauswahlschemas (PSS) bei der Auswahl von physischen Pfaden für E/A-Anforderungen.

Sie können den Befehl vSphere Client oder `esxcli` verwenden, um den Standard-Pfadauswahlmechanismus zu ändern.

Informationen zum Konfigurieren der Pfadmechanismen im vSphere Client finden Sie unter Ändern der Pfadauswahl-Richtlinie. Informationen zum Konfigurieren mit dem `esxcli`-Befehl finden Sie unter ESXi- esxcli-HPP-Befehle.

ESXi unterstützt die folgenden Pfadauswahlmechanismen.

FEST

Mit diesem Schema wird ein festgelegter bevorzugter Pfad für E/A-Anforderungen verwendet. Wenn der bevorzugte Pfad nicht zugewiesen ist, wählt der Host den ersten funktionierenden Pfad aus, der beim Systemstart ermittelt wird. Ist der bevorzugte Pfad nicht mehr verfügbar, wählt der Host einen alternativen verfügbaren Pfad aus. Der Host kehrt zum zuvor definierten bevorzugten Pfad zurück, wenn dieser wieder verfügbar ist.

Wenn Sie **FEST** als Pfadauswahlmechanismus konfigurieren, wählen Sie den bevorzugten Pfad aus.

LB-RR (Lastausgleich – Round Robin)

Dies ist das Standardschema für die von HPP beanspruchten Geräte. Nach der Übertragung einer angegebenen Anzahl von Byte oder E/A-Vorgängen auf einem aktuellen Pfad wählt das Schema den Pfad mithilfe des Round Robin-Algorithmus aus.

Um den **LB-RR**-Pfadauswahlmechanismus zu konfigurieren, geben Sie die folgenden Eigenschaften an:

- **IOPS** gibt die E/A-Anzahl auf dem Pfad an, die als Kriterium zum Wechseln eines Pfads für das Gerät verwendet werden soll.
- **Byte** gibt die Byte-Anzahl auf dem Pfad an, die als Kriterium zum Wechseln eines Pfads für das Gerät verwendet werden soll.

LB-IOPS (Lastausgleich – IOPS)

Nach der Übertragung einer angegebenen Anzahl von E/A-Vorgängen auf einem aktuellen Pfad (Standardwert: 1000) wählt das System einen optimalen Pfad aus, der die geringste Anzahl ausstehender E/A-Vorgänge aufweist.

Geben Sie beim Konfigurieren dieses Mechanismus den **IOPS**-Parameter an, um die E/A-Anzahl auf dem Pfad anzugeben, die als Kriterium zum Wechseln eines Pfads für das Gerät verwendet werden soll.

LB-BYTES (Lastausgleich – Byte)

Nach der Übertragung einer festgelegten Anzahl von Byte auf einem aktuellen Pfad (Standardwert: 10 MB) wählt das System einen optimalen Pfad mit der geringsten Anzahl an ausstehenden Byte aus.

Um diesen Mechanismus zu konfigurieren, verwenden Sie den Parameter **Byte**, um die Anzahl der Byte auf dem Pfad anzugeben, die als Kriterium zum Wechseln eines Pfads für das Gerät verwendet werden soll.

Lastausgleich – Latenz (LB-Latenz)

Um bessere Ergebnisse beim Lastausgleich zu erzielen, wählt der Mechanismus dynamisch einen optimalen Pfad unter Berücksichtigung der folgenden Pfadmerkmale aus:

- Der Parameter **Zeit für die Latenzauswertung** gibt an, in welchem Zeitintervall (in Millisekunden) die Latenz der Pfade ausgewertet werden muss.
- Der Parameter **Sampling-E/As pro Pfad** steuert, wie viele Sampling-E/A-Vorgänge auf jedem Pfad ausgegeben werden müssen, um die Latenz des Pfads zu berechnen.

Empfohlene Vorgehensweisen für das HPP

Um den schnellsten Durchsatz mit einem Hochgeschwindigkeits-Speichergerät zu erzielen, sollten Sie diese Empfehlungen beachten.

- Verwenden Sie die vSphere-Version, die das HPP unterstützt.
- Verwenden Sie das HPP für lokale NVMe- und SCSI-Geräte sowie für NVMe-oF-Geräte.
- Wenn Sie NVMe over Fibre Channel-Geräte verwenden, folgen Sie den allgemeinen Empfehlungen für Fibre Channel-Speicher. Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwenden von ESXi mit Fibre-Channel-SAN.
- Wenn Sie NVMe-oF verwenden, dürfen Sie keine Transporttypen kombinieren, um auf denselben Namespace zuzugreifen.
- Stellen Sie bei Verwendung von NVMe-oF-Namespaces sicher, dass die aktiven Pfade dem Host angezeigt werden. Die Namespaces können erst registriert werden, nachdem der aktive Pfad erkannt wurde.
- Konfigurieren Sie Ihre VMs zur Verwendung von VMware Paravirtual-Controllern. Informationen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Legen Sie den latenzsensitiven Schwellenwert fest.
- Wenn eine einzelne VM einen erheblichen Anteil an der E/A-Arbeitslast des Geräts hat, ziehen Sie die Verteilung des E/A-Durchsatzes auf mehrere virtuelle Festplatten in Betracht. Verbinden Sie die Festplatten mit separaten virtuellen Controllern in der VM.

  Andernfalls wird der E/A-Durchsatz aufgrund der Auslastung des CPU-Kerns, der für die Verarbeitung von E/A-Vorgängen auf einem bestimmten virtuellen Speichercontroller verantwortlich ist, möglicherweise beschränkt.

Weitere Informationen zu Gerätebezeichnern für NVMe-Geräte, die ausschließlich das ID-Format NGUID unterstützen, finden Sie unter NVMe-Geräte mit NGUID-Gerätebezeichnern.

Aktivieren des Hochleistungs-Plug-Ins und der Pfadauswahlschemas

Das Hochleistungs-Plug-In (HPP) ist das Standard-Plug-In, das lokale NVMe- und SCSI-Geräte sowie NVMe-oF-Ziele beansprucht. Sie können es nach Bedarf durch NMP ersetzen. In vSphere Version 7.0 Update 1 und früher bleibt NMP das Standard-Plug-In für lokale NVMe- und SCSI-Geräte. Sie können es jedoch durch HPP ersetzen.

Verwenden Sie den Befehl `esxcli storage core claimrule add` , um den HPP oder NMP auf Ihrem ESXi zu aktivieren.

Zum Ausführen der `esxcli storage core claimrule add` können Sie ESXi Shell oder vSphere CLI nutzen. Weitere Informationen finden Sie unter *Erste Schritte mit ESXCLI* und *ESXCLI – Referenz*.

Beispiele in diesem Thema zeigen, wie HPP aktiviert und die Pfadauswahlschemata (PSS) eingerichtet werden.

Hinweis Das Aktivieren des Hochleistungs-Plug-Ins wird von per PXE gestarteten ESXi-Hosts nicht unterstützt.

Voraussetzungen

Richten Sie Ihre VMware NVMe-Speicherumgebung ein. Weitere Informationen finden Sie unter Kapitel 16 NVMe-Speicher von VMware.

Verfahren

1 Erstellen Sie eine HPP-Beanspruchungsregel, indem Sie den Befehl `esxcli storage core claimrule add` ausführen.

Verwenden Sie eine der folgenden Methoden, um die Beanspruchungsregel hinzuzufügen:

Methode	Beschreibung
Basierend auf dem NVMe-Controller-Modell	**`esxcli storage core claimrule add --type vendor --nvme-controller-model`** Beispiel: **`esxcli storage core claimrule add --rule 429 --type vendor --nvme-controller-model "ABCD*" --plugin HPP`**
Basierend auf der PCI-Anbieter-ID und Unteranbieter-ID	**`esxcli storage core claimrule add --type vendor --pci-vendor-id --pci-sub-vendor-id`** Beispiel: **`esxcli storage core claimrule add --rule 429 --type vendor --pci-vendor-id 8086 --pci-sub-vendor-id 8086 --plugin HPP`**.

2 Konfigurieren Sie das PSS.

Verwenden Sie eine der folgenden Methoden:

Methode	Beschreibung
Festlegen des PSS basierend auf der Geräte-ID	**`esxcli storage hpp device set`** Beispiel: **`esxcli storage hpp device set --device=`*`device`*` --pss=FIXED --path=preferred path`**
Festlegen des PSS basierend auf dem Anbieter/Modell	Verwenden Sie die Option **`--config-string`** mit dem Befehl **`esxcli storage core claimrule add`**. Beispiel: **`esxcli storage core claimrule add -r 914 -t vendor -V `*`vendor`*` -M `*`model`*` -P HPP --config-string "pss=LB-Latency,latency-eval-time=40000"`**

3 Starten Sie den Host neu, damit Ihre Änderungen wirksam werden.

Festlegen des latenzsensitiven Schwellenwerts

Wenn Sie HPP für Ihre Speichergeräte verwenden, legen Sie den latenzsensitiven Schwellenwert für das Gerät fest, damit der E/A-Scheduler für E/A-Daten umgangen werden kann.

Standardmäßig werden alle E/A-Daten von ESXi über den E/A-Scheduler geleitet. Die Verwendung des Schedulers kann jedoch zum Auftreten von internen Warteschlangen führen, wodurch die Effizienz von Hochgeschwindigkeits-Speichergeräten eingeschränkt wird.

Sie können den latenzsensitiven Schwellenwert konfigurieren und den Mechanismus für die direkte Übermittlung aktivieren, mit dem die E/A-Daten bei der Umgehung des Schedulers unterstützt werden. Wenn dieser Mechanismus aktiviert ist, werden die E/A-Daten direkt von PSA über HPP an den Gerätetreiber übermittelt.

Damit die direkte Übermittlung fehlerfrei funktioniert, muss die beobachtete durchschnittliche E/A-Latenz niedriger als der von Ihnen angegebene Latenzschwellenwert sein. Wenn die E/A-Latenz den Latenzschwellenwert überschreitet, bricht das System die direkte Übermittlung ab und wird auf die Verwendung des E/A-Schedulers zurückgesetzt. Die direkte Übermittlung wird fortgesetzt, wenn der Wert für die durchschnittliche E/A-Latenz wieder niedriger als der Latenzschwellenwert ist.

Sie können den Latenzschwellenwert für eine Gerätefamilie festlegen, die von HPP beansprucht wird. Ziehen Sei beim Festlegen des Schwellenwerts für die Latenz das Anbieter- und Modellpaar, das Controller-Modell oder das PCIe-Anbieter-ID- und Unteranbieter-ID-Paar heran.

Verfahren

1 Legen Sie den latenzsensitiven Schwellenwert für das Gerät fest, indem Sie den folgenden Befehl ausführen:

esxcli storage core device latencythreshold set -t *Wert in Millisekunden*

Verwenden Sie eine der folgenden Optionen:

Option	Beispiel
Anbieter/Modell	Legen Sie den Parameter für den latenzsensitiven Schwellenwert für alle Geräte mit dem angegebenen Anbieter und Modell fest: **esxcli storage core device latencythreshold set -v 'vendor1' -m 'model1' -t 10**
NVMe-Controller-Modell	Legen Sie den latenzsensitiven Schwellenwert für alle NVMe-Geräte mit dem angegebenen Controller-Modell fest: **esxcli storage core device latencythreshold set -c 'controller_model1' -t 10**
PCIe-Anbieter/-Unteranbieter-ID	Legen Sie den latenzsensitiven Schwellenwert für Geräte mit 0x8086 als PCIe-Anbieter-ID und 0x8086 als PCIe-Unteranbieter-ID fest. **esxcli storage core device latencythreshold set -p '8086' -s '8086' -t 10**

2 Stellen Sie sicher, dass der Latenzschwellenwert festgelegt ist:

esxcli storage core device latencythreshold list

```
Device                Latency Sensitive Threshold
--------------------  ---------------------------
naa.55cd2e404c1728aa               0 milliseconds
naa.500056b34036cdfd               0 milliseconds
naa.55cd2e404c172bd6              50 milliseconds
```

3 Überwachen Sie den Status des latenzsensitiven Schwellenwerts. Suchen Sie in den VMkernel-Protokollen die folgenden Einträge:

- `Latency Sensitive Gatekeeper turned on for device` *`Gerät`*`. Threshold of` *`XX`* `msec is larger than max completion time of` *`YYY`* `msec`
- `Latency Sensitive Gatekeeper turned off for device` *`Gerät`*`. Threshold of` *`XX`* `msec is exceeded by command completed in` *`YYY`* `msec`

ESXi- esxcli-HPP-Befehle

Sie können die ESXi-Shell- oder vSphere-CLI-Befehle verwenden, um das Hochleistungs-Plug-In zu konfigurieren und zu überwachen.

Unter *Erste Schritte mit ESXCLI* finden Sie eine Einführung und unter *ESXCLI – Referenz* Details zur Verwendung des Befehls `esxcli`.

Befehl	Beschreibung	Optionen
`esxcli storage hpp path list`	Auflisten der Pfade, die derzeit vom Hochleistungs-Plug-In beansprucht werden.	`-d|--device=`*`device`* Zeigt Informationen für ein bestimmtes Gerät an. `-p|--path=`*`path`* Begrenzt die Ausgabe auf einen bestimmten Pfad.
`esxcli storage hpp device list`	Auflisten der Geräte, die derzeit vom Hochleistungs-Plug-In gesteuert werden.	`-d|--device=`*`device`* Zeigt ein bestimmtes Gerät an.

Befehl	Beschreibung	Optionen

`esxcli storage hpp device set`	Konfigurieren der Einstellungen für ein HPP-Gerät.	`-B|--bytes=long` Maximale Byte auf dem Pfad, nach denen der Pfad gewechselt wird.
		`--cfg-file` Aktualisieren Sie die Konfigurationsdatei und die Laufzeit mit der neuen Einstellung. Wenn das Gerät von einem anderen PSS beansprucht wird, ignorieren Sie beim Anwenden auf die Laufzeitkonfiguration alle Fehler.
		`-d|--device=device` Das HPP-Gerät, mit dem gearbeitet wird. Verwenden einer der UIDs, die das Gerät meldet. Erforderlich.
		`-I|--iops=long` Maximale IOPS auf dem Pfad, nach denen der Pfad gewechselt wird.
		`-T|--latency-eval-time=long` Steuert, nach welchem Intervall in ms die Latenz der Pfade ausgewertet werden muss.
		`-L|--mark-device-local= bool` Legen Sie HPP fst, um das Gerät als lokal zu behandeln oder nicht.
		`-M|--mark-device-ssd=bool` Gibt an, ob HPP das Gerät als eine SSD-Festplatte behandelt.
		`-p|--path=str` Der Pfad, der als bevorzugter Pfad für das Gerät festgelegt werden soll.
		`-P|--pss=pss_name` Das Pfadauswahlschema, das dem Gerät zugewiesen werden soll. Wenn Sie den Wert nicht angeben, wählt das System die Standardeinstellung aus. Eine Beschreibung der Pfadauswahlschemas finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas. Zu den Optionen gehören:
		■ **FEST**
		Verwenden Sie die Unteroption `-p|--path=str`, um den bevorzugten Pfad festzulegen.
		■ **LB-Byte**
		Verwenden Sie die Unteroption `-B|--bytes=long`, um die Eingabe anzugeben.
		■ **LB-IOPs**
		Verwenden Sie die Unteroption `-I|--iops=long`, um die Eingabe anzugeben.
		■ **LB-Latenz**
		Zu den Unteroptionen gehören:
		`-T|--latency-eval-time=long`
		`-S|--sampling-ios-per-path=long`
		■ **LB-RR** Standard

Befehl	Beschreibung	Optionen
		Zu den Unteroptionen gehören: `-B|--bytes=`*`long`* `-I|--iops=`*`long`* `-S|--sampling-ios-per-path=`*`long`* Steuert, wie viele Beispiel-E/A-Vorgänge auf jedem Pfad ausgegeben werden müssen, um die Latenz des Pfads zu berechnen. `-U|--use-ano=`*`bool`* Legen Sie die Option auf `true` fest, um nicht optimierte Pfade in den Satz aktiver Pfade aufzunehmen, die zur Ausgabe von E/As auf diesem Gerät verwendet werden. Legen Sie die Option andernfalls auf `false` fest.
`esxcli storage hpp device usermarkedssd list`	Listen Sie die Geräte auf, die vom Benutzer als SSD gekennzeichnet oder nicht gekennzeichnet wurden.	`-d|--device=`*`device`* Begrenzen der Ausgabe auf ein bestimmtes Gerät.

Anzeigen und Verwalten von Pfaden

Wenn Sie Ihren ESXi-Host starten oder Ihren Speicheradapter erneut prüfen, ermittelt der Host alle physischen Pfade zu Speichergeräten, die für den Host verfügbar sind. Basierend auf einem Satz von Beanspruchungsregeln bestimmt der Host, welches Multipathing-Modul (das NMP, das HPP oder ein MPP) die Pfade zu einem bestimmten Gerät besitzt.

Das Modul, das das Gerät besitzt, ist verantwortlich für das Verwalten der Multipathing-Unterstützung für das Gerät. Standardmäßig führt der Host alle fünf Minuten eine periodische Pfadauswertung durch und weist die nicht beanspruchten Pfade dem entsprechenden Modul zu.

Für die vom NMP-Modul verwalteten Pfade wird ein zweiter Satz von Beanspruchungsregeln verwendet. Diese Regeln weisen jedem Speichergerät ein SATP- und ein PSP-Modul zu und legen fest, welche Speicher-Array-Typ-Richtlinie und Pfadauswahl-Richtlinie angewendet werden.

Verwenden Sie den vSphere Client, um die Speicher-Array-Typ-Richtlinie und die Pfadauswahl-Richtlinie anzuzeigen, die einem bestimmten Speichergerät zugewiesen sind. Außerdem können Sie den Status aller verfügbaren Pfade für dieses Speichergerät überprüfen. Bei Bedarf können Sie die standardmäßige Pfadauswahl-Richtlinie mithilfe des Clients ändern.

Um das Standard-Multipathing-Modul oder SATP zu ändern, ändern Sie Beanspruchungsregeln mithilfe der vSphere-CLI.

Informationen zum Ändern von Beanspruchungsregeln finden Sie unter Verwenden von Beanspruchungsregeln.

Anzeigen von Speichergerätepfaden

Zeigen Sie an, welche Mehrfachpfad-Richtlinien der Host für ein bestimmtes Speichergerät verwendet, und ermitteln Sie den Status aller verfügbaren Pfade für dieses Speichergerät.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte**.

4 Wählen Sie das Speichergerät, dessen Pfade Sie ansehen möchten.

5 Klicken Sie auf die Registerkarte **Eigenschaften** und überprüfen Sie das Modul, dem das Gerät zugeordnet ist, z. B. NMP oder HPP.

   Unter „Mehrfachpfad-Richtlinien“ sehen Sie auch die Pfadauswahlrichtlinie und ggf. die Speicher-Array-Typ-Richtlinie, die dem Gerät zugewiesen sind.

6 Klicken Sie auf die Registerkarte **Pfade**, um alle für das Speichergerät verfügbaren Pfade und deren Status zu überprüfen. Es können die folgenden Informationen zum Pfadstatus angezeigt werden:

Status	Beschreibung
Aktiv (E/A)	Funktionierender Pfad oder mehrere Pfade, die derzeit Daten übertragen.
Standby	Pfade, die inaktiv sind. Wenn der aktive Pfad fehlschlägt, können sie in den betriebsbereiten Zustand wechseln und mit der E/A-Übertragung beginnen.
Deaktiviert	Pfade, die vom Administrator deaktiviert wurden.
Ausgefallen	Pfade, die nicht mehr für die Verarbeitung von E/A verfügbar sind. Ein Fehler bei einem physischen Medium oder die fehlerhafte Konfiguration eines Arrays kann diesen Zustand hervorrufen.

   Wenn Sie die Pfadrichtlinie **Fest** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Sternchen (*) in der bevorzugten Spalte gekennzeichnet.

Anzeigen von Datenspeicherpfaden

Überprüfen Sie die Pfade, die eine Verbindung zu Speichergeräten herstellen, auf denen Ihre VMFS-Datenspeicher gesichert werden.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

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

3 Klicken Sie auf **Konnektivität und Mehrfachpfad**.

4 Wählen Sie einen Host aus, um die Multipathing-Details der zugehörigen Geräte anzuzeigen.

5 Prüfen Sie unter „Mehrfachpfad-Richtlinien“ das Modul, das das Gerät besitzt, zum Beispiel NMP. Sie können auch die Pfadauswahlrichtlinie und die Speicher-Array-Typ-Richtlinie anzeigen, die dem Gerät zugewiesenen sind.

   Möglicherweise wird Folgendes angezeigt:

Pfadauswahlrichtlinie	Bevorzugter Pfad
Speicher-Array-Typ-Richtlinie	VMW_SATP_LOCAL
Besitzer-Plug-In	NMP

6 Prüfen Sie unter „Pfade“ die Gerätepfade und den Status jedes einzelnen Pfads. Es können die folgenden Informationen zum Pfadstatus angezeigt werden:

Status	Beschreibung
Aktiv (E/A)	Funktionierender Pfad oder mehrere Pfade, die derzeit Daten übertragen.
Standby	Pfade, die inaktiv sind. Wenn der aktive Pfad fehlschlägt, können sie in den betriebsbereiten Zustand wechseln und mit der E/A-Übertragung beginnen.
Deaktiviert	Pfade, die vom Administrator deaktiviert wurden.
Ausgefallen	Pfade, die nicht mehr für die Verarbeitung von E/A verfügbar sind. Ein Fehler bei einem physischen Medium oder die fehlerhafte Konfiguration eines Arrays kann diesen Zustand hervorrufen.

Wenn Sie die Pfadrichtlinie **Fest** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Sternchen (*) in der bevorzugten Spalte gekennzeichnet.

Ändern der Pfadauswahl-Richtlinie

In der Regel müssen Sie die standardmäßigen Mehrfachpfad-Einstellungen nicht ändern, die Ihr ESXi-Host für ein bestimmtes Speichergerät verwendet. Wenn Sie Änderungen vornehmen möchten, nutzen Sie das Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten**, um die Pfadauswahlrichtlinie zu ändern. Sie können in diesem Dialogfeld auch Multipathing für SCSI-basierte Protokollendpunkte ändern.

Verfahren

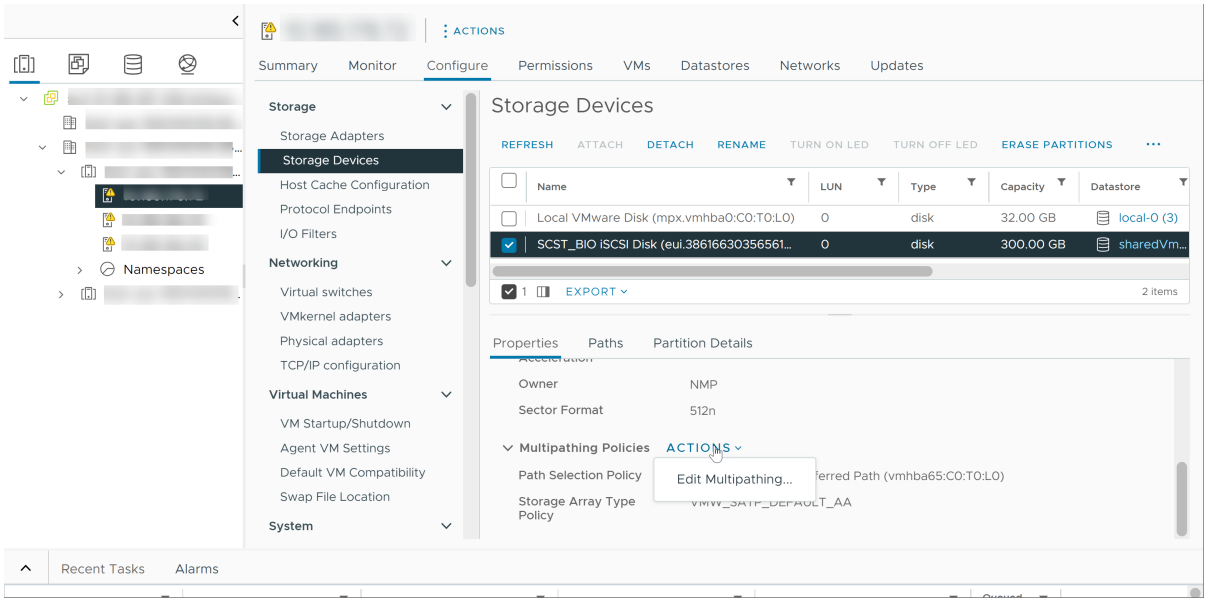
1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Speichergeräte** oder **Protokollendpunkte**.

4 Wählen Sie das Element aus, dessen Pfade Sie ändern möchten, und klicken Sie auf die Registerkarte **Eigenschaften**.

5 Wählen Sie unter „Mehrfachpfad-Richtlinien“ die Option **Mehrfachpfad bearbeiten** aus dem Menü **Aktionen** aus.



6 Wählen Sie eine Pfadrichtlinie aus und konfigurieren Sie deren Einstellungen. Ihre Optionen ändern sich je nach Typ des Speichergeräts, das Sie verwenden.

- Informationen zu Pfadrichtlinien für SCSI-Geräte finden Sie unter Pfadauswahl-Plug-Ins und Richtlinien.
- Weitere Informationen zu Pfadmechanismen für NVMe-Geräte finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas.

7 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Ändern der Standardparameter für Latenz-Round-Robin

Auf dem ESXi-Host ist der Latenzmechanismus für die Round-Robin-Pfadauswahlrichtlinie standardmäßig aktiviert. Der Mechanismus berücksichtigt die E/A-Bandbreite und Pfadlatenz, um einen optimalen Pfad für E/A auszuwählen. Wenn Sie den Latenzmechanismus verwenden, kann die Round-Robin-Richtlinie dynamisch den optimalen Pfad auswählen und bessere Lastausgleichergebnisse erzielen.

Sie verwenden den Befehl `esxcli`, um die Standardparameter des Latenzmechanismus zu ändern oder den Mechanismus zu deaktivieren.

Voraussetzungen

Legen Sie die Pfadauswahl-Richtlinie auf Round-Robin fest. Weitere Informationen hierzu finden Sie unter Ändern der Pfadauswahl-Richtlinie.

Verfahren

1 Konfigurieren Sie den Latenzmechanismus unter Verwendung des folgenden Befehls.

```
esxcli storage nmp psp roundrobin deviceconfig set --type=latency --device=Geräte-ID:
```

Der Befehl verfügt über die folgenden Parameter:

Parameter	Beschreibung
-S|--num-sampling-cycles=*Probewert*	Wenn `--type` auf `latency` festgelegt ist, steuert dieser Parameter, wie viele E/A verwendet werden sollen, um die durchschnittliche Latenz jedes einzelnen Pfades zu berechnen. Der Standardwert dieses Parameters beträgt 16.
-T|--latency-eval-time=*Zeit in ms*	Wenn `--type` auf `latency` festgelegt ist, steuert dieser Parameter die Frequenz, in der die Pfadlatenz aktualisiert wird. Der Standardwert ist 3 Minuten.

2 Überprüfen Sie, ob die Round-Robin-Latenz und ihre Parameter ordnungsgemäß konfiguriert sind.

```
esxcli storage nmp psp roundrobin deviceconfig get --device=Geräte-ID:
```

oder

```
esxcli storage nmp device list --device=Geräte-ID:
```

Die Ausgabe des folgenden Beispiels zeigt den Konfigurationspfad:

```
 Path Selection Policy: VMW_PSP_RR
   Path Selection Policy Device Config:
{policy=latency,latencyEvalTime=180000,samplingCycles=16,curSamplingCycle=16,useANO=0;
CurrentPath=vmhba1:C0:T0:L0: NumIOsPending=0,latency=0}
```

Nächste Schritte

Ändern Sie den `Misc.EnablePSPLatencyPolicy`-Parameter in den erweiterten Systemeinstellungen für Ihren Host auf 0, um den Latenzmechanismus zu deaktivieren.

Deaktivieren von Speicherpfaden

Pfade können zu Wartungszwecken oder aus anderen Gründen vorübergehend deaktiviert werden.

Sie deaktivieren einen Pfad mithilfe des Bereichs „Pfade“. Für den Zugriff auf den Bereich „Pfade“ stehen Ihnen mehrere Möglichkeiten zur Verfügung: über einen Datenspeicher, ein Speichergerät, einen Adapter oder über eine Virtual Volumes-Protokollendpunkt-Ansicht.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf einen der folgenden Elemente:

- **Speicheradapter**
- **Speichergeräte**
- **Protokollendpunkte**

4 Wählen Sie im rechten Bereich das Element aus, dessen Pfade Sie deaktivieren möchten – einen Adapter, ein Speichergerät oder einen Protokollendpunkt – und klicken Sie auf die Registerkarte **Pfade**.

5 Wählen Sie den Pfad aus, der deaktiviert werden soll, und klicken Sie auf **Deaktivieren**.

Der Pfadstatus wird in „Deaktiviert“ geändert.

Verwenden von Beanspruchungsregeln

Beanspruchungsregeln legen fest, welches Multipathing-Modul die Pfade zu einem bestimmten Speichergerät besitzt. Mit diesen Regeln kann auch der Typ der Multipathing-Unterstützung definiert werden, die der Host dem Gerät bietet.

Die Beanspruchungsregeln sind in der Datei `/etc/vmware/esx.conf` des Hosts aufgeführt.

Die Regeln werden in diese Kategorien unterteilt:

Core-Beanspruchungsregeln

Diese Beanspruchungsregeln legen fest, welches Multipathing-Modul (das NMP, HPP oder ein Drittanbieter-MPP) das bestimmte Gerät beansprucht.

SATP-Beanspruchungsregeln

Je nach Art des Geräts weisen diese Regeln ein bestimmtes SATP-Untermodul zu, das dem Gerät die herstellerspezifische Multipathing-Verwaltung bereitstellt.

Sie können die `esxcli`-Befehle verwenden, um die Core- und SATP-Beanspruchungsregeln hinzuzufügen oder zu ändern. Normalerweise fügen Sie die Beanspruchungsregeln zum Laden eines Drittanbieter-MPPs oder zum Ausblenden einer LUN auf Ihrem Host hinzu. Beanspruchungsregeln müssen möglicherweise geändert werden, wenn die Standardeinstellungen für ein bestimmtes Gerät nicht ausreichend sind.

Weitere Informationen zu Befehlen, die für die Verwaltung von PSA-Beanspruchungsregeln verfügbar sind, finden Sie unter *Erste Schritte mit ESXCLI*.

Eine Liste der Speicher-Arrays und der entsprechenden SATPs und PSPs finden Sie im Abschnitt „Speicher/SAN“ im *vSphere Compatibility Guide*.

Überlegungen zu Multipathing

Beim Verwalten von Speicher-Multipathing-Plug-Ins und -Beanspruchungsregeln muss Folgendes beachtet werden.

Beachten Sie im Umgang mit Multipathing die folgenden Überlegungen:

- Wenn dem Gerät anhand der Beanspruchungsregeln kein SATP zugewiesen ist, lautet das Standard-SATP für iSCSI- oder FC-Geräte VMW_SATP_DEFAULT_AA. Das Standard-PSP lautet VMW_PSP_FIXED.
- Wenn das System die SATP-Regeln zur Ermittlung eines SATP für ein angegebenes Gerät durchsucht, werden zuerst die Treiberregeln durchsucht. Ist die Suche dort nicht erfolgreich, werden die Hersteller- bzw. Modellregeln und anschließend die Übertragungsregeln durchsucht. Wird keine übereinstimmende Regel gefunden, wählt NMP ein Standard-SATP für das Gerät aus.
- Wenn VMW_SATP_ALUA einem bestimmten Speichergerät zugewiesen ist, dieses Gerät ALUA jedoch nicht erkennt, gibt es für dieses Gerät keine Übereinstimmung der Beanspruchungsregeln. Das Gerät wird vom Standard-SATP gemäß dem Übertragungstyp des Geräts beansprucht.
- Das Standard-PSP für alle von VMW_SATP_ALUA beanspruchten Geräte lautet VMW_PSP_MRU. Das VMW_PSP_MRU wählt wie vom VMW_SATP_ALUA angegeben einen aktiven/optimierten Pfad oder einen aktiven/nicht optimierten Pfad aus, falls kein aktiver/optimierter Pfad vorhanden ist. Dieser Pfad wir so lange verwendet, bis ein besserer Pfad verfügbar ist (MRU). Wenn das VMW_PSP_MRU derzeit einen aktiven/nicht optimierten Pfad verwendet und ein aktiver/optimierter Pfad verfügbar wird, wechselt das VMW_PSP_MRU vom aktuellen Pfad zum aktiven/optimierten Pfad,
- Während VMW_PSP_MRU normalerweise standardmäßig für ALUA-Arrays gewählt wird, müssen gewisse ALUA-Speicher-Arrays VMW_PSP_FIXED verwenden. Informationen dazu, ob Ihr Speicher-Array VMW_PSP_FIXED benötigt, finden Sie im *VMware-Kompatibilitätshandbuch* oder wenden Sie sich an Ihren Speicheranbieter. Wenn Sie VMW_PSP_FIXED mit ALUA-Arrays verwenden, wählt der ESXi-Host den optimalen Arbeitspfad aus und legt ihn als bevorzugten Standardpfad fest, es sei denn, Sie geben explizit einen bevorzugten Pfad an. Ist der vom Host ausgewählte Pfad nicht mehr verfügbar, wählt der Host einen alternativen verfügbaren Pfad aus. Wenn Sie den bevorzugten Pfad allerdings explizit auswählen, bleibt er ungeachtet dessen Status der bevorzugte Pfad.
- Die PSA-Beanspruchungsregel 101 maskiert standardmäßig Pseudo-Array-Geräte von Dell. Löschen Sie diese Regel nur, wenn die Maskierung dieser Geräte aufgehoben werden soll.

Auflisten von Multipathing-Beanspruchungsregeln für den Host

Verwenden Sie den `esxcli`-Befehl, um die verfügbaren Multipathing-Beanspruchungsregeln aufzulisten.

Die Beanspruchungsregeln geben an, ob das NMP, das HPP oder ein Drittanbieter-MPP einen vorhandenen physischen Pfad verwaltet. Jede Beanspruchungsregel gibt einen Satz an Pfaden basierend auf folgenden Parametern an:

- Anbieter-/Modellzeichenfolgen
- Transport, wie z. B. SATA, IDE, Fibre Channel

- Adapter, Ziel- oder LUN-Speicherort
- Gerätetreiber, zum Beispiel Mega-RAID

Verfahren

- Führen Sie zum Auflisten der Multipathing-Beanspruchungsregeln den Befehl **`esxcli storage core claimrule list --claimrule-class=MP`** aus.

  Wenn Sie die Option `claimrule-class` nicht verwenden, wird MP automatisch als Regelklasse angenommen.

Beispiel: Beispielausgabe des Befehls „esxcli storage core claimrule list“

```
Rule Class  Rule   Class    Type       Plugin     Matches
MP           10    runtime  vendor     HPP        vendor=NVMe model=*
MP           10    file     vendor     HPP        vendor=NVMe model=*
MP           50    runtime  transport  NMP        transport=usb
MP           51    runtime  transport  NMP        transport=sata
MP           52    runtime  transport  NMP        transport=ide
MP           53    runtime  transport  NMP        transport=block
MP           54    runtime  transport  NMP        transport=unknown
MP          101    runtime  vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          101    file     vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          200    runtime  vendor     MPP_1      vendor=NewVend model=*
MP          200    file     vendor     MPP_1      vendor=NewVend model=*
MP          201    runtime  location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          201    file     location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          202    runtime  driver     MPP_3      driver=megaraid
MP          202    file     driver     MPP_3      driver=megaraid
MP          65535  runtime  vendor     NMP        vendor=* model=*
```

Dieses Beispiel zeigt Folgendes an:

- Das NMP beansprucht alle mit den Speichergeräten verbundenen Pfade, die USB-, SATA-, IDE- und Block SCSI-Übertragung verwenden.
- Die Regeln für HPP, MPP_1, MPP_2 und MPP_3 wurden hinzugefügt, damit die Module die angegebenen Geräte beanspruchen können. Das HPP beansprucht beispielsweise alle Geräte des Anbieters NVMe. Alle vom Inbox-NVMe-Treiber gehandhabten Geräte werden unabhängig vom tatsächlichen Anbieter beansprucht. Das MPP_1-Modul beansprucht alle mit einem beliebigen Modell des NewVend-Speicher-Arrays verbundenen Pfade.
- Sie können mit dem Modul MASK_PATH nicht genutzte Geräte vor dem Host verbergen. Standardmäßig maskiert die PSA-Beanspruchungsregel 101 Dell-Array-Pseudogeräte mit der Anbieterzeichenfolge „`DELL`“ und der Modellzeichenfolge „`Universal Xport`“.
- Die Spalte „Rule Class“ der Ausgabe beschreibt die Kategorie einer Beanspruchungsregel. Sie kann MP (Multipathing-Plug-In), Filter oder VAAI sein.

- Die Class-Spalte zeigt, welche Regeln definiert und welche geladen sind. Der Parameter `file` in der Class-Spalte gibt an, dass die Regel definiert ist. Der Parameter `runtime` gibt an, dass die Regel in Ihr System geladen wurde. Damit eine benutzerdefinierte Beanspruchungsregel aktiv wird, müssen zwei Zeilen mit derselben Regelnummer vorhanden sein, eine Zeile für die Regel mit dem Parameter `file` und eine Zeile mit `runtime`. Einige standardmäßig im System definierte Regeln verfügen lediglich über eine Zeile mit der Class-Spalte `runtime`. Sie können diese Regeln nicht ändern.
- Die Standardregel 65535 weist alle freien Pfade dem NMP zu. Löschen Sie diese Regel nicht.

Hinzufügen von Multipathing-Beanspruchungsregeln

Verwenden Sie die `esxcli`-Befehle, um dem Satz der Beanspruchungsregeln im System eine Multipathing-PSA-Beanspruchungsregel hinzuzufügen. Zur Aktivierung der neuen Beanspruchungsregeln müssen Sie diese zunächst definieren und dann in Ihr System laden.

Beispiele für das Hinzufügen einer PSA-Beanspruchungsregel:

- Sie laden ein neues Multipathing-Plug-In (MPP) von einem Drittanbieter und müssen die Pfade, die dieses Modul beansprucht, definieren.
- Sie müssen das native HPP aktivieren.

Warnung Sie können keine Regeln erstellen, bei denen zwei verschiedene Plug-Ins Pfade zum selben Gerät beanspruchen. Ihre Versuche, diese Beanspruchungsregeln zu erstellen, scheitern mit einer Warnung in der Datei `vmkernel.log`.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Verwenden Sie zum Definieren einer neuen Beanspruchungsregel den folgenden Befehl:

`esxcli storage core claimrule add`

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
`-A|--adapter=<adapter>`	Adapter der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `location` ist.
`-u|--autoassign`	Fügt eine Beanspruchungsregel basierend auf deren Merkmale hinzu. Die Regelnummer ist nicht erforderlich.
`-C|--channel=<channel>`	Kanal der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `location` ist.

Option	Beschreibung
-c|--claimrule-class=<cl>	Die Beanspruchungsregel-Klasse, die für diesen Vorgang verwendet werden soll. Sie können `MP` (Standard) `Filter` oder `VAAI` angeben. Um Hardwarebeschleunigung für einen neuen Array zu konfigurieren, fügen Sie zwei Beanspruchungsregeln hinzu, eine für den VAAI-Filter und eine andere für das VAAI-Plug-In. Detaillierte Anweisungen finden Sie unter Hinzufügen von Hardwarebeschleunigungs-Beanspruchungsregeln.
-d|--device=<device_uid>	UID des Geräts. Nur gültig, wenn `--type` gleich `device` ist.
-D|--driver=<driver>	Treiber für den HBA der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `driver` ist.
-f|--force	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
--force-reserved	Überschreibschutz für reservierte Regel-ID-Bereiche. Reservierte Beanspruchungsregeln sind Regeln mit einer ID unter 100. Sie können sie dazu verwenden, bestimmten Plug-Ins lokale Geräte neu zuzuordnen, z. B. das NVMe-Gerät dem HPP.
--if-unset=<str>	Führen Sie diesen Befehl aus, falls diese erweiterte Benutzervariable nicht auf 1 festgelegt ist.
-i|--iqn=<iscsi_name>	iSCSI Qualified Name für das Ziel. Nur gültig, wenn `--type` gleich `target` ist.
-L|--lun=<lun_id>	LUN der Pfade. Nur gültig, wenn `--type` gleich `location` ist. Wert der LUN-ID darf nicht höher sein als der Wert der erweiterten Konfigurationsoption /Disk/MaxLUN.
-M|--model=<model>	Modell der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `vendor` ist. Gültige Werte sind Werte für die Modellzeichenfolge aus der SCSI-Anfragezeichenfolge. Führen Sie auf jedem Gerät `vicfg-scsidevs <conn_options> -l` aus, um Werte für die Modellzeichenfolge anzuzeigen.
-P|--plugin=<plugin>	Zu verwendendes PSA-Plug-In. Die möglichen Werte sind `NMP`, `MASK_PATH` oder `HPP`. Drittanbieter können auch ihr eigenes PSA-Plug-In bereitstellen. Erforderlich.
-r|--rule=<rule_ID>	Zu verwendende Regel-ID. Die Regel-ID gibt die Reihenfolge an, in der die Beanspruchungsregel ausgewertet werden soll. Benutzerdefinierte Beanspruchungsregeln werden in numerischer Reihenfolge ihrer IDs, beginnend mit 101, ausgewertet. Sie können den Befehl `esxcli storage core claimrule list` ausführen , um zu ermitteln, welche Regel-IDs verfügbar sind.
-T|--target=<target>	Ziel der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `location` ist.

Option	Beschreibung
-R|--transport=<transport>	Transport der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `transport` ist. Folgende Werte werden unterstützt: ■ `block` – Blockspeicher ■ `fc` – Fibre Channel ■ `iscsivendor` – iSCSI ■ `iscsi` – wird derzeit nicht verwendet ■ `ide` – IDE-Speicher ■ `sas` – SAS-Speicher ■ `sata` – SATA-Speicher ■ `usb` – USB-Speicher ■ `parallel` – Parallel ■ `fcoe` – FCoE ■ `unknown`
-t|--type=<type>	Art des für den Vorgang zu verwendenden Abgleichs. Gültige Werte sind die folgenden. Erforderlich. ■ `vendor` ■ `location` ■ `driver` ■ `transport` ■ `device` ■ `target`
-V|--vendor=<vendor>	Anbieter der zu verwendenden Pfade. Nur gültig, wenn `--type` gleich `vendor` ist. Gültige Werte sind Werte für die Herstellerzeichenfolge aus der SCSI-Abfragezeichenfolge. Führen Sie auf jedem Gerät `vicfg-scsidevs <conn_options> -l` aus, um Werte für die Herstellerzeichenfolge anzuzeigen.
--wwnn=<wwnn>	World Wide Node Number für das Ziel.
--wwpn=<wwpn>	World Wide Port Number für das Ziel.
-a|--xcopy-use-array-values	Verwenden Sie die vom Array übermittelten Werte zum Konstruieren des XCOPY-Befehls, der an das Speicher-Array gesendet werden soll. Dies betrifft nur VAAI-Beanspruchungsregeln.
-s|--xcopy-use-multi-segs	Verwenden Sie mehrere Segmente, wenn Sie eine XCOPY-Anforderung übermitteln. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.
-m|--xcopy-max-transfer-size	Maximale Datenübertragungsgröße in MB, wenn Sie eine andere Übertragungsgröße als die vom Array gemeldete verwenden. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.
-k|--xcopy-max-transfer-size-kib	Maximale Übertragungsgröße in KiB für die XCOPY-Befehle, wenn Sie eine andere Übertragungsgröße als die vom Array gemeldete verwenden. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.

2 Verwenden Sie den folgenden Befehl, um die neue Beanspruchungsregel in Ihr System zu laden:

```
esxcli storage core claimrule load
```

Dieser Befehl lädt alle neu erstellten Multipathing-Beanspruchungsregeln aus der Konfigurationsdatei `esx.conf` in den VMkernel. Der Befehl hat keine Optionen.

3 Um geladene Beanspruchungsregeln anzuwenden, verwenden Sie den folgenden Befehl:

`esxcli storage core claimrule run`

Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
`-A|--adapter=<adapter>`	Wenn `--type` gleich `location` ist, der Name des HBAs für die Pfade, auf die die Beanspruchungsregeln angewendet werden sollen. Um Beanspruchungsregeln auf Pfade von allen Adaptern anzuwenden, lassen Sie diese Option weg.
`-C|--channel=<channel>`	Wenn `--type` gleich `location` ist, der Wert der SCSI-Kanalnummer für die Pfade, auf die die Beanspruchungsregeln angewendet werden sollen. Um Beanspruchungsregeln auf Pfade mit beliebiger Kanalnummer anzuwenden, lassen Sie diese Option weg.
`-c|--claimrule-class=<cl>`	Die Beanspruchungsregel-Klasse, die für diesen Vorgang verwendet werden soll.
`-d|--device=<device_uid>`	UID des Geräts.
`-L|--lun=<lun_id>`	Wenn `--type` gleich `location` ist, der Wert der SCSI-LUN für die Pfade, auf die die Beanspruchungsregeln angewendet werden sollen. Um Beanspruchungsregeln auf Pfade mit beliebiger LUN anzuwenden, lassen Sie diese Option weg.
`-p|--path=<path_uid>`	Wenn `--type` gleich `path` ist, zeigt diese Option die eindeutige Pfad-ID (UID) oder den Laufzeitnamen eines Pfads an, auf den die Beanspruchungsregeln angewendet werden sollen.
`-T|--target=<target>`	Wenn `--type` gleich `location` ist, der Wert der SCSI-Zielnummer für die Pfade, auf die die Beanspruchungsregeln angewendet werden sollen. Um Beanspruchungsregeln auf Pfade mit beliebiger Zielnummer anzuwenden, lassen Sie diese Option weg.
`-t|--type=<location|path|all>`	Typ der durchzuführenden Beanspruchung. Verwendet standardmäßig `all`, d. h., die Beanspruchungsregeln werden ohne Beschränkung auf bestimmte Pfade oder SCSI-Adressen angewendet. Gültige Werte sind `location`, `path` und `all`.
`-w|--wait`	Sie können diese Option nur dann verwenden, wenn Sie auch `--type all` verwenden. Wenn die Option einbezogen wird, wartet der Beanspruchungsprozess vor dem Ausführen des Beanspruchungsvorgangs darauf, dass zu beanspruchende Pfade gefunden werden. In diesem Fall startet das System den Beanspruchungsprozess erst dann, wenn es wahrscheinlich ist, dass alle Pfade im System erkannt sind, bevor es den Prozess gestartet hat. Nach dem Starten des Beanspruchungsprozesses kehrt der Befehl erst zurück, wenn die Geräteregistrierung abgeschlossen ist. Wenn Sie während des Beanspruchungs- oder Erkennungsprozesses Pfade hinzufügen oder entfernen, funktioniert diese Option möglicherweise nicht korrekt.

Beispiel: Definieren von Multipathing-Beanspruchungsregeln

Im folgenden Beispiel fügen Sie Regel Nummer 500 hinzu und laden diese. Die Regel beansprucht alle Pfade mit der Modellzeichenfolge „NewMod“ und der Herstellerzeichenfolge „NewVend“ für das NMP-Plug-In.

```
# esxcli storage core claimrule add -r 500 -t vendor -V NewVend -M NewMod -P
NMP
```

```
# esxcli storage core claimrule load
```

Nachdem Sie den Befehl **`esxcli storage core claimrule list`** ausgeführt haben, wird die neue Beanspruchungsregel in der Liste angezeigt.

Die folgende Ausgabe gibt an, dass die Beanspruchungsregel 500 in das System geladen wurde und aktiv ist.

```
Rule Class  Rule   Class    Type       Plugin     Matches
...         ...    ...      ...        ...        ...
MP          500    runtime  vendor     NMP        vendor=NewVend model=NewMod
MP          500    file     vendor     NMP        vendor=NewVend model=NewMod
```

Löschen von Multipathing-Beanspruchungsregeln

Mithilfe des `esxcli`-Befehls können Sie eine Multipathing-PSA-Beanspruchungsregel aus dem Beanspruchungsregelsatz auf dem System entfernen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Führen Sie zum Löschen einer Beanspruchungsregel aus dem Satz von Beanspruchungsregeln den folgenden Befehl aus.

   `esxcli storage core claimrule remove`

   Hinweis Die PSA-Beanspruchungsregel 101 maskiert standardmäßig Pseudo-Array-Geräte von Dell. Löschen Sie diese Regel nur, wenn die Maskierung dieser Geräte aufgehoben werden soll.

   Der Befehl verfügt über die folgenden Optionen:

Option	Beschreibung
`-c|--claimrule-class=<str>`	Gibt die Beanspruchungsregelklasse (MP, Filter, VAAI) an.
`-P|--plugin=<str>`	Gibt das Plug-In an.
`-r|--rule=<long>`	Gibt die Regel-ID an.

   Mit diesem Schritt wird die Beanspruchungsregel aus der Klasse „File“ entfernt.

2 Löschen Sie die Beanspruchungsregel aus dem System.

```
esxcli storage core claimrule load
```

Mit diesem Schritt wird die Beanspruchungsregel aus der Klasse „Runtime“ entfernt.

Maskierung von Pfaden

Sie können verhindern, dass der Host auf Speichergeräte oder LUNs zugreift oder einzelne Pfade zu einer LUN verwendet. Verwenden Sie die `esxcli`-Befehle, um die Pfade zu maskieren. Beim Maskieren von Pfaden können Sie Beanspruchungsregeln erstellen, die das MASK_PATH-Plug-In bestimmten Pfaden zuordnen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Prüfen Sie, welche die nächste verfügbare Regel-ID ist:

```
esxcli storage core claimrule list
```

Die Beanspruchungsregeln, die Sie zum Maskieren von Pfaden verwenden, haben Regel-IDs im Bereich von 101 bis 200. Wenn dieser Befehl zeigt, dass die Regeln 101 und 102 vorhanden sind, können Sie 103 für die Regel angeben, die Sie hinzufügen möchten.

2 Weisen Sie das MASK_PATH-Plug-In einem Pfad zu, indem Sie eine neue Beanspruchungsregel für das Plug-In erstellen.

```
esxcli storage core claimrule add -P MASK_PATH
```

3 Laden Sie die MASK_PATH-Beanspruchungsregel in Ihr System.

```
esxcli storage core claimrule load
```

4 Prüfen Sie, ob die MASK_PATH-Beanspruchungsregel ordnungsgemäß hinzugefügt wurde.

```
esxcli storage core claimrule list
```

5 Falls für den maskierten Pfad eine Beanspruchungsregel vorhanden ist, entfernen Sie die Regel.

```
esxcli storage core claiming unclaim
```

6 Führen Sie die Pfadbeanspruchungsregeln aus.

```
esxcli storage core claimrule run
```

Ergebnisse

Nach dem Zuweisen des MASK_PATH-Plug-Ins zu einem Pfad verliert der Pfadstatus an Bedeutung und wird nicht länger vom Host verwaltet. Befehle, die Informationen zum maskierten Pfad bereitstellen, zeigen den Pfadstatus als nicht verfügbar (dead) an.

Beispiel: Maskieren einer LUN

Im vorliegenden Beispiel wird die LUN 20 auf den Zielen T1 und T2 maskiert, auf die über die Speicheradapter vmhba2 und vmhba3 zugegriffen wird.

1
```
#esxcli storage core claimrule list
```

2
```
#esxcli storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L
20
```

3
```
#esxcli storage core claimrule load
```

4
```
#esxcli storage core claimrule list
```

5
```
#esxcli storage core claiming unclaim -t location -A vmhba2
#esxcli storage core claiming unclaim -t location -A vmhba3
```

6
```
#esxcli storage core claimrule run
```

Aufheben der Maskierung von Pfaden

Falls es erforderlich ist, dass der Host Zugriff auf das maskierte Speichergerät erhält, müssen Sie die Maskierung der Pfade zu diesem Gerät aufheben.

Hinweis Wenn Sie die Beanspruchung einer Geräteeigenschaft, zum Beispiel Geräte-ID oder Anbieter, aufheben, wird die Beanspruchung der Pfade durch das MASK_PATH-Plug-In nicht aufgehoben. Das MASK_PATH-Plug-In verfolgt nicht die Geräteeigenschaft der Pfade, die es beansprucht.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Löschen Sie die Beanspruchungsregel „MASK_PATH“.

`esxcli storage core claimrule remove -r rule#`

2 Stellen Sie sicher, dass die Beanspruchungsregel ordnungsgemäß gelöscht wurde.

`esxcli storage core claimrule list`

3 Laden Sie die Pfadbeanspruchungsregeln aus der Konfigurationsdatei neu in den VMkernel.

esxcli storage core claimrule load

4 Führen Sie den Befehl **esxcli storage core claiming unclaim** für jeden Pfad auf das maskierte Speichergerät aus.

Beispiel:

esxcli storage core claiming unclaim -t location -A vmhba0 -C 0 -T 0 -L 149

5 Führen Sie die Pfadbeanspruchungsregeln aus.

esxcli storage core claimrule run

Ergebnisse

Ihr Host hat jetzt Zugriff auf das zuvor maskierte Speichergerät.

Definieren von NMP SATP-Regeln

Die NMP SATP-Beanspruchungsregeln legen fest, welches SATP ein Speichergerät verwalten soll. In der Regel können Sie die für Speichergeräte bereitgestellten Standard-SATPs verwenden. Sollten Standardeinstellungen nicht ausreichen, verwenden Sie die `esxcli`-Befehle, um das SATP für ein bestimmtes zu Gerät ändern.

Beim Installieren eines Drittanbieter-SATP für eine bestimmtes Speicher-Array müssen Sie unter Umständen eine SATP-Regel erstellen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Führen Sie zum Hinzufügen einer Beanspruchungsregel für ein bestimmtes SATP den Befehl **esxcli storage nmp satp rule add** aus. Der Befehl verfügt über die folgenden Optionen.

Option	Beschreibung
-b|--boot	Diese Regel ist eine Standard-Systemregel, die zur Startzeit hinzugefügt wird. Ändern Sie die Datei `esx.conf` nicht und fügen Sie sie nicht zu einem Hostprofil hinzu.
-c|--claim-option=*Zeichenfolge*	Legt die Zeichenfolge der Beanspruchungsoption beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-e|--description=*Zeichenfolge*	Legt die Beschreibung der Beanspruchungsregel beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-d|--device=*Zeichenfolge*	Legt das Gerät beim Hinzufügen von SATP-Beanspruchungsregeln fest. Geräteregeln und Anbieter/Modell- sowie Treiberregeln schließen sich gegenseitig aus.

Option	Beschreibung
-D|--driver=*Zeichenfolge*	Legt die Treiberzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Treiberregeln und Anbieter/Modell-Regeln schließen sich gegenseitig aus.
-f|--force	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
-h|--help	Zeigt die Hilfemeldung an.
-M|--model=*Zeichenfolge*	Legt die Modellzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.
-o|--option=*Zeichenfolge*	Legt die Optionszeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-P|--psp=*Zeichenfolge*	Legt das Standard-PSP für die SATP-Beanspruchungsregel fest.
-O|--psp-option=*Zeichenfolge*	Legt die PSP-Optionen für die SATP-Beanspruchungsregel fest.
-s|--satp=*Zeichenfolge*	Das SATP, für das eine neue Regel hinzugefügt wird.
-R|--transport=*Zeichenfolge*	Legt die Zeichenfolge für den Beanspruchungs-Transporttyp beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-t|--type=*Zeichenfolge*	Legt den Beanspruchungstyp beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-V|--vendor=*Zeichenfolge*	Legt die Herstellerzeichenfolge beim Hinzufügen von SATP-Beanspruchungsregeln fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.

Hinweis Beim Durchsuchen der SATP-Regeln zur Ermittlung eines SATP für ein vorhandenes Gerät werden zunächst die Treiberregeln vom NMP durchsucht. Ist die Suche dort nicht erfolgreich, werden die Anbieter/Modell-Regeln und anschließend die Übertragungsregeln durchsucht. Werden immer noch keine Ergebnisse angezeigt, wählt NMP ein Standard-SATP für das Gerät aus.

2 Starten Sie Ihren Host neu.

Beispiel: Definieren einer NMP SATP-Regel

Der folgende Beispielbefehl ordnet das VMW_SATP_INV-Plug-In zu, um Speicher-Arrays mit der Herstellerzeichenfolge „NewVend“ und der Modellzeichenfolge „NewMod“ zu verwalten.

```
# esxcli storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

Wenn Sie den Befehl **`esxcli storage nmp satp list -s VMW_SATP_INV`** ausführen, können Sie die neue Regel sehen, die zur Liste der VMW_SATP_INV-Regeln hinzugefügt wurde.

Planungswarteschlangen für VM-E/A

vSphere bietet standardmäßig einen Mechanismus zur Erstellung von Planungswarteschlangen für jede VM-Datei. Jede Datei, etwa „`.vmdk`“, erhält eine eigene Bandbreitenkontrolle.

Dieser Mechanismus gewährleistet, dass jede E/A einer VM-Datei eine eigene Warteschlange erhält und nicht mit anderer Datei-E/A kollidiert.

Diese Funktion ist standardmäßig aktiviert. Sie können die Befehle vSphere Client oder `esxcli` verwenden, um die Funktion zu deaktivieren oder erneut zu aktivieren.

Bearbeiten der E/A-Planung nach Datei im vSphere Client

Der erweiterte Parameter `VMkernel.Boot.isPerFileSchedModelActive` steuert den E/A-Planungsmechanismus nach Datei auf VMFS- und NFS 3-Datenspeichern. Der Mechanismus ist auf dem ESXi-Host standardmäßig aktiviert. Sie können den Mechanismus mithilfe des Dialogfelds **Erweiterte Systemeinstellungen** deaktivieren.

Wenn Sie das E/A-Planung nach Datei-Modell deaktivieren, wird Ihr Host auf einen älteren Planungsmechanismus zurückgesetzt. Der Legacy-Planungsmechanismus wendet nur eine E/A-Warteschlange für jede virtuelle Maschine und jedes Speichergerätepaar an. Alle E/A-Vorgänge zwischen der virtuellen Maschine und ihren virtuellen Festplatten werden in diese Warteschlange verschoben. Folglich wirken sich E/A-Vorgänge verschiedener virtueller Festplatten möglicherweise auf E/A-Vorgänge der anderen virtuellen Festplatten bei der gemeinsamen Nutzung der Bandbreite aus und beeinflussen möglicherweise die jeweilige Leistungsfähigkeit.

Hinweis Deaktivieren Sie die Planung nach Datei nicht, wenn das HPP-Plug-In und der Parameter für den latenzsensitiven Schwellenwert für lokale Hochgeschwindigkeitsgeräte konfiguriert sind. Die Deaktivierung der Planung nach Datei kann zu unvorhersehbarem Verhalten führen.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Bearbeiten Sie den Wert des Parameters **VMkernel.Boot.isPerFileSchedModelActive**.

Option	Beschreibung
Falsch	Deaktivieren Sie den Planungsmechanismus nach Datei.
True (Standard)	Aktivieren Sie den Planungsmechanismus nach Datei erneut.

5. Starten Sie den Host neu, damit die Änderungen wirksam werden.

Verwenden von esxcli-Befehlen zur Aktivierung bzw. Deaktivierung der E/A-Planung nach Datei

Sie können die `esxcli`-Befehle verwenden, um die E/A-Planungsfunktion für VMFS-, NFS 3- und NFS 4.1-Datenspeicher auf Ihrem ESXi-Host zu ändern. Diese Funktion ist standardmäßig aktiviert.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie die folgenden Befehle aus, um die E/A-Planung nach Datei zu aktivieren bzw. zu deaktivieren:

Option	Beschreibung
`esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE`	Deaktiviert die E/A-Planung nach Datei für VMFS und NFS 3.
`esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE`	Aktiviert die E/A-Planung nach Datei für VMFS und NFS 3.
`esxcli system module parameters list -m nfs41client`	Listet den aktuellen Status der Planung nach Datei für NFS 4.1 auf.
`esxcli system module parameters set -m nfs41client -p fileBasedScheduler=0`	Deaktiviert die dateibasierte Planung für NFS 4.1.
`esxcli system module parameters set -m nfs41client -p fileBasedScheduler=1`	Aktiviert die dateibasierte Planung für NFS 4.1.

Raw-Gerätezuordnung

19

Die Raw-Gerätezuordnung bietet virtuellen Maschinen einen Mechanismus für den direkten Zugriff auf eine LUN im physischen Speichersubsystem.

Die folgenden Themen enthalten Informationen über RDMs und bieten Anleitungen zum Erstellen und Verwalten von RDMs.

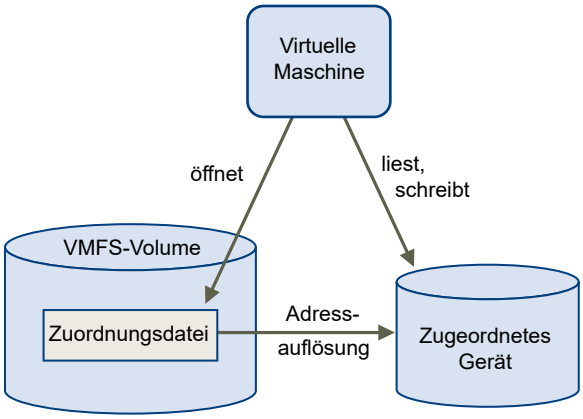
Dieses Kapitel enthält die folgenden Themen:

Wissenswertes zur Raw-Gerätezuordnung

Eine Raw-Gerätezuordnung (RDM) ist eine Zuordnungsdatei in einem separaten VMFS-Volume, die als Proxy für ein physisches Speichergerät fungiert. Mithilfe der RDM kann eine virtuelle Maschine direkt auf das Speichergerät zugreifen und dieses verwenden. Die RDM enthält Metadaten, mit denen Festplattenzugriffe auf das physische Gerät verwaltet und umgeleitet werden.

Die Datei bietet Ihnen einige der Vorteile des direkten Zugriffs auf ein physisches Gerät, während Sie gleichzeitig verschiedene Vorteile einer virtuellen Festplatte im VMFS nutzen können. Folglich verbindet die Datei die VMFS-Verwaltungs- und Wartungsfreundlichkeit mit einem Raw-Gerätezugriff.

Abbildung 19-1. Raw-Gerätezuordnung



In der Regel verwenden Sie VMFS-Datenspeicher für die meisten virtuellen Festplattenspeicher. In Einzelfällen verwenden Sie Raw-LUNs oder logische Festplatten, die sich in einem SAN befinden.

So ist es beispielsweise in folgenden Situationen erforderlich, Raw-LUNs zusammen mit RDMs zu verwenden:

- Wenn in der virtuellen Maschine ein SAN-Snapshot oder auf Ebenen basierende Anwendungen ausgeführt werden. Die Raw-Gerätezuordnung unterstützt Systeme zur Auslagerung von Datensicherungen, indem SAN-eigene Funktionen verwendet werden.
- In allen MSCS-Clusterszenarien mit physischen Hosts, wie z. B. Virtuell-zu-virtuell-Cluster und Physisch-zu-virtuell-Cluster. In diesem Fall sollten Clusterdaten und Quorumfestplatten vorzugsweise als Raw-Gerätezuordnungen konfiguriert werden und nicht als virtuelle Festplatten auf einem freigegebenen VMFS.

Stellen Sie sich eine RDM als eine symbolische Verknüpfung zwischen einem VMFS-Volume und einer Raw-LUN vor. Die Zuordnung zeigt die LUNs wie Dateien auf einem VMFS-Volume an. In der Konfiguration der virtuellen Maschine wird auf die Raw-Gerätezuordnung und nicht auf die Raw-LUN verwiesen. Die Raw-Gerätezuordnung enthält einen Verweis auf die Raw-LUN.

Für Raw-Gerätezuordnungen gibt es zwei Kompatibilitätsmodi:

- Im virtuellen Kompatibilitätsmodus verhält sich die RAW-Gerätezuordnung wie eine virtuelle Festplattendatei. Die RAW-Gerätezuordnung kann Snapshots verwenden.
- Im physischen Kompatibilitätsmodus bietet die Raw-Gerätezuordnung direkten Zugriff auf das SCSI-Gerät für Anwendungen, für die eine niedrigere Steuerungsebene erforderlich ist.

Vorteile von Raw-Gerätezuordnungen

Eine Raw-Gerätezuordnung bietet mehrere Vorteile, sollte aber nicht ständig verwendet werden. In der Regel sind virtuelle Festplattendateien aufgrund ihrer Verwaltungsfreundlichkeit Raw-Gerätezuordnungen vorzuziehen. Wenn Sie jedoch Raw-Geräte benötigen, müssen Sie die Raw-Gerätezuordnung verwenden.

RDM bietet verschiedene Vorteile:

Benutzerfreundliche, dauerhafte Namen

Stellt einen benutzerfreundlichen Namen für ein zugeordnetes Gerät bereit. Wenn Sie eine Raw-Gerätezuordnung verwenden, müssen Sie nicht auf das Gerät über den Gerätenamen verweisen. Sie verwenden stattdessen den Namen der Zuordnungsdatei, zum Beispiel:

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

Dynamische Namensauflösung

Speichert eindeutige Identifikationsinformationen für jedes zugeordnete Gerät. VMFS ordnet jede RDM unabhängig von Änderungen der physischen Konfiguration des Servers aufgrund von Änderungen an der Adapterhardware, Verzeichniswechseln, Geräteverschiebungen usw. dem aktuellen SCSI-Gerät zu.

Verteilte Dateisperrung

Die Raw-Gerätezuordnung ermöglicht die Verwendung einer verteilten VMFS-Sperrung für Raw-SCSI-Geräte. Die verteilte Sperrung für eine Raw-Gerätezuordnung ermöglicht die Verwendung einer freigegebenen Raw-LUN ohne Datenverlustrisiko, wenn zwei virtuelle Maschinen auf verschiedenen Servern versuchen, auf die gleiche LUN zuzugreifen.

Dateizugriffsberechtigungen

Die Raw-Gerätezuordnung ermöglicht Dateizugriffsberechtigungen. Die Berechtigungen für die Zuordnungsdatei werden beim Öffnen der Datei erzwungen, um das zugeordnete Volume zu schützen.

Dateisystemfunktionen

Die Raw-Gerätezuordnung ermöglicht bei der Arbeit mit einem zugeordneten Volume die Verwendung von Dienstprogrammen des Dateisystems, wobei die Zuordnungsdatei als Stellvertreter verwendet wird. Die meisten Vorgänge, die auf eine normale Datei angewendet werden können, können auf die Zuordnungsdatei angewendet werden und werden dann auf das zugeordnete Gerät umgeleitet.

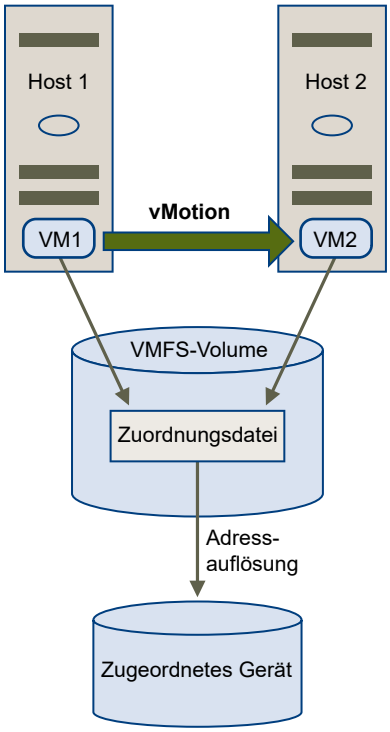
Snapshots

Die Raw-Gerätezuordnung ermöglicht die Verwendung von Snapshots virtueller Maschinen auf einem zugeordneten Volume. Snapshots stehen nicht zur Verfügung, wenn die Raw-Gerätezuordnung im Modus „Physische Kompatibilität“ verwendet wird.

vMotion

Mithilfe der Raw-Gerätezuordnung können Sie eine virtuelle Maschine mit vMotion migrieren. Die Zuordnungsdatei fungiert als Stellvertreter, sodass vCenter Server die virtuelle Maschine mit dem gleichen Mechanismus migrieren kann, der für die Migration virtueller Festplattendateien verwendet wird.

Abbildung 19-2. vMotion einer virtuellen Maschine über eine Raw-Gerätezuordnung



SAN-Management-Agenten

Die Raw-Gerätezuordnung ermöglicht die Ausführung bestimmter SAN-Management-Agenten innerhalb einer virtuellen Maschine. Außerdem kann jede Software, die Zugriff auf ein Gerät über hardwarespezifische SCSI-Befehle benötigt, in einer virtuellen Maschine ausgeführt werden. Diese Art der Software wird auch SCSI-Ziel-basierte Software genannt. Wenn Sie SAN-Verwaltungs-Agenten verwenden, müssen Sie den physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung auswählen.

N-Port-ID-Virtualisierung (NPIV)

Ermöglicht den Einsatz der NPIV-Technologie, die es einem einzelnen Fibre-Channel-HBA-Port ermöglicht, sich mit dem Fibre-Channel-Fabric anhand mehrerer WWPNs (Worldwide Port Names) zu registrieren. Dadurch kann der HBA-Port in Form mehrerer virtueller Ports angezeigt werden, die alle über eine eigene ID und einen eigenen virtuellen Portnamen verfügen. Virtuelle Maschinen können anschließend jeden dieser virtuellen Ports beanspruchen und für den gesamten zur Raw-Gerätezuordnung gehörenden Datenverkehr nutzen.

Hinweis Sie können NPIV nur für virtuelle Maschinen mit RDM-Festplatten verwenden.

VMware kooperiert mit Anbietern von Speicherverwaltungssoftware, damit deren Software in Umgebungen wie ESXi ordnungsgemäß funktioniert. Beispiele sind:

- SAN-Verwaltungssoftware
- Software zur Verwaltung von Speicherressourcen

- Snapshot-Software
- Replikationssoftware

Diese Software verwendet für Raw-Gerätezuordnungen den Modus „Physische Kompatibilität“, damit sie direkt auf SCSI-Geräte zugreifen kann.

Verschiedene Verwaltungsprodukte werden am besten zentral (nicht auf der ESXi-Maschine) ausgeführt, während andere problemlos in den virtuellen Maschinen funktionieren. VMware zertifiziert diese Anwendungen nicht und stellt auch keine Kompatibilitätsmatrix zur Verfügung. Wenn Sie wissen möchten, ob eine SAN-Verwaltungsanwendung in einer ESXi-Umgebung unterstützt wird, wenden Sie sich an den Anbieter der SAN-Verwaltungssoftware.

RDM-Überlegungen und -Einschränkungen

Bei der Verwendung von Raw-Gerätezuordnungen gelten bestimmte Überlegungen und Einschränkungen.

- Die RDM steht für direkt verbundenen Blockgeräte oder gewisse RAID-Geräte nicht zur Verfügung. Die RDM verwendet eine SCSI-Seriennummer, um das zugeordnete Gerät zu identifizieren. Da Block- und bestimmte direkt angeschlossene RAID-Geräte Seriennummern nicht exportieren, können sie nicht in Raw-Gerätezuordnungen verwendet werden.
- Wenn Sie die RDM im physischen Kompatibilitätsmodus verwenden, können Sie keinen Snapshot mit der Festplatte verwenden. Im physischen Kompatibilitätsmodus kann die virtuelle Maschine eigene, speicherbasierte Snapshots oder Spiegelungsoperationen durchführen.

  Snapshots virtueller Maschinen stehen für RDMs mit virtuellem Kompatibilitätsmodus zur Verfügung.
- Eine Festplattenpartition kann nicht zugeordnet werden. Für RDMs ist es erforderlich, dass das zugeordnete Gerät eine vollständige LUN ist.
- Wenn Sie vMotion zum Migrieren von virtuellen Maschinen mit RDMs verwenden, stellen Sie sicher, dass die LUN-IDs für RDMs auf allen teilnehmenden ESXi-Hosts konsistent bleiben.

Raw-Gerätezuordnungseigenschaften

Eine Raw-Gerätezuordnung ist eine spezielle Datei auf einem VMFS-Volume, mit deren Hilfe die Metadaten für das zugeordnete Gerät verwaltet werden. Die Verwaltungssoftware erkennt die Zuordnungsdatei als normale Festplattendatei, die für normale Dateisystemoperationen zur Verfügung steht. Die virtuelle Maschine erkennt das zugeordnete Gerät aufgrund der Speichervirtualisierungsebene als virtuelles SCSI-Gerät.

Zu den wichtigsten Metadaten in der Zuordnungsdatei gehören der Speicherort (Namensauflösung) sowie der Sperrstatus des zugeordneten Geräts, Berechtigungen usw.

Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“ für RDM

Sie können RDMs in virtuellen oder physischen Kompatibilitätsmodi verwenden. Der virtuelle Modus legt die vollständige Virtualisierung des zugeordneten Geräts fest. Der physische Modus legt eine minimale SCSI-Virtualisierung des zugeordneten Geräts fest, wodurch eine optimale Flexibilität der SAN-Verwaltungssoftware erreicht wird.

Im virtuellen Modus sendet der VMkernel nur „Lesen“ und „Schreiben“ an das zugeordnete Gerät. Das Gastbetriebssystem erkennt keinen Unterschied zwischen einem zugeordneten Gerät und einer virtuellen Festplattendatei auf einem VMFS-Volume. Die tatsächlichen Hardwaremerkmale sind verborgen. Wenn Sie eine Raw-Festplatte im virtuellen Modus verwenden, können Sie die Vorteile von VMFS wie leistungsfähige Dateisperrung zum Datenschutz und Snapshots zur Vereinfachung von Entwicklungsprozessen nutzen. Der virtuelle Modus ist auch besser zwischen Speichergeräten portierbar als der physische Modus, da er das gleiche Verhalten wie virtuelle Festplattendateien aufweist.

Im physischen Modus leitet der VMkernel alle SCSI-Befehle bis auf eine Ausnahme an das Gerät weiter: Der Befehl REPORT LUNs ist virtualisiert, damit der VMkernel die LUN für die entsprechende virtuelle Maschine isolieren kann. Ansonsten sind alle physischen Charakteristika der zu Grunde liegenden Hardware sichtbar. Der physische Modus ist für die Ausführung von SAN-Verwaltungs-Agenten oder anderer SCSI-Ziel-basierter Software in der virtuellen Maschine bestimmt. Der physische Modus ermöglicht auch zum kostengünstigen Erzielen einer hohen Verfügbarkeit die Bildung von VM-PC-Clustern.

VMFS5 und VMFS6 unterstützen Festplattengrößen von mehr als 2 TB für RDMs im virtuellen und physischen Modus.

Dynamische Namensauflösung

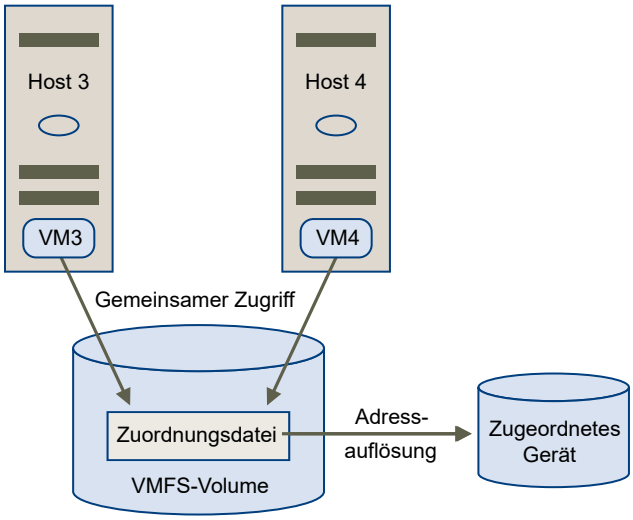
Die RDM-Datei unterstützt die dynamische Namensauflösung, wenn sich ein Pfad zu einem Raw-Device ändert.

Alle zugeordneten Speichergeräte werden durch VMFS eindeutig bezeichnet. Die Bezeichnung wird in den internen LUN-Datenstrukturen gespeichert. Alle Änderungen am Pfad zu einem Raw-Device, z. B. ein Fibre-Channel-Switchfehler oder das Hinzufügen eines neuen HBAs, können den Gerätenamen ändern. Die dynamische Namensauflösung löst diese Änderungen auf und verknüpft das ursprüngliche Gerät automatisch mit seinem neuen Namen.

Raw-Gerätezuordnung für Cluster aus virtuellen Maschinen

Die Verwendung einer Raw-Gerätezuordnung ist für Cluster mit virtuellen Maschinen erforderlich, die zur Sicherstellung von Failover auf die gleiche Raw-LUN zugreifen müssen. Die Einrichtung ist vergleichbar mit der Einrichtung eines solchen Clusters mit Zugriff auf dieselbe virtuelle Festplattendatei. Die virtuelle Festplattendatei wird dabei allerdings durch die Raw-Gerätezuordnung ersetzt.

Abbildung 19-3. Zugriff aus virtuellen Maschinen in Clustern



Vergleichen der verfügbaren Zugriffmodi für SCSI-Geräte

Zu den Möglichkeiten, auf ein SCSI-basiertes Speichergerät zuzugreifen, gehören eine virtuelle Festplattendatei auf einem VMFS-Datenspeicher, RDM im virtuellen Modus und RDM im physischen Modus.

Die folgende Tabelle bietet einen Vergleich der in den verschiedenen Modi zur Verfügung stehenden Funktionen.

Tabelle 19-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Gerätezuordnungen

Funktionen von ESXi	Virtuelle Festplattendatei	Raw-Gerätezuordnung – Virtueller Modus	Raw-Gerätezuordnung – Physischer Modus
Weitergabe von SCSI-Befehlen	Nein	Nein	Ja Der Befehl `REPORT LUNs` wird nicht weitergegeben
Unterstützung von vCenter Server	Ja	Ja	Ja
Snapshots	Ja	Ja	Nein
Verteilte Sperrung	Ja	Ja	Ja
Clusterbildung	Nur systeminterne Cluster	Systeminterne Cluster Systemübergreifende Cluster	Physisch-zu-Virtuell-Clustering Systemübergreifende Cluster
SCSI-Ziel-basierte Software	Nein	Nein	Ja

Verwenden Sie für systeminterne Cluster virtuelle Festplattendateien. Wenn Sie systeminterne Cluster als systemübergreifende Cluster rekonfigurieren möchten, verwenden Sie für systeminterne Cluster Raw-Gerätezuordnungen.

Erstellen von virtuellen Maschinen mit Raw-Gerätezuordnungen

Wenn Sie eine virtuelle Maschine mit einem Direktzugriff auf eine Raw-SAN-LUN versehen, erstellen Sie eine RDM-Festplatte, die sich in einem VMFS-Datenspeicher befindet und auf die LUN verweist. Sie können die Raw-Gerätezuordnung als Ausgangsfestplatte für eine neue virtuelle Maschine erstellen oder sie einer vorhandenen virtuellen Maschine hinzufügen. Beim Erstellen der Raw-Gerätezuordnung geben Sie die zuzuordnende LUN und den Datenspeicher an, in dem die Raw-Gerätezuordnung abgelegt werden soll.

Wenngleich die RDM-Festplattendatei dieselbe `.vmdk`-Erweiterung wie eine herkömmliche virtuelle Festplattendatei hat, enthält die RDM nur Zuordnungsinformationen. Die eigentlichen virtuellen Festplattendaten werden direkt in der LUN gespeichert.

Bei diesem Verfahren wird vorausgesetzt, dass Sie eine neue virtuelle Maschine erstellen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Verfahren

1 Erstellen Sie eine virtuelle Maschine.

   a Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datencenter, Ordner, Cluster, Ressourcenpool oder Host, und wählen Sie die Option **Neue virtuelle Maschine** aus.

   b Wählen Sie **Eine neue virtuelle Maschine erstellen** und klicken Sie auf **Weiter**.

   c Befolgen Sie sämtliche Anweisungen zum Erstellen einer virtuellen Maschine.

2 Klicken Sie auf der Seite „Hardware anpassen“ auf die Registerkarte **Virtuelle Hardware**.

3 (Optional) Um die virtuelle Standardfestplatte zu löschen, die vom System für ihre virtuelle Maschine erstellt wurde, bewegen Sie den Cursor über die Festplatte und klicken Sie auf das Symbol **Entfernen**.

4 Fügen Sie eine RDM-Festplatte hinzu.

   a Klicken Sie auf **Neue Geräte hinzufügen** und wählen Sie **RDM-Festplatte** in der Liste aus.

   b Wählen Sie eine Ziel-Raw-LUN in der Liste der LUNs aus und klicken Sie auf **OK**.

   Das System erstellt eine RDM-Festplatte, die Ihre virtuelle Maschine der Ziel-LUN zuordnet. Die RDM-Festplatte wird in der Liste der virtuellen Geräte als neue Festplatte angezeigt.

5 Konfigurieren Sie die RDM-Festplatte.

a Klicken Sie auf das Dreieck **Neue Festplatte**, um die Eigenschaften für die RDM-Festplatte zu erweitern.

b Wählen Sie einen Speicherort für die RDM aus.

Sie können die RDM im selben Datenspeicher ablegen, in dem sich die Konfigurationsdateien der virtuellen Maschine befinden, oder einen anderen Datenspeicher auswählen.

Hinweis Um vMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die RDM-Dateien und die Dateien der virtuellen Maschinen im selben Datenspeicher befinden. Sie können Storage vMotion nicht durchführen, wenn NPIV aktiviert ist.

c Wählen Sie den Kompatibilitätsmodus aus.

Option	Beschreibung
Physisch	Ermöglicht es dem Gastbetriebssystem, auf die Hardware direkt zuzugreifen. Der physische Kompatibilitätsmodus bietet sich an, wenn Sie SAN-fähige Anwendungen in der virtuellen Maschine einsetzen. Eine virtuelle Maschine, die für einen physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung konfiguriert ist, kann jedoch weder geklont noch in eine Vorlage umgewandelt noch migriert werden, wenn für die Migration die Festplatte kopiert werden muss.
Virtuell	Ermöglicht es der RDM, sich wie eine virtuelle Festplatte zu verhalten, sodass Sie Funktionen wie Snapshot-Erstellung, Klonen usw. verwenden können. Wenn Sie die Festplatte klonen oder eine Vorlage daraus erstellen, wird der Inhalt der LUN in eine virtuelle Festplattendatei `.vmdk` kopiert. Wenn Sie eine RDM im virtuellen Kompatibilitätsmodus migrieren, können Sie die Zuordnungsdatei migrieren oder den Inhalt der LUN in eine virtuelle Festplatte kopieren.

d Wenn Sie den virtuellen Kompatibilitätsmodus ausgewählt haben, wählen Sie einen Festplattenmodus.

Festplattenmodi stehen für RDM-Festplatten mit physischem Kompatibilitätsmodus nicht zur Verfügung.

Option	Beschreibung
Abhängig	Abhängige Festplatten sind in Snapshots enthalten.
Unabhängig – Persistent	Festplatten im persistenten Modus verhalten sich wie konventionelle Festplatten auf einem physischen Computer. Sämtliche Daten, die im persistenten Modus auf eine Festplatte geschrieben werden, werden permanent auf die Festplatte geschrieben.
Unabhängig – Nicht persistent	Änderungen, die im nicht persistenten Modus an Festplatten vorgenommen werden, werden beim Ausschalten oder Zurücksetzen der virtuellen Maschine verworfen. Der nicht persistente Modus sorgt dafür, dass sich die virtuelle Festplatte einer virtuellen Maschine bei jedem Neustart in demselben Zustand befindet. Änderungen an der Festplatte werden in eine Redo-Protokolldatei geschrieben und daraus gelesen. Diese Datei wird beim Ausschalten oder Zurücksetzen gelöscht.

6 Schließen Sie die Konfiguration der virtuellen Maschine ab.

Verwalten von Pfaden in zugeordneten LUNs

Wenn Sie virtuelle Maschinen mit RDMs verwenden, können Sie Pfade für zugeordnete Raw-LUNs verwalten.

Verfahren

1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

2 Klicken Sie auf die Registerkarte **Virtuelle Hardware** und dann auf **Festplatte**, um das Menü mit den Festplattenoptionen zu erweitern.

3 Klicken Sie auf die Geräte-ID, die neben **Physische LUN** angezeigt wird, um das Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten** zu öffnen.

4 Im Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten** können Sie Ihre Pfade aktivieren oder deaktivieren, eine Multipathing-Richtlinie festlegen und den bevorzugten Pfad angeben.

   Weitere Informationen zur Verwaltung von Pfaden finden Sie unter Kapitel 18 Grundlegende Informationen zu Multipathing und Failover.

Virtuelle Maschinen mit RDMs müssen den SCSI INQUIRY-Cache ignorieren

Bestimmte virtuelle Maschinen mit RDMs müssen die SCSI INQUIRY-Informationen aus der LUN und nicht aus den in SCSI INQUIRY zwischengespeicherten Daten abrufen ESXi.

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 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. Antworten für nachfolgende SCSI INQUIRY-Befehle werden aus dem Cache zurückgegeben.

Bestimmte Gastbetriebssysteme jedoch, die in virtuellen Maschinen mit RDMs ausgeführt werden, müssen die LUN anstelle der von ESXi im Cache-Speicher gespeicherten SCSI INQUIRY-Daten abfragen. In diesen Fällen können Sie die virtuelle Maschine dahingehend konfigurieren, das SCSI INQUIRY-Cache zu ignorieren.

Lösung

- Verwenden Sie eine der folgenden Methoden:

Option	Beschreibung
Ändern Sie die .vmx-Datei für die virtuelle Maschine mit der RDM.	Verwenden Sie diese Methode für die virtuellen Maschinen mit Hardwareversion 8 oder höher. a Fügen Sie der Datei den folgenden Parameter hinzu: `scsi`*x*`:`*y*`.ignoreDeviceInquiryCache = "true"` wobei *x* die Nummer des SCSI-Controllers und *y* die SCSI-Zielnummer der RDM ist. b Starten Sie die virtuelle Maschine neu.
Verwenden Sie den Befehl `esxcli`.	Da Sie die Einstellung auf Host-Ebene konfigurieren, gelten keine Einschränkungen bei VM-Hardwareversionen. `esxcli storage core device inquirycache set --device` *`device id`* `--ignore true` Es ist kein VM-Neustart erforderlich.

Unabhängig davon, welche Methode Sie verwenden, um den SCSI INQUIRY-Cache-Parameter auf „true“ zu setzen, die VM nimmt direkt eine Verbindung mit der LUN auf, um SCSI INQUIRY-Daten abzurufen.

Parameter ignoreDeviceInquiryCache in vmx	Parameter inquirycache in esxcli ignorieren	Anfrageanforderung bearbeitet in
True	True	LUN
„False“ (Standard, wenn der Parameter nicht vorhanden ist)	True	LUN
True	False	LUN
„False“ (Standard, wenn der Parameter nicht vorhanden ist)	False	Cache

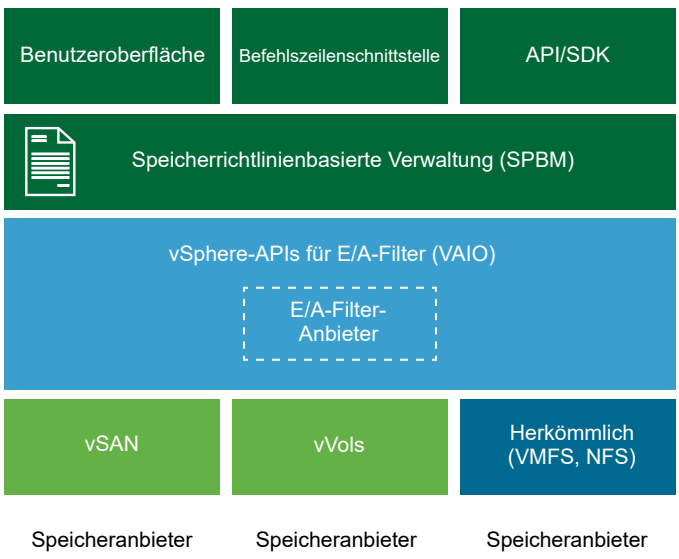
Speicherrichtlinienbasierte Verwaltung

20

Innerhalb eines softwaredefinierten Datencenters spielt speicherrichtlinienbasierte Verwaltung (Storage Policy Based Management, SPBM) eine entscheidende Rolle bei der Abstimmung der Speicherkapazität mit den Anwendungsanforderungen der virtuellen Maschinen. SPBM stellt ein Speicherrichtlinien-Framework bereit, das als einheitliche Steuerzentrale für ein breites Spektrum von Datendiensten und Speicherlösungen fungiert.

Als Abstraktionsschicht abstrahiert SPBM Speicherdienste, die von Virtual Volumes, vSAN, E/A-Filtern oder anderen Speicherelementen bereitgestellt werden.

Statt der Integration mit jedem einzelnen Speicher- und Datendiensttyp stellt SPBM ein universelles Framework für verschiedene Arten von Speicherelementen zur Verfügung.



SPBM stellt die folgenden Mechanismen zur Verfügung:

- Ankündigung von Speicherfunktionen und Datendiensten, die Arrays und andere Elemente, beispielsweise E/A-Filter, anbieten.
- Bidirektionale Kommunikation zwischen ESXi und vCenter Server auf der einen Seite und Speicher-Arrays und Elementen auf der anderen.
- Bereitstellung virtueller Maschinen basierend auf VM-Speicherrichtlinien.

Dieses Kapitel enthält die folgenden Themen:

Speicherrichtlinien für virtuelle Maschinen

VM-Speicherrichtlinien sind entscheidend für die Bereitstellung von virtuellen Maschinen über SPBM. Mit den Richtlinien wird gesteuert, welcher Speichertyp für die virtuelle Maschine bereitgestellt wird und wie die virtuelle Maschine innerhalb des Speichers platziert wird. Sie bestimmen außerdem, welche Datendienste die virtuelle Maschine nutzen kann.

vSphere bietet Standardspeicherrichtlinien. Darüber hinaus können Sie eigene Richtlinien definieren und virtuellen Maschinen zuweisen.

Mithilfe der Schnittstelle für VM-Speicherrichtlinien können Sie eine Speicherrichtlinie erstellen. Wenn Sie die Richtlinie definieren, geben Sie verschiedene Speicheranforderungen für Anwendungen an, die auf den virtuellen Maschinen ausgeführt werden. Sie können auch mithilfe von Speicherrichtlinien bestimmte Datendienste für virtuelle Festplatten anfordern. Zu diesen Diensten gehören beispielsweise Caching oder Replizierung.

Sie wenden die Speicherrichtlinie an, wenn Sie die virtuelle Maschine erstellen, klonen oder migrieren. Nachdem Sie die Speicherrichtlinie angewendet haben, unterstützt Sie der SPBM-Mechanismus bei der Platzierung der virtuellen Maschine in einem passenden Datenspeicher. In bestimmten Speicherumgebungen legt SPBM fest, wie die VM-Speicherobjekte bereitgestellt und innerhalb der Speicherressource zugewiesen werden, um die erforderliche Dienstebene zu garantieren. SPBM aktiviert auch angeforderte Datendienste für die virtuelle Maschine und unterstützt Sie bei der Überwachung der Richtlinieneinhaltung.

Workflow für VM-Speicherrichtlinien

Der Vorgang zum Erstellen und Verwalten von Speicherrichtlinien umfasst üblicherweise mehrere Schritte.

Ob die einzelnen Schritte ausgeführt müssen, hängt möglicherweise vom Speichertyp oder den Datendiensten in Ihrer Umgebung ab.

Schritt	Beschreibung
Füllen Sie die Richtlinie für VM-Speicherrichtlinien mit den entsprechenden Daten auf.	Die Schnittstelle für VM-Speicherrichtlinien wird mit den Informationen zu Datenspeichern und Datendiensten aufgefüllt, die in Ihrer Speicherumgebung verfügbar sind. Diese Informationen werden von Speicheranbietern und Datenspeicher-Tags bezogen. ■ Überprüfen Sie für Elemente, die von Speicheranbietern dargestellt werden, ob ein entsprechender Anbieter registriert ist. Zu den Elementen, die die Speicheranbieter verwenden, zählen vSAN, Virtual Volumes und E/A-Filter. Je nach Typ des Speicherelements handelt es sich bei einigen Anbietern um selbstregistrierte Anbieter. Andere Anbieter hingegen müssen manuell registriert werden. Siehe Verwenden von Speicheranbietern zum Auffüllen der Schnittstelle für VM-Speicherrichtlinien und Registrieren von Virtual Volumes-Speicheranbietern. ■ Tag-Datenspeicher, die nicht von Speicheranbietern repräsentiert werden. Mithilfe von Tags können Sie auch eine Eigenschaft angeben, die nicht über der Speicheranbieter übertragen wird, beispielsweise einen geografischen Standort oder eine Administratorengruppe. Weitere Informationen hierzu finden Sie unter Zuweisen von Tags zu Datenspeichern.
Erstellen Sie vordefinierte Speicherrichtlinienkomponenten.	Eine Speicherrichtlinienkomponente beschreibt einen einzelnen Datendienst (beispielsweise Replizierung), der für die virtuelle Maschine bereitgestellt werden muss. Sie können die Komponente im Voraus definieren und mehreren VM-Speicherrichtlinien zuordnen. Die Komponenten sind wiederverwendbar und austauschbar. Weitere Informationen hierzu finden Sie unter Erstellen von Speicherrichtlinienkomponenten.
Erstellen Sie die VM-Speicherrichtlinien.	Beim Definieren von Speicherrichtlinien für virtuelle Maschinen geben Sie die Speicheranforderungen für die Anwendungen an, die auf den virtuellen Maschinen ausgeführt werden. Weitere Informationen hierzu finden Sie unter Erstellen und Verwalten von VM-Speicherrichtlinien.
Wenden Sie die VM-Speicherrichtlinie auf die virtuelle Maschine an.	Sie können die Speicherrichtlinie anwenden, wenn Sie die virtuelle Maschine bereitstellen oder deren virtuelle Festplatten konfigurieren. Weitere Informationen hierzu finden Sie unter Zuweisen von Speicherrichtlinien zu virtuellen Maschinen.
Prüfen Sie die Übereinstimmung mit der VM-Speicherrichtlinie.	Überprüfen Sie, ob die virtuelle Maschine den Datenspeicher verwendet, der der zugewiesenen Speicherrichtlinie entspricht. Weitere Informationen hierzu finden Sie unter Prüfen der Übereinstimmung für eine VM-Speicherrichtlinie.

Zum Erstellen und Verwalten Ihrer Speicherrichtlinien verwenden Sie die Schnittstelle für VM-Speicherrichtlinien des vSphere Client.

Auffüllen der Schnittstelle für VM-Speicherrichtlinien

Vor dem Erstellen von VM-Speicherrichtlinien müssen Sie die Schnittstelle für VM-Speicherrichtlinien mit Informationen über Speicherentitäten und Datendienste befüllen, die in Ihrer Speicherumgebung verfügbar sind.

Diese Informationen werden von Speicheranbietern bezogen, die auch als VASA-Anbieter bezeichnet werden. Eine weitere Quelle sind Datenspeicher-Tags.

Speicherfunktionen und Dienste

Bestimmte Datenspeicher, beispielsweise Virtual Volumes und vSAN, werden durch die Speicheranbieter repräsentiert. Über die Speicheranbieter können die Datenspeicher ihre Funktionen in der Schnittstelle für VM-Speicherrichtlinien ankündigen. Die Schnittstelle für VM-Speicherrichtlinien wird mit diesen Datenspeicherfunktionen, Datendiensten und sonstigen Merkmalen mit Wertebereichen befüllt.

Diese Merkmale werden beim Definieren datenspeicherbasierter Platzierungs- und Dienstregeln für Ihre Speicherrichtlinie verwendet.

Datendienste

E/A-Filter auf Ihren Hosts werden auch durch die Speicheranbieter repräsentiert. Der Speicheranbieter stellt der Schnittstelle für VM-Speicherrichtlinien Informationen zu den Datendiensten der Filter bereit. Sie können diese Informationen verwenden, wenn Sie die Regeln für hostbasierte Datendienste, die auch als allgemeine Regeln bezeichnet werden, definieren. Anders als datenspeicherspezifische Regeln definieren diese Regeln keine Speicherplatzierung und Speicheranforderungen für die virtuelle Maschine. Stattdessen aktivieren sie den angeforderten E/A-Filter für die virtuelle Maschine.

Tags

In der Regel werden VMFS- und NFS-Datenspeicher nicht von einem Speicheranbieter repräsentiert. Ihre Funktionen und Datendienste werden nicht in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Informationen über diese Datenspeicher können mithilfe von Tags kodiert werden. Beispielsweise können Sie Ihre VMFS-Datenspeicher zur Darstellung verschiedener Dienstebenen mit VMFS-Gold- und VMFS-Silver-Tags versehen.

Für Virtual Volumes- und vSAN-Datenspeicher können Sie Tags verwenden, um Informationen zu verschlüsseln, die nicht vom Speicheranbieter angekündigt werden, wie beispielsweise den geografischen Standort (Palo Alto) oder die Verwaltungsgruppe (Buchhaltung).

Ähnlich wie Speicherfunktionen und -merkmale werden alle mit Datenspeichern verbundenen Tags in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Die Tags können Sie beim Definieren Tag-basierter Platzierungsregeln verwenden.

Verwenden von Speicheranbietern zum Auffüllen der Schnittstelle für VM-Speicherrichtlinien

Überprüfen Sie für Elemente, die von Speicheranbietern (VASA) repräsentiert werden, ob ein entsprechender Anbieter registriert ist. Nachdem die Speicheranbieter registriert wurden, wird die Schnittstelle für VM-Speicherrichtlinien mit Informationen über die von den Anbietern repräsentierten Datenspeicher und Datendienste aufgefüllt.

Zu den Elementen, die die Speicheranbieter verwenden, zählen vSAN, Virtual Volumes und E/A-Filter. Je nach Elementtyp handelt es sich bei einigen Anbietern um selbstregistrierte Anbieter. Andere Anbieter, wie beispielsweise der Virtual Volumes-Speicheranbieter, müssen manuell registriert werden. Nachdem die Speicheranbieter registriert wurden, liefern sie die folgenden Daten an die Schnittstelle für VM-Speicherrichtlinien:

- Speicherfunktionen und Merkmale für Datenspeicher wie Virtual Volumes und vSAN
- Von den E/A-Filtern bereitgestellte Datendienste.

Voraussetzungen

Registrieren Sie die Speicheranbieter, die manuell registriert werden müssen. Weitere Informationen finden Sie in der entsprechenden Dokumentation .

- *Verwalten von VMware vSAN*
- Kapitel 22 Arbeiten mit VMware vSphere Virtual Volumes
- Kapitel 23 Filtern der E/A einer virtuellen Maschine

Verfahren

1. Navigieren Sie zur vCenter Server-Instanz.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
3. Zeigen Sie in der Liste der Speicheranbieter die bei vCenter Server registrierten Speicheranbieter an.

   Die Liste enthält allgemeine Informationen, wie beispielsweise den Namen des Speicheranbieters, die URL und den Status sowie die Speicherelemente, die der Anbieter repräsentiert.
4. Wenn Sie weitere Details anzeigen möchten, wählen Sie einen bestimmten Speicheranbieter oder seine Komponente in der Liste aus.

Zuweisen von Tags zu Datenspeichern

Verwenden Sie Tags, um Informationen über einen Datenspeicher zu kodieren. Die Tags sind hilfreich, wenn der Datenspeicher nicht durch einen Speicheranbieter repräsentiert wird und seine Dienste nicht in der Schnittstelle für VM-Speicherrichtlinien angezeigt werden. Mithilfe der Tags können Sie auch eine Eigenschaft angeben, die nicht über einen Speicheranbieter übertragen wird, beispielsweise einen geografischen Standort oder eine Administratorengruppe.

Sie können ein neues Tag anwenden, das allgemeine Speicherinformationen für einen Datenspeicher enthält. Weitere Informationen über die Tags, ihre Kategorien und die Verwaltung von Tags finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Voraussetzungen

Erforderliche Rechte:

- **vSphere Tagging.vSphere Tag erstellen** für die Root-Instanz von vCenter Server
- **vSphere Tagging.vSphere Tag-Kategorie erstellen** für die Root-Instanz von vCenter Server
- **vSphere Tagging.vSphere Tag zuweisen oder Zuweisung aufheben** für die Root-Instanz von vCenter Server

Verfahren

1 Erstellen Sie im vSphere Client eine Kategorie für Speicher-Tags.

   a Klicken Sie im Menü „Home“ auf **Tags und benutzerdefinierte Attribute**.

   b Klicken Sie auf die Registerkarte **Tags** und anschließend auf **Kategorien**.

   c Klicken Sie auf das Symbol **Kategorie hinzufügen**.

   d Geben Sie die Eigenschaften der Kategorie an. Betrachten Sie das folgende Beispiel.

Kategorieeigenschaften	Beispiel
Kategoriename	Speicherort
Beschreibung	Kategorie für Tags, die mit dem Speicherort zusammenhängen
Tags pro Objekt	**Viele Tags**
Zuweisbare Objekttypen	**Datenspeicher** und **Datenspeicher-Cluster**

   e Klicken Sie auf **OK**.

2 Erstellen Sie ein Speicher-Tag.

   a Klicken Sie auf die Registerkarte **Tags** und anschließend auf **Tags**.

   b Klicken Sie auf das Symbol **Tag hinzufügen**.

   c Geben Sie die Eigenschaften des Tags an. Betrachten Sie das folgende Beispiel.

Tag-Eigenschaft	Beispiel
Name	Texas
Beschreibung	Datenspeicher, der sich in Texas befindet
Kategorie	Speicherort

   d Klicken Sie auf **OK**.

3 Wenden Sie das Tag auf den Datenspeicher an.

a Navigieren Sie zum Datenspeicher.

b Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Tags und benutzerdefinierte Attribute > Tag zuweisen** aus.

c Wählen Sie in der Liste der Tags ein entsprechendes Tag aus (z. B. „Texas“ in der Kategorie „Speicherort“) und klicken Sie dann auf **Zuweisen**.

Ergebnisse

Das neue Tag wird dem Datenspeicher zugewiesen und auf der Registerkarte **Übersicht** des Datenspeichers im Bereich **Tags** eingeblendet.

Nächste Schritte

Beim Erstellen einer VM-Speicherrichtlinie können Sie auf das Tag verweisen, um den mit Tags versehenen Datenspeicher in die Liste der kompatiblen Speicherressourcen aufzunehmen. Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für die Tag-basierte Platzierung.

Sie können den mit Tags versehenen Datenspeicher auch aus der VM-Speicherrichtlinie ausschließen. Beispielsweise kann die VM-Speicherrichtlinie Virtual Volumes-Datenspeicher umfassen, die sich in Texas und Kalifornien befinden, während Datenspeicher in Nevada ausgeschlossen werden.

Im folgenden Video erhalten Sie weitere Informationen zur Verwendung der Tags in VM-Speicherrichtlinien.

 (Verwenden von Tags in Speicherrichtlinien)

Regeln und Regelsätze

Nachdem die Schnittstelle für VM-Speicherrichtlinien mit den entsprechenden Daten aufgefüllt wurde, können Sie mit der Erstellung der Speicherrichtlinien beginnen. Das Erstellen einer Richtlinie umfasst das Definieren von bestimmten Regeln zur Speicherplatzierung und Regeln zum Konfigurieren von Datendiensten.

Regeln

Eine Regel ist ein grundlegendes Element der VM-Speicherrichtlinie. Bei jeder einzelnen Regel handelt es sich um eine Aussage, die eine einzelne Anforderung für VM-Speicher und Datendienste beschreibt.

Regelsätze

Innerhalb einer Speicherrichtlinie sind einzelne Regeln in Regelsammlungen oder Regelsätzen organisiert. Regelsätze können üblicherweise zu einer der folgenden Kategorien gehören: Regeln für hostbasierte Dienste und datenspeicherspezifische Regeln.

Datenspeicherspezifische Regelsätze

Jeder Regelsatz muss Platzierungsregeln enthalten, die Anforderungen für die Speicherressourcen virtueller Maschinen beschreiben. Alle Platzierungsregeln in einem einzelnen Regelsatz stellen ein einzelnes Speicherelement dar. Diese Regeln können auf Speicherfunktionen oder Tags basieren.

Darüber hinaus kann ein datenspeicherspezifischer Regelsatz optionale Regeln oder Speicherrichtlinienkomponenten enthalten, die Datendienste beschreiben, die für die virtuelle Maschine bereitgestellt werden sollen. Normalerweise werden mit diesen Regeln Dienste wie Caching, Replizierung und weitere von Speichersystemen bereitgestellte Dienste angefordert.

Zum Definieren der Speicherrichtlinie ist nur ein datenspeicherspezifischer Satz erforderlich. Zusätzliche Regelsätze sind optional. Eine einzelne Richtlinie kann mehrere Regelsätze nutzen, um alternative Speicherplatzierungsparameter zu definieren, die häufig von mehreren Speicheranbietern stammen.

Platzierungsregeln: Funktionsbasiert

Mithilfe von Platzierungsregeln wird eine bestimmte Speicheranforderung für die VM angegeben, und SPBM erhält die Möglichkeit, unter allen Datenspeichern im Bestand die kompatiblen Datenspeicher zu ermitteln. Diese Regeln beschreiben auch, wie die VM-Speicherobjekte innerhalb des Datenspeichers zugeteilt werden, um die erforderliche Dienstebene zu erhalten. Beispiel: In den Regeln kann Virtual Volumes als Ziel aufgeführt und das maximale Recovery Point Objective (RPO) für die Virtual Volumes-Objekte definiert sein.

Bei der Bereitstellung der virtuellen Maschine wird die Entscheidung, die SPBM bezüglich der Platzierung der virtuellen Maschine trifft, durch diese Regeln bestimmt. SPBM findet den Virtual Volumes-Datenspeicher, der die Regeln einhalten und die Speicheranforderungen der virtuellen Maschine erfüllen kann. Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für Virtual Volumes.

Platzierungsregeln: Tag-basiert

Tag-basierte Regeln verweisen auf Datenspeicher-Tags. Mit diesen Regeln kann die VM-Platzierung definiert werden. So können beispielsweise alle Datenspeicher mit dem VMFS-Gold-Tag als Ziel angefordert werden. Mithilfe der Tag-basierten Regeln kann Ihre VM-Platzierungsanforderung auch noch weitergehend optimiert werden. Sie können beispielsweise Datenspeicher mit dem Palo Alto-Tag aus der Liste Ihrer Virtual Volumes-Datenspeicher ausschließen. Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für die Tag-basierte Platzierung.

Regeln für hostbasierte Dienste

Mit diesem Regelsatz werden vom Host bereitgestellte Datendienste aktiviert. Der Satz für hostbasierte Dienste kann Regeln oder Speicherrichtlinienkomponenten enthalten, die bestimmte Datendienste, wie beispielsweise Verschlüsselung und Replizierung, beschreiben.

Anders als bei datenspeicherspezifischen Regeln enthält dieser Satz keine Platzierungsregeln. Regeln für hostbasierte Dienste gelten für alle Speichertypen und sind nicht abhängig vom Datenspeicher. Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für hostbasierte Datendienste.

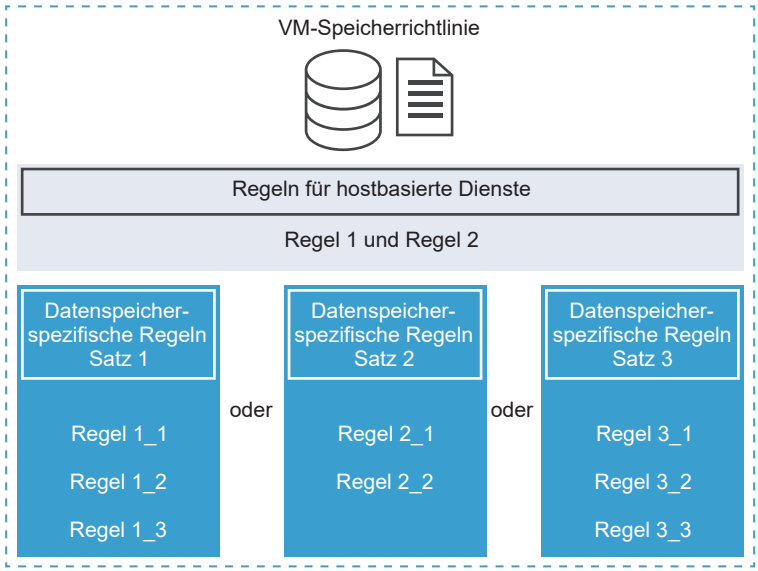
Tabelle 20-1. Struktur einer VM-Speicherrichtlinie

Regeln für hostbasierte Dienste	Datenspeicherspezifische Regelsätze
Regeln oder vordefinierte Speicherrichtlinienkomponenten zum Aktivieren von Datendiensten, die auf ESXi-Hosts installiert sind. Beispiel: Replizierung mittels E/A-Filter	Funktionsbasierte oder Tag-basierte Platzierungsregeln, die Anforderungen für die Speicherressourcen virtueller Maschinen beschreiben. Beispiel: Virtual Volumes-Platzierung.
	Regeln oder vordefinierte Speicherrichtlinienkomponenten, die vom Speicher bereitgestellte Datendienste aktivieren. Beispiel: Zwischenspeicherung durch Virtual Volumes.

Beziehungen zwischen Regeln und Regelsätzen

Der boolesche Operator `OR` definiert die Beziehung zwischen den datenspeicherspezifischen Regelsätzen innerhalb der Richtlinie. Der Operator `AND` definiert die Beziehung zwischen allen Regeln innerhalb eines Regelsatzes. Die Richtlinie kann nur einen Regelsatz für hostbasierte Dienste oder nur einen datenspeicherspezifischen Regelsatz oder beides enthalten.

Wenn kein Regelsatz für hostbasierte Dienste vorhanden ist, ist die Einhaltung aller Regeln eines einzelnen datenspeicherspezifischen Regelsatzes ausreichend zur Einhaltung der gesamten Richtlinie. Ist der Regelsatz für hostbasierte Dienste vorhanden, entspricht die Richtlinie dem Datenspeicher, der die Hostdiensteregeln und alle Regeln in einem der datenspeicherspezifischen Sätze erfüllt.



Erstellen und Verwalten von VM-Speicherrichtlinien

Zum Erstellen und Verwalten von Speicherrichtlinien für virtuelle Maschinen verwenden Sie die Schnittstelle für VM-Speicherrichtlinien.

Erstellen einer VM-Speicherrichtlinie für hostbasierte Datendienste

Zum Definieren der VM-Speicherrichtlinie in vSphere Client verwenden Sie den Assistenten **VM-Speicherrichtlinie erstellen**. In dieser Aufgabe erstellen Sie Regeln für Datendienste, die von ESXi-Hosts angeboten werden. Die VM-Speicherrichtlinie, die diese Regeln enthält, aktiviert angegebene Datendienste für die virtuelle Maschine.

Verfügbare Datendienste sind unter anderem Verschlüsselung, E/A-Steuerung oder Zwischenspeicherung. Bestimmte Datendienste, wie zum Beispiel die Verschlüsselung, werden von VMware zur Verfügung gestellt. Andere Dienste können von Drittanbieter-E/A-Filtern bereitgestellt werden, die Sie auf Ihrem Host installieren.

Die Datendienste gelten in der Regel für alle Speichertypen und sind nicht abhängig vom Datenspeicher. Sie können der Speicherrichtlinie optional datenspeicherspezifische Regeln hinzufügen.

Wenn Sie datenspeicherspezifische Regeln hinzufügen und die E/A-Filter auf dem Host und im Speicher denselben Diensttyp (z. B. Verschlüsselung) anbieten, kann Ihre Richtlinie diesen Dienst von beiden Anbietern anfordern. Infolgedessen werden die Daten der virtuellen Maschine zweimal verschlüsselt, und zwar durch den E/A-Filter und Ihren Speicher. Die von Virtual Volumes bereitgestellte Replizierung und die vom E/A-Filter bereitgestellte Replizierung können jedoch nicht in derselben Speicherrichtlinie parallel verwendet werden.

Voraussetzungen

- Informationen zum Verschlüsseln virtueller Maschinen finden Sie im Handbuch *vSphere-Sicherheit*.
- Informationen zu E/A-Filtern finden Sie unter Kapitel 23 Filtern der E/A einer virtuellen Maschine.
- Informationen zu Speicherrichtlinienkomponenten finden Sie unter Informationen zu Speicherrichtlinienkomponenten.
- Erforderliche Rechte: **VM-Speicherrichtlinien.Aktualisieren** und **VM-Speicherrichtlinien.Anzeigen**.

Verfahren

1. Öffnen Sie den Assistenten **VM-Speicherrichtlinie erstellen**.
   a. Klicken Sie auf **Menü > Richtlinien und Profile**.
   b. Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
   c. Klicken Sie auf **Erstellen**.

2 Geben Sie den Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.

Option	Aktion
vCenter Server	Wählen Sie die vCenter Server-Instanz aus.
Name	Geben Sie den Namen der Speicherrichtlinie ein.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Aktivieren Sie auf der Seite **Richtlinienstruktur** unter **Hostbasierte Dienste** hostbasierte Regeln.

4 Definieren Sie auf der Seite **Hostbasierte Dienste** Regeln zum Aktivieren und Konfigurieren der von Ihrem Host bereitgestellten Datendienste.

a Klicken Sie auf die Registerkarte für die Datendienstkategorie, beispielsweise **Replizierung**.

b Definieren Sie benutzerdefinierte Regeln für die Datendienstkategorie oder verwenden Sie vordefinierte Komponenten.

Option	Beschreibung
Deaktiviert	Hostbasierte Dienste sind standardmäßig deaktiviert.
Speicherrichtlinienkomponente verwenden	Wählen Sie im Dropdown-Menü eine Speicherrichtlinienkomponente aus. Diese Option ist nur verfügbar, wenn Ihre Datenbank vordefinierte Komponenten enthält.
Benutzerdefiniert	Legen Sie benutzerdefinierte Regeln für die Datendienstkategorie fest, indem Sie einen entsprechenden Anbieter und Werte für die Regeln angeben.

Hinweis Sie können mehrere Datendienste aktivieren. Bei Verwendung der Verschlüsselung mit anderen Datendiensten setzen Sie den Parameter **E/A-Filter vor Verschlüsselung zulassen** auf **True**, damit andere Dienste wie beispielsweise die Replizierung Klartextdaten analysieren können, bevor diese verschlüsselt werden.

5 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen.

Die Datenspeicher müssen, damit ihre Kompatibilität mit der Richtlinie für hostbasierte Dienste gewährleistet ist, mit dem Host verbunden sein, der diese Dienste bereitstellt. Wenn Sie der Richtlinie datenspeicherspezifische Regelsätze hinzufügen, müssen die kompatiblen Datenspeicher auch die Speicheranforderungen der Richtlinie erfüllen.

6 Überprüfen Sie auf der Seite **Überprüfen und beenden** die Einstellungen der Speicherrichtlinie und klicken Sie auf **Beenden**.

Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

Ergebnisse

Die neue VM-Speicherrichtlinie für hostbasierte Datendienste wird in der Liste angezeigt.

Erstellen einer VM-Speicherrichtlinie für Virtual Volumes

Zum Definieren der VM-Speicherrichtlinie in vSphere Client verwenden Sie den Assistenten **VM-Speicherrichtlinie erstellen**. In dieser Aufgabe erstellen Sie eine mit Virtual Volumes kompatible benutzerdefinierte Speicherrichtlinie. Wenn Sie die VM-Speicherrichtlinie für Virtual Volumesdefinieren, erstellen Sie Regeln zum Konfigurieren des Speichers und der Datendienste, die vom Virtual Volumes-Datenspeicher bereitgestellt werden. Die Regeln werden angewendet, wenn die virtuelle Maschine im Virtual Volumes-Datenspeicher platziert wird. Die benutzerdefinierte Speicherrichtlinie kann die von VMware bereitgestellte Standardspeicherrichtlinie ohne Anforderungen für Virtual Volumes ersetzen.

Das Verfahren setzt voraus, dass Sie die VM-Speicherrichtlinie für Virtual Volumes erstellen. Informationen zur vSAN-Speicherrichtlinie finden Sie in der *Verwalten von VMware vSAN*-Dokumentation.

Voraussetzungen

- Vergewissern Sie sich, dass der Virtual Volumes-Speicheranbieter verfügbar und aktiv ist. Weitere Informationen hierzu finden Sie unter Registrieren von Virtual Volumes-Speicheranbietern.
- Stellen Sie sicher, dass die Schnittstelle der VM-Speicherrichtlinie mit den Informationen über Speicherelemente und Datendiensten aufgefüllt wird, die in Ihrer Speicherumgebung verfügbar sind. Weitere Informationen hierzu finden Sie unter Auffüllen der Schnittstelle für VM-Speicherrichtlinien.
- Legen Sie entsprechende Komponenten für die Speicherrichtlinie fest. Weitere Informationen hierzu finden Sie unter Erstellen von Speicherrichtlinienkomponenten.
- Erforderliche Rechte: **VM-Speicherrichtlinien.Aktualisieren** und **VM-Speicherrichtlinien.Anzeigen**.

Verfahren

1 Öffnen Sie den Assistenten **VM-Speicherrichtlinie erstellen**.

   a Klicken Sie auf **Menü > Richtlinien und Profile**.

   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.

   c Klicken Sie auf **Erstellen**.

2 Geben Sie den Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.

Option	Aktion
vCenter Server	Wählen Sie die vCenter Server-Instanz aus.
Name	Geben Sie den Namen der Speicherrichtlinie ein, z. B. „Virtual Volumes-Speicherrichtlinie“.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Aktivieren Sie auf der Seite **Richtlinienstruktur** unter „Datenspeicherspezifische Regeln“ die Regeln für einen Zielspeichertyp, beispielsweise für Virtual Volumes-Speicher.

Sie können Regeln für mehrere Datenspeicher aktivieren. Mehrere Regelsätze ermöglichen eine einzelne Richtlinie zur Definition von alternativen Speicherplatzierungsparametern, häufig von mehreren Speicheranbietern.

4 Definieren Sie auf der Seite *Virtual Volumes* für Regeln Speicherplatzierungsregeln für den Virtual Volumes-Zieldatenspeicher.

a Klicken Sie auf die Registerkarte **Platzierung** und dann auf **Regel hinzufügen**.

b Wählen Sie im Dropdown-Menü „Regel hinzufügen“ eine verfügbare Funktion aus und geben Sie ihren Wert an.

Sie können beispielsweise die Anzahl der Lesevorgänge pro Sekunde für die Virtual Volumes-Objekte angeben.

Sie können so viele Regeln wie notwendig für das ausgewählte Speicherelement hinzufügen. Stellen Sie sicher, dass die angegebenen Werte innerhalb des Wertebereichs des Virtual Volumes-Datenspeichers liegen.

c Wenn Sie Ihre Platzierungsanforderung weiter optimieren möchten, klicken Sie auf die Registerkarte **Tags** und fügen Sie eine Tag-basierte Regel hinzu.

Mit Tag-basierten Regeln können Datenspeicher gefiltert werden, indem bestimmte Platzierungskriterien ein- oder ausgeschlossen werden. Beispielsweise kann die VM-Speicherrichtlinie Virtual Volumes-Datenspeicher umfassen, die sich in Texas und Kalifornien befinden, während Datenspeicher in Nevada ausgeschlossen werden.

5 (Optional) Definieren Sie Regeln, um datenspeicherspezifische Dienste zu konfigurieren.

Die Datendienste – wie Verschlüsselung, Zwischenspeicherung oder Replizierung – werden vom Speicher angeboten. Die auf die Datendienste verweisende VM-Speicherrichtlinie fordert diese Dienste für die virtuelle Maschine an, wenn diese im Virtual Volumes-Datenspeicher platziert wird.

a Klicken Sie auf die Registerkarte für die Datendienstkategorie, beispielsweise **Replizierung**.

b Definieren Sie benutzerdefinierte Regeln für die Datendienstkategorie oder verwenden Sie vordefinierte Komponenten.

Option	Beschreibung
Deaktiviert	Datenspeicherspezifische Dienste sind standardmäßig deaktiviert.
Speicherrichtlinienkomponente verwenden	Wählen Sie im Dropdown-Menü eine Speicherrichtlinienkomponente aus. Diese Option ist nur verfügbar, wenn Ihre Datenbank vordefinierte Komponenten enthält.
Benutzerdefiniert	Legen Sie benutzerdefinierte Regeln für die Datendienstkategorie fest, indem Sie einen entsprechenden Anbieter und Werte für die Regeln angeben.

6 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen.

Wenn die Richtlinie mehrere Regelsätze enthält, muss der Datenspeicher mindestens einen Regelsatz sowie alle Regeln in diesem Regelsatz erfüllen.

7 Überprüfen Sie auf der Seite **Überprüfen und beenden** die Einstellungen der Speicherrichtlinie und klicken Sie auf **Beenden**.

Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

Ergebnisse

Die mit Virtual Volumes kompatible neue VM-Speicherrichtlinie wird in der Liste angezeigt.

Nächste Schritte

Sie können diese Richtlinie nun einer virtuellen Maschine zuweisen oder als Standard festlegen.

Erstellen einer VM-Speicherrichtlinie für die Tag-basierte Platzierung

Tag-basierte Regeln verweisen auf die Tags, die Sie den Datenspeichern zuweisen, und können die zur Platzierung der virtuellen Maschinen verwendeten Datenspeicher filtern. Zum Definieren der Tag-basierten Platzierung im vSphere Client verwenden Sie den Assistenten **VM-Speicherrichtlinie erstellen**.

Voraussetzungen

- Stellen Sie sicher, dass die Schnittstelle der VM-Speicherrichtlinie mit den Informationen über Speicherelemente und Datendiensten aufgefüllt wird, die in Ihrer Speicherumgebung verfügbar sind. Weitere Informationen hierzu finden Sie unter Auffüllen der Schnittstelle für VM-Speicherrichtlinien.
- Erforderliche Rechte: **VM-Speicherrichtlinien.Aktualisieren** und **VM-Speicherrichtlinien.Anzeigen**.

Verfahren

1 Öffnen Sie den Assistenten **VM-Speicherrichtlinie erstellen**.

   a Klicken Sie auf **Menü > Richtlinien und Profile**.

   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.

   c Klicken Sie auf **Erstellen**.

2 Geben Sie den Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.

Option	Aktion
vCenter Server	Wählen Sie die vCenter Server-Instanz aus.
Name	Geben Sie den Namen der Speicherrichtlinie ein.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Aktivieren Sie auf der Seite **Richtlinienstruktur** unter „Datenspeicherspezifische Regeln“ Tag-basierte Platzierungsregeln.

4 Erstellen Sie auf der Seite **Tag-basierte Platzierung** die Tag-Regeln.

   a Klicken Sie auf **Tag-Regel hinzufügen** und definieren Sie die Kriterien der Tag-basierten Platzierung. Beispiel:

Option	Beispiel
Tag-Kategorie	Dienstebene
Nutzungsoption	Speicher verwenden, die mit folgenden Tags versehen sind:
Tags	Gold

   Alle Datenspeicher mit dem Gold-Tag werden als Speicherplatzierungsziel kompatibel.

   b (Optional) Fügen Sie weitere Tag-basierte Regeln hinzu.

5 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen.

6 Überprüfen Sie auf der Seite **Überprüfen und beenden** die Einstellungen der Speicherrichtlinie und klicken Sie auf **Beenden**.

   Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

Ergebnisse

Die mit Datenspeichern, die mit Tags versehen sind, kompatible neue VM-Speicherrichtlinie wird in der Liste angezeigt.

Bearbeiten oder Klonen einer VM-Speicherrichtlinie

Wenn sich die Speicheranforderungen für virtuelle Maschinen und virtuelle Festplatten ändern, können Sie die Speicherrichtlinie bearbeiten. Außerdem können Sie durch Klonen eine Kopie der bestehenden VM-Speicherrichtlinie erstellen. Beim Klonen können Sie optional wählen, ob die zugrunde liegende Speicherrichtlinie angepasst werden soll.

Voraussetzungen

Erforderliche Berechtigung: **StorageProfile.View**

Verfahren

1 Navigieren Sie im vSphere Client zur Speicherrichtlinie.
   a Klicken Sie auf **Menü > Richtlinien und Profile**.
   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
2 Wählen Sie die Speicherrichtlinie aus und klicken Sie auf eines der folgenden Symbole:
   - **Bearbeiten**
   - **Klonen**
3 (Optional) Ändern Sie die Richtlinie und klicken Sie auf **OK**.
4 Wenn die Speicherrichtlinie, die Sie bearbeiten, von einer virtuellen Maschine verwendet wird, wenden Sie die Richtlinie erneut auf die virtuelle Maschine an.

Option	Beschreibung
Manuell später	Wenn Sie diese Option auswählen, wird der Übereinstimmungsstatus für alle virtuellen Festplatten und für alle Home-Objekte der virtuellen Maschine, die der Speicherrichtlinie zugeordnet sind, in „Veraltet“ geändert. Um die Konfiguration und die Übereinstimmung zu aktualisieren, wenden Sie die Speicherrichtlinie manuell erneut auf alle verknüpften Elemente an. Weitere Informationen hierzu finden Sie unter Erneutes Anwenden der VM-Speicherrichtlinien.
Jetzt	Aktualisieren Sie die virtuelle Maschine und den Übereinstimmungsstatus unmittelbar nach der Bearbeitung der Speicherrichtlinie.

Informationen zu Speicherrichtlinienkomponenten

Eine VM-Speicherrichtlinie kann einen oder mehrere wiederverwendbare und austauschbare Bausteine enthalten. Diese werden als Speicherrichtlinienkomponenten bezeichnet. Jede Komponente beschreibt einen bestimmten Datendienst, der für die virtuelle Maschine

bereitgestellt werden muss. Sie können die Richtlinienkomponenten im Voraus definieren und mehreren VM-Speicherrichtlinien zuordnen.

Sie können die vordefinierte Komponente einer virtuellen Maschine oder einer virtuellen Festplatte nicht direkt zuweisen. Stattdessen müssen Sie die Komponente der VM-Speicherrichtlinie hinzufügen und die Richtlinie der virtuellen Maschine zuweisen.

Die Komponente beschreibt einen Diensttyp von einem Dienstanbieter. Die Dienste können je nach genutzten Anbietern unterschiedlich sein, gehören jedoch generell zu einer der folgenden Kategorien.

- Komprimierung
- Zwischenspeicherung
- Verschlüsselung
- Replizierung

Beim Erstellen der Speicherrichtlinienkomponente definieren Sie die Regeln für einen bestimmten Diensttyp und -grad.

Im folgenden Beispiel haben die virtuellen Maschinen VM1 und VM2 identische Platzierungsanforderungen, benötigen jedoch einen unterschiedlichen Grad von Replizierungsdiensten. Sie können die Speicherrichtlinienkomponenten mit verschiedenen Replizierungsparametern erstellen und diese Komponenten den zugehörigen Speicherrichtlinien hinzufügen.

Tabelle 20-2. Speicherrichtlinienkomponenten

Virtuelle Maschine	Platzierungsregeln	Speicherrichtlinienkomponente
VM1 muss alle 2 Stunden repliziert werden	Virtual Volumes-Datenspeicher	2-Stunden-Replizierung
VM2 muss alle 4 Stunden repliziert werden	Virtual Volumes-Datenspeicher	4-Stunden-Replizierung

Der Anbieter des Diensts kann ein Speichersystem, ein E/A-Filter oder ein anderes Element sein. Wenn die Komponente auf einen E/A-Filter verweist, wird sie den hostbasierten Regeln der Speicherrichtlinie hinzugefügt. Komponenten, die auf andere Elemente als E/A-Filter verweisen (zum Beispiel ein Speichersystem), werden den datenspeicherspezifischen Regelsätzen hinzugefügt.

Befolgen Sie bei der Arbeit mit Komponenten die nachstehenden Richtlinien:

- Jede Komponente kann nur einen Regelsatz enthalten. Alle Merkmale in diesem Regelsatz gehören zu einem einzigen Anbieter der Datendienste.
- Wenn in der VM-Speicherrichtlinie auf die Komponente verwiesen wird, können Sie die Komponente nicht löschen. Bevor Sie die Komponente löschen, müssen Sie sie aus der Speicherrichtlinie entfernen oder die Speicherrichtlinie löschen.

- Wenn Sie der Richtlinie Komponenten hinzufügen, können Sie nur eine Komponente aus derselben Kategorie (beispielsweise Caching) pro Regelsatz verwenden.

Erstellen von Speicherrichtlinienkomponenten

Eine Speicherrichtlinienkomponente beschreibt einen einzelnen Datendienst (beispielsweise Replizierung), der für die virtuelle Maschine bereitgestellt werden muss. Sie können die Komponente im Voraus definieren und mehreren VM-Speicherrichtlinien zuordnen. Die Komponenten sind wiederverwendbar und austauschbar.

Verfahren

1. Öffnen Sie im vSphere Client das Dialogfeld **Neue Speicherrichtlinienkomponente**.
   a. Klicken Sie auf **Menü > Richtlinien und Profile**.
   b. Klicken Sie unter **Richtlinien und Profile** auf **Speicherrichtlinienkomponenten**.
2. Klicken Sie auf **Speicherrichtlinienkomponente erstellen**.
3. Wählen Sie die vCenter Server-Instanz aus.
4. Geben Sie einen Namen (z. B. 4-Stunden-Replizierung) und eine Beschreibung der Richtlinienkomponente ein.

   Vergewissern Sie sich, dass der Name keinen Konflikt mit den Namen anderer Komponenten oder Speicherrichtlinien aufweist.
5. Wählen Sie die Dienstkategorie aus, zum Beispiel **Replizierung**.
6. Wählen Sie den Dienstanbieter aus.
7. Definieren Sie Regeln für die ausgewählte Kategorie.

   Beispiel: Wenn Sie eine 4-Stunden-Replizierung konfigurieren, legen Sie den Wert des Recovery Point Objective (RPO) auf 4 fest.

   Legen Sie bei auf E/A-Filtern basierender Verschlüsselung den Parameter **E/A-Filter vor Verschlüsselung zulassen** fest. Für die vom Speicher bereitgestellte Verschlüsselung ist dieser Parameter nicht erforderlich.

Option	Beschreibung
False (Standard)	Die Verwendung anderer E/A-Filter vor dem Verschlüsselungsfilter ist nicht zulässig.
True	Die Verwendung anderer E/A-Filter vor dem Verschlüsselungsfilter ist zulässig. Andere Filter wie beispielsweise die Replizierung können Klartextdaten analysieren, bevor diese verschlüsselt werden.

8. Klicken Sie auf **OK**.

Ergebnisse

Die neue Komponente wird in der Liste der Speicherrichtlinienkomponenten angezeigt.

Nächste Schritte

Sie können die Komponente der VM-Speicherrichtlinie hinzufügen. Wenn der Datendienst, auf den die Komponente verweist, durch die E/A-Filter bereitgestellt wird, fügen Sie die Komponente den hostbasierten Regeln der Speicherrichtlinie hinzu. Komponenten, die auf andere Elemente als E/A-Filter verweisen (zum Beispiel ein Speichersystem), werden den datenspeicherspezifischen Regelsätzen hinzugefügt.

Bearbeiten oder Klonen von Speicherrichtlinienkomponenten

Die vorhandenen Speicherrichtlinienkomponenten können bearbeitet werden. Außerdem können Sie durch Klonen eine Kopie der vorhandenen Komponente erstellen.

Verfahren

1 Navigieren Sie im vSphere Client zu der Speicherrichtlinienkomponente, die Sie bearbeiten oder klonen möchten.

   a Klicken Sie auf **Menü > Richtlinien und Profile**.

   b Klicken Sie unter **Richtlinien und Profile** auf **Speicherrichtlinienkomponenten**.

2 Wählen Sie die Komponente aus und klicken Sie auf eines der folgenden Symbole:

Option	Beschreibung
Einstellungen bearbeiten	Bei der Bearbeitung können Sie die Kategorie des Datendienstes und den Anbieter nicht ändern. Beispiel: Wenn die ursprüngliche Komponente auf die von E/A-Filtern bereitgestellte Replizierung verweist, müssen diese Einstellungen unverändert bleiben.
Klonen	Beim Klonen können Sie alle Einstellungen der ursprünglichen Komponente anpassen.

3 Ändern Sie die entsprechenden Werte und klicken Sie auf **OK**.

4 Wenn eine VM-Speicherrichtlinie, die einer virtuellen Maschine zugewiesen ist, auf die von Ihnen bearbeitete Richtlinienkomponente verweist, wenden Sie die Speicherrichtlinie erneut auf die virtuelle Maschine an.

Menüelement	Beschreibung
Manuell später	Wenn Sie diese Option auswählen, wird der Übereinstimmungsstatus für alle virtuellen Festplatten und für alle Home-Objekte der virtuellen Maschine, die der Speicherrichtlinie zugeordnet sind, in „Veraltet“ geändert. Um die Konfiguration und die Übereinstimmung zu aktualisieren, wenden Sie die Speicherrichtlinie manuell erneut auf alle verknüpften Elemente an. Weitere Informationen hierzu finden Sie unter Erneutes Anwenden der VM-Speicherrichtlinien.
Jetzt	Aktualisieren Sie die virtuelle Maschine und den Übereinstimmungsstatus unmittelbar nach der Bearbeitung der Speicherrichtlinie.

Speicherrichtlinien und virtuelle Maschinen

Nach dem Definieren einer VM-Speicherrichtlinie können Sie sie auf eine virtuelle Maschine anwenden. Die Speicherrichtlinie wird angewendet, wenn Sie die virtuelle Maschine bereitstellen oder deren virtuelle Festplatten konfigurieren. Abhängig von Typ und Konfiguration kann die Richtlinie unterschiedlichen Zwecken dienen. Durch die Richtlinie kann der am besten geeignete Datenspeicher für die virtuelle Maschine ausgewählt und die erforderliche Dienstebene erzwungen werden. Es können jedoch auch bestimmte Datendienste für die virtuelle Maschine und deren Festplatten aktiviert werden.

Wenn Sie die Speicherrichtlinie nicht angeben, verwendet das System die Standardspeicherrichtlinie des Datenspeichers. Wenn sich Ihre Speicheranforderungen für die Anwendungen auf der virtuellen Maschine ändern, können Sie die ursprünglich zugewiesene Speicherrichtlinie entsprechend bearbeiten.

Zuweisen von Speicherrichtlinien zu virtuellen Maschinen

Sie können eine VM-Speicherrichtlinie beim anfänglichen Bereitstellen einer virtuellen Maschine oder beim Durchführen anderer VM-Vorgänge, wie Klonen oder Migrieren, zuweisen.

Bei diesem Thema wird beschrieben, wie Sie die VM-Speicherrichtlinie beim Erstellen einer virtuellen Maschine zuweisen. Informationen zu anderen Bereitstellungsmethoden, wie Klonen, Bereitstellung über eine Vorlage usw., finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Sie können dieselbe Speicherrichtlinie auf die Konfigurationsdatei der virtuellen Maschine und alle ihre virtuellen Festplatten anwenden. Wenn Sie unterschiedliche Speicheranforderungen an die Konfigurationsdatei und die virtuellen Festplatten haben, können sie ihnen auch eigene Speicherrichtlinien zuweisen.

Verfahren

1 Starten Sie den Vorgang zur Bereitstellung von virtuellen Maschinen und befolgen Sie die entsprechenden Schritte.

2 Weisen Sie allen VM-Dateien und Festplatten dieselbe Speicherrichtlinie zu.

a Wählen Sie auf der Seite **Speicher auswählen** eine Speicherrichtlinie im Dropdown-Menü **VM-Speicherrichtlinie** aus.

Je nach ihrer Konfiguration unterteilt die Speicherrichtlinie alle Datenspeicher in kompatibel und inkompatibel. Wenn die Richtlinie auf Datendienste verweist, die von einem speziellen Speicherelement wie zum Beispiel Virtual Volumes angeboten werden, enthält die kompatible Liste Datenspeicher, die nur diesen Speichertyp darstellen.

b Wählen Sie einen geeigneten Datenspeicher in der Liste kompatibler Datenspeicher aus.

Der Datenspeicher wird zum Zielspeicherelement für die VM-Konfigurationsdatei und alle virtuellen Festplatten.

c Geben Sie bei Verwendung des Replizierungsdienstes mit Virtual Volumes die Replizierungsgruppe an.

Replizierungsgruppen geben an, welche VMs und virtuellen Festplatten gemeinsam auf eine Zielsite repliziert werden müssen.

Option	Beschreibung
Vorkonfigurierte Replizierungsgruppe	Replizierungsgruppen, die auf der Speicherseite vorkonfiguriert wurden. vCenter Server und ESXi erkennen die Replizierungsgruppen, verwalten jedoch nicht deren Lebenszyklus.
Automatische Replizierungsgruppe	Virtual Volumes erstellt eine Replizierungsgruppe und ordnet alle VM-Objekte dieser Gruppe zu.

3 Ändern Sie die VM-Speicherrichtlinie für den virtuellen Datenträger.

Verwenden Sie diese Option, wenn Sie für virtuelle Festplatten andere Anforderungen bezüglich der Speicherplatzierung haben. Sie können diese Option auch zum Aktivieren von E/A-Filterdiensten wie Caching und Replizierung für Ihre virtuellen Festplatten verwenden.

a Erweitern Sie auf der Seite **Hardware anpassen** den Bereich **Neue Festplatte**.

b Wählen Sie im Dropdown-Menü **VM-Speicherrichtlinie** die der virtuellen Festplatte zuzuweisende Speicherrichtlinie aus.

c (Optional) Ändern Sie den Speicherort der virtuellen Festplatte.

Verwenden Sie diese Option zum Speichern des virtuellen Datenträgers auf einem anderen Datenspeicher als demjenigen, auf dem sich die VM-Konfigurationsdatei befindet.

4 Schließen Sie die Bereitstellung der virtuellen Maschine ab.

Ergebnisse

Nach der Erstellung der virtuellen Maschine zeigt die Registerkarte **Übersicht** die zugewiesenen Speicherrichtlinien und deren Übereinstimmungsstatus an.

Nächste Schritte

Wenn sich die Speicherplatzierungsanforderungen für die Konfigurationsdatei oder die virtuellen Festplatten zu einem späteren Zeitpunkt ändern sollten, können Sie die Zuweisung der VM-Richtlinie entsprechend anpassen.

Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten

Wenn Ihre Speicheranforderungen für die Anwendungen auf der virtuellen Maschine sich ändern, können Sie die Speicherrichtlinie bearbeiten, die ursprünglich auf die virtuelle Maschine angewendet wurde.

Sie können die Speicherrichtlinie für eine ausgeschaltete oder eingeschaltete virtuelle Maschine bearbeiten.

Beim Ändern der VM-Speicherrichtlinienzuweisung können Sie dieselbe Speicherrichtlinie auf die Konfigurationsdatei der virtuellen Maschine und alle ihre virtuellen Festplatten anwenden. Sie können die verschiedenen Speicherrichtlinien auch der VM-Konfigurationsdatei und den virtuellen Festplatten zuordnen. Sie können unterschiedliche Richtlinien anwenden, wenn beispielsweise die Speicheranforderungen für Ihre virtuellen Festplatten und die Konfigurationsdatei voneinander abweichen.

Verfahren

1 Navigieren Sie im vSphere Client zur virtuellen Maschine.
   a Klicken Sie auf **Menü > Richtlinien und Profile**.
   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
   c Klicken Sie auf die Speicherrichtlinie, die Sie ändern möchten, und klicken Sie auf **VM-Übereinstimmung**.

      Die Liste der virtuellen Maschinen, die diese Speicherrichtlinie nutzen, wird angezeigt.
   d Klicken Sie auf die virtuelle Maschine, deren Richtlinie Sie ändern möchten.
2 Klicken Sie auf die Registerkarte **Konfigurieren** und dann auf **Richtlinien**.
3 Klicken Sie auf **VM-Speicherrichtlinie bearbeiten**.
4 Legen Sie die VM-Speicherrichtlinie für Ihre virtuelle Maschine fest.

Option	Aktionen
Wenden Sie dieselbe Speicherrichtlinie auf alle VM-Objekte an	Wählen Sie die Richtlinie aus dem Dropdown-Menü **VM-Speicherrichtlinie** aus.
Wenden Sie auf das VM-Home-Objekt und virtuelle Festplatten unterschiedliche Speicherrichtlinien an	a Aktivieren Sie die Option **Pro Datenträger konfigurieren**. b Wählen Sie das Objekt aus, z. B. „VM Home“. c Wählen Sie in der Spalte „VM-Speicherrichtlinie“ die Richtlinie im Dropdown-Menü aus.

5 Wenn Sie eine Virtual Volumes-Richtlinie mit Replizierung verwenden, konfigurieren Sie die Replizierungsgruppe.

Replizierungsgruppen geben an, welche VMs und virtuellen Festplatten gemeinsam auf eine Zielsite repliziert werden müssen.

Alle Speicherobjekte einer VM müssen zur selben Replizierungsgruppe gehören. Sie können nicht verschiedenen Speicherobjekten einer VM unterschiedliche Replizierungsgruppen zuweisen.

6 Klicken Sie auf **OK**, um die Änderungen an der VM-Speicherrichtlinie zu speichern.

Ergebnisse

Die Speicherrichtlinie wird der virtuellen Maschine und ihren Festplatten zugeordnet.

Prüfen der Übereinstimmung für eine VM-Speicherrichtlinie

Sie können prüfen, ob der Datenspeicher einer virtuellen Maschine mit den in der VM-Speicherrichtlinie festgelegten Speicheranforderungen kompatibel ist.

Voraussetzungen

Stellen Sie sicher, dass der virtuellen Maschine eine Speicherrichtlinie zugeordnet ist.

Verfahren

1 Wechseln Sie im vSphere Client zur virtuellen Maschine.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und dann auf **Richtlinien**.

3 Klicken Sie auf **Einhaltung der VM-Speicherrichtlinien prüfen**.

Das System verifiziert die Übereinstimmung.

4 Zeigen Sie den Übereinstimmungsstatus an.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, der von der virtuellen Maschine oder der virtuellen Festplatte verwendet wird, weist die mit den Richtlinienanforderungen kompatiblen Speicherfunktionen auf.
Nicht übereinstimmend	Der Datenspeicher, der von der virtuellen Maschine oder der virtuellen Festplatte verwendet wird, weist nicht die mit den Richtlinienanforderungen kompatiblen Speicherfunktionen auf. Sie können die Dateien der virtuellen Maschine und die virtuellen Festplatten auf übereinstimmende Datenspeicher migrieren.
Veraltet	Der Status gibt an, dass die Richtlinie bearbeitet wurde, aber die neuen Anforderungen wurden nicht an den Datenspeicher weitergegeben, in dem sich die Objekte der virtuellen Maschine befinden. Um die Änderungen zu kommunizieren, wenden Sie die Richtlinie erneut auf die veralteten Objekte an.
Nicht anwendbar	Diese Speicherrichtlinie verweist auf Datenspeicherfunktionen, die vom Datenspeicher, in dem sich die virtuelle Maschine befindet, nicht unterstützt werden.

Nächste Schritte

Wenn Sie für den Datenspeicher mit dem Status „Keine Übereinstimmung“ die Übereinstimmung nicht wiederherstellen können, migrieren Sie die Dateien oder virtuellen Festplatten in einen kompatiblen Datenspeicher. Weitere Informationen hierzu finden Sie unter Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine.

Wenn der Status „Veraltet“ lautet, wenden Sie die Richtlinie erneut auf die Objekte an. Weitere Informationen hierzu finden Sie unter Erneutes Anwenden der VM-Speicherrichtlinien.

Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine

Ermitteln Sie, welcher Datenspeicher mit der Speicherrichtlinie Ihrer virtuellen Maschine kompatibel ist.

Es kann vorkommen, dass eine einer virtuellen Maschine zugewiesene Speicherrichtlinie den Status „Keine Übereinstimmung“ aufweist. Dieser Status ist ein Hinweis darauf, dass die virtuelle Maschine oder deren Festplatten Datenspeicher verwenden, die nicht mit der Richtlinie kompatibel sind. Sie können die Dateien der virtuellen Maschine und die virtuellen Festplatten in kompatible Datenspeicher migrieren.

Bestimmen Sie mithilfe dieser Aufgabe, welche Datenspeicher die Anforderungen der Richtlinie erfüllen.

Verfahren

1. Stellen Sie sicher, dass sich die Speicherrichtlinie für die virtuelle Maschine im Status „Nicht übereinstimmend“ befindet.
   a. Wechseln Sie im vSphere Client zur virtuellen Maschine.
   b. Klicken Sie auf die Registerkarte **Übersicht**.

      Im Bereich „VM-Speicherrichtlinien“ wird unter „VM-Speicherrichtlinieneinhaltung“ der Status „Nicht übereinstimmend“ angezeigt.
2. Navigieren Sie zu der nicht übereinstimmenden Speicherrichtlinie.
   a. Klicken Sie auf **Menü > Richtlinien und Profile**.
   b. Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
3. Zeigen Sie die Liste der kompatiblen Datenspeicher für die nicht übereinstimmende Speicherrichtlinie an.
   a. Klicken Sie auf die Speicherrichtlinie.
   b. Klicken Sie auf **Speicherkompatibilität**.

   Die Liste der Datenspeicher, die den Anforderungen der Richtlinie entsprechen, wird angezeigt.

Nächste Schritte

Sie können die virtuelle Maschine oder deren Datenträger in einen Datenspeicher aus der Liste migrieren.

Erneutes Anwenden der VM-Speicherrichtlinien

Nachdem Sie eine Speicherrichtlinie bearbeitet haben, die bereits einem VM-Objekt zugeordnet ist, müssen Sie die Richtlinie erneut anwenden. Durch die erneute Anwendung der Richtlinie teilen Sie dem Datenspeicher, in dem sich das VM-Objekt befindet, neue Speicheranforderungen mit.

Voraussetzungen

Der Übereinstimmungsstatus für eine virtuelle Maschine lautet „Veraltet“. Der Status gibt an, dass die Richtlinie bearbeitet wurde, aber die neuen Anforderungen wurden nicht an den Datenspeicher weitergegeben.

Verfahren

1. Wechseln Sie im vSphere Client zur virtuellen Maschine.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und dann auf **Richtlinien**.
3. Vergewissern Sie sich, dass als Übereinstimmungsstatus „Veraltet“ angezeigt wird.
4. Klicken Sie auf **VM-Speicherrichtlinie erneut anwenden**.
5. Überprüfen Sie den Übereinstimmungsstatus.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, der von der virtuellen Maschine oder virtuellen Festplatte verwendet wird, hat die Speicherfunktionen, die die Richtlinie erfordert.
Nicht übereinstimmend	Der Datenspeicher unterstützt festgelegte Speicheranforderungen, kann jedoch zurzeit nicht die Speicherrichtlinie erfüllen. Der Status kann z. B. in „Keine Übereinstimmung“ wechseln, wenn physische Ressourcen für den Datenspeicher nicht verfügbar sind. Sie können den Datenspeicher in Übereinstimmung bringen, indem Sie Änderungen an der physischen Konfiguration Ihres Host-Clusters vornehmen. Fügen Sie beispielsweise Hosts oder Festplatten zum Cluster hinzu. Wenn weitere Ressourcen die Speicherrichtlinie erfüllen, ändert sich der Status in „Übereinstimmung“. Wenn Sie für den Datenspeicher mit dem Status „Keine Übereinstimmung“ die Übereinstimmung nicht wiederherstellen können, migrieren Sie die Dateien oder virtuellen Festplatten in einen kompatiblen Datenspeicher. Weitere Informationen hierzu finden Sie unter Suchen einer kompatiblen Speicherressource für eine nicht kompatible virtuelle Maschine.
Nicht anwendbar	Die Speicherrichtlinie verweist auf Datenspeicherkapazitäten, die vom Datenspeicher nicht unterstützt werden.

Standardspeicherrichtlinien

Wenn Sie eine virtuelle Maschine auf einem Datenspeicher bereitstellen, müssen Sie ihr eine kompatible VM-Speicherrichtlinie zuweisen. Falls Sie die Speicherrichtlinie nicht konfigurieren und explizit der virtuellen Maschine zuweisen, verwendet das System eine Standardspeicherrichtlinie.

Von VMware bereitgestellte Standardspeicherrichtlinie

Die von ESXi bereitgestellte generische Standardspeicherrichtlinie gilt für alle Datenspeicher und enthält keine spezifischen Regeln für bestimmte Speichertypen.

Darüber hinaus bietet ESXi die Standardspeicherrichtlinien für objektbasierte Datenspeicher, vSAN oder Virtual Volumes. Durch diese Richtlinien wird die optimale Platzierung für Objekte virtueller Maschinen innerhalb des objektbasierten Speichers gewährleistet.

Weitere Informationen zur Standardspeicherrichtlinie für Virtual Volumes finden Sie unter Virtual Volumes und VM-Speicherrichtlinien.

VMFS- und NFS-Datenspeicher weisen keine spezifischen Standardrichtlinien auf und können die generische Standardrichtlinie oder eine benutzerdefinierte Richtlinie nutzen, die Sie für diese definieren.

Benutzerdefinierte Standardspeicherrichtlinien

Sie können eine VM-Speicherrichtlinie erstellen, die mit vSAN oder Virtual Volumes kompatibel ist. Anschließend können Sie diese Richtlinie als Standardrichtlinie für vSAN- und Virtual Volumes-Datenspeicher festlegen. Die benutzerdefinierte Standardrichtlinie ersetzt die Standardspeicherrichtlinie von VMware.

Jeder vSAN - und Virtual Volumes-Datenspeicher darf nur jeweils eine Standardrichtlinie aufweisen. Sie können jedoch eine einzelne Speicherrichtlinie mit mehreren Platzierungsregelsätzen erstellen, sodass sie mehreren vSAN- und Virtual Volumes-Datenspeichern entspricht. Diese Richtlinie können Sie als Standardrichtlinie für alle Datenspeicher festlegen.

Wenn die VM-Speicherrichtlinie zur Standardrichtlinie eines Datenspeichers wird, können Sie sie nur dann löschen, wenn Sie sie vom Datenspeicher abtrennen.

Ändern der Standardspeicherrichtlinie für einen Datenspeicher

Für Virtual Volumes- und vSAN-Datenspeicher bietet VMware Speicherrichtlinien, die beim Bereitstellen der virtuellen Maschinen als Standard verwendet werden. Sie können die Standardspeicherrichtlinie für einen ausgewählten Virtual Volumes- oder vSAN-Datenspeicher ändern.

Hinweis Legen Sie keine Speicherrichtlinie mit Replizierungsregeln als Standard-Speicherrichtlinie fest. da Sie ansonsten keine Verifizierungsgruppen auswählen können.

Voraussetzungen

Erstellen Sie eine Speicherrichtlinie, die mit Virtual Volumes oder vSAN kompatibel ist. Sie können eine Richtlinie erstellen, die für beide Speicherarten geeignet ist.

Verfahren

1. Navigieren Sie im vSphere Client zum Datenspeicher.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Allgemein**.
3. Klicken Sie im Bereich „Standardspeicherrichtlinie“ auf **Bearbeiten**.
4. Wählen Sie in der Liste der verfügbaren Speicherrichtlinien eine Richtlinie aus, die als Standard verwendet werden soll, und klicken Sie auf **OK**.

Ergebnisse

Die ausgewählte Speicherrichtlinie wird zur Standardrichtlinie für den Datenspeicher. Das System weist diese Richtlinie allen virtuellen Maschinenobjekten zu, die Sie im Datenspeicher bereitstellen, wenn explizit keine anderen Richtlinien ausgewählt wurden.

Verwenden von Speicheranbietern

21

Ein Speicheranbieter ist eine Softwarekomponente, die von VMware angeboten oder von einem Drittanbieter über die vSphere-APIs für Storage Awareness (VASA) entwickelt wird. Der Speicheranbieter kann auch als VASA-Anbieter bezeichnet werden. Die Speicheranbieter sind auf verschiedene Speicherelemente abgestimmt, darunter externe physische Speicher und Speicherabstraktionen wie vSAN und Virtual Volumes. Speicheranbieter können auch Softwarelösungen wie E/A-Filter unterstützen.

Dieses Kapitel enthält die folgenden Themen:

Grundlegendes zu Speicheranbietern

Im Allgemeinen verwenden vCenter Server und ESXi die Speicheranbieter zum Abrufen von Informationen zur Speicherkonfiguration, zum Status und zu Speicherdatendiensten, die in Ihrer Umgebung angeboten werden. Diese Informationen werden im vSphere Client angezeigt. Mit diesen Informationen können Sie leichter die richtige Entscheidung in Bezug auf die Platzierung der virtuellen Maschine treffen, die Speicheranforderungen festlegen und Ihre Speicherumgebung überwachen.

Persistenzspeicheranbieter

Speicheranbieter, die Arrays und Speicherabstraktionen verwalten, werden als Persistenzspeicheranbieter bezeichnet. Anbieter, die Virtual Volumes oder vSAN unterstützen, gehören zu dieser Kategorie. Neben Speicher können Persistenzanbieter auch andere Datendienste, wie beispielsweise die Replizierung, anbieten.

Datendienstanbieter

Eine weitere Kategorie von Anbietern sind E/A-Filter-Speicheranbieter oder Datendiensteanbieter. Diese Anbieter bieten Datendienste an, die hostbasiertes Caching, Komprimierung und Verschlüsselung umfassen.

Sowohl Persistenzspeicher- als auch Datendienstanbieter können zu einer dieser Kategorien gehören.

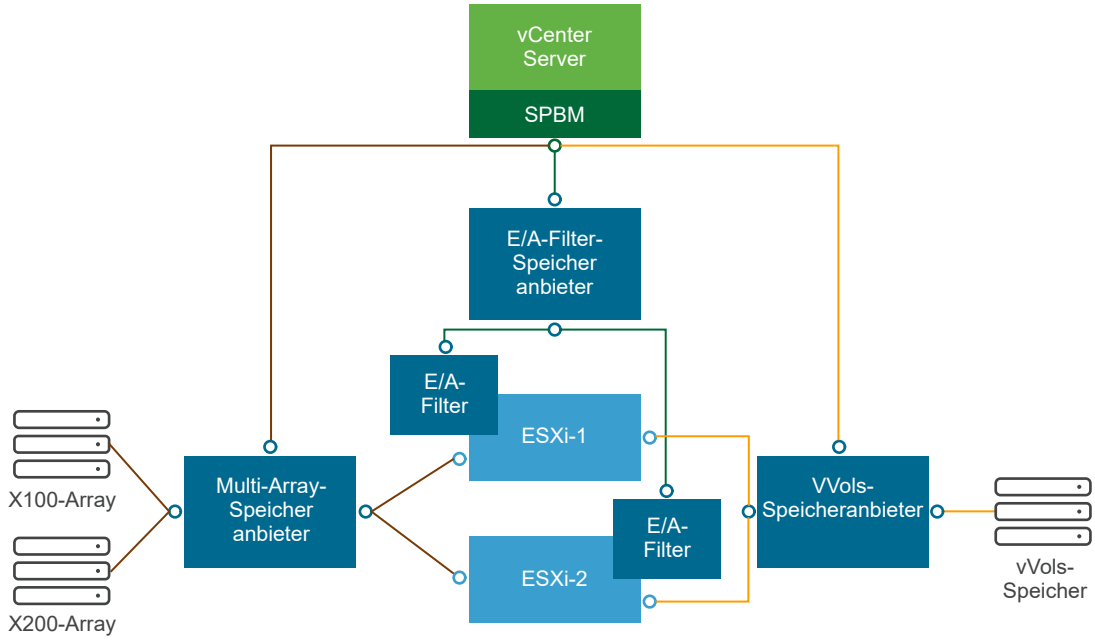
Integrierte Speicheranbieter

Integrierte Speicheranbieter werden von VMware bereitgestellt. Sie müssen in der Regel nicht registriert werden. Zum Beispiel Speicheranbieter, die vSAN oder E/A-Filter unterstützen und deren Speicher integriert sind und automatisch registriert werden.

Speicheranbieter einer Drittpartei

Bei einem Speicheranbieter einer Drittpartei muss dieser normalerweise registriert werden. Ein Beispiel für einen derartigen Anbieter ist der Virtual Volumes-Anbieter. Jede Speicheranbieterkomponente wird im vSphere Client registriert und verwaltet.

Die folgende Grafik zeigt, wie verschiedene Arten von Speicheranbietern die Kommunikation zwischen vCenter Server und ESXi sowie weiteren Komponenten der Speicherumgebung erleichtern. Zu den Komponenten können z. B. Speicher-Arrays, Virtual Volumes-Speicher und E/A-Filter gehören.



Speicheranbieter und Darstellung von Daten

vCenter Server und ESXi kommunizieren mit dem Speicheranbieter, um Informationen zu erhalten, die der Speicheranbieter aus dem zugrunde liegenden physischen und softwaredefinierten Speicher oder aus verfügbaren E/A-Filtern zusammenstellt. vCenter Server kann dann die Speicherdaten im vSphere Client anzeigen.

Die vom Speicheranbieter bereitgestellten Informationen können in die folgenden Kategorien aufgeteilt werden:

- Speicherdatendienste und -funktionen. Diese Art von Informationen sind maßgeblich für Funktionen wie vSAN, Virtual Volumes und E/A-Filter. Der Speicheranbieter, der diese Funktionen darstellt, wird mit dem SPBM-Mechanismus (speicherrichtlinienbasierte Verwaltung, Storage Policy Based Management) vernetzt. Der Speicheranbieter erfasst Informationen über die Datendienste, die von den zugrunde liegenden Speicherelementen oder verfügbaren E/A-Filtern angeboten werden.

  Sie beziehen sich auf diese Datendienste, wenn Sie Speicheranforderungen für virtuelle Maschinen und virtuelle Festplatten in einer Speicherrichtlinie definieren. Je nach Umgebung stellt der SPBM-Mechanismus den geeigneten Speicherort für eine virtuelle Maschine sicher oder aktiviert spezifische Datendienste für virtuelle Festplatten. Weitere Informationen finden Sie unter Erstellen und Verwalten von VM-Speicherrichtlinien.

- Speicherstatus. Diese Kategorie enthält Berichte zum Status verschiedener Speicherelemente. Sie enthält zudem Alarme und Ereignisse zum Senden von Benachrichtigungen über Konfigurationsänderungen.

  Diese Informationen sind nützlich beim Beheben von Fehlern bei der Speicherverbindung und von Leistungsproblemen. Sie sind zudem hilfreich, um Array-generierte Ereignisse und Alarme mit den entsprechenden Leistungs- und Laständerungen am Array zu korrelieren.

- Informationen über Storage DRS für die verteilte Ressourcenplanung für Blockgeräte oder Dateisysteme. Mit diesen Informationen kann sichergestellt werden, dass die Entscheidungen, die von Storage DRS vorgenommen werden, mit den Entscheidungen der Ressourcenverwaltung innerhalb der Speichersysteme übereinstimmen.

Anforderungen und Überlegungen hinsichtlich Speicheranbietern

Wenn Sie externe Speicheranbieter verwenden, sind bestimmte Anforderungen und Überlegungen zu berücksichtigen.

Üblicherweise sind Hersteller dafür verantwortlich, Speicheranbieter zur Verfügung zu stellen. Das VASA-Programm von VMware definiert eine Architektur, in der externe Speicheranbieter in die vSphere-Umgebung integriert werden, sodass vCenter Server- und ESXi-Hosts mit den Speicheranbietern kommunizieren können.

Um Speicheranbieter zu verwenden, müssen diese Anforderungen erfüllt sein:

- Stellen Sie sicher, dass jeder Speicheranbieter, den Sie verwenden, durch VMware zertifiziert und ordnungsgemäß bereitgestellt ist. Weitere Informationen zur Bereitstellung der Speicheranbieter erhalten Sie von Ihrem Speicherhersteller.
- Stellen Sie sicher, dass der Speicheranbieter mit den vCenter Server- und ESXi-Versionen kompatibel ist. Weitere Informationen hierzu finden Sie unter *VMware-Kompatibilitätshandbuch*.

- Installieren Sie den VASA-Anbieter nicht auf dem gleichen System wie vCenter Server.
- Falls Ihre Umgebung ältere Versionen von Speicheranbietern enthält, können vorhandene Funktionen weiterhin verwendet werden. Damit Sie neue Funktionen nutzen können, sollten Sie jedoch Ihren Speicheranbieter auf eine neue Version aktualisieren.
- Beim Upgrade eines Speicheranbieters auf eine neuere VASA-Version müssen Sie die Registrierung zunächst aufheben und anschließend den Anbieter neu registrieren. Nach der Registrierung stehen vCenter Server die Funktionen der neuen VASA-Version zur Verfügung.

Registrieren von Speicheranbietern

Sie müssen zum Herstellen einer Verbindung zwischen vCenter Server und einem Speicheranbieter den Speicheranbieter registrieren. Verwenden Sie den vSphere Client, um einen separaten Speicheranbieter für jeden Host in einem Cluster zu registrieren.

Beim Upgrade eines Speicheranbieters auf eine neuere VASA-Version müssen Sie die Registrierung zunächst aufheben und anschließend den Anbieter neu registrieren. Nach der Registrierung stehen vCenter Server die Funktionen der neuen VASA-Version zur Verfügung.

Hinweis Wenn Sie vSAN verwenden, werden die Speicheranbieter für vSAN registriert und automatisch in der Liste der Speicheranbieter angezeigt. vSAN unterstützt keine manuelle Registrierung von Speicheranbietern. Informationen finden Sie in der Dokumentation *Verwalten von VMware vSAN*.

Voraussetzungen

Stellen Sie sicher, dass die Speicheranbieter-Komponente auf der Speicherseite installiert ist, und fragen Sie Ihren Speicheradministrator nach den Anmeldedaten.

Verfahren

1. Navigieren Sie zu vCenter Server.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
3. Klicken Sie auf das Symbol **Add**.
4. Geben Sie die Verbindungsinformationen für den Speicheranbieter ein, einschließlich des Namens, der URL und der Anmeldedaten.
5. Geben Sie die Sicherheitsmethode an.

Aktion	Beschreibung
Verweisen Sie vCenter Server auf das Speicheranbieterzertifikat	Wählen Sie die Option **Zertifikat des Speicheranbieters verwenden** aus und geben Sie den Speicherort des Zertifikats an.
Verwenden Sie einen Fingerabdruck des Speicheranbieterzertifikats.	Wenn Sie vCenter Server nicht an das Speicherzertifikat verweisen, wird der Fingerabdruck des Zertifikats angezeigt. Sie können den Fingerabdruck überprüfen und ihn genehmigen. vCenter Server fügt das Zertifikat dem Truststore hinzu und fährt mit dem Herstellen der Verbindung fort.

Der Speicheranbieter fügt das vCenter Server-Zertifikat dem Truststore hinzu, wenn sich vCenter Server zum ersten Mal mit dem Anbieter verbindet.

6 Klicken Sie auf **OK**.

Ergebnisse

vCenter Server registriert den Speicheranbieter und richtet eine sichere SSL-Verbindung mit ihm ein.

Nächste Schritte

Vorschläge zur Behebung von Fehlern bei der Registrierung Ihres Speicheranbieters finden Sie im VMware Knowledgebase-Artikel https://kb.vmware.com/s/article/49798.

Anzeigen von Speicheranbieterinformationen

Nachdem Sie eine Speicheranbieterkomponente bei vCenter Server registriert haben, wird der Speicheranbieter in der Liste der Speicheranbieter angezeigt. Bestimmte Speicheranbieter sind selbstregistriert und werden automatisch in der Liste angezeigt, nachdem Sie das von ihnen dargestellte Element, wie beispielsweise vSAN oder E/A-Filter, eingerichtet haben.

Verwenden Sie den vSphere Client, um die allgemeinen Informationen zum Speicheranbieter und die Details für jede Speicherkomponente anzuzeigen.

Verfahren

1 Navigieren Sie zu vCenter Server.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.

3 Zeigen Sie in der Liste der Speicheranbieter die bei vCenter Server registrierten Speicheranbieter an.

Die Liste enthält allgemeine Informationen, wie beispielsweise den Namen des Speicheranbieters, die URL und den Status, die Version der VASA-APIs und die Speicherelemente, die der Anbieter darstellt.

4 Wenn Sie weitere Details anzeigen möchten, wählen Sie einen bestimmten Speicheranbieter oder seine Komponente in der Liste aus.

Hinweis Ein einzelner Speicheranbieter kann Speichersysteme von zahlreichen verschiedenen Anbietern unterstützen.

Speicheranbieter verwalten

Verwenden Sie den vSphere Client zum Durchführen verschiedener Verwaltungsvorgänge für die registrierten Speicheranbieter.

Verfahren

1 Navigieren Sie zu vCenter Server.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.

3 Wählen Sie in der Liste der Speicheranbieter einen Speicheranbieter aus und klicken Sie auf eines der folgenden Symbole.

Option	Beschreibung
Speicheranbieter synchronisieren	Alle Speicheranbieter werden mit dem aktuellen Zustand der Umgebung synchronisiert.
Erneut prüfen	Die Speicherdaten für den Anbieter werden aktualisiert. vCenter Server aktualisiert die Speicherdaten in seiner Datenbank in regelmäßigen Abständen. Die Aktualisierungen sind unvollständig und spiegeln nur die Änderungen wider, die Speicheranbieter zum betreffenden Zeitpunkt an vCenter Server übertragen. Bei Bedarf können Sie eine vollständige Datenbanksynchronisierung für den ausgewählten Speicheranbieter durchführen.
Entfernen	Heben Sie die Registrierung für nicht verwendete Speicheranbieter auf. Danach schließt vCenter Server die Verbindung und entfernt den Speicheranbieter aus der Konfiguration. **Hinweis** Die Registrierung bestimmter Speicheranbieter, die von VMware zur Verfügung gestellt werden, wie beispielsweise vSAN-Speicheranbieter, kann nicht manuell aufgehoben werden. Diese Option eignet sich auch beim Upgrade eines Speicheranbieters auf eine neuere VASA-Version. In diesem Fall müssen Sie die Registrierung des Anbieters aufheben und ihn dann neu registrieren. Nach der Registrierung stehen vCenter Server die Funktionen der neuen VASA-Version zur Verfügung.
Zertifikat aktualisieren	vCenter Server informiert Sie, wenn ein Zertifikat, das einem Speicheranbieter zugewiesen ist, in Kürze abläuft. Sie können das Zertifikat aktualisieren, um den Anbieter weiterhin zu nutzen. Wenn Sie das Zertifikat nicht vor Ablauf aktualisiert haben, verwendet vCenter Server den betreffenden Anbieter nicht mehr.

Ergebnisse

vCenter Server schließt die Verbindung und entfernt den Speicheranbieter aus der Konfiguration.

Arbeiten mit VMware vSphere Virtual Volumes

22

VMware vSphere Virtual Volumes, auch vVols genannt, virtualisiert SAN- und NAS-Geräte durch Abstrahieren physischer Hardwareressourcen in logische Kapazitätspools. Mit der Funktionalität für Virtual Volumes wird bei der Speicherverwaltung nicht mehr der Speicherplatz innerhalb von Datenspeichern verwaltet, sondern es werden abstrakte, von Speicher-Arrays gehandhabte Speicherobjekte verwaltet.

Dieses Kapitel enthält die folgenden Themen:

Informationen zu Virtual Volumes

Mit Virtual Volumes wird eine einzelne virtuelle Maschine anstelle des Datenspeichers zur Einheit für die Speicherverwaltung, und die Speicherhardware erhält vollständige Kontrolle über den Inhalt, das Layout und die Verwaltung virtueller Datenträger.

Früher wurde in der vSphere-Speicherverwaltung ein Ansatz verwendet, bei dem Datenspeicher im Mittelpunkt standen. Bei diesem Ansatz besprechen die Speicheradministratoren und die vSphere-Administratoren im Voraus die zugrunde liegenden Speicheranforderungen für virtuelle Maschinen. Der Speicheradministrator richtet dann LUNs oder NFS-Freigaben ein und stellt sie

den ESXi-Hosts bereit. Der vSphere-Administrator erstellt Datenspeicher, die auf LUNs oder NFS basieren, und verwendet diese Datenspeicher als Speicher für virtuelle Maschinen. In der Regel ist aus der Speicherperspektive der Datenspeicher die niedrigste Granularitätsstufe, auf der die Datenverwaltung erfolgt. Ein einzelner Datenspeicher enthält jedoch mehrere virtuelle Maschinen, für die u. U. unterschiedliche Anforderungen gelten können. Mit dem traditionellen Ansatz lassen sich die Anforderungen einer einzelnen virtuellen Maschine nur schwer erfüllen.

Die Virtual Volumes-Funktionalität trägt zur Verbesserung der Granularität bei. und ermöglicht die Differenzierung von Diensten auf virtuellen Maschinen für einzelne Anwendungen. Sie bietet somit einen neuen Ansatz für die Speicherverwaltung. Anstatt den Speicher um Funktionen eines Speichersystems anzuordnen, wird der Speicher mit Virtual Volumes entsprechend den Bedürfnissen einzelner virtueller Maschinen angeordnet, sodass im Mittelpunkt des Speichers die virtuellen Maschinen stehen.

Mit Virtual Volumes werden virtuelle Datenträger und deren Derivate, Klone, Snapshots und Replikate direkt Objekten, den so genannten Virtual Volumes, in einem Speichersystem zugewiesen. Mit dieser Zuordnung kann vSphere intensive Speichervorgänge wie Snapshots, Klonerstellung und Replikation an das Speichersystem übertragen.

Indem Sie ein Volume für jeden virtuellen Datenträger erstellen, können Sie Richtlinien auf der optimalen Ebene einrichten. Sie können im Voraus über die Speicheranforderungen einer Anwendung entscheiden und diese dem Speichersystem übermitteln. Das Speichersystem erstellt eine entsprechende virtuelle Festplatte basierend auf diesen Anforderungen. Wenn Ihre virtuelle Maschine beispielsweise ein Speicher-Array vom Typ „Aktiv/Aktiv“ benötigt, brauchen Sie keinen Datenspeicher mehr zu wählen, der das Modell „Aktiv/Aktiv“ unterstützt. Stattdessen erstellen Sie ein einzelnes virtuelles Volume, das automatisch im Speicher-Array vom Typ „Aktiv/Aktiv“ platziert wird.

Virtual Volumes-Konzepte

Mit Virtual Volumes ersetzen abstrakte Speichercontainer traditionelle Speichervolumes basierend auf LUNs oder NFS-Freigaben. In vCenter Server werden die Speichercontainer durch Virtual Volumes-Datenspeicher dargestellt. In Virtual Volumes-Datenspeichern werden Virtual Volumes gespeichert, Objekte, in denen Dateien von virtuellen Maschinen gekapselt sind.

Weitere Informationen zu den verschiedenen Komponenten der Virtual Volumes-Funktionalität erhalten Sie im entsprechenden Video.

 (Virtual Volumes, Teil 1: Konzepte)

- Virtual Volume-Objekte

  Virtuelle Volumes sind Verkapselungen der Dateien und virtuellen Festplatten von virtuellen Maschinen sowie deren Derivate.

- Virtual Volumes-Speicheranbieter

  Ein Virtual Volumes-Speicheranbieter, auch VASA-Anbieter genannt, ist eine Softwarekomponente, die für vSphere die Aufgaben eines Storage-Awareness-Diensts übernimmt. Der Anbieter ermöglicht die Out-of-Band-Kommunikation zwischen vCenter Server und ESXi-Hosts auf einer Seite und einem Speichersystem auf der anderen.

- Virtual Volumes-Speichercontainer

  Im Unterschied zu traditionellem LUN- und NFS-basiertem Speicher sind für die Funktionalität von Virtual Volumes keine vorkonfigurierten Volumes auf Speicherseite erforderlich. Stattdessen verwenden Virtual Volumes einen Speichercontainer, d. h. einen Pool von Rohspeicherkapazität bzw. eine Zusammenfassung von Speicherfunktionen, die ein Speichersystem für virtuelle Volumes bereitstellen kann.

- Protokollendpunkte

  Obwohl Speichersysteme alle Aspekte von virtuellen Volumes verwalten, haben ESXi-Hosts keinen Direktzugriff auf virtuelle Volumes auf der Speicherseite. Stattdessen verwenden ESXi-Hosts einen logischen E/A-Proxy, den so genannten Protokollendpunkt, zum Kommunizieren mit virtuellen Volumes und virtuellen Festplattendateien, die virtuelle Volumes enthalten. ESXi verwendet Protokollendpunkte zum Einrichten eines Datenpfads auf Anforderung von virtuellen Maschinen zu ihren jeweiligen virtuellen Volumes.

- Bindung und Aufheben der Bindung von virtuellen Volumes an Protokollendpunkte

  Zum Zeitpunkt seiner Erstellung stellt das virtuelle Volume ein passives Element dar, das nicht sofort für E/A bereit ist. Für den Zugriff auf das virtuelle Volume sendet ESXi oder vCenter Server eine Bindungsanforderung.

- Virtual Volumes-Datenspeicher

  Ein Virtual Volumes-Datenspeicher stellt einen Speichercontainer in vCenter Server und im vSphere Client dar.

- Virtual Volumes und VM-Speicherrichtlinien

  Für eine virtuelle Maschine, die auf einem Virtual Volumes-Datenspeicher ausgeführt wird, ist eine VM-Speicherrichtlinie erforderlich.

Virtual Volume-Objekte

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 mit Ihren ESXi-Hosts verbunden ist. Sie werden als Objekte von einem kompatiblen Speichersystem exportiert und vollständig von der Hardware auf Speicherseite verwaltet.
In der Regel wird ein virtuelles Volume von einer eindeutigen GUID identifiziert. Virtuelle Volumes werden nicht im Voraus bereitgestellt, sondern automatisch erstellt, wenn Sie Verwaltungsvorgänge an virtuellen Maschinen durchführen. Zu diesen Vorgängen zählen die VM-Erstellung, das Klonen und das Erstellen von Snapshots. +ESXi und vCenter Server ordnen einen oder mehrere virtuelle Volumes einer virtuellen Maschine zu.

Typen von Virtual Volumes

Das System erstellt die folgenden Typen virtueller Volumes für die Kernelemente einer virtuellen Maschine:

Data-vVol

Ein virtuelles Daten-Volume, das direkt jeder `.vmdk`-Datei der virtuellen Festplatte entspricht. Wie virtuelle Festplattendateien in herkömmlichen Datenspeichern werden virtuelle Volumes den virtuellen Maschinen als SCSI-Festplatten angezeigt. Data-vVols können Thick- oder Thin-bereitgestellt sein.

Config-vVol

Ein virtuelles Konfigurations-Volume bzw. Stammverzeichnis stellt ein kleines Verzeichnis mit Metadatendateien für eine virtuelle Maschine dar. Die Datei umfasst eine `.vmx`-Datei, Deskriptordateien für virtuelle Festplatten, Protokolldateien usw. Das virtuelle Konfigurations-Volume wird mit einem Dateisystem formatiert. Wenn ESXi das SCSI-Protokoll für die Verbindung mit dem Speicher verwendet, werden virtuelle Konfigurations-Volumes mit VMFS konfiguriert. Beim NFS-Protokoll werden virtuelle Konfigurations-Volumes als NFS-Verzeichnis angezeigt. In der Regel ist es Thin-bereitgestellt.

Swap-vVol

Wird beim erstmaligen Einschalten einer virtuellen Maschine erstellt. Es stellt ein virtuelles Volume dar, auf dem Kopien von Speicherseiten virtueller Maschinen gespeichert werden, die nicht im Arbeitsspeicher beibehalten werden können. Seine Größe wird von der Speichergröße der virtuellen Maschine festgelegt. Standardmäßig ist es Thick-bereitgestellt.

Snapshot-vVol

Ein virtuelles Speichervolume, auf dem der Inhalt des Arbeitsspeichers einer virtuellen Maschine für einen Snapshot gespeichert wird. Thick-bereitgestellt.

Andere

Ein virtuelles Volume für bestimmte Funktionen. So wird beispielsweise ein virtuelles Digest-Volume für Content-Based Read Cache (CBRC) erstellt.

Eine virtuelle Maschine erstellt im allgemeinen mindestens drei virtuelle Volumes: data-vVol, config-vVol und swap-vVol. Die maximale Anzahl hängt davon ab, wie viele virtuelle Festplatten und Snapshots sich in der virtuellen Maschine befinden.

So verfügt der folgende SQL-Server beispielsweise über sechs virtuelle Volumes:

- Config-vVol
- Data-vVol für das Betriebssystem
- Data-vVol für die Datenbank
- Data-vVol für das Protokoll
- Swap-vVol beim Einschalten

- Snapshot-vVol

Indem Sie unterschiedliche virtuelle Volumes für verschiedene VM-Komponenten verwenden, können Sie Speicherrichtlinien auf der feinsten Granularitätsstufe anwenden und handhaben. Beispiel: Ein virtuelles Volume, das eine virtuelle Festplatte enthält, kann mehr Dienste enthalten als das virtuelle Volume für das VM-Startlaufwerk. Ebenso kann ein virtuelles Snapshot-Volume eine andere Speicherebene als das aktuelle virtuelle Volume verwenden.

Festplattenbereitstellung

Die Virtual Volumes-Funktionalität unterstützt das Konzept von Thin- und Thick-bereitgestellten virtuellen Festplatten. Vom E/A-Standpunkt aus betrachtet ist die Implementierung und Verwaltung von Thin oder Thick Provisioning durch die Arrays jedoch für die ESXi-Hosts transparent. ESXi lagert alle Funktionen im Zusammenhang mit Thin Provisioning in die Speicher-Arrays aus. Im Datenpfad behandelt ESXi die virtuellen Thin- oder Thick-Volumes gleich.

Sie wählen den Typ „Thin“ oder „Thick“ für die virtuelle Festplatte bei der Erstellung der VM aus. Handelt es sich um eine Festplatte vom Typ „Thin“ und befindet sie sich in einem Virtual Volumes-Datenspeicher, können Sie diesen Typ später nicht durch Vergrößern der Festplatte ändern.

Gemeinsam genutzte Festplatten

Sie können eine gemeinsam genutzte Festplatte auf einem Virtual Volumes-Speicher ablegen, der dauerhafte SCSI-Reservierungen für Virtual Volumes unterstützt. Sie können diese Festplatte als Quorum-Festplatte verwenden und RDMs in den MSCS-Clustern vermeiden. Weitere Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Virtual Volumes-Speicheranbieter

Ein Virtual Volumes-Speicheranbieter, auch VASA-Anbieter genannt, ist eine Softwarekomponente, die für vSphere die Aufgaben eines Storage-Awareness-Diensts übernimmt. Der Anbieter ermöglicht die Out-of-Band-Kommunikation zwischen vCenter Server und ESXi-Hosts auf einer Seite und einem Speichersystem auf der anderen.

Der Speicheranbieter wird über VMware APIs für Storage Awareness (VASA) implementiert und verwaltet alle Aspekte der Virtual Volumes-Speicherung. Bei der Kommunikation mit vCenter Server und ESXi-Hosts arbeitet er eng mit dem im Lieferumfang von vSphere enthaltenen Speicherüberwachungsdienst (Storage Monitoring Service, SMS) zusammen.

Der Speicheranbieter liefert Informationen vom zugrunde liegenden Datenspeicher. Die Funktionen des Speichercontainers werden in vCenter Server und dem vSphere Client angezeigt. Anschließend übermittelt er die Speicheranforderungen der virtuellen Maschine, die Sie in Form einer Speicherrichtlinie definieren können, an die Speicherebene. Der Integrationsprozess stellt sicher, dass ein in der Speicherebene erstelltes virtuelles Volume die Anforderungen in der Richtlinie erfüllt.

Speicheranbieter, die in vSphere integriert werden können und Virtual Volumes unterstützen, werden üblicherweise von externen Herstellern bezogen. Jeder Speicheranbieter muss von VMware zertifiziert sein und ordnungsgemäß bereitgestellt werden. Informationen zum Bereitstellen und Aktualisieren des Virtual Volumes-Speicheranbieters auf eine Version, die mit der aktuellen Version von ESXi kompatibel ist, erhalten Sie bei Ihrem Speicheranbieter.

Nach der Bereitstellung des Speicheranbieters müssen Sie ihn in vCenter Server registrieren, damit er über den SMS mit vSphere kommunizieren kann.

Virtual Volumes-Speichercontainer

Im Unterschied zu traditionellem LUN- und NFS-basiertem Speicher sind für die Funktionalität von Virtual Volumes keine vorkonfigurierten Volumes auf Speicherseite erforderlich. Stattdessen verwenden Virtual Volumes einen Speichercontainer, d. h. einen Pool von Rohspeicherkapazität bzw. eine Zusammenfassung von Speicherfunktionen, die ein Speichersystem für virtuelle Volumes bereitstellen kann.

Ein Speichercontainer ist ein Teil der logischen Speicher-Fabric und eine logische Einheit der zugrunde liegenden Hardware. Der Speichercontainer gruppiert virtuelle Volumes logisch basierend auf den Verwaltungs- und Administratoranforderungen. Der Speichercontainer kann zum Beispiel alle virtuellen Volumes enthalten, die für einen Mandanten in einer Mehrmandantenbereitstellung oder eine Abteilung in einer Unternehmensbereitstellung erstellt wurden. Jeder Speichercontainer dient als Speicher für virtuelle Volumes, und virtuelle Volumes werden entsprechend der Kapazität des Speichercontainers zugeteilt.

In der Regel definiert ein Speicheradministrator auf der Speicherseite Speichercontainer. Die Anzahl der Speichercontainer, deren Kapazität und Größe hängen von einer anbieterspezifischen Implementierung ab. Es ist mindestens ein Container pro Speichersystem erforderlich.

Hinweis Ein einzelner Speichercontainer kann sich nicht über verschiedene physische Arrays erstrecken.

Nach dem Registrieren eines mit dem Speichersystem verknüpften Speicheranbieters erkennt vCenter Server alle konfigurierten Speichercontainer zusammen mit ihren Speicherfunktionsprofilen, Protokollendpunkten und anderen Attributen. Ein einzelner Speichercontainer kann mehrere Funktionsprofile exportieren. Deshalb können virtuelle Maschinen mit verschiedenen Anforderungen und verschiedenen Speicherrichtlinieneinstellungen Teil desselben Speichercontainers sein.

Anfangs ist keiner der erkannten Speichercontainer mit einem bestimmten Host verbunden, und sie werden im vSphere Client nicht angezeigt. Zum Mounten eines Speichercontainers müssen Sie diesen einem Virtual Volumes-Datenspeicher zuordnen.

Protokollendpunkte

Obwohl Speichersysteme alle Aspekte von virtuellen Volumes verwalten, haben ESXi-Hosts keinen Direktzugriff auf virtuelle Volumes auf der Speicherseite. Stattdessen verwenden ESXi-Hosts einen logischen E/A-Proxy, den so genannten Protokollendpunkt, zum Kommunizieren

mit virtuellen Volumes und virtuellen Festplattendateien, die virtuelle Volumes enthalten. ESXi verwendet Protokollendpunkte zum Einrichten eines Datenpfads auf Anforderung von virtuellen Maschinen zu ihren jeweiligen virtuellen Volumes.

Jedes virtuelle Volume ist an einen speziellen Protokollendpunkt gebunden. Wenn eine virtuelle Maschine auf dem Host einen E/A-Vorgang ausführt, leitet der Protokollendpunkt die E/A zum entsprechenden virtuellen Volume. Im Allgemeinen benötigt ein Speichersystem nur einige wenige Protokollendpunkte. Ein einzelner Protokollendpunkt kann mit Hunderten oder Tausenden von virtuellen Volumes verbunden werden.

Auf der Speicherseite konfiguriert ein Speicheradministrator Protokollendpunkte, einen oder mehrere pro Speichercontainer. Die Protokollendpunkte sind ein Teil des physischen Speicher-Fabric. Das Speichersystem exportiert die Protokollendpunkte mit den dazugehörigen Speichercontainern über den Speicheranbieter. Nach dem Zuordnen des Speichercontainers zu einem Virtual Volumes-Datenspeicher erkennt der ESXi-Host die Protokollendpunkte, die anschließend im vSphere Client sichtbar werden. Die Protokollendpunkte können auch während der Neuprüfung eines Speichers erkannt werden. Die Protokollendpunkte können von mehreren Hosts erkannt und gemountet werden.

Im vSphere Client sieht die Liste verfügbarer Protokollendpunkte ähnlich wie die Liste der Hostspeichergeräte aus. Sie können verschiedene Speichertransporte verwenden, um die Protokollendpunkte für ESXi offenzulegen. Wenn der SCSI-basierte Transport verwendet wird, stellt der Protokollendpunkt eine durch eine T10-basierte LUN WWN definierte Proxy-LUN dar. Für das NFS-Protokoll ist der Protokollendpunkt ein Mount-Punkt, wie zum Beispiel eine IP-Adresse und ein Freigabename. Sie können Mehrfachpfade auf dem SCSI-basierten Protokollendpunkt, aber nicht auf dem NFS-basierten Protokollendpunkt konfigurieren. Unabhängig vom verwendeten Protokoll kann ein Speicher-Array mehrere Protokollendpunkte zu Verfügbarkeitszwecken bereitstellen.

Protokollendpunkte werden pro Array verwaltet. ESXi und vCenter Server gehen davon aus, dass alle zu einem Array gemeldeten Protokollendpunkte mit allen Containern in diesem Array verknüpft sind. Wenn es in einem Array beispielsweise zwei Container und drei Protokollendpunkte gibt, geht ESXi davon aus, dass die virtuellen Volumes in beiden Containern an alle drei Protokollendpunkte gefunden werden können.

Bindung und Aufheben der Bindung von virtuellen Volumes an Protokollendpunkte

Zum Zeitpunkt seiner Erstellung stellt das virtuelle Volume ein passives Element dar, das nicht sofort für E/A bereit ist. Für den Zugriff auf das virtuelle Volume sendet ESXi oder vCenter Server eine Bindungsanforderung.

Das Speichersystem antwortet mit einer Protokollendpunkt-ID, die zu einem Zugriffspunkt zum virtuellen Volume wird. Der Protokollendpunkt nimmt alle E/A-Anforderungen an das virtuelle Volume an. Diese Bindung besteht so lange, bis ESXi eine Anforderung zum Aufheben der Bindung für das virtuelle Volume sendet.

Für spätere Bindungsanforderungen zum selben virtuellen Volume kann das Speichersystem unterschiedliche Protokollendpunkt-IDs zurückgeben.

Wenn von mehreren ESXi-Hosts gleichzeitige Bindungsanforderungen zu einem virtuellen Volume eingehen, kann das Speichersystem für jeden anfordernden ESXi-Host dieselben oder andere Endpunktbindungen zurückgeben. Anders ausgedrückt, das Speichersystem kann verschiedene gleichzeitige Hosts über unterschiedliche Endpunkte an dasselbe virtuelle Volume binden.

Bei der Aufhebung der Bindung wird der D/A-Zugriffspunkt vom virtuellen Volume entfernt. Das Speichersystem kann die Bindung des virtuellen Volumes zu seinem Protokollendpunkt sofort oder verzögert aufheben oder eine andere Aktion durchführen. Ein gebundenes virtuelles Volume kann erst gelöscht werden, nachdem die Bindung aufgehoben wurde.

Virtual Volumes-Datenspeicher

Ein Virtual Volumes-Datenspeicher stellt einen Speichercontainer in vCenter Server und im vSphere Client dar.

Nachdem vCenter Server von Speichersystemen exportierte Speichercontainer erkannt hat, müssen Sie diese als Virtual Volumes-Datenspeicher bereitstellen. Die Virtual Volumes-Datenspeicher werden nicht auf herkömmliche Art und Weise formatiert, wie z. B. VMFS-Datenspeicher. Sie müssen sie dennoch erstellen, da das Datenspeicher-Konstrukt für alle vSphere-Funktionen einschließlich FT, HA, DRS usw. ordnungsgemäß funktionieren muss.

Mit dem Assistenten zum Erstellen von Datenspeichern im vSphere Client ordnen Sie einen Speichercontainer einem Virtual Volumes-Datenspeicher zu. Der erstellte Virtual Volumes-Datenspeicher entspricht direkt dem jeweiligen Speichercontainer.

Vom Standpunkt eines vSphere-Administrators aus ähnelt der Virtual Volumes-Datenspeicher jedem beliebigen anderen Datenspeicher und wird als Behälter für virtuelle Maschinen verwendet. Wie andere Datenspeicher kann der Virtual Volumes-Datenspeicher durchsucht werden; dabei werden virtuelle Volumes nach dem Namen der virtuellen Maschine aufgelistet. Wie traditionelle Datenspeicher unterstützt der Virtual Volumes-Datenspeicher Unmounten und Mounten. Bestimmte Vorgänge wie beispielsweise Aktualisieren oder Vergrößern/Verkleinern sind allerdings nicht auf den Virtual Volumes-Datenspeicher anwendbar. Die Kapazität des Virtual Volumes-Datenspeichers kann vom Speicheradministrator außerhalb von vSphere konfiguriert werden.

Sie können die Virtual Volumes-Datenspeicher mit herkömmlichen VMFS- und NFS-Datenspeichern und mit vSAN verwenden.

Hinweis Die Größe eines virtuellen Volumes muss ein Vielfaches von 1 MB bei einer Mindestgröße von 1 MB sein. Daher müssen alle virtuellen Festplatten, die Sie auf einem Virtual Volumes-Datenspeicher bereitstellen, ein gerades Vielfaches von 1 MB sein. Wenn die Kapazität der virtuellen Festplatte, die Sie in den Virtual Volumes-Datenspeicher migrieren, kein gerades Vielfaches von 1 MB ist, erweitern Sie den Datenträger auf das nächste gerade Vielfache von 1 MB.

Virtual Volumes und VM-Speicherrichtlinien

Für eine virtuelle Maschine, die auf einem Virtual Volumes-Datenspeicher ausgeführt wird, ist eine VM-Speicherrichtlinie erforderlich.

VM-Speicherrichtlinien sind Regelsätze, die die Platzierungs- und Dienstqualitätsanforderungen für eine virtuelle Maschine beschreiben. Die Richtlinie setzt die angemessene Platzierung der virtuellen Maschine im Virtual Volumes-Speicher durch und sorgt dafür, dass der Speicher die Anforderungen der virtuellen Maschine erfüllen kann.

Mithilfe der Schnittstelle für VM-Speicherrichtlinien können Sie eine Virtual Volumes-Speicherrichtlinie erstellen. Wenn Sie der virtuellen Maschine die neue Richtlinie zuweisen, bewirkt diese, dass der Virtual Volumes-Speicher die Anforderungen erfüllt.

Virtual VolumesStandardspeicherrichtlinie

Für Virtual Volumes bietet VMware eine Standardspeicherrichtlinie, die keine Regeln oder Speicheranforderungen enthält. Diese wird als Virtual Volumes-Richtlinie ohne Anforderungen bezeichnet. Diese Richtlinie wird auf VM-Objekte angewendet, wenn Sie keine andere Richtlinie für die virtuelle Maschine im Virtual Volumes-Datenspeicher festlegen. Mit der Richtlinie „Keine Anforderungen“ können Speicher-Arrays die optimale Platzierung für die VM-Objekte bestimmen.

Die von VMware zur Verfügung gestellte Standardrichtlinie „Keine Anforderungen“ weist die folgenden Merkmale auf:

- Sie können diese Richtlinie nicht löschen, bearbeiten oder klonen.
- Die Richtlinie ist nur mit den Virtual Volumes-Datenspeichern kompatibel.
- Sie können eine VM-Speicherrichtlinie für Virtual Volumes erstellen und als Standard festlegen.

Virtual Volumes und Speicherprotokolle

Ein Virtual Volumes-Speichersystem stellt Protokollendpunkte bereit, die im physischen Speicher-Fabric erkennbar sind. ESXi-Hosts verwenden die Protokollendpunkte zum Herstellen einer Verbindung zu virtuellen Volumes im Speicher. Der Betrieb der Protokollendpunkte hängt von den Speicherprotokollen ab, die die Endpunkte für ESXi-Hosts offenlegen.

Virtual Volumes unterstützt NFS-Version 3 und 4.1, iSCSI, Fibre Channel und FCoE.

Unabhängig vom verwendeten Speicherprotokoll bieten Protokollendpunkte einheitlichen Zugriff sowohl auf SAN- als auch auf NAS-Speicher. Ein virtuelles Volume, wie z. B. eine Datei auf einem anderen traditionellen Datenspeicher, wird auf einer virtuellen Maschine als SCSI-Datenträger dargestellt.

Hinweis Ein Speichercontainer wird SCSI oder NAS zugewiesen und kann nicht von diesen Protokolltypen gemeinsam genutzt werden. Ein Array kann einen Speichercontainer mit SCSI-Endpunkten und einen anderen Container mit NFS-Protokollendpunkten darstellen. Eine Kombination aus SCSI- und NFS-Protokollendpunkten kann der Container nicht verwenden.

Virtual Volumes und SCSI-basierter Transport

Auf Festplatten-Arrays unterstützt Virtual Volumes Fibre Channel-, FCoE- und iSCSI-Protokolle.

Wenn das SCSI-basierte Protokoll verwendet wird, stellt der Protokollendpunkt eine durch eine T10-basierte LUN WWN definierte Proxy-LUN dar.

Protokollendpunkte werden wie blockbasierte LUNs mithilfe von LUN-Standard-Erkennungsbefehlen erkannt. Der ESXi-Host prüft regelmäßig auf neue Geräte und erkennt asynchron blockbasierte Protokollendpunkte. Auf den Protokollendpunkt kann von mehreren Pfaden zugegriffen werden. Der Datenverkehr auf diesen Pfaden befolgt bekannte Richtlinien zur Pfadauswahl, wie dies für LUNs typisch ist.

ESXi erstellt auf SCSI-basierten Festplatten-Arrays zum Zeitpunkt der Erstellung der virtuellen Maschine ein virtuelles Volume und formatiert dieses als VMFS. Auf diesem kleinen virtuellen Volume werden alle Metadaten der virtuellen Maschine gespeichert. Es wird als Konfigurations-vVol bezeichnet. Das Konfigurations-vVol fungiert als Speicher-Locator der virtuellen Maschine für vSphere.

Virtual Volumes auf Festplatten-Arrays unterstützt denselben Satz von SCSI-Befehlen wie VMFS und verwenden ATS als Sperrmechanismus.

CHAP-Unterstützung für iSCSI-Endpoints

Virtual Volumes unterstützt das Challenge Handshake Access Protocol (CHAP) mit iSCSI-Zielen. Mit dieser Option können ESXi-Hosts die Anmeldedaten des CHAP-Initiators an Virtual Volumes-Speicheranbieter, auch als VASA-Anbieter bezeichnet, freigeben und Virtual Volumes-Speicheranbietern die Möglichkeit geben, Systemereignisse auszugeben, die vCenter Server über Änderungen an den Anmeldedaten des CHAP-Ziels auf dem Speicher-Array benachrichtigen.

Jeder ESXi-Host kann über mehrere HBAs verfügen, und für jeden HBA können Eigenschaften konfiguriert werden. Eine dieser Eigenschaften ist die Authentifizierungsmethode, die der HBA verwenden muss. Die Authentifizierung ist optional, aber wenn sie implementiert wird, muss sie sowohl vom Initiator als auch vom Ziel unterstützt werden. CHAP ist eine Authentifizierungsmethode, die in beiden Richtungen zwischen Initiator und Ziel verwendet werden kann.

Weitere Informationen zu verschiedenen CHAP-Authentifizierungsmethoden finden Sie unter Auswählen der CHAP-Authentifizierungsmethode. Informationen zum Konfigurieren von CHAP auf dem ESXi-Host finden Sie unter Konfigurieren von CHAP-Parametern für iSCSI- oder iSER-Speicheradapter..

Virtual Volumes und NFS-Transport

Beim NAS-Speicher stellt ein Protokollendpunkt eine NFS-Freigabe dar, die der ESXi-Host unter Verwendung der IP-Adresse oder des DNS-Namens und eines Freigabenamens mountet. Virtual Volumes unterstützt die NFS-Versionen 3 und 4.1 für den Zugriff auf den NAS-Speicher. Sowohl IPv4- als auch IPv6-Formate werden unterstützt.

Unabhängig von der verwendeten Version kann ein Speicher-Array mehrere Protokollendpunkte zu Verfügbarkeitszwecken bereitstellen.

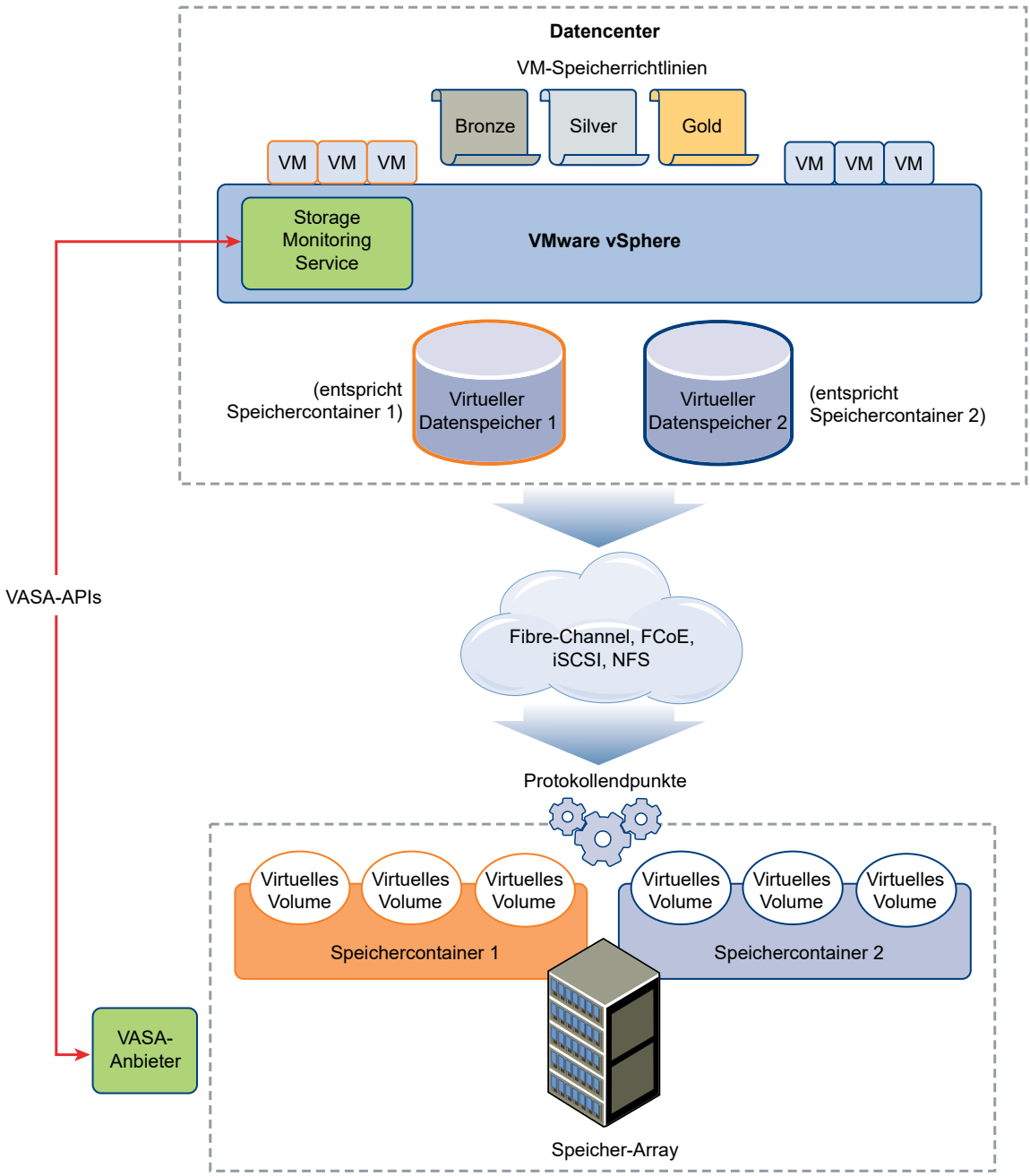
Darüber hinaus werden mit NFS-Version 4.1 Trunking-Mechanismen eingeführt, die den Lastausgleich und das Multipathing ermöglichen.

Virtual Volumes auf NAS-Geräten unterstützt dieselben NFS-RPCs (Remote Procedure Calls), die ESXi-Hosts zum Verbinden mit NFS-Mount-Punkten verwenden.

Auf NAS-Geräten stellt ein Konfigurations-vVol eine Verzeichnisunterstruktur dar, die einem Konfigurations-vVolID entspricht. Das Konfigurations-vVol muss Verzeichnisse und andere Vorgänge unterstützen, die für NFS erforderlich sind.

Virtual Volumes – Architektur

Ein architektonisches Diagramm bietet eine Übersicht darüber, wie alle Komponenten der Virtual Volumes-Funktionalität miteinander interagieren.



Virtuelle Volumes sind Objekte, die von einem kompatiblen Speichersystem exportiert wurden, und entsprechen in der Regel exakt einer VM-Festplatte und anderen VM-bezogenen Dateien. Ein virtuelles Volume wird durch einen VASA-Anbieter out-of-band und nicht im Datenpfad erstellt und geändert.

Ein VASA-Anbieter bzw. ein Speicheranbieter wird durch vSphere-APIs für Storage Awareness entwickelt. Der Speicheranbieter ermöglicht die Kommunikation zwischen dem ESXi-Hosts, vCenter Server und dem vSphere Client auf der einen Seite und dem Speichersystem auf der anderen Seite. Der VASA-Anbieter wird auf der Speicherseite ausgeführt und ist auf den vSphere-Speicherüberwachungsdienst (SMS) zum Verwalten aller Aspekte des Virtual Volumes-Speichers abgestimmt. Der VASA-Anbieter ordnet Objekte virtueller Festplatten und deren Ableitungen, wie Klone, Snapshots und Repliken, direkt den virtuellen Volumes auf dem Speichersystem zu.

Die ESXi-Hosts haben keinen Direktzugriff auf den Speicher für virtuelle Volumes. Stattdessen greifen die Hosts durch eine Zwischenstelle im Datenpfad, den so genannten Protokollendpunkt, auf die virtuellen Volumes zu. Die Protokollendpunkte richten auf Anforderung einen Datenpfad von virtuellen Maschinen zu ihren jeweiligen virtuellen Volumes ein. Die Protokollendpunkte dienen als Gateway für direktes in-Band E/A zwischen ESXi-Host und dem Speichersystem. ESXi kann Fibre-Channel-, FCoE-, iSCSI- und NFS-Protokolle für In-Band-Datenaustausch verwenden.

Die virtuellen Volumes befinden sich in Speichercontainern, die logisch einen Pool von physischen Festplatten im Speichersystem darstellen. Auf der Seite von vCenter Server und ESXi werden Speichercontainer als Virtual Volumes-Datenspeicher dargestellt. Ein einzelner Speichercontainer kann mehrere Speicherfunktionssätze exportieren und verschiedenen virtuellen Volumes verschiedene Dienstebenen bieten.

Informationen zur Architektur von Virtual Volumes erhalten Sie im entsprechenden Video.

 (Virtual Volumes, Teil 2: Architektur)

Virtual Volumes und VMware Certificate Authority

vSphere beinhaltet die VMware Certificate Authority (VMCA). VMCA generiert standardmäßig alle internen Zertifikate, die in der vSphere-Umgebung verwendet werden. Hierzu zählen auch Zertifikate für neu hinzugefügte ESXi-Hosts und VASA-Speicheranbieter, die Virtual Volumes-Speichersysteme verwalten oder repräsentieren.

Die Kommunikation mit dem VASA-Anbieter wird durch SSL-Zertifikate geschützt. Diese Zertifikate können vom VASA-Anbieter oder von der VMCA stammen.

- Zertifikate können direkt vom VASA-Anbieter für die langfristige Verwendung bereitgestellt werden. Sie können entweder selbstgeneriert und selbstsigniert sein oder aber von einer externen Zertifizierungsstelle stammen.
- Zertifikate können von der VMCA für die Verwendung durch den VASA-Anbieter generiert werden.

Wenn ein Host oder VASA-Anbieter registriert ist, führt VMCA diese Schritte automatisch aus, ohne dass der vSphere-Administrator eingreifen muss.

1 Wenn ein VASA-Anbieter erstmalig zum Speicherverwaltungsdienst (Storage Management Service, SMS) von vCenter Server hinzugefügt wird, wird ein selbstsigniertes Zertifikat erstellt.

2 Nach der Überprüfung des Zertifikats fordert der Speicherverwaltungsdienst eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) vom VASA-Anbieter an.

3 Nach dem Empfang und der Überprüfung der CSR wird sie vom Speicherverwaltungsdienst im Namen des VASA-Anbieters gegenüber der VMCA präsentiert und es wird ein von der Zertifizierungsstelle signiertes Zertifikat angefordert.

   Die VMCA kann als eigenständige Zertifizierungsstelle oder als untergeordnete Zertifizierungsstelle für eine Unternehmenszertifizierungsstelle konfiguriert werden. Wenn Sie die VMCA als untergeordnete Zertifizierungsstelle einrichten, signiert VMCA die CSR mit der vollständigen Zertifizierungskette.

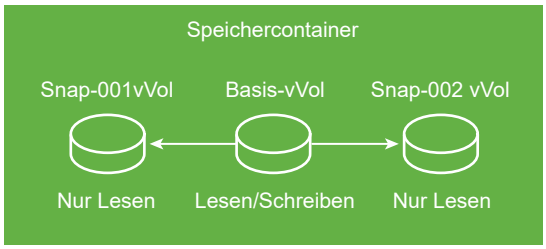
4 Das signierte Zertifikat wird zusammen mit dem Rootzertifikat an den VASA-Anbieter übergeben. Der VASA-Anbieter kann alle zukünftigen sicheren Verbindungen, die vom Speicherverwaltungsdienst ausgehen, in vCenter Server und auf ESXi-Hosts authentifizieren.

Virtual Volume-Snapshots

Beim Erstellen eines Snapshots werden der gesamte Status und alle Daten der virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung erfasst. Snapshots sind hilfreich, wenn Sie wiederholt zu einem bestimmten Status der virtuellen Maschine zurückkehren müssen, aber nicht mehrere virtuelle Maschinen erstellen möchten. Snapshots von virtuellen Volumes dienen zahlreichen Zwecken, Sie können sie zum Erstellen einer stillgelegten Kopie zu Sicherungs- oder Archivierungszwecken oder zum Erstellen einer Test- und Rollback-Umgebung für Anwendungen verwenden. Sie können sie auch verwenden, um Anwendungs-Images sofort bereitzustellen.

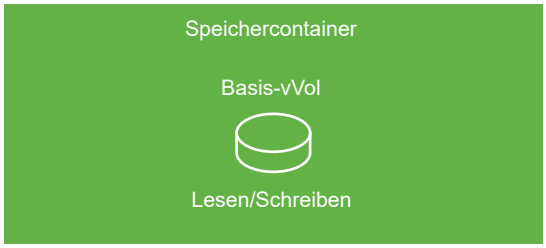
In einer Virtual Volumes-Umgebung werden Snapshots von ESXi und vCenter Server verwaltet, jedoch vom Speicher-Array durchgeführt.

Jeder Snapshot erstellt ein zusätzliches virtuelles Volume-Objekt, ein virtuelles Snapshot-Volume, das den Inhalt des Speichers der virtuellen Maschine enthält. Die Originaldaten der virtuellen Maschine werden in dieses Objekt kopiert und sind schreibgeschützt, damit das Gastbetriebssystem nicht in den Snapshot schreiben kann. Die Größe des virtuellen Volumes im Snapshot kann nicht geändert werden. Wenn die virtuelle Maschine repliziert wird, wird dessen virtuelles Volume im Snapshot im Allgemeinen ebenfalls repliziert.



Das virtuelle Basis-Volume bleibt aktiv oder mit Lese-Schreibberechtigung. Bei Erstellen eines weiteren Snapshots bleiben der neue Status und die Daten der virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung erhalten.

Wenn Sie Snapshots löschen, bleibt nur das virtuelle Basis-Volume erhalten, während die virtuellen Snapshot-Volume-Objekte verworfen werden. Das virtuelle Basis-Volume bleibt bestehen; es stellt den aktuellsten Status der virtuellen Maschine dar. Anders als bei Snapshot in den traditionellen Datenspeichern müssen die virtuellen Snapshot-Volumes nicht in das virtuelle Basis-Volume übernommen zu werden.



Informationen zum Erstellen und Verwalten von Snapshots finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Vor dem Aktivieren von Virtual Volumes

Für die Arbeit mit Virtual Volumes müssen Sie sicherstellen, dass Ihre Speicherumgebung und Ihre vSphere-Umgebung korrekt eingerichtet sind.

Vorbereiten des Speichersystems für Virtual Volumes

Befolgen Sie bei der Vorbereitung Ihrer Speichersystemumgebung für die Virtual Volumesnachstehenden Richtlinien: Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

- Das verwendete Speichersystem oder Speicherarray muss Virtual Volumes unterstützen und über vSphere-APIs for Storage Awareness (VASA) in die vSphere-Komponenten integriert werden können. Das Speicherarray muss Thin Provisioning und das Erstellen von Snapshots unterstützen.
- Der Virtual Volumes-Speicheranbieter muss bereitgestellt werden.
- Folgende Komponenten müssen auf der Speicherseite konfiguriert werden:
  - Protokollendpunkte
  - Speichercontainer
  - Speicherprofile
  - Replizierungskonfigurationen, wenn Virtual Volumes mit Replizierung verwendet werden sollen. Weitere Informationen hierzu finden Sie unter Anforderungen für die Replizierung mit Virtual Volumes.

Vorbereitung der vSphere-Umgebung

- Befolgen Sie die Setup-Richtlinien für den verwendeten Speichertyp: Fibre Channel, FCoE, iSCSI oder NFS. Falls erforderlich, installieren und konfigurieren Sie Speicheradapter auf Ihren ESXi-Hosts.
  - Bei Verwendung von iSCSI aktivieren Sie die Software-iSCSI-Adapter auf Ihren ESXi-Hosts. Konfigurieren Sie die dynamische Erkennung und geben Sie die IP-Adresse Ihres Virtual Volumes-Speichersystems ein. Weitere Informationen hierzu finden Sie unter Konfigurieren des Software-iSCSI-Adapters.
- Synchronisieren Sie alle Komponenten im Speicherarray mit vCenter Server und allen ESXi-Hosts. Verwenden Sie dazu das Network Time Protocol (NTP).

Weitere Informationen erhalten Sie bei Ihrem Händler sowie unter *VMware-Kompatibilitätshandbuch*.

Synchronisieren der vSphere Storage-Umgebung mit einem NTP-Server

Wenn Sie Virtual Volumes verwenden, konfigurieren Sie Network Time Protocol (NTP), um sicherzustellen, dass alle ESXi-Hosts auf dem vSphere-Netzwerk synchronisiert sind.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter **System** die Option **Uhrzeitkonfiguration** aus.
4. Klicken Sie auf **Bearbeiten** und richten Sie den NTP-Server ein.
   a. Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.
   b. Legen Sie die Startrichtlinie für den NTP-Dienst fest.
   c. Geben Sie die IP-Adressen des NTP-Servers für die Synchronisierung ein.
   d. Klicken Sie im Abschnitt „NTP-Dienststatus“ auf **Starten** oder **Neu starten**.
5. Klicken Sie auf **OK**.

   Der Host wird mit dem NTP-Server synchronisiert.

Konfigurieren von Virtual Volumes

Führen Sie eine Reihe von Schritten aus, um Ihre Virtual Volumes-Umgebung zu konfigurieren.

Voraussetzungen

Befolgen Sie die Anweisungen in Vor dem Aktivieren von Virtual Volumes.

Verfahren

1 Registrieren von Virtual Volumes-Speicheranbietern

Ihre Virtual Volumes-Umgebung muss Speicheranbieter umfassen, auch als VASA-Anbieter bezeichnet. In der Regel entwickeln Drittanbieter Speicheranbieter über die VMware APIs for Storage Awareness (VASA). Speicheranbieter ermöglichen die Kommunikation zwischen vSphere und dem Speicher. Verwenden Sie den vSphere Client, um die Virtual Volumes-Speicheranbieter zu registrieren.

2 Erstellen eines Virtual Volumes-Datenspeichers

Virtual Volumes-Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

3 Prüfen und Verwalten von Protokoll-Endpoints

ESXi-Hosts verwenden einen logischen E/A-Proxy, Protokollendpunkt genannt, um mit virtuellen Volumes und den Dateien auf virtuellen Festplatten zu kommunizieren. Protokollendpunkte werden vom Speichersystem über einen Speicheranbieter gemeinsam mit den zugehörigen Speichercontainern exportiert. Protokollendpunkte werden im vSphere Client nach der Zuordnung eines Speichercontainers zu einem Virtual Volumes-Datenspeicher angezeigt. Sie können die Eigenschaften von Protokollendpunkten prüfen und einzelne Einstellungen ändern.

4 (Optional) Ändern der Pfadauswahlrichtlinie für einen Protokoll-Endpoint

Wenn Ihr ESXi-Host SCSI-basierten Transport zur Kommunikation mit den Protokollendpunkten eines Speicherarrays verwendet, können Sie die standardmäßigen Mehrfachpfad-Richtlinien ändern, die den Protokollendpunkten zugewiesen sind. Die Pfadauswahlrichtlinie ändern Sie im Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten**.

Nächste Schritte

Sie können jetzt virtuelle Maschinen auf dem Virtual Volumes-Datenspeicher bereitstellen. Informationen zum Erstellen von virtuellen Maschinen finden Sie unter Bereitstellen von virtuellen Maschinen in Virtual Volumes-Datenspeichern und in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Registrieren von Virtual Volumes-Speicheranbietern

Ihre Virtual Volumes-Umgebung muss Speicheranbieter umfassen, auch als VASA-Anbieter bezeichnet. In der Regel entwickeln Drittanbieter Speicheranbieter über die VMware APIs for Storage Awareness (VASA). Speicheranbieter ermöglichen die Kommunikation zwischen vSphere und dem Speicher. Verwenden Sie den vSphere Client, um die Virtual Volumes-Speicheranbieter zu registrieren.

Nach der Registrierung kommuniziert der Virtual Volumes-Anbieter mit vCenter Server. Der Anbieter meldet die Merkmale der zugrunde liegenden Speicher- und Datendienste wie beispielsweise Replizierung, die das Speichersystem bereitstellt. Die Merkmale werden auf der Schnittstelle für VM-Speicherrichtlinien angezeigt und können verwendet werden, um eine VM-Speicherrichtlinie zu erstellen, die mit dem Virtual Volumes-Datenspeicher kompatibel ist. Nachdem Sie diese Speicherrichtlinie auf eine virtuelle Maschine angewandt haben, wird die Richtlinie an den Virtual Volumes-Speicher übertragen. Die Richtlinie setzt die optimale Platzierung der virtuellen Maschine im Virtual Volumes-Speicher durch und sorgt dafür, dass der Speicher die Anforderungen der virtuellen Maschine erfüllen kann. Wenn Ihr Speicher Extradienste wie beispielsweise Caching oder Replizierung bietet, werden diese durch die Richtlinie für die virtuelle Maschine aktiviert.

Voraussetzungen

Stellen Sie sicher, dass die richtige Version des Virtual Volumes-Speicheranbieters auf der Speicherseite installiert ist. Bitten Sie Ihren Speicheranbieter um die Anmeldedaten.

Verfahren

1. Navigieren Sie zu vCenter Server.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
3. Klicken Sie auf das Symbol **Add**.
4. Geben Sie die Verbindungsinformationen für den Speicheranbieter ein, einschließlich des Namens, der URL und der Anmeldedaten.
5. Geben Sie die Sicherheitsmethode an.

Aktion	Beschreibung
Verweisen Sie vCenter Server auf das Speicheranbieterzertifikat	Wählen Sie die Option **Zertifikat des Speicheranbieters verwenden** aus und geben Sie den Speicherort des Zertifikats an.
Verwenden Sie einen Fingerabdruck des Speicheranbieterzertifikats.	Wenn Sie vCenter Server nicht an das Speicherzertifikat verweisen, wird der Fingerabdruck des Zertifikats angezeigt. Sie können den Fingerabdruck überprüfen und ihn genehmigen. vCenter Server fügt das Zertifikat dem Truststore hinzu und fährt mit dem Herstellen der Verbindung fort.

   Der Speicheranbieter fügt das vCenter Server-Zertifikat dem Truststore hinzu, wenn sich vCenter Server zum ersten Mal mit dem Anbieter verbindet.
6. Klicken Sie auf **OK**, um die Registrierung abzuschließen.

Ergebnisse

vCenter Server erkennt und registriert den Virtual Volumes-Speicheranbieter.

Erstellen eines Virtual Volumes-Datenspeichers

Virtual Volumes-Datenspeicher werden mit dem Assistenten **Neuer Datenspeicher** erstellt.

Verfahren

1 Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.

2 Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.

3 Wählen Sie **vVol** als Datenspeichertyp aus.

4 Geben Sie den Namen des Datenspeichers ein und wählen Sie aus der Liste der Speichercontainer einen Backing-Speichercontainer aus.

   Achten Sie darauf, für jeden Datenspeicher in Ihrer Datenspeicherumgebung einen eindeutigen Namen zu vergeben.

   Beim Mounten eines Virtual Volumes-Datenspeichers auf mehreren Hosts muss der Datenspeichername auf allen Hosts gleich sein.

5 Wählen Sie die Hosts aus, die Zugriff auf den Datenspeicher benötigen.

6 Überprüfen Sie die Konfigurationsoptionen und klicken Sie auf **Beenden**.

Nächste Schritte

Nach der Erstellung des Virtual Volumes-Datenspeichers können Sie ihn umbenennen, Datenspeicherdateien durchsuchen, den Datenspeicher unmounten und weitere Datenspeicheraktionen ausführen.

Sie können den Virtual Volumes-Datenspeicher nicht einem Datenspeicher-Cluster hinzufügen.

Prüfen und Verwalten von Protokoll-Endpoints

ESXi-Hosts verwenden einen logischen E/A-Proxy, Protokollendpunkt genannt, um mit virtuellen Volumes und den Dateien auf virtuellen Festplatten zu kommunizieren. Protokollendpunkte werden vom Speichersystem über einen Speicheranbieter gemeinsam mit den zugehörigen Speichercontainern exportiert. Protokollendpunkte werden im vSphere Client nach der Zuordnung eines Speichercontainers zu einem Virtual Volumes-Datenspeicher angezeigt. Sie können die Eigenschaften von Protokollendpunkten prüfen und einzelne Einstellungen ändern.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Protokollendpunkte**.

4 Um Details eines bestimmten Elements anzuzeigen, wählen Sie das Element aus der Liste aus.

5 Auf den Registerkarten unter „Details zu Protokollendpunkten“ finden Sie weitere Informationen und können die Eigenschaften des ausgewählten Endpunkts ändern.

Registerkarte	Beschreibung
Eigenschaften	Zeigen Sie die Eigenschaften und Merkmale des Elements an. Bei SCSI-(Block-)Elementen können Sie die Mehrfachpfad-Richtlinien anzeigen und bearbeiten.
Pfade (nur SCSI-Protokollendpunkte)	Anzeigen der für den Protokollendpunkt verfügbaren Pfade. Deaktivieren oder Aktivieren eines ausgewählten Pfads. Ändern der Pfadauswahl-Richtlinie.
Datenspeicher	Anzeigen eines entsprechenden Virtual Volumes-Datenspeichers. Ausführen von Vorgängen zur Datenspeicherverwaltung.

Ändern der Pfadauswahlrichtlinie für einen Protokoll-Endpoint

Wenn Ihr ESXi-Host SCSI-basierten Transport zur Kommunikation mit den Protokollendpunkten eines Speicherarrays verwendet, können Sie die standardmäßigen Mehrfachpfad-Richtlinien ändern, die den Protokollendpunkten zugewiesen sind. Die Pfadauswahlrichtlinie ändern Sie im Dialogfeld **Mehrfachpfad-Richtlinien bearbeiten**.

Verfahren

1 Navigieren Sie im vSphere Client zum ESXi-Host.

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

3 Klicken Sie unter **Speicher** auf **Protokollendpunkte**.

4 Wählen Sie den Protokollendpunkt aus, dessen Pfade Sie ändern möchten, und klicken Sie auf die Registerkarte **Eigenschaften**.

5 Wählen Sie unter „Mehrfachpfad-Richtlinien“ die Option **Mehrfachpfad bearbeiten** aus dem Menü **Aktionen** aus.

6 Wählen Sie eine Pfadrichtlinie aus und konfigurieren Sie deren Einstellungen. Ihre Optionen ändern sich je nach Typ des Speichergeräts, das Sie verwenden.

   Die für Ihre Auswahl verfügbaren Pfadrichtlinien richten sich nach der Unterstützung durch den Speicheranbieter.

   - Informationen zu Pfadrichtlinien für SCSI-Geräte finden Sie unter Pfadauswahl-Plug-Ins und Richtlinien.
   - Weitere Informationen zu Pfadmechanismen für NVMe-Geräte finden Sie unter VMware High Performance-Plug-In und Pfadauswahlschemas.

7 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Bereitstellen von virtuellen Maschinen in Virtual Volumes-Datenspeichern

Sie können virtuelle Maschinen auf einem Virtual Volumes-Datenspeicher bereitstellen.

Hinweis Die Kapazität aller virtuellen Festplatten, die Sie auf einem Virtual Volumes-Datenspeicher bereitstellen, muss ein gerades Vielfaches von 1 MB sein.

Für eine virtuelle Maschine, die auf einem Virtual Volumes-Datenspeicher ausgeführt wird, ist eine geeignete VM-Speicherrichtlinie erforderlich.

Nach der Bereitstellung der virtuellen Maschine können Sie typische Verwaltungsaufgaben für die virtuelle Maschine ausführen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Verfahren

1 Definieren Sie eine VM-Speicherrichtlinie für Virtual Volumes.

   VMware stellt für Virtual Volumes eine Standardspeicherrichtlinie für zur Verfügung, die keine Anforderungen enthält. Bei Bedarf können Sie eine mit Virtual Volumes kompatible benutzerdefinierte Speicherrichtlinie erstellen.

   Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für Virtual Volumes.

2 Weisen Sie die Virtual Volumes-Speicherrichtlinie der virtuellen Maschine zu.

   Um zu gewährleisten, dass der Virtual Volumes-Datenspeicher beim Zuordnen einer virtuellen Maschine die spezifischen Datenspeicheranforderungen erfüllt, weisen Sie die Virtual Volumes-Speicherrichtlinie der virtuellen Maschine zu.

   Weitere Informationen hierzu finden Sie unter Zuweisen von Speicherrichtlinien zu virtuellen Maschinen.

3 Ändern Sie die Standardspeicherrichtlinie für einen Virtual Volumes-Datenspeicher.

   Für virtuelle Maschinen, die auf Virtual Volumes-Datenspeichern bereitgestellt sind, stellt VMware eine Standardrichtlinie ohne Anforderungen bereit. Diese Richtlinie kann nicht bearbeitet werden; Sie können jedoch eine neu erstellt Richtlinie als Standard bereitstellen.

   Weitere Informationen hierzu finden Sie unter Ändern der Standardspeicherrichtlinie für einen Datenspeicher.

Virtual Volumes und Replizierung

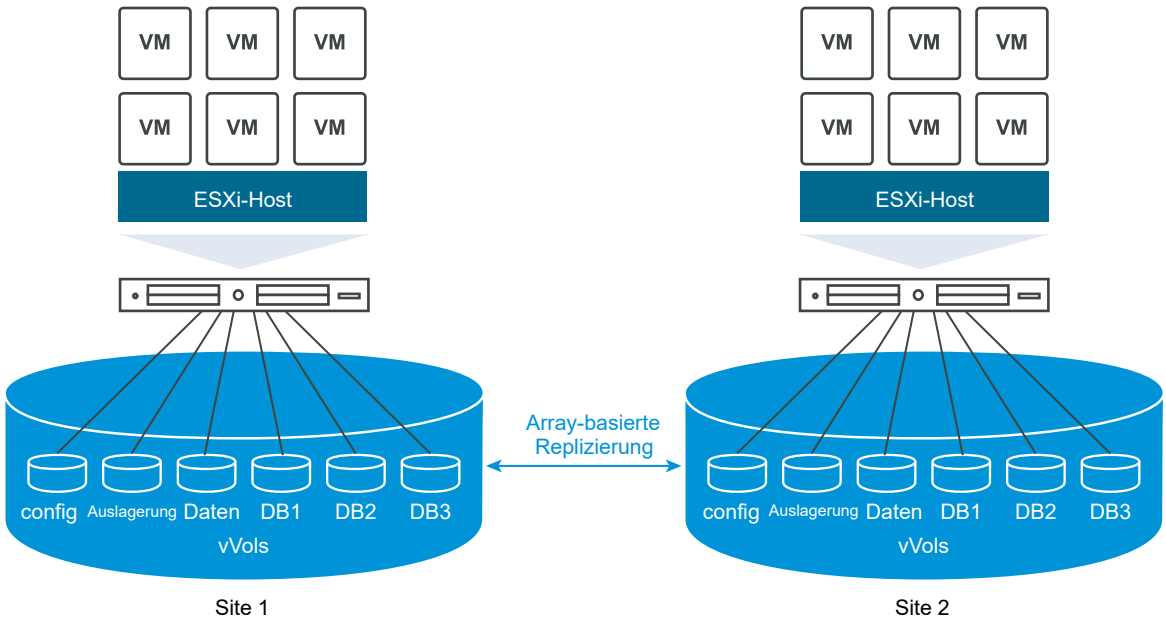
Virtual Volumes unterstützt Replizierung und Notfallwiederherstellung. Mit der Array-basierten Replizierung können Sie die Replizierung virtueller Maschinen auf Ihr Speicher-Array auslagern und anschließend alle Replizierungsfunktionen des Arrays nutzen. Sie können ein einzelnes Objekt einer virtuellen Maschine wie beispielsweise eine virtuelle Festplatte replizieren. Es ist

ebenso möglich, mehrere Objekte einer virtuellen Maschine oder mehrere virtuelle Maschinen zu gruppieren und sie als Einheit zu replizieren.

Die Array-basierte Replizierung ist richtliniengesteuert. Nachdem Sie den Virtual Volumes-Speicher für die Replizierung konfiguriert haben, werden Informationen zu den Replizierungsfunktionen und Replizierungsgruppen vom Array über den Speicheranbieter bereitgestellt. Diese Informationen werden in der Schnittstelle für VM-Speicherrichtlinien von vCenter Server angezeigt.

Mit der VM-Speicherrichtlinie können Sie die Replizierungsanforderungen für Ihre virtuellen Maschinen beschreiben. Die Parameter, die Sie in der Speicherrichtlinie festlegen, hängen von der Art und Weise ab, wie Ihr Array die Replizierung implementiert. So kann Ihre VM-Speicherrichtlinie beispielsweise Parameter wie den Replizierungszeitplan, die Replizierungshäufigkeit oder das Recovery Point Objective (RPO) enthalten. Des Weiteren können Sie in der Richtlinie das Replizierungsziel oder einen sekundären Ort, an dem die virtuellen Maschinen repliziert werden, angeben oder festlegen, ob Replikate gelöscht werden müssen.

Durch Zuweisen der Replizierungsrichtlinie während der Bereitstellung der virtuellen Maschine fordern Sie Replizierungsdienste für Ihre virtuelle Maschine an. Anschließend übernimmt das Array die Verwaltung aller Replizierungszeitpläne und -prozesse.



Anforderungen für die Replizierung mit Virtual Volumes

Wenn Sie Virtual Volumes mit Replizierung aktivieren, muss Ihre Umgebung neben den allgemeinen Anforderungen zu Virtual Volumes mehrere bestimmte Vorbedingungen erfüllen.

Informationen zu den allgemeinen Anforderungen für Virtual Volumes finden Sie unter Vor dem Aktivieren von Virtual Volumes.

Speicheranforderungen

Die Implementierung der Replizierung mit Virtual Volumes hängt von Ihrem Array ab und kann von einem Speicheranbieter zum anderen variieren. Die folgenden Anforderungen gelten im Allgemeinen für alle Anbieter.

- Die Speicher-Arrays, die Sie zur Implementierung der Replizierung verwenden, müssen mit Virtual Volumes kompatibel sein.
- Die Arrays müssen in die Version des (VASA)-Speicheranbieters integriert werden können, die mit der Replizierung mit Virtual Volumes kompatibel ist.
- Die Speicher-Arrays müssen für die Replizierung geeignet und so konfiguriert sein, dass sie vom Anbieter bereitgestellte Replizierungsmechanismen verwenden. Typische Konfigurationen weisen im Allgemeinen ein oder zwei Replizierungsziele auf. Alle erforderlichen Konfigurationen wie beispielsweise das Koppeln der replizierten und der Zielsite müssen auch auf der Speicherseite vorgenommen werden.
- Ggf. müssen Replizierungsgruppen und Fault Domains für Virtual Volumes auf der Speicherseite vorkonfiguriert werden.

Weitere Informationen erhalten Sie bei Ihrem Händler sowie unter *VMware-Kompatibilitätshandbuch*.

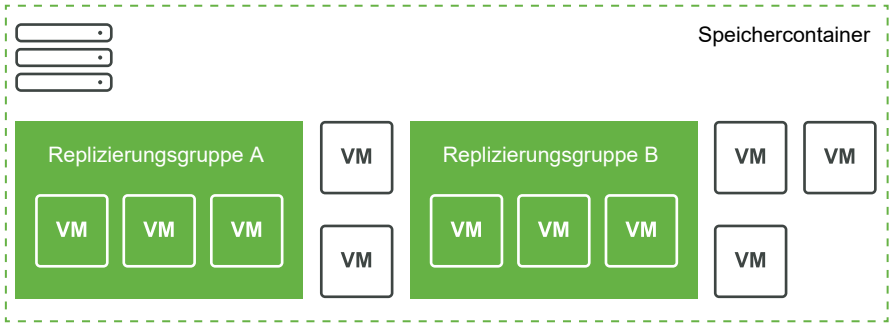
vSphere-Anforderungen

- Verwenden Sie die Versionen vCenter Server und ESXi, die die Replizierung mit Virtual Volumes-Speichern unterstützen. vCenter Server- und ESXi-Hosts, die älter sind als Version 6.5, unterstützen die Replizierung mit Virtual Volumes-Speichern nicht. Versuche, eine replizierte virtuelle Maschine auf einem inkompatiblen Host zu erstellen, schlagen mit einer Fehlermeldung fehl. Weitere Informationen finden Sie unter *VMware-Kompatibilitätshandbuch*.
- Wenn Sie die Migration einer virtuellen Maschine planen, vergewissern Sie sich, dass die Zielressourcen wie die ESXi-Hosts und die Virtual Volumes-Datenspeicher die Speicherreplizierung unterstützen.

Virtual Volumes und Replizierungsgruppen

Wenn Ihr Speicher neben Speichercontainern und Protokollendpunkten Replizierungsdienste bietet, kann der Speicheradministrator Replizierungsgruppen auf der Speicherseite konfigurieren.

vCenter Server und ESXi können die Replizierungsgruppen erkennen, verwalten jedoch nicht deren Lebenszyklus. Replizierungsgruppen, auch Konsistenzgruppen genannt, geben an, welche VMs und virtuellen Festplatten gemeinsam auf eine Zielsite repliziert werden müssen. Komponenten wie beispielsweise die VM-Konfigurationsdatei und virtuelle Festplatten können von einer virtuellen Maschine unterschiedlichen vorkonfigurierten Replizierungsgruppen zugewiesen werden. Außerdem können bestimmte Komponenten der virtuellen Maschine von der Replizierung ausgeschlossen werden.



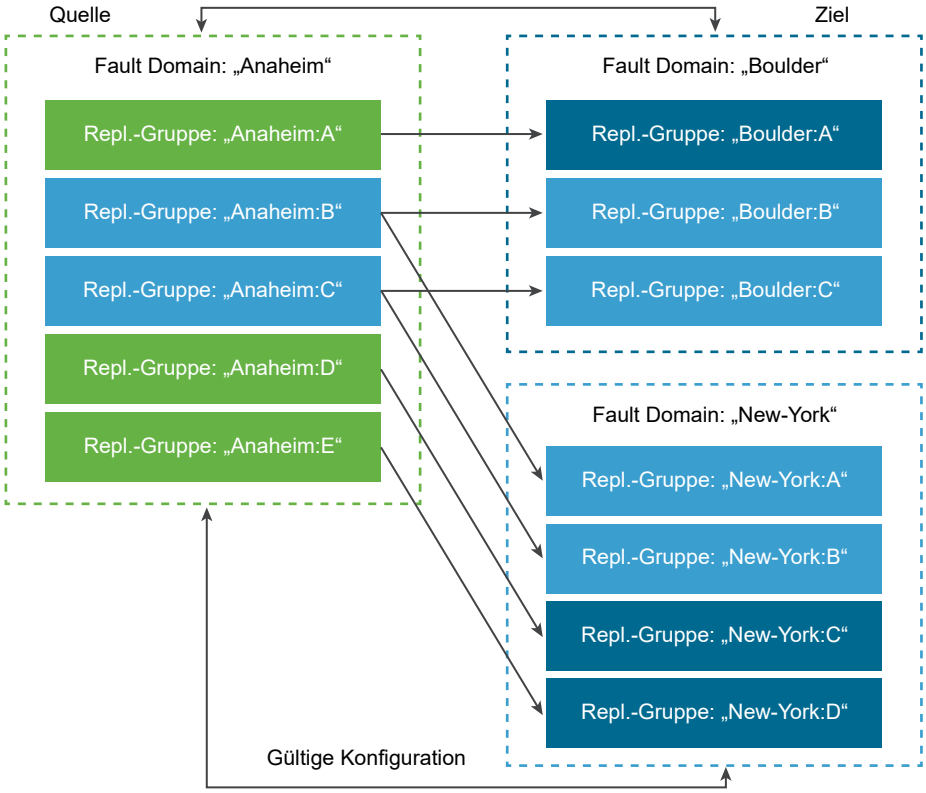
Wenn keine vorkonfigurierten Gruppen verfügbar sind, kann Virtual Volumes eine automatische Methode verwenden. Mit der automatischen Methode erstellt Virtual Volumes eine Replizierungsgruppe auf Anforderung und verknüpft diese mit einem Virtual Volumes-Objekt, das bereitgestellt wird. Bei Verwendung der automatischen Replizierungsgruppe werden alle Komponenten einer virtuellen Maschine der Gruppe zugewiesen. Vorkonfigurierte und automatische Replizierungsgruppen für Komponenten ein und derselben Maschine können nicht gemischt werden.

Virtual Volumes und Fault Domains

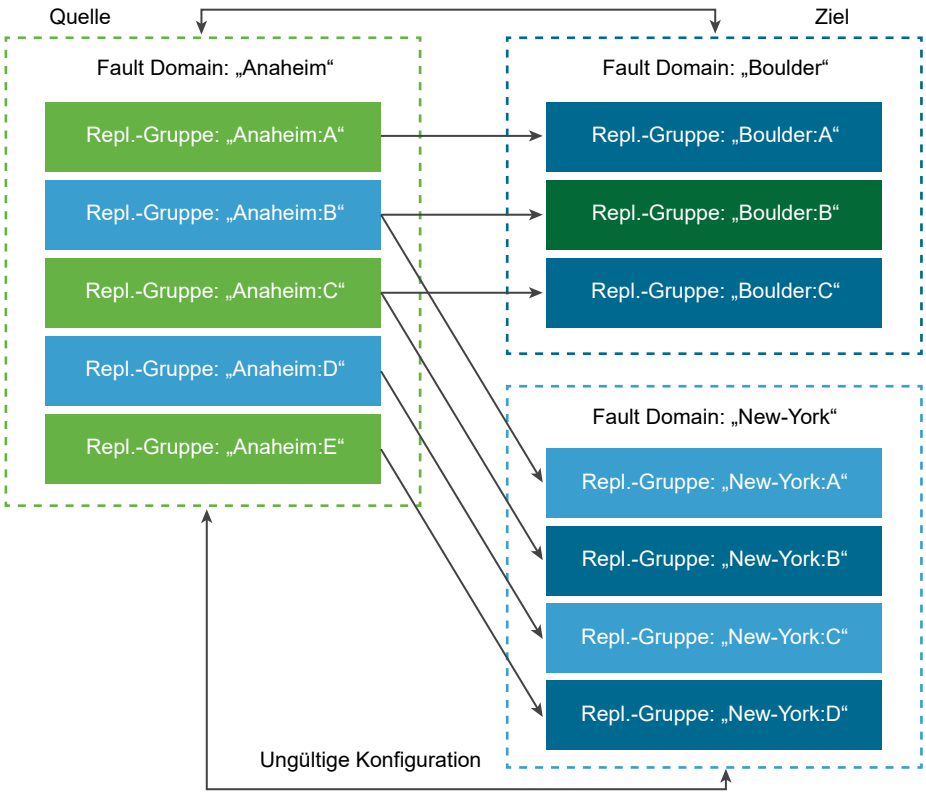
In der Virtual Volumes-Umgebung definieren Fault Domains, wie bestimmte Replizierungsgruppen kombiniert werden müssen, wenn sie von einer Quell- auf eine Zielsite repliziert werden.

Fault Domains werden vom Speicher-Array konfiguriert und gemeldet und sind nicht im vSphere Client verfügbar. Der SPBM-Mechanismus (speicherrichtlinienbasierte Verwaltung, Storage Policy Based Management) erkennt Fault Domains und verwendet sie zu Validierungszwecken während der Erstellung virtueller Maschinen.

Beispiel: Es wird eine virtuelle Maschine mit zwei Festplatten bereitgestellt, von denen die eine mit der Replizierungsgruppe Anaheim:B und die andere mit der Replizierungsgruppe Anaheim:C verknüpft ist. SPBM validiert die Bereitstellung, da beide Festplatten auf denselben Ziel-Fault Domains repliziert werden.



Nun wird eine virtuelle Maschine mit zwei Festplatten bereitgestellt, von denen die eine mit der Replizierungsgruppe Anaheim:B und die andere mit der Replizierungsgruppe Anaheim:D verknüpft ist. Diese Konfiguration ist ungültig. Beide Replizierungsgruppen werden auf die Fault Domain New York, jedoch wird nur eine auf die Fault Domain Boulder repliziert.



Virtual Volumes-Replizierungs-Workflow

Wenn in vCenter Server Informationen zu den Replizierungsfunktionen des Virtual Volumes-Speicher-Arrays angezeigt werden, können Sie die Replizierung für Ihre virtuellen Maschinen aktivieren.

Zum Workflow für das Aktivieren der Replizierung für Ihre virtuellen Maschinen gehören typische Schritte für die Bereitstellung von virtuellen Maschinen in einem Virtual Volumes-Speicher.

1 Definieren Sie die VM-Speicherrichtlinie, die mit dem Replizierungsspeicher kompatibel ist. Die datenspeicherbasierten Regeln der Richtlinie müssen die Replizierungskomponente umfassen. Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für Virtual Volumes.

   Nachdem Sie die Speicherrichtlinie, die die Replizierung enthält, konfiguriert haben, erkennt vCenter Server verfügbare Replizierungsgruppen.

2 Weisen Sie die Replizierungsrichtlinie Ihrer virtuellen Maschine zu. Wählen Sie eine kompatible Replizierungsgruppe aus, sofern eine solche konfiguriert ist, oder verwenden Sie die automatische Zuweisung. Weitere Informationen hierzu finden Sie unter Zuweisen von Speicherrichtlinien zu virtuellen Maschinen.

Richtlinien und Überlegungen zur Replizierung

Bei der Verwendung der Replizierung mit Virtual Volumes gelten spezielle Anforderungen.

- Die Replizierungs-Speicherrichtlinie kann nur auf ein virtuelles Konfigurations-Volume und ein virtuelles Daten-Volume angewendet werden. Andere Objekte der virtuellen Maschine übernehmen die Replizierungsrichtlinie auf die folgende Art und Weise:
  - Das virtuelle Speicher-Volume übernimmt die Richtlinie des virtuellen Konfigurations-Volumes.
  - Das virtuelle Digest-Volume übernimmt die Richtlinie des virtuellen Daten-Volumes.
  - Der virtuelle Auslagerungs-Volume, das nur besteht, während eine virtuelle Maschine eingeschaltet wird, wird von der Replizierung ausgeschlossen.
- Wenn Sie die Replizierungsrichtlinie nicht auf eine VM-Festplatte anwenden, wird die Festplatte nicht repliziert.
- Die Replizierungs-Speicherrichtlinie sollte nicht als Standard-Speicherrichtlinie für einen Datenspeicher verwendet werden. da Sie ansonsten keine Verifizierungsgruppen auswählen können.
- Bei der Replizierung bleibt der Snapshot-Verlauf erhalten. Wenn ein Snapshot erstellt und repliziert wurde, können Sie den anwendungskonsistenten Snapshot wiederherstellen.
- Verknüpfte Klone können repliziert werden. Wenn ein verknüpfter Klon ohne seinen übergeordneten Klon repliziert wird, wird er zu einem vollständigen Klon.
- Wenn eine Deskriptordatei zu einer virtuellen Festplatte einer virtuellen Maschine gehört, sich jedoch im VM Home einer anderen virtuellen Maschine befindet, müssen sich beide Maschinen in derselben Replizierungsgruppe befinden. Wenn sich die virtuellen Maschinen in unterschiedlichen Replizierungsgruppen befinden, muss an beiden Gruppen gleichzeitig ein Failover durchgeführt werden, da der Deskriptor andernfalls nach dem Failover möglicherweise nicht mehr verfügbar ist. Die virtuelle Maschine kann dann möglicherweise nicht mehr eingeschaltet werden.
- In Ihrer Virtual Volumes-Umgebung mit Replizierung sollten Sie in bestimmten Abständen einen Test-Failover-Workflow ausführen, um sicherzustellen, dass die wiederhergestellten Arbeitslasten nach einem Failover funktionsfähig sind.

  Die dabei erstellten Test-VMs sind voll funktionsfähig und für allgemeine administrative Vorgänge geeignet. Beachten Sie jedoch die folgenden Aspekte:
  - Alle während des Test-Failovers erstellten VMs müssen gelöscht werden, bevor das Test-Failover beendet wird. Durch das Löschen wird sichergestellt, dass Snapshots oder virtuelle Volumes im Zusammenhang mit Snapshots, die Bestandteil der VM sind (z. B. das virtuelle Volume für Snapshots), das Beenden des Test-Failovers nicht behindern.
  - Sie können vollständige Klone der Test-VMs erstellen.

- Schnelle Klone können nur erstellt werden, wenn die auf die neue VM angewendete Richtlinie dieselbe Replizierungsgruppen-ID wie die geklonte VM enthält. Versuche, die untergeordnete VM außerhalb der Replizierungsgruppe der übergeordneten VM zu platzieren, schlagen fehl.

Best Practices für die Arbeit mit Virtual Volumes

Beachten Sie bei der Verwendung von Virtual Volumes mit ESXi und vCenter Server die folgenden Empfehlungen.

- Richtlinien und Einschränkungen bei der Verwendung von Virtual Volumes

  Für eine optimale Erfahrung mit den Funktionen von Virtual Volumes müssen Sie bestimmte Richtlinien einhalten.

- Best Practices für die Bereitstellung von Speichercontainern

  Halten Sie sich bei der Bereitstellung von Speichercontainern auf dem Virtual Volumes-Array an die folgenden Best Practices.

- Best Practices für die Virtual Volumes-Leistung

  Halten Sie sich an die folgenden Empfehlungen, um eine optimale Leistung von Virtual Volumes sicherzustellen.

Richtlinien und Einschränkungen bei der Verwendung von Virtual Volumes

Für eine optimale Erfahrung mit den Funktionen von Virtual Volumes müssen Sie bestimmte Richtlinien einhalten.

Virtual Volumes unterstützt die folgenden Funktionen und VMware-Produkte:

- Mit Virtual Volumes können Sie erweiterte Speicherdienste wie Replikation, Verschlüsselung, Deduplizierung und Komprimierung auf einzelnen virtuellen Festplatten verwenden. Informationen zu den mit Virtual Volumes unterstützten Diensten erhalten Sie von Ihrem Speicheranbieter.
- Die Funktionen von Virtual Volumes unterstützen Sicherungssoftware, die vSphere APIs - Data Protection verwendet. Virtuelle Volumes werden auf virtuellen Festplatten modelliert. Sicherungsprodukte, die vSphere APIs - Data Protection verwenden, werden auf virtuellen Volumes ebenso unterstützt wie auf VMDK-Dateien in einer LUN. Snapshots, die die Sicherungssoftware mithilfe von vSphere APIs - Data Protection erstellt, werden in vSphere und der Sicherungssoftware wie Nicht-vVols-Snapshots behandelt.

  Hinweis Der SAN-Transportmodus wird von Virtual Volumes nicht unterstützt. vSphere APIs - Data Protection wählt automatisch eine alternative Datenübertragungsmethode aus.

  Weitere Informationen zur Integration mit vSphere Storage APIs - Data Protection erhalten Sie vom Hersteller Ihrer Sicherungssoftware.

- Virtual Volumes unterstützt vSphere-Funktionen wie vSphere vMotion, Storage vMotion, Snapshots, verknüpfte Klone und DRS.
- Sie können Clustering-Produkte wie beispielsweise Oracle Real Application Clusters mit Virtual Volumes verwenden. Hierzu aktivieren Sie die Multiwrite-Einstellung für eine im Virtual Volumes-Datenspeicher gespeicherte virtuelle Festplatte.

Weitere Informationen finden Sie im Knowledgebase-Artikel unter http://kb.vmware.com/kb/2112039. Eine Liste der von Virtual Volumes unterstützten Funktionen und Produkte finden Sie in der *VMware-Produkt-Interoperabilitätsmatrix*.

Einschränkungen von Virtual Volumes

Wenn Sie sich über die folgenden Einschränkungen bewusst sind, können Sie Ihre Erfahrung mit Virtual Volumes optimieren:

- Da für die Umgebung der Virtual Volumes vCenter Server erforderlich ist, können Sie Virtual Volumes nicht mit einem eigenständigen Host verwenden.
- Virtual Volumes-Funktionen unterstützen RDMs nicht.
- Ein Virtual Volumes-Speichercontainer kann nicht mehrere physische Arrays umfassen. Einige Anbieter stellen mehrere physische Arrays als einen einzigen Array dar. In diesen Fällen verwenden Sie technisch gesehen nach wie vor nur ein logisches Array.
- Hostprofile, die Virtual Volumes-Datenspeicher enthalten, sind vCenter Server-spezifisch. Nachdem Sie diesen Hostprofiltyp extrahiert haben, können Sie ihn nur an Hosts oder Cluster anbinden, die vom gleichen vCenter Server wie der Referenzhost verwaltet werden.

Best Practices für die Bereitstellung von Speichercontainern

Halten Sie sich bei der Bereitstellung von Speichercontainern auf dem Virtual Volumes-Array an die folgenden Best Practices.

Erstellen von Containern basierend auf Grenzwerten

Speichercontainer wenden beim Gruppieren von Virtual Volumes logische Grenzwerte an. Deshalb muss der Container mit den Grenzwerten übereinstimmen, die Sie anwenden möchten.

Beispiele hierfür sind ein Container, der für einen Mandanten in einer Bereitstellung mit mehreren Mandanten erstellt wird, bzw. ein Container für eine Abteilung in einer Unternehmensbereitstellung.

- Organisationen oder Abteilungen wie beispielsweise die Personalabteilung und die Finanzabteilung
- Gruppen oder Projekte wie beispielsweise „Team A“ und „Rotes Team“
- Kunden

Alle Speicherfunktionen in einem einzelnen Container

Speichercontainer sind einzelne Datenspeicher. Ein einzelner Speichercontainer kann mehrere Speicherfunktionsprofile exportieren. Deshalb können virtuelle Maschinen mit verschiedenen Anforderungen und verschiedenen Speicherrichtlinieneinstellungen Teil desselben Speichercontainers sein.

Die Änderung von Speicherprofilen muss auf der Array-Seite vorgenommen werden. Es handelt sich dabei nicht um eine Speichermigration auf einen anderen Container.

Vermeiden der übermäßigen Bereitstellung von Speichercontainern

Bei der Bereitstellung eines Speichercontainers sind die Speicherplatzgrenzwerte, die Sie im Rahmen der Containerkonfiguration anwenden, lediglich logische Grenzwerte. Stellen Sie den Container nicht größer als für den geplanten Zweck erforderlich bereit. Wenn Sie später den Container vergrößern, müssen Sie ihn nicht neu formatieren oder neu partitionieren.

Verwenden der speicherspezifischen Management-UI zum Bereitstellen von Protokollendpunkten

Jeder Speichercontainer benötigt Protokollendpunkte (PEs), auf die ESXi-Hosts zugreifen können.

Bei Verwendung des Blockspeichers stellt der PE eine Proxy-LUN dar, die durch einen T10-basierten LUN-WWN definiert wird. Für NFS-Speicher ist der PE ein Einhängepunkt, wie zum Beispiel eine IP-Adresse oder ein DNS-Name und ein Freigabename.

Die Konfiguration von PEs ist in der Regel Array-spezifisch. Bei der Konfiguration von PEs müssen Sie ihnen möglicherweise spezifische Speicherprozessoren oder bestimmte Hosts zuordnen. Sie sollten PEs nicht manuell konfigurieren, um Fehler zu vermeiden. Verwenden Sie stattdessen nach Möglichkeit speicherspezifische Verwaltungstools.

Keine Zuweisung von IDs höher als Disk.MaxLUN zu Protokollendpunkt-LUNs

Standardmäßig kann ein ESXi-Host auf LUN-IDs im Bereich 0 bis 1023 zugreifen. Wenn die ID der Protokollendpunkt-LUN, die Sie konfigurieren, größer als 1023 ist, wird der PE möglicherweise vom Host ignoriert.

Wenn in Ihrer Umgebung LUN-IDs verwendet werden, die größer als 1023 sind, ändern Sie die Anzahl der gescannten LUNs über den Parameter `Disk.MaxLUN`. Weitere Informationen hierzu finden Sie unter Ändern der Anzahl gescannter Speichergeräte.

Best Practices für die Virtual Volumes-Leistung

Halten Sie sich an die folgenden Empfehlungen, um eine optimale Leistung von Virtual Volumes sicherzustellen.

Verwenden unterschiedlicher VM-Speicherrichtlinien für einzelne Virtual Volume-Komponenten

Standardmäßig weisen alle Komponenten einer virtuellen Maschine in der Virtual Volumes-Umgebung eine einzelne VM-Speicherrichtlinie auf. Die Leistungsmerkmale unterschiedlicher Komponenten können jedoch variieren, beispielsweise eine virtuelle Festplatte für die Datenbank und eine entsprechende virtuelle Festplatte für das Protokoll. In Abhängigkeit von den Leistungsanforderungen können Sie einzelnen virtuellen Festplatten und der VM-Home-Datei oder config-VVol unterschiedliche VM-Speicherrichtlinien zuweisen.

Wenn Sie den vSphere Client verwenden, können Sie die zugewiesene VM-Speicherrichtlinie für swap-vVol, memory-vVol oder snapshot-vVol nicht ändern.

Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für Virtual Volumes.

Erstellen eines Hostprofils mit Virtual Volumes

Zum Erstellen eines Hostprofils mit Virtual Volumes wird empfohlen, einen Referenzhost zu konfigurieren und dessen Profil zu extrahieren. Wenn Sie ein vorhandenes Hostprofil im vSphere Client manuell bearbeiten und das bearbeitete Profil an den neuen Host anhängen, kann es zu Compliance-Fehlern und anderen unvorhersehbaren Problemen kommen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 2146394.

Überwachen der E/A-Last auf einem einzelnen Protokollendpunkt

- Die E/A-Abwicklung eines virtuellen Volumes erfolgt vollständig über Protokollendpunkte (PEs). Arrays wählen Protokollendpunkte aus mehreren PEs aus, auf die ein ESXi-Host Zugriff hat. Arrays können den Lastausgleich durchführen und den Bindungspfad ändern, der das virtuelle Volume und den PE miteinander verbindet. Weitere Informationen hierzu finden Sie unter Bindung und Aufheben der Bindung von virtuellen Volumes an Protokollendpunkte.
- Beim Blockspeicher verwendet ESXi aufgrund der potenziell hohen Anzahl von virtuellen Volumes einen hohen Warteschlangentiefewert für E/A. Der Parameter `Scsi.ScsiVVolPESNRO` kontrolliert die Anzahl der E/A-Instanzen, die für PEs zur Warteschlange hinzugefügt werden können. Diesen Parameter können Sie auf der Seite „Erweiterte Systemeinstellungen“ des vSphere Client konfigurieren.

Überwachen der Array-Grenzwerte

Eine einzelne VM kann mehrere virtuelle Volumes belegen. Weitere Informationen hierzu finden Sie unter Virtual Volume-Objekte.

Angenommen, Ihre VM weist zwei virtuelle Festplatten auf und Sie erstellen zwei Snapshots des Arbeitsspeichers. Ihre VM kann bis zu 10 Virtual Volumes-Objekte belegen: ein config-vVol, ein swap-vVol, zwei data-vVols, vier snapshot-vVols und zwei Arbeitsspeicher-snapshot-vVols.

Sicherstellen der Verfügbarkeit des Speicheranbieters

Für den Zugriff auf Virtual Volumes-Speicher benötigt Ihr ESXi-Host einen Speicheranbieter (VASA-Anbieter). Halten Sie sich an die folgenden Richtlinien, um sicherzustellen, dass der Speicheranbieter immer verfügbar ist:

- Migrieren Sie eine Speicheranbieter-VM nicht auf Virtual Volumes-Speicher.
- Sichern Sie Ihre Speicheranbieter-VM.
- Verwenden Sie im Bedarfsfall vSphere HA oder Site Recovery Manager für den Schutz der Speicheranbieter-VM.

Fehlerbehebung für Virtual Volumes

Die Fehlerbehebungsthemen bieten Lösungen für Probleme, die bei Verwendung von Virtual Volumes auftreten können.

- Virtual Volumes und esxcli-Befehle

  Die `esxcli storage vvol`-Befehle können Sie für die Fehlerbehebung Ihrer Virtual Volumes-Umgebung verwenden.
- Erfassen statistischer Informationen für Virtual Volumes

  Sie können den Befehl `vvol stats` in Ihrem ESXi-Host verwenden, um Leistungsstatistiken zu verfolgen.
- Auf den Virtual Volumes-Datenspeicher kann nicht zugegriffen werden

  Nachdem Sie einen Virtual Volumes-Datenspeicher erstellt haben, kann nicht darauf zugegriffen werden.
- Fehler beim Migrieren von virtuellen Maschinen oder beim Bereitstellen von VM-OVFs auf Virtual Volumes-Datenspeichern

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

Virtual Volumes und esxcli-Befehle

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

Die folgenden Befehlsoptionen sind verfügbar.

Tabelle 22-1. `esxcli storage vvol`-Befehle

Namespace	Befehlsoption	Beschreibung
`esxcli storage core device`	`list`	Protokollendpunkte identifizieren Der Ausgabeeintrag `Is VVOL PE: true` zeigt an, dass das Speichergerät ein Protokollendpunkt ist.
`esxcli storage vvol daemon`	`unbindall`	Hebt die Bindung für alle virtuellen Volumes aller VASA-Anbieter auf, die dem ESXi-Host bekannt sind.
`esxcli storage vvol protocolendpoint`	`list`	Listet alle Protokollendpunkte auf, auf die Ihr Host zugreifen kann.
`esxcli storage vvol storagecontainer`	`list` `abandonedvvol scan`	Listet alle verfügbaren Speichercontainer auf. Durchsucht den angegebenen Speichercontainer auf aufgegebene virtuelle Volumes.
`esxcli storage vvol vasacontext`	`get`	Zeigt den VASA-Kontext (VC-UUID), der mit dem Host verbunden ist, an.
`esxcli storage vvol vasaprovider`	`list`	Listet alle mit dem Host verbundenen Speicher-Anbieter (VASA) auf.

Erfassen statistischer Informationen für Virtual Volumes

Sie können den Befehl `vvol stats` in Ihrem ESXi-Host verwenden, um Leistungsstatistiken zu verfolgen.

Die folgenden Befehlsoptionen sind verfügbar.

Befehl	Beschreibung	Optionen
`esxcli storage vvol stats get`	Statistiken für alle VASA-Anbieter (Standard) oder für den angegebenen Namespace oder die angegebene Entität im angegebenen Namespace abrufen.	`-e|--entity= str` Geben Sie die Einheits-ID ein. `-n|--namespace= str` Geben Sie den Ausdruck für den Knoten-Namespace ein. `-r|--raw` Ausgabe des Raw-Formats aktivieren.
`esxcli storage vvol stats list`	Listet alle Statistikknoten (Standard) oder Knoten unter einem angegebenen Namespace auf.	`-n|--namespace= str` Geben Sie den Ausdruck für den Knoten-Namespace ein.

Befehl	Beschreibung	Optionen
`esxcli storage vvol stats enable`	Aktivieren Sie die Statistiknachverfolgung für den kompletten Namespace.	
`esxcli storage vvol stats disable`	Deaktivieren Sie die Statistiknachverfolgung für den kompletten Namespace.	
`esxcli storage vvol stats add`	Aktivieren Sie die Statistiknachverfolgung für eine bestimmte Einheit unter einem bestimmten Namespace.	`-e|--entity= str` Geben Sie die Einheits-ID ein. `-n|--namespace= str` Geben Sie den Ausdruck für den Knoten-Namespace ein.
`esxcli storage vvol stats remove`	Entfernt eine bestimmte Einheit für die Statistiknachverfolgung unter dem angegebenen Namespace.	`-e|--entity= str` Geben Sie die Einheits-ID ein. `-n|--namespace= str` Geben Sie den Ausdruck für den Knoten-Namespace ein.
`esxcli storage vvol stats reset`	Setzen Sie den Statistikzähler für den angegebenen Statistik-Namespace oder das angegebene Element zurück.	`-e|--entity= str` Geben Sie die Einheits-ID ein. `-n|--namespace= str` Geben Sie den Ausdruck für den Knoten-Namespace ein.

Auf den Virtual Volumes-Datenspeicher kann nicht zugegriffen werden

Nachdem Sie einen Virtual Volumes-Datenspeicher erstellt haben, kann nicht darauf zugegriffen werden.

Problem

Der vSphere Client zeigt den Datenspeicher als nicht zugänglich an. 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 Virtual Volumes-Datenspeichern

Versuche, eine virtuelle Maschine zu migrieren oder VM-OVF in virtuellen Virtual Volumes-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-Volume den Grenzwert von 4 GB überschreitet, schlägt die Migration oder die Bereitstellung in einem virtuellen Datenspeicher fehl.

Ursache

Das virtuelle Konfigurations-Volume bzw. config-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 config-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.

Config-vVols werden als virtuelle 4-GB-Volumes erstellt. Der allgemeine Inhalt des config-vVol belegt gewöhnlich nur einen Bruchteil der reservierten 4 GB, weshalb config-vVols in der Regel per Thin Provisioning 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 config-vVol den Grenzwert von 4 GB überschreitet. Falls solche Dateien in einer OVF-Vorlage enthalten sind, schlägt die Bereitstellung von VM-OVF in Virtual Volumes-Speicher fehl. Falls diese Dateien Bestandteil einer vorhandenen virtuellen Maschine sind, schlägt die Migration dieser virtuellen Maschine von einem traditionellen Datenspeicher zu 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 config-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 Virtual Volumes-Speicher.

Filtern der E/A einer virtuellen Maschine

23

E/A-Filter sind Softwarekomponenten, die auf ESXi-Hosts installiert werden und zusätzliche Datendienste für virtuelle Maschinen anbieten können. Die Filter verarbeiten E/A-Anforderungen, die zwischen dem Gastbetriebssystem einer virtuellen Maschine und virtuellen Festplatten verschoben werden.

Die E/A-Filter können von VMware angeboten oder von Drittanbietern über vSphere APIs for I/O Filtering (VAIO) erstellt werden.

Dieses Kapitel enthält die folgenden Themen:

Grundlegendes zu E/A-Filtern

E/A-Filter können direkten Zugriff auf den E/A-Pfad der virtuellen Maschine erhalten. Sie können den E/A-Filter für eine einzelne Ebene einer virtuellen Festplatte aktivieren. Die E/A-Filter sind unabhängig von der Speichertopologie.

VMware bietet bestimmte Kategorien von E/A-Filtern an. Außerdem können die E/A-Filter von Drittanbietern erstellt werden. Normalerweise werden sie als Pakete verteilt, die ein Installationsprogramm beinhalten, um die Filterkomponenten in Hostclustern von vCenter Server und ESXi bereitzustellen.

Nachdem die E/A-Filter bereitgestellt wurden, konfiguriert und registriert vCenter Server automatisch einen E/A-Filter-Speicheranbieter – auch als VASA-Anbieter bezeichnet – für jeden Host im Cluster. Die Speicheranbieter kommunizieren mit vCenter Server und vom E/A-Filter angebotene Datendienste werden in der Schnittstelle für VM-Speicherrichtlinien angezeigt. Beim Festlegen gemeinsamer Regeln für eine VM-Richtlinie können Sie auf diese Datendienste zurückgreifen. Nachdem Sie diese Richtlinie virtuellen Festplatten zugeordnet haben, werden die E/A-Filter auf den virtuellen Festplatten aktiviert.

Unterstützung von Datenspeichern

E/A-Filter unterstützen alle Arten von Datenspeichern, einschließlich der folgenden:

- VMFS
- NFS 3
- NFS 4.1
- vVol
- vSAN

E/A-Filtertypen

VMware stellt verschiedene Kategorien von E/A-Filtern zur Verfügung, die auf Ihren ESXi-Hosts installiert werden. Darüber hinaus können VMware-Partner die E/A-Filter über das vSphere APIs für E/A-Filter (VAIO)-Entwicklerprogramm erstellen. Die E/A-Filter können für verschiedene Zwecke verwendet werden.

Es werden u. a. die folgenden Filtertypen unterstützt:

- Replizierung. Repliziert alle E/A-Schreibvorgänge in einem externen Zielspeicherort, wie beispielsweise auf einem anderen Host oder Cluster.
- Verschlüsselung. Angeboten von VMware. Stellt Verschlüsselungsmechanismen für virtuelle Maschinen zur Verfügung. Weitere Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.
- Zwischenspeicherung. Implementiert einen Cache für virtuelle Festplattendaten. Der Filter kann mit einem lokalen Flash-Speichergerät die Daten zwischenspeichern und die E/A-Vorgänge pro Sekunde (IOPS) und die Hardwarenutzungsraten für die virtuelle Festplatte erhöhen. Bei Verwendung des Cache-Filters müssen Sie möglicherweise eine vFlash-Ressource konfigurieren.

- Storage I/O Control. Angeboten von VMware. Drosselt die E/A-Last zu einem Datenspeicher und steuert die Menge an Speicher-E/A, die virtuellen Maschinen in Zeiträumen von E/A-Überlastung zugeteilt wird. Weitere Informationen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Hinweis Sie können mehrere Filter aus derselben Kategorie (z. B. „Zwischenspeicherung“) auf Ihrem ESXi-Host installieren. Pro virtueller Festplatte ist jedoch nur ein Filter aus derselben Kategorie möglich.

E/A-Filterkomponenten

Mehrere Komponenten sind an der E/A-Filterung beteiligt.

Es gibt die folgenden grundlegenden E/A-Filterkomponenten:

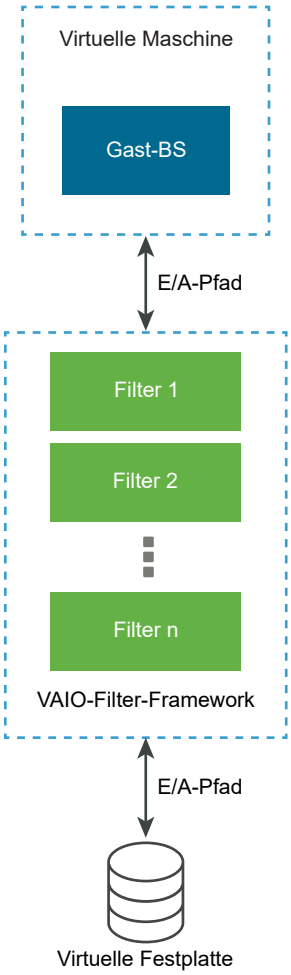
VAIO-Filter-Framework

Eine von ESXi bereitgestellte Kombination aus Benutzer-World und VMkernel-Infrastruktur. Mit dem Framework können Sie die Filter-Plug-ins zum E/A-Pfad zu und von virtuellen Festplatten hinzufügen. Die Infrastruktur umfasst einen E/A-Filter-Speicheranbieter (VASA-Anbieter). Der Anbieter wird mit dem speicherrichtlinienbasierten Verwaltungssystem (Storage Policy Based Management, SPBM) vernetzt und exportiert Filterfunktionen in vCenter Server.

E/A-Filter-Plug-In

Eine von VMware bereitgestellte oder von VMware-Partnern entwickelte Softwarekomponente, die E/A-Daten, die zwischen virtuellen Festplatten und Gastbetriebssystemen übertragen werden, abfängt und filtert. Wenn der E/A-Filter von VMware-Partnern entwickelt wird, enthält er möglicherweise zusätzliche optionale Komponenten, die seine Konfiguration und Verwaltung vereinfachen.

Die folgende Abbildung veranschaulicht die Komponenten der E/A-Filterung und den E/A-Workflow zwischen dem Gastbetriebssystem und der virtuellen Festplatte.



Jede VMX-Komponente (Virtual Machine Executable) einer virtuellen Maschine enthält ein Filter-Framework zur Verwaltung der mit der virtuellen Festplatte verbundenen E/A-Filter-Plug-Ins. Das Filter-Framework ruft Filter auf, wenn die E/A-Anforderungen zwischen dem Gastbetriebssystem und der virtuellen Festplatte übertragen werden. Darüber hinaus fängt der Filter jeden E/A-Zugriff auf die virtuelle Festplatte ab, der außerhalb einer ausgeführten virtuellen Maschine erfolgt.

Die Filter werden nacheinander in der angegebenen Reihenfolge ausgeführt. Beispielsweise wird ein Replizierungsfilter vor einem Cache-Filter ausgeführt. Auf der virtuellen Festplatte können mehrere Filter eingesetzt werden, aber pro Kategorie ist nur ein Filter möglich.

Nachdem alle Filter für die betreffende Festplatte die E/A-Anforderung überprüft haben, wird die Anforderung an ihr Ziel übertragen, also entweder an die virtuelle Maschine oder die virtuelle Festplatte.

Da die Filter im Benutzerspeicherplatz ausgeführt werden, betreffen etwaige Filterfehler nur die virtuelle Maschine, jedoch nicht den ESXi-Host.

Speicheranbieter für E/A-Filter

Wenn E/A-Filter auf ESXi-Hosts installiert wurden, konfiguriert und registriert das E/A-Filter-Framework einen auch als VASA-Anbieter bezeichneten Speicheranbieter für jeden Host im Cluster.

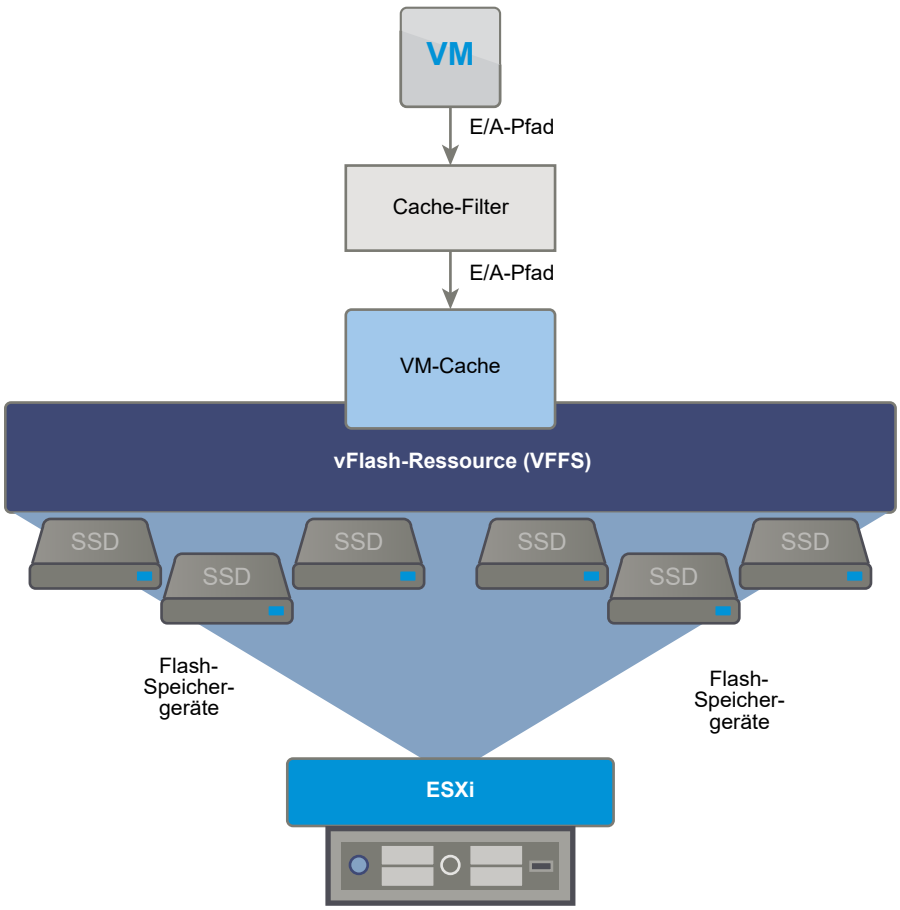
Speicheranbieter für die E/A-Filterung sind von vSphere angebotene Softwarekomponenten. Sie werden mit E/A-Filtern und Bericht-Datendienstfunktionen, die von E/A-Filtern unterstützt werden, in vCenter Server integriert.

Die Schnittstelle für VM-Speicherrichtlinien wird durch die Funktionen aufgefüllt, und in einer VM-Speicherrichtlinie kann darauf verwiesen werden. Anschließend können Sie diese Richtlinie auf virtuelle Festplatten anwenden, sodass die E/A-Filter E/A-Vorgänge für die Festplatten verarbeiten können.

Verwenden von Flash-Speichergeräten mit Cache-E/A-Filtern

Ein Cache-E/A-Filter kann ein lokales Flash-Gerät zum Zwischenspeichern von Daten virtueller Maschinen verwenden.

Wenn Ihr Cache-E/A-Filter lokale Flash-Geräte verwendet, müssen Sie eine virtuelle Flash-Ressource bzw. vFlash-Ressource, die auch als VFFS-Volume bezeichnet wird, konfigurieren. Konfigurieren Sie die Ressource auf Ihrem ESXi-Host, bevor Sie den Filter aktivieren. Bei der Verarbeitung der E/A-Lesevorgänge der virtuellen Maschine erstellt der Filter einen VM-Cache und platziert ihn auf dem VFFS-Volume.



Zum Einrichten einer vFlash-Ressource verwenden Sie Flash-Geräte, die mit dem Host verbunden sind. Wenn Sie die Kapazität der vFlash-Ressource erhöhen möchten, können Sie weitere Flash-Geräte hinzufügen. Ein einzelnes Flash-Laufwerk muss einer vFlash-Ressource exklusiv zugeteilt werden und kann nicht gemeinsam mit einem anderen vSphere-Dienst (z. B. vSAN oder VMFS) genutzt werden. Weitere Informationen finden Sie unter Einrichten der vFlash-Ressource.

Systemanforderungen für E/A-Filter

Um E/A-Filter in Ihrer Umgebung nutzen zu können, müssen bestimmte Anforderungen erfüllt werden.

Die folgenden Anforderungen müssen erfüllt werden.

- Verwenden Sie die neueste Version von ESXi und vCenter Server, die mit E/A-Filtern kompatibel ist. Ältere Versionen unterstützen möglicherweise keine E/A-Filter oder bieten nur teilweise Unterstützung.
- Prüfen Sie, ob für einzelne Partnerlösungen möglicherweise weitere Anforderungen bestehen. In bestimmten Fällen sind in Ihrer Umgebung möglicherweise Flash-Geräte, zusätzlicher physischer Arbeitsspeicher oder zusätzliche Netzwerkkonnektivität und Bandbreite erforderlich. Weitere Informationen erhalten Sie von Ihrem Anbieter oder Ihrem VMware-Repräsentanten.

- Webserver zum Hosten von Partnerpaketen für die Filterinstallation. Der Server muss nach der Erstinstallation verfügbar bleiben. Wenn ein neuer Host dem Cluster hinzugefügt wird, verschiebt der Server die entsprechenden E/A-Filterkomponenten auf den Host.

Konfigurieren von E/A-Filtern in der vSphere-Umgebung

Führen Sie die folgenden Schritte aus, um Datendienste einzurichten, die die E/A-Filter für Ihre virtuellen Maschinen bereitstellen.

Voraussetzungen

- Erstellen Sie einen Cluster, der mindestens einen ESXi-Host enthält.
- Weitere Informationen zu von Drittanbietern bereitgestellten E/A-Filtern erhalten Sie von Ihrem Anbieter oder Ihrem Ansprechpartner bei VMware.

Verfahren

1 Installieren von E/A-Filtern in einem Cluster

   Wenn Sie von Drittanbietern zur Verfügung gestellte E/A-Filter verwenden, installieren Sie die E/A-Filter in einem ESXi-Host-Cluster.

2 Anzeigen von E/A-Filtern und Speicheranbietern

   Verwenden Sie den vSphere Client, um die in Ihrer Umgebung verfügbaren E/A-Filter zu überprüfen und sicherzustellen, dass die Anbieter von E/A-Filtern erwartungsgemäß angezeigt werden und aktiv sind.

Installieren von E/A-Filtern in einem Cluster

Wenn Sie von Drittanbietern zur Verfügung gestellte E/A-Filter verwenden, installieren Sie die E/A-Filter in einem ESXi-Host-Cluster.

VMware-Partner können E/A-Filter über das vSphere APIs für E/A-Filter (VAIO)-Entwicklerprogramm erstellen.

Die Filterpakete werden als Lösungs-ZIP-Pakete verteilt, die E/A-Filter-Daemon, E/A-Filterbibliotheken, CIM-Anbieter und andere zugehörige Komponenten enthalten können.

Zum Bereitstellen der Filter führen Sie üblicherweise das von den Anbietern zur Verfügung gestellte Installationsprogramm aus. Die Installation wird auf ESXi-Cluster-Ebene durchgeführt. Die Filter können nicht direkt auf bestimmten Hosts installiert werden.

Hinweis Wenn Sie E/A-Filter auf einem Cluster mit vSphere 7.0 und höher installieren, kann dieser Cluster keine ESXi 6.x-Hosts enthalten. Mithilfe des vSphere 6.x VAIO-Programms erstellte Filter können auf ESXi-Hosts der Version 7.0 und höher nicht ausgeführt werden, da der CIM-Anbieter 32 Bit auf ESXi 6.x und 64 Bit auf ESXi 7.0 und höher aufweist. Im Gegenzug werden Filter, die mit dem VAIO-Programm in vSphere 7.0 und höher erstellt wurden, auf ESXi 6.x-Hosts nicht unterstützt.

Voraussetzungen

- Erforderliche Rechte: **Host.Configuration.Query-Patch**.
- Stellen Sie sicher, dass die E/A-Filterlösung von VMware zertifiziert ist.

Verfahren

- Führen Sie das vom Anbieter bereitgestellte Installationsprogramm aus.

  Das Installationsprogramm stellt die entsprechende E/A-Filtererweiterung für vCenter Server und die Filterkomponenten auf allen Hosts in einem Cluster bereit.

  Ein Speicheranbieter (auch als VASA-Anbieter bezeichnet) wird automatisch für jeden ESXi-Host im Cluster registriert. Die erfolgreiche automatische Registrierung der E/A-Filter-Speicheranbieter löst ein Ereignis auf der Hostebene aus. Falls die Speicheranbieter nicht automatisch registriert werden können, löst das System einen Alarm auf den Hosts aus.

Anzeigen von E/A-Filtern und Speicheranbietern

Verwenden Sie den vSphere Client, um die in Ihrer Umgebung verfügbaren E/A-Filter zu überprüfen und sicherzustellen, dass die Anbieter von E/A-Filtern erwartungsgemäß angezeigt werden und aktiv sind.

Wenn Sie einen E/A-Filter eines Drittanbieters installieren, wird ein auch als VASA-Anbieter bezeichneter Speicheranbieter automatisch für jeden ESXi-Host im Cluster registriert. Die erfolgreiche automatische Registrierung der E/A-Filter-Speicheranbieter löst ein Ereignis auf der Hostebene aus. Falls die Speicheranbieter nicht automatisch registriert werden können, löst das System einen Alarm auf den Hosts aus.

Verfahren

1. Überprüfen Sie, ob die E/A-Filter-Speicheranbieter erwartungsgemäß angezeigt werden und aktiv sind.
   a. Navigieren Sie zu vCenter Server.
   b. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.
   c. Prüfen Sie die Speicheranbieter für E/A-Filter.

   Wenn die Anbieter der E/A-Filter ordnungsgemäß registriert wurden, wird die Schnittstelle für VM-Speicherrichtlinien mit den Funktionen und Datendiensten der Filter aufgefüllt.

2 Überprüfen Sie, ob die E/A-Filterkomponenten in Ihrem Cluster und auf den ESXi-Hosts aufgelistet sind.

Option	Aktionen
E/A-Filter in einem Cluster anzeigen	a Navigieren Sie zum Cluster. b Klicken Sie auf die Registerkarte **Konfigurieren**. c Klicken Sie unter **Konfiguration** auf **E/A-Filter**, um die im Cluster installierten Filter zu überprüfen.
E/A-Filter auf einem Host anzeigen	a Navigieren Sie zum Host. b Klicken Sie auf die Registerkarte **Konfigurieren**. c Klicken Sie unter **Speicher** auf **E/A-Filter**, um die auf dem Host installierten Filter zu überprüfen.

Aktivieren von E/A-Filter-Datendiensten auf virtuellen Festplatten

Die Aktivierung der von E/A-Filtern bereitgestellten Datendienste erfolgt in zwei Schritten: Sie erstellen eine Richtlinie für virtuelle Maschinen basierend auf den von E/A-Filtern bereitgestellten Datendiensten und fügen dann diese Richtlinie einer virtuellen Maschine hinzu.

Voraussetzungen

Für die Cache-E/A-Filter konfigurieren Sie die vFlash-Ressource auf Ihrem ESXi-Host, bevor Sie den Filter aktivieren. Weitere Informationen hierzu finden Sie unter Einrichten der vFlash-Ressource.

Verfahren

1 Definieren Sie eine VM-Richtlinie basierend auf E/A-Filterdiensten.

Vergewissern Sie sich, dass die Richtlinie für die virtuelle Maschine die von den E/A-Filtern bereitgestellten Datendienste auflistet.

Weitere Informationen hierzu finden Sie unter Erstellen einer VM-Speicherrichtlinie für hostbasierte Datendienste.

2 Weisen Sie die E/A-Filterrichtlinie einer virtuellen Maschine zu.

Zum Aktivieren der von E/A-Filtern bereitgestellten Datendienste ordnen Sie die E/A-Filterrichtlinien virtuellen Festplatten zu. Sie können die Richtlinie beim Bereitstellen der virtuellen Maschine zuweisen.

Weitere Informationen hierzu finden Sie unter Zuweisen der E/A-Filterrichtlinie zu virtuellen Maschinen.

Nächste Schritte

Falls Sie den E/A-Filter für eine virtuelle Maschine zu einem späteren Zeitpunkt deaktivieren möchten, können Sie die Filterregeln von der VM-Speicherrichtlinie entfernen und die Richtlinie erneut anwenden. Weitere Informationen hierzu finden Sie unter Bearbeiten oder Klonen einer VM-Speicherrichtlinie. Sie können die Einstellungen der virtuellen Maschine auch bearbeiten und eine andere Speicherrichtlinie auswählen, die den Filter nicht enthält.

Zuweisen der E/A-Filterrichtlinie zu virtuellen Maschinen

Zum Aktivieren der von E/A-Filtern bereitgestellten Datendienste ordnen Sie die E/A-Filterrichtlinien virtuellen Festplatten zu. Die Richtlinie können Sie beim Erstellen oder Bearbeiten einer virtuellen Maschine zuweisen.

Die E/A-Filterrichtlinie kann bei der anfänglichen Bereitstellung einer virtuellen Maschine zugewiesen werden. In diesem Thema wird beschrieben, wie Sie die Richtlinie beim Erstellen einer neuen virtuellen Maschine zuweisen. Informationen zu anderen Bereitstellungsmethoden finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Hinweis Die E/A-Filterrichtlinie kann beim Migrieren oder Klonen einer virtuellen Maschine nicht geändert oder zugewiesen werden.

Voraussetzungen

Stellen Sie sicher, dass der E/A-Filter auf dem ESXi-Host installiert ist, auf dem die virtuelle Maschine ausgeführt wird.

Verfahren

1. Starten Sie den Vorgang zur Bereitstellung von virtuellen Maschinen und befolgen Sie die entsprechenden Schritte.
2. Weisen Sie allen VM-Dateien und Festplatten dieselbe Speicherrichtlinie zu.
   a. Wählen Sie auf der Seite **Speicher auswählen** eine Speicherrichtlinie im Dropdown-Menü **VM-Speicherrichtlinie** aus.
   b. Wählen Sie in der Liste der kompatiblen Datenspeicher den gewünschten Datenspeicher aus und klicken Sie auf **Weiter**.

      Der Datenspeicher wird zum Zielspeicherelement für die VM-Konfigurationsdatei und alle virtuellen Festplatten. Diese Richtlinie aktiviert auch E/A-Filterdienste für die virtuellen Festplatten.

3 Ändern Sie die VM-Speicherrichtlinie für den virtuellen Datenträger.

Verwenden Sie diese Option, um E/A-Filter nur für Ihre virtuellen Festplatten zu aktivieren.

a Erweitern Sie auf der Seite **Hardware anpassen** den Bereich **Neue Festplatte**.

b Wählen Sie im Dropdown-Menü **VM-Speicherrichtlinie** die der virtuellen Festplatte zuzuweisende Speicherrichtlinie aus.

c (Optional) Ändern Sie den Speicherort der virtuellen Festplatte.

Verwenden Sie diese Option zum Speichern des virtuellen Datenträgers auf einem anderen Datenspeicher als demjenigen, auf dem sich die VM-Konfigurationsdatei befindet.

4 Schließen Sie die Bereitstellung der virtuellen Maschine ab.

Ergebnisse

Nach der Erstellung der virtuellen Maschine zeigt die Registerkarte **Übersicht** die zugewiesenen Speicherrichtlinien und deren Übereinstimmungsstatus an.

Nächste Schritte

Die Zuweisung der VM-Richtlinie kann später geändert werden. Weitere Informationen hierzu finden Sie unter Ändern der Speicherrichtlinienzuweisung für VM-Dateien und -Festplatten.

Verwalten von E/A-Filtern

Sie können das von Ihrem Anbieter bereitgestellte Installationsprogramm ausführen, um E/A-Filter zu installieren, deinstallieren oder aktualisieren.

Bei Verwendung von E/A-Filtern sollten Sie Folgendes beachten:

- vCenter Server verwendet ESX Agent Manager (EAM) zum Installieren und Deinstallieren von E/A-Filtern. Rufen Sie als Administrator niemals EAM-APIs direkt für EAM-Agencys auf, die von vCenter Server erstellt oder verwendet werden. Alle Vorgänge im Zusammenhang mit E/A-Filtern müssen über VIM-APIs durchgeführt werden. Falls Sie versehentlich eine von vCenter Server erstellte EAM-Agency ändern, müssen Sie die Änderungen rückgängig machen. Falls Sie versehentlich eine von E/A-Filtern verwendete EAM-Agency löschen, müssen Sie `Vim.IoFilterManager#uninstallIoFilter` aufrufen, um die betroffenen E/A-Filter zu deinstallieren. Führen Sie nach der Deinstallation eine Neuinstallation durch.
- Wenn ein neuer Host einem Cluster beitritt, der E/A-Filter aufweist, werden die auf dem Cluster installierten Filter auf dem Host bereitgestellt. vCenter Server registriert den E/A-Filter-Speicheranbieter für den Host. Clusteränderungen werden in der Schnittstelle für VM-Speicherrichtlinien des vSphere Client angezeigt.
- Wenn Sie einen Host aus einem Cluster verschieben oder aus vCenter Server entfernen, werden die E/A-Filter auf dem Host deinstalliert. Die Registrierung des E/A-Filter-Speicheranbieters wird in vCenter Server aufgehoben.

- Wenn Sie einen statusfreien ESXi-Host verwenden, gehen möglicherweise während eines Neustarts dessen E/A-Filter-VIBs verloren. vCenter Server überprüft die auf dem Host installierten Pakete nach dem Neustart und verschiebt die E/A-Filter-VIBs ggf. auf den Host.

Deinstallieren von E/A-Filtern in einem Cluster

In einem ESXi-Hostcluster bereitgestellte E/A-Filter können deinstalliert werden.

Voraussetzungen

- Erforderliche Rechte: **Host.Config.Patch**.

Verfahren

1. Deinstallieren Sie den E/A-Filter durch Ausführen des Installationsprogramms Ihres Anbieters.

   Während der Deinstallation versetzt das Installationsprogramm für E/A-Filter eines Drittanbieters die Hosts automatisch in den Wartungsmodus.

   Falls die Deinstallation erfolgreich ist, werden der Filter und alle zugehörigen Komponenten von den Hosts entfernt.
2. Stellen Sie sicher, dass die E/A-Filterkomponenten auf Ihren ESXi-Hosts ordnungsgemäß deinstalliert wurden. Verwenden Sie eine der folgenden Methoden:
   - Führen Sie den Befehl `esxcli software vib list` aus.
   - Zeigen Sie die E/A-Filter im vSphere Client an. Weitere Informationen hierzu finden Sie unter Anzeigen von E/A-Filtern und Speicheranbietern.

   Der deinstallierte Filter wird nicht mehr aufgeführt.

Aktualisieren von E/A-Filtern in einem Cluster

Nach dem Upgrade Ihrer ESXi-Hosts auf Version 7.0 und höher verwenden Sie Installationsprogramme, die von E/A-Filteranbietern zur Verfügung gestellt werden, um die im ESXi-Hostcluster bereitgestellten E/A-Filter zu aktualisieren.

Wenn Sie ein Upgrade eines ESXi 6.x-Hosts mit benutzerdefinierten E/A-Filter-VIBs auf Version 7.0 vornehmen, werden alle unterstützten benutzerdefinierten VIBs migriert. Die älteren E/A-Filter funktionieren jedoch auf ESXi 7.0 und höher nicht. Die Filter enthalten in der Regel 32-Bit-CIM-Anbieter, während ESXi 7.0 und höher 64-Bit-CIM-Anwendungen benötigt. Sie müssen die alten Filter aktualisieren, um sie kompatibel zu machen.

Ein Upgrade besteht aus dem Deinstallieren der alten Filterkomponenten und dem Ersetzen durch die neuen Filterkomponenten. Um festzustellen, ob es sich bei einer Installation um ein Upgrade handelt, prüft vCenter Server die Namen und Versionen vorhandener Filter. Falls die Namen der vorhandenen Filter mit den Namen der neuen Filter übereinstimmen, aber unterschiedliche Versionen aufweisen, gilt die Installation als Upgrade.

Voraussetzungen

- Erforderliche Rechte: **Host.Config.Patch**.

- Führen Sie ein Upgrade der Hosts auf ESXi 7.0 und höher durch. Wenn Sie vSphere Lifecycle Manager für das Upgrade verwenden, finden Sie weitere Informationen dazu in der *Verwalten des Lebenszyklus von Host und Cluster*.-Dokumentation.

Verfahren

1 Führen Sie zum Aktualisieren des Filters das vom Anbieter zur Verfügung gestellte Installationsprogramm aus.

   Während des Upgrades versetzt das Installationsprogramm für E/A-Filter eines Drittanbieters die Hosts automatisch in den Wartungsmodus.

   Das Installationsprogramm identifiziert vorhandene Filterkomponenten und entfernt sie vor der Installation der neuen Filterkomponenten.

2 Stellen Sie sicher, dass die E/A-Filterkomponenten auf Ihren ESXi-Hosts ordnungsgemäß aktualisiert wurden. Verwenden Sie eine der folgenden Methoden:

   - Führen Sie den Befehl `esxcli software vib list` aus.
   - Zeigen Sie die E/A-Filter im vSphere Client an. Weitere Informationen hierzu finden Sie unter Anzeigen von E/A-Filtern und Speicheranbietern.

Ergebnisse

Nach dem Upgrade versetzt das System die Hosts wieder in den Betriebsmodus.

Richtlinien und empfohlene Vorgehensweisen für E/A-Filter

Halten Sie sich bei der Verwendung von E/A-Filtern in Ihrer Umgebung an spezielle Richtlinien und empfohlene Vorgehensweisen.

- Da E/A-Filter datenspeicherunabhängig sind, sind alle Arten von Datenspeichern, einschließlich VMFS, NFS, Virtual Volumes und vSAN, mit E/A-Filtern kompatibel.
- E/A-Filter unterstützen RDMs im virtuellen Kompatibilitätsmodus. RDMs im physischen Kompatibilitätsmodus werden von E/A-Filtern nicht unterstützt.
- Die E/A-Filterrichtlinie kann beim Migrieren oder Klonen einer virtuellen Maschine nicht geändert oder zugewiesen werden. Sie können die Richtlinie nach Abschluss des Migrations- oder Klonvorgangs ändern.
- Wenn Sie eine virtuelle Maschine mit einer E/A-Filterrichtlinie von einem Host zu einem anderen klonen oder migrieren, muss für den Zielhost ein kompatibler Filter installiert sein. Diese Anforderung gilt für Migrationen, die von einem Administrator oder mit Funktionen wie HA oder DRS gestartet werden.
- Wenn Sie eine Vorlage in eine virtuelle Maschine konvertieren und für die Vorlage eine E/A-Filterrichtlinie konfiguriert ist, muss für den Zielhost der kompatible E/A-Filter installiert sein.

- Wenn Sie mit vCenter Site Recovery Manager virtuelle Festplatten replizieren, weisen die daraus resultierenden Festplatten auf der Wiederherstellungs-Site keine E/A-Filterrichtlinien auf. Sie müssen die E/A-Filterrichtlinien für die Wiederherstellungs-Site erstellen und erneut zu den replizierten Festplatten hinzufügen.
- Falls der virtuellen Maschine eine Snapshot-Struktur zugeordnet wurde, können Sie die E/A-Filterrichtlinie für die virtuelle Maschine nicht hinzufügen, ändern oder entfernen.

Migrieren von virtuellen Maschinen mit E/A-Filtern

Bei der Migration einer virtuellen Maschine mit E/A-Filtern gelten spezielle Anforderungen.

Wenn Sie Storage vMotion zum Migrieren einer virtuellen Maschine mit E/A-Filtern verwenden, muss ein Zieldatenspeicher mit Hosts mit installierten kompatiblen E/A-Filtern verbunden sein.

Möglicherweise müssen Sie eine virtuelle Maschine mit E/A-Filtern zwischen verschiedenen Datenspeichertypen migrieren, beispielsweise zwischen VMFS und Virtual Volumes. Achten Sie in diesem Fall darauf, dass die VM-Speicherrichtlinie Regelsätze für jeden Datenspeichertyp enthält, den Sie verwenden möchten. Wenn Sie beispielsweise Ihre virtuelle Maschine zwischen einem VMFS-Datenspeicher und einem Datenspeicher für Virtual Volumes migrieren, sollten Sie eine gemischte VM-Speicherrichtlinie erstellen, die folgende Regeln beinhaltet:

- Gemeinsame Regeln für die E/A-Filter
- Regelsatz 1 für den VMFS-Datenspeicher. Da das speicherrichtlinienbasierte Management keine explizite VMFS-Richtlinie bietet, muss der Regelsatz Tag-basierte Regeln für den VMFS-Datenspeicher enthalten.
- Regelsatz 2 für den Virtual Volumes-Datenspeicher.

Wenn die virtuelle Maschine mit Storage vMotion migriert wird, wird der entsprechende Regelsatz für den Zieldatenspeicher ausgewählt. Die E/A-Filterregeln bleiben unverändert.

Falls Sie keine Regeln für Datenspeicher angeben und nur gemeinsame Regeln für die E/A-Filter definieren, wendet das System Standardspeicherrichtlinien für die Datenspeicher an.

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`.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Installieren Sie die VIBs durch Ausführen des folgenden Befehls:

esxcli 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 *ESXCLI – Referenz*.

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

esxcli software vib list

Speicherhardware-Beschleunigung

24

Mithilfe der Hardwarebeschleunigung kann der ESXi-Host in konforme Speichersysteme integriert werden. Der Host kann bestimmte VM- und Speicherverwaltungsvorgänge auf die Speichersysteme auslagern. Mit der Speicherhardware-Unterstützung führt Ihr Host diese Vorgänge schneller aus und verbraucht weniger CPU, Arbeitsspeicher und Speicher-Fabric-Bandbreite.

Die Hardwarebeschleunigung wird von Blockspeichergeräten, Fibre-Channel und iSCSI sowie NAS-Geräten unterstützt.

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1021976.

Dieses Kapitel enthält die folgenden Themen:

- Vorteile der Hardwarebeschleunigung
- Anforderungen der Hardwarebeschleunigung
- Status der Hardwarebeschleunigungs-Unterstützung
- Hardwarebeschleunigung für Blockspeichergeräte
- Hardwarebeschleunigung auf NAS-Geräten
- Überlegungen bei der Hardwarebeschleunigung

Vorteile der Hardwarebeschleunigung

Wenn die Hardwarebeschleunigungs-Funktion unterstützt wird, kann der Host Hardwareunterstützung erhalten und etliche Aufgaben schneller und effizienter ausführen:

Der Host kann Unterstützung bei den folgenden Aktivitäten erhalten:

- Migrieren von virtuellen Maschinen mit Storage vMotion
- Bereitstellen von virtuellen Maschinen anhand von Vorlagen
- Klonen virtueller Maschinen oder Vorlagen
- VMFS Clustered Locking und Metadatenvorgänge für Dateien virtueller Maschinen
- Bereitstellen von virtuellen Festplatten mit Thick Provisioning
- Erstellen von fehlertoleranten virtuellen Maschinen

- Erstellen und Klonen von Thick-Festplatten auf NFS-Datenspeichern

Anforderungen der Hardwarebeschleunigung

Die Hardwarebeschleunigungs-Funktion kann nur mit einer geeigneten Kombination aus Host und Speicher-Array verwendet werden.

Tabelle 24-1. Speicheranforderungen der Hardwarebeschleunigung

ESXi	Blockspeichergeräte	NAS-Geräte
ESXi	Unterstützen T10 SCSI Standard- oder Blockspeicher-Plug-Ins für die Array-Integration (VAAI)	Unterstützen NAS-Plug-Ins für die Array-Integration

Hinweis Wenn Ihr SAN- oder NAS-Speicher-Fabric vor dem die Hardwarebeschleunigung unterstützenden Speichersystem eine dazwischenliegende Appliance verwendet, muss die dazwischenliegende Appliance die Hardwarebeschleunigung ebenfalls unterstützen und ordnungsgemäß zertifiziert sein. Bei der dazwischenliegenden Appliance kann es sich um eine Speichervirtualisierungs-Appliance, eine E/A-Beschleunigungs-Appliance, eine Verschlüsselungs-Appliance usw. handeln.

Status der Hardwarebeschleunigungs-Unterstützung

vSphere Client zeigt den Status der Hardwarebeschleunigungs-Unterstützung für jedes Speichergerät und jeden Datenspeicher an.

Die Statuswerte lauten „Unbekannt“, „Unterstützt“ und „Nicht unterstützt“. Der Anfangswert ist „Unbekannt“.

Bei Blockgeräten ändert sich der Status in „Unterstützt“, wenn der Host den Auslagerungsvorgang erfolgreich ausgeführt hat. Wenn der Auslagerungsvorgang fehlschlägt, ändert sich der Status in „Nicht unterstützt“. Der Status bleibt „Unbekannt“, wenn das Gerät die Hardwarebeschleunigung nur teilweise unterstützt.

Bei NAS ist der Status „Unterstützt“, wenn der Speicher mindestens einen Hardwareablagerungsvorgang durchführen kann.

Wenn Speichergeräte die Hostvorgänge nicht oder nur teilweise unterstützen, kehrt der Host für die Ausführung nicht unterstützter Vorgänge zu seinen nativen Methoden zurück.

Hardwarebeschleunigung für Blockspeichergeräte

Mithilfe der Hardwarebeschleunigung kann der Host mit Blockspeichergeräten, Fibre-Channel oder iSCSI integriert werden und bestimmte Speicher-Array-Vorgänge verwenden.

Die ESXi-Hardwarebeschleunigung unterstützt die folgenden Array-Vorgänge:

- „Full Copy“ (wird auch als „Clone Blocks“ oder „Copy Offload“ bezeichnet). Ermöglicht den Speicher-Arrays, vollständige Kopien von Daten innerhalb des Arrays zu erstellen, ohne dass der Host die Daten lesen und schreiben muss. Dieser Vorgang reduziert die Zeit und die Netzwerkauslastung beim Klonen von virtuellen Maschinen, beim Bereitstellen einer Vorlage oder beim Migrieren mit vMotion.
- „Block zeroing“ (wird auch als „write same“ bezeichnet). Ermöglicht den Speicher-Arrays, eine große Anzahl von Blöcken mit Nullbyte zu füllen, um neu zugeteilten Speicher, der keine bereits geschriebenen Daten enthält, bereitzustellen. Dieser Vorgang reduziert die Zeit und die Netzwerkauslastung beim Erstellen von virtuellen Maschinen und beim Formatieren von virtuellen Festplatten.
- „Hardware assisted locking“ (wird auch als „atomic test and set [ATS]“ bezeichnet). Unterstützt das separate Sperren einer virtuellen Maschine, ohne SCSI-Reservierungen verwenden zu müssen. Diese Operation erlaubt das Sperren von Festplatten auf Sektorbasis anstatt der gesamten LUN (wie bei der Verwendung von SCSI-Reservierungen).

Wenden Sie sich hinsichtlich der Unterstützung der Hardwarebeschleunigung an Ihren Anbieter. Für bestimmte Speicher-Arrays ist es erforderlich, dass Sie die Unterstützung auf der Speicherseite aktivieren.

Auf Ihrem Host ist die Hardwarebeschleunigung standardmäßig aktiviert. Falls Ihr Speicher die Hardwarebeschleunigung nicht unterstützt, können Sie sie deaktivieren.

Neben der Unterstützung der Hardwarebeschleunigung bietet ESXi auch Unterstützung für das Thin Provisioning. Weitere Informationen hierzu finden Sie unter ESXi und Array-Thin Provisioning.

Deaktivieren der Hardwarebeschleunigung für Blockspeichergeräte

Auf Ihrem Host ist die Hardwarebeschleunigung für Blockspeichergeräte standardmäßig aktiviert. Sie können die erweiterten Einstellungen des vSphere Client verwenden, um die Hardwarebeschleunigungsvorgänge zu deaktivieren.

Wenden Sie sich, wie bei allen erweiterten Einstellungen, an den VMware-Support, bevor Sie die Hardwarebeschleunigung deaktivieren.

Verfahren

1. Navigieren Sie im vSphere Client zum ESXi-Host.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Ändern Sie den Wert für eine beliebige Option auf 0 (deaktiviert):
   - VMFS3.HardwareAcceleratedLocking
   - DataMover.HardwareAcceleratedMove

- DataMover.HardwareAcceleratedInit

Verwalten der Hardwarebeschleunigung auf Blockspeichergeräten

Um eine Integration mit den Blockspeicher-Arrays zu ermöglichen, verwendet vSphere die ESXi-Erweiterungen, die als „Storage APIs - Array Integration“ bezeichnet werden (früher VAAI). Mit dieser Integration kann vSphere die Array-Hardwarevorgänge verwenden.

In vSphere 5.x und höher werden diese Erweiterungen als T10 SCSI-Befehle implementiert. Folglich kann der ESXi-Host direkt mit den Geräten, die den T10 SCSI-Standard unterstützen, kommunizieren, d. h., die VAAI-Plug-Ins sind nicht erforderlich.

Wenn das Gerät T10 SCSI nicht oder nur teilweise unterstützt, kehrt ESXi zur Verwendung der auf dem Host installierten VAAI-Plug-Ins zurück. Der Host kann auch eine Kombination aus T10 SCSI-Befehlen und Plug-Ins verwenden. Die VAAI-Plug-Ins sind anbieterspezifisch und können entweder von VMware oder von Partnern entwickelt worden sein. Zum Verwalten des VAAI-fähigen Geräts hängt der Host den VAAI-Filter und das anbieterspezifische VAAI-Plug-In an das Gerät an.

Informationen darüber, ob Ihr Speicher VAAI Plug-Ins benötigt oder die Hardwarebeschleunigung über T10 SCSI-Befehle unterstützt, finden Sie im *VMware-Kompatibilitätshandbuch* oder kontaktieren Sie Ihren Speicheranbieter.

Sie können mehrere `esxcli`-Befehle verwenden, um Speichergeräte nach den Informationen zur Unterstützung der Hardwarebeschleunigung abzufragen. Geräten, die VAAI-Plug-Ins benötigen, stehen zudem die Beanspruchungsregeln zur Verfügung. Weitere Informationen zu `esxcli`-Befehlen finden Sie unter *Erste Schritte mit ESXCLI*.

Anzeigen der Hardwarebeschleunigungs-Plug-Ins und des Hardwarebeschleunigungsfilters

Um mit den Geräten zu kommunizieren, die die T10 SCSI-Norm nicht unterstützen, verfügt Ihr Host über einen einzigen VAAI-Filter und ein anbieterspezifisches VAAI-Plug-In. Verwenden Sie den `esxcli` -Befehl, um den Hardwarebeschleunigungsfilter und die Plug-Ins anzuzeigen, die derzeit in Ihrem System geladen sind.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den Befehl **`esxcli storage core plugin list --plugin-class=value`** aus.

  Geben Sie für *Wert* einen der folgenden Parameter ein:

  - Geben Sie `VAAI` ein, um die Plug-Ins anzuzeigen.

Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
#esxcli storage core plugin list --plugin-class=VAAI
Plugin name         Plugin class
VMW_VAAIP_EQL       VAAI
VMW_VAAIP_NETAPP    VAAI
VMW_VAAIP_CX        VAAI
```

- Geben Sie `Filter` ein, um den Filter anzuzeigen.

  Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
esxcli storage core plugin list --plugin-class=Filter
Plugin name  Plugin class
VAAI_FILTER  Filter
```

Verifizieren des Status der Hardwarebeschleunigungs-Unterstützung

Verwenden Sie den `esxcli`-Befehl, um den Hardwarebeschleunigungs-Unterstützungsstatus eines bestimmten Speichergeräts zu überprüfen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus: **`esxcli storage core device list -d=`*`device_ID`***.

  Die Ausgabe zeigt den Hardwarebeschleunigungs- oder VAAI-Status an, der „Unbekannt“, „Unterstützt“ oder „Nicht unterstützt“ lauten kann.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 XXXXXXXXXXXXXXXX
 Attached Filters: VAAI_FILTER
 VAAI Status: supported
 XXXXXXXXXXXXXXXX
```

Verifizieren der Details der Hardwarebeschleunigungs-Unterstützung

Verwenden Sie den Befehl `esxcli`, um abzufragen, ob das Blockspeichergerät die Hardwarebeschleunigungs-Unterstützung bietet.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus: **esxcli storage core device vaai status get -d=*device_ID***.

  Wenn ein VAAI-Plug-In das Gerät verwaltet, wird bei der Ausgabe der Name des Plug-Ins angezeigt, der dem Gerät zugewiesen ist. Die Ausgabe zeigt zudem den Unterstützungsstatus für jedes T10 SCSI-basierte einfache Plug-In an, falls verfügbar. Dies ist ein Beispiel für eine Ausgabe:

```
# esxcli storage core device vaai status get -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 VAAI Plugin Name: VMW_VAAIP_SYMM
 ATS Status: supported
 Clone Status: supported
 Zero Status: supported
 Delete Status: unsupported
```

Auflisten der Hardwarebeschleunigungs-Beanspruchungsregeln

Jedes von einem VAAI-Plug-In verwaltete Blockspeichergerät benötigt zwei Beanspruchungsregeln. Eine Beanspruchungsregel gibt den Hardwarebeschleunigungsfilter an, die andere das Hardwarebeschleunigungs-Plug-In für das Gerät. Sie können die Beanspruchungsregeln für den Hardwarebeschleunigungsfilter und das Hardwarebeschleunigungs-Plug-In mithilfe der `esxcli`-Befehle auflisten.

Verfahren

1. Führen Sie zum Auflisten der Filterbeanspruchungsregeln den Befehl **esxcli storage core claimrule list --claimrule-class=Filter** aus.

   In diesem Beispiel geben die Filterbeanspruchungsregeln die Geräte an, die der VAAI_FILTER-Filter beansprucht.

```
# esxcli storage core claimrule list --claimrule-class=Filter
Rule Class   Rule   Class   Type   Plugin      Matches                     XCOPY Use Array
Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
Filter       65430  runtime vendor VAAI_FILTER
vendor=EMC model=SYMMETRIX                          False
False                            0
Filter       65430  file    vendor VAAI_FILTER
vendor=EMC model=SYMMETRIX                          False
False                            0
Filter       65431  runtime vendor VAAI_FILTER
vendor=DGC model=*                                  False
False                            0
Filter       65431  file    vendor VAAI_FILTER
vendor=DGC model=*                                  False
False                            0
```

2 Führen Sie zum Auflisten der VAAI-Plug-In-Beanspruchungsregeln den Befehl **esxcli storage core claimrule list --claimrule-class=VAAI** aus.

In diesem Beispiel geben die VAAI-Beanspruchungsregeln die Geräte an, die das VAAI-Plug-In beansprucht.

```
esxcli storage core claimrule list --claimrule-class=VAAI
Rule Class   Rule   Class   Type    Plugin         Matches                   XCOPY Use
Array Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
VAAI         65430  runtime vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                         False
False                            0
VAAI         65430  file    vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                         False
False                            0
VAAI         65431  runtime vendor  VMW_VAAIP_CX
vendor=DGC model=*                                 False
False                            0
VAAI         65431  file    vendor  VMW_VAAIP_CX
vendor=DGC model=*                                 False
False                            0
```

Hinzufügen von Hardwarebeschleunigungs-Beanspruchungsregeln

Um die Hardwarebeschleunigung für einen neuen Array zu konfigurieren, fügen Sie zwei Beanspruchungsregeln hinzu, eine für den VAAI-Filter und einen für das VAAI-Plug-In. Zur Aktivierung der neuen Beanspruchungsregeln müssen Sie diese zunächst definieren und in Ihr System laden.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Definieren Sie eine neue Beanspruchungsregel für den VAAI-Filter, indem Sie den Befehl **esxcli storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER** ausführen.

2 Definieren Sie eine neue Beanspruchungsregel für das VAAI-Plug-In, indem Sie den Befehl **esxcli storage core claimrule add --claimrule-class=VAAI** ausführen.

3 Laden Sie beide Beanspruchungsregeln, indem Sie die folgenden Befehle ausführen:

esxcli storage core claimrule load --claimrule-class=Filter

esxcli storage core claimrule load --claimrule-class=VAAI

4 Führen Sie die VAAI-Filter-Beanspruchungsregel und dazu den Befehl **`esxcli storage core claimrule run --claimrule-class=Filter`** aus.

Hinweis Nur die Filterklasse-Regeln müssen ausgeführt werden. Wenn der VAAI-Filter ein Gerät beansprucht, findet er automatisch das richtige VAAI-Plug-In, das angehängt werden muss.

Beispiel: Definieren von Hardwarebeschleunigungs-Beanspruchungsregeln

Dieses Beispiel zeigt, wie die Hardwarebeschleunigung für IBM-Arrays mithilfe des VMW_VAAIP_T10-Plug-Ins konfiguriert werden. Verwenden Sie die folgende Befehlsfolge. Weitere Informationen zu den Befehlsoptionen finden Sie unter Hinzufügen von Multipathing-Beanspruchungsregeln.

```
# esxcli storage core claimrule add --claimrule-class=Filter --
plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign

# esxcli storage core claimrule add --claimrule-class=VAAI --
plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign

# esxcli storage core claimrule load --claimrule-class=Filter

# esxcli storage core claimrule load --claimrule-class=VAAI

# esxcli storage core claimrule run --claimrule-class=Filter
```

Konfigurieren von XCOPY-Parametern

XCOPY ist eines der VAAI-Primitive, die zum Auslagern von Aufgaben in den Speicher-Array verwendet werden. Mit XCOPY können Sie beispielsweise Vorgänge wie die Migration oder das Klonen von virtuellen Maschinen in den Array auslagern, statt zur Durchführung dieser Aufgaben vSphere-Ressourcen zu verbrauchen.

Sie können den XCOPY-Mechanismus bei allen Speicher-Arrays verwenden, die das von VMware entwickelte und auf den SCSI-Standards von T10 basierende VMW_VAAIP_T10-Plug-In unterstützen. Zum Aktivieren des XCOPY-Mechanismus erstellen Sie eine Beanspruchungsregel der VAAI-Klasse.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Verwenden Sie den folgenden Befehl und geben Sie die XCOPY-Optionen ein:

  ```
  esxcli storage core claimrule add --claimrule-class=VAAI
  ```

Weitere Informationen zu den Befehlsoptionen finden Sie unter Hinzufügen von Multipathing-Beanspruchungsregeln.

Option	Beschreibung
-a|--xcopy-use-array-values	Für XCOPY-Befehle werden vom Array gemeldete Werte verwendet.
-s|--xcopy-use-multi-segs	Für XCOPY-Befehle werden mehrere Segmente verwendet. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.
-m|--xcopy-max-transfer-size	Maximale Übertragungsgröße in MB für die XCOPY-Befehle, wenn Sie eine andere Übertragungsgröße als die vom Array gemeldete verwenden. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.
-k|--xcopy-max-transfer-size-kib	Maximale Übertragungsgröße in KiB für die XCOPY-Befehle, wenn Sie eine andere Übertragungsgröße als die vom Array gemeldete verwenden. Nur gültig, wenn `--xcopy-use-array-values` angegeben ist.

Beispiel: Konfigurieren von XCOPY

- ```
  # esxcli storage core claimrule add -r 914 -t vendor -V XtremIO -M XtremApp -P
  VMW_VAAIP_T10 -c VAAI -a -s -k 64
  ```
- ```
  # esxcli storage core claimrule add -r 65430 -t vendor -V EMC -M SYMMETRIX -P
  VMW_VAAIP_SYMM -c VAAI -a -s -m 200
  ```

Löschen von Hardwarebeschleunigungs-Beanspruchungsregeln

Mithilfe des `esxcli`-Befehls können Sie vorhandene Hardwarebeschleunigungs-Beanspruchungsregeln löschen.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie folgende Befehle aus:

  `esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=Filter`

  `esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=VAAI`

Hardwarebeschleunigung auf NAS-Geräten

Mithilfe der Hardwarebeschleunigung können ESXi-Hosts auf NAS-Geräte abgestimmt werden und mehrere vom NAS-Speicher bereitgestellte Hardwarevorgänge nutzen. Die Hardwarebeschleunigung verwendet vSphere-APIs für die Array-Integration (VAAI), um Daten zwischen den Hosts und Speichergeräten auszutauschen.

Das VAAI-NAS-Framework unterstützt beide Versionen von NFS-Speicher (NFS 3 und NFS 4.1).

Der VAAI-NAS verwendet eine Gruppe von Speicherprimitiven, um Speichervorgänge vom Host auf das Array auszulagern. In der folgenden Liste werden die unterstützten NAS-Vorgänge aufgeführt:

Vollständiges Klonen von Dateien

Unterstützt die Fähigkeit eines NAS-Geräts, virtuelle Festplattendateien zu klonen. Dieser Vorgang ähnelt dem VMFS-Blockklonen mit der Ausnahme, dass NAS-Geräte ganze Dateien anstatt Dateisegmente klonen. Zu den Aufgaben, die vom vollständigen Klonen von Dateien profitieren, gehören das Klonen von VMs, Storage vMotion sowie die Bereitstellung von VMs über Vorlagen.

Wenn der ESXi-Host Daten mit VAAI-NAS kopiert, müssen die Daten weder aus dem NAS gelesen noch in den NAS zurückgeschrieben werden. Der Host sendet einfach den Kopierbefehl, mit dem die Daten in den NAS ausgelagert werden. Der Kopiervorgang wird im NAS durchgeführt, wodurch die Last auf dem Host reduziert wird.

Schnelles Klonen von Dateien

Dieser Vorgang, auch als Array-basierte oder native Snapshots bezeichnet, lagert die Erstellung von VM-Snapshots und verknüpften Klonen in das Array aus.

Speicherplatz reservieren

Unterstützt die Fähigkeit eines Speicher-Arrays, Speicherplatz für eine virtuelle Festplattendatei im Thick-Format zuzuteilen.

In der Regel legt der NAS-Server die Zuweisungsrichtlinie fest, wenn Sie eine virtuelle Festplatte auf einem NFS-Datenspeicher erstellen. Die Standardzuweisungsrichtlinie auf den meisten NAS-Servern ist „Thin“ und garantiert keinen Backing-Speicher für die Datei. Allerdings kann der Vorgang „Speicherplatz reservieren“ das NAS-Gerät anweisen, anbieterspezifische Mechanismen zu verwenden, um Speicherplatz für eine virtuelle Festplatte zu reservieren. Folglich können Sie virtuelle Festplatten im Thick-Format auf dem NFS-Datenspeicher erstellen, wenn der zugrunde liegende NAS-Server den Vorgang zum Reservieren von Speicherplatz unterstützt.

Erweiterte Statistiken

Unterstützt Transparenz bei der Speicherplatznutzung auf NAS-Geräten. Mithilfe dieses Vorgangs können Sie Details zur Speicherauslastung für virtuelle Festplatten in NFS-Datenspeichern abfragen. Zu diesen Details gehören die Größe sowie der Speicherverbrauch einer virtuellen Festplatte. Diese Funktion eignet sich für Thin-Bereitstellungen.

Bei NAS-Speichergeräten wird die Integration der Hardwarebeschleunigung über anbieterspezifische NAS-Plug-Ins implementiert. Diese Plug-Ins werden in der Regel von Anbietern erstellt und als Anbieterpakete vertrieben. Die NAS-Plug-Ins funktionieren ohne Beanspruchungsregeln.

Verschiedene Tools zum Installieren und Aktualisieren von NAS-Plug-Ins stehen zur Verfügung. Dazu gehören die `esxcli`-Befehle und vSphere Lifecycle Manager. Weitere Informationen finden Sie unter *VMware ESXi-Upgrade* und *Verwalten des Lebenszyklus von Host und Cluster*. Installations- und Update-Empfehlungen finden Sie im Knowledgebase-Artikel.

Hinweis NAS-Speicheranbieter stellen unter Umständen zusätzliche Einstellungen bereit, die sich auf die Leistung und den Betrieb der VAAI auswirken können. Halten Sie sich an die Empfehlungen des Anbieters und konfigurieren Sie die entsprechenden Einstellungen auf dem NAS-Speicher-Array und ESXi. Weitere Informationen finden Sie in der Dokumentation Ihres Speicheranbieters.

Aktivieren nativer NAS-Snapshots auf virtuellen Maschinen

Wenn Ihre Bereitstellung NAS-Arrays enthält, die die vSphere APIs for Array Integration (VAAI) unterstützen, können Sie die Fast File Clone-Technologie, auch systemeigene NFS-Snapshots genannt, verwenden, um Snapshots von virtuellen Maschinen zu erstellen. Mit dieser Technologie kopiert das NFS-Gerät die virtuelle Maschine, ohne dass der ESXi-Host die Daten lesen und schreiben muss. Dieser Vorgang reduziert möglicherweise die Zeit und die Netzwerklast beim Erstellen von VM-Snapshots.

Standardmäßig unterstützen alle neu erstellten VMs herkömmliche ESXi-Snapshot-Technologie. Um die native NFS-Snapshot-Technologie zu verwenden, aktivieren Sie sie für die VM.

Voraussetzungen

- Stellen Sie sicher, dass das NAS-Array den Vorgang des schnellen Dateiklons mit dem VAAI NAS-Programm unterstützt.
- Installieren Sie den anbieterspezifischen NAS-Plug-In, der das schnelle Klonen von Dateien mit VAAI unterstützt, auf Ihrem ESXi-Host.
- Folgen Sie den Empfehlungen Ihres NAS-Speicheranbieters, um alle erforderlichen Einstellungen sowohl auf dem NAS-Array als auch auf ESXi zu konfigurieren. Weitere Informationen finden Sie in der Dokumentation Ihres Speicheranbieters.

Verfahren

1. Klicken Sie im vSphere Client mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.
2. Klicken Sie auf die Registerkarte **VM-Optionen**, und erweitern Sie das Menü **Erweitert**.
3. Klicken Sie auf **Konfiguration bearbeiten** neben den Konfigurationsparametern.
4. Konfigurieren Sie den Parameter **`snapshot.alwaysAllowNative`**.

   Wenn der Parameter vorhanden ist, stellen Sie sicher, dass sein Wert auf „True“ festgelegt ist. Wenn der Parameter nicht vorhanden ist, können Sie ihn hinzufügen und den Wert auf „True“ setzen.

Name	Wert
`snapshot.alwaysAllowNative`	True

Überlegungen bei der Hardwarebeschleunigung

Bei Verwendung der Hardwarebeschleunigung mit ESXi muss Folgendes beachtet werden.

Es gibt mehrere mögliche Gründe für das Fehlschlagen eines hardwarebeschleunigten Vorgangs.

Für jedes Primitiv, das das Array nicht implementiert, gibt das Array einen Fehler zurück. Der Fehler sorgt dafür, dass der ESXi-Host versucht, den Vorgang unter Verwendung seiner nativen Methoden durchzuführen.

Der VMFS Data Mover nutzt keine Hardware-Offloads. Stattdessen werden in den folgenden Fällen Software-Datenverschiebungen verwendet:

- Die Quell- und Ziel-VMFS-Datenspeicher haben unterschiedliche Blockgrößen.
- Der Typ der Quelldatei ist RDM und der Typ der Zieldatei ist Nicht-RDM (normale Datei).
- Der VMDK-Typ der Quelle ist „eagerzeroedthick“ und der VMDK-Typ des Ziels ist „thin“.
- Das Format der Quell- oder Ziel-VMDK ist „sparse“ oder „hosted“.
- Die virtuelle Quellmaschine hat einen Snapshot.
- Die logische Adresse und die Übertragungslänge des angeforderten Vorgangs sind nicht auf die vom Speichergerät erforderliche Mindestausrichtung ausgerichtet. Alle mit dem vSphere Client erstellten Datenspeicher werden automatisch ausgerichtet.
- Das VMFS hat mehrere LUNs oder Erweiterungen und sie befinden sich auf unterschiedlichen Arrays.

Das Klonen von Hardware zwischen Arrays, auch innerhalb desselben VMFS-Datenspeichers, funktioniert nicht.

Speicher-Provisioning und Speicherplatzrückforderung

25

vSphere unterstützt zwei Formate der Bereitstellung von Speicher, Thick Provisioning und Thin Provisioning.

Thick Provisioning

Hierbei handelt es sich um das herkömmliche Modell der Speicherbereitstellung. Beim Thick Provisioning wird eine große Menge an Speicherplatz im Voraus in Erwartung zukünftiger Speicheranforderungen bereitgestellt. Möglicherweise bleibt der Speicherplatz jedoch ungenutzt, was dazu führen kann, dass die Speicherkapazität nicht voll ausgenutzt wird.

Thin Provisioning

Bei dieser Methode können Sie im Unterschied zum Format „Thick“ Probleme mit zu geringer Auslastung des Speichers beseitigen, indem Speicherplatz auf flexible Weise nach Bedarf zugeteilt wird. Mit ESXi können Sie zwei Modelle des Thin Provisioning verwenden: Thin Provisioning auf Array-Ebene und Thin Provisioning auf der Ebene der virtuellen Festplatte.

Beim Thin Provisioning erhalten Sie die Möglichkeit mehr virtuellen Speicherplatz zu melden, als reale physische Kapazität vorhanden ist. Diese Abweichung kann zu einer Speicherüberbuchung führen, die auch als Überbereitstellung bezeichnet wird. Beim Thin Provisioning wird die tatsächliche Speichernutzung überwacht, um Situationen zu vermeiden, in denen kein physischer Speicherplatz vorhanden ist.

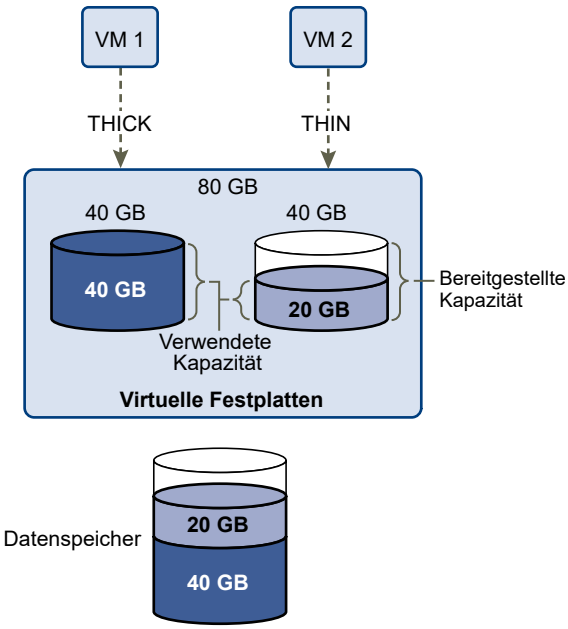
Dieses Kapitel enthält die folgenden Themen:

Thin Provisioning virtueller Festplatten

Wenn Sie eine virtuelle Maschine erstellen, wird ein bestimmter Teil des Speicherplatzes auf einem Datenspeicher für die virtuellen Festplattendateien bereitgestellt.

Standardmäßig bietet ESXi eine herkömmliche Speicherbereitstellungsmethode für virtuelle Maschinen. Mit dieser Methode schätzen Sie zuerst, wie viel Speicher die virtuelle Maschine für den gesamten Lebenszyklus wahrscheinlich benötigt. Anschließend stellen Sie im Voraus eine feste Menge an Speicherplatz für die virtuelle Festplatte der virtuellen Maschine bereit, beispielsweise 40 GB. Der gesamte bereitgestellte Speicherplatz wird der virtuellen Festplatte zugeteilt. Eine virtuelle Festplatte, die sofort den gesamten bereitgestellten Speicherplatz belegt, ist eine Thick-Festplatte.

ESXi unterstützt Thin Provisioning für virtuelle Festplatten. Die Thin Provisioning-Funktion auf Festplattenebene ermöglicht Ihnen das Erstellen von virtuellen Festplatten in einem Thin-Format. ESXi teilt einer virtuellen Festplatte im Thin-Format den gesamten für aktuelle und zukünftige Aktionen erforderlichen Speicherplatz zu, beispielsweise 40 GB. Allerdings verwendet die Thin-Festplatte nur so viel Speicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. In diesem Beispiel belegt die Thin-bereitgestellte Festplatte nur 20 GB an Speicherplatz. Wenn die Festplatte mehr Speicherplatz benötigt, kann sie bis auf die 40 GB an bereitgestelltem Speicherplatz anwachsen.



Informationen zu Bereitstellungsrichtlinien für virtuelle Festplatten

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

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

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

Thick-Provision Lazy-Zeroed

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

Thick-Provision Eager-Zeroed

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

Thin-bereitstellen

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

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

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

Erstellen von virtuellen Thin-bereitgestellten Festplatten

Um Speicherplatz zu sparen, können Sie eine virtuelle Festplatte im per Thin Provisioning bereitgestellten Format erstellen. Die Größe der virtuellen per Thin Provisioning bereitgestellten Festplatte ist zunächst gering und steigt an, sobald mehr virtueller Festplattenspeicher erforderlich ist. Sie können Thin-Festplatten nur auf Datenspeichern erstellen, die Thin Provisioning auf Festplattenebene unterstützen.

Bei diesem Verfahren wird vorausgesetzt, dass Sie eine neue virtuelle Maschine erstellen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Verfahren

1 Erstellen Sie eine virtuelle Maschine.

   a Klicken Sie mit der rechten Maustaste auf ein Bestandslistenobjekt, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datencenter, Ordner, Cluster, Ressourcenpool oder Host, und wählen Sie die Option **Neue virtuelle Maschine** aus.

   b Wählen Sie **Eine neue virtuelle Maschine erstellen** und klicken Sie auf **Weiter**.

   c Befolgen Sie sämtliche Anweisungen zum Erstellen einer virtuellen Maschine.

2 Konfigurieren Sie die virtuelle Festplatte im Thin-Format.

   a Klicken Sie auf der Seite „Hardware anpassen“ auf die Registerkarte **Virtuelle Hardware**.

   b Klicken Sie auf das Dreieck **Neue Festplatte**, um die Festplattenoptionen zu erweitern.

   c (Optional) Passen Sie die Standardfestplattengröße an.

      Mit einer virtuellen Thin-Festplatte zeigt der Wert für die Datenträgergröße an, wie viel Speicher auf der Festplatte bereitgestellt und garantiert wird. Am Anfang verwendet die virtuelle Festplatte möglicherweise nicht den gesamten bereitgestellten Speicher. Der tatsächliche Speichernutzungswert kann geringer als die Größe der virtuellen Festplatte sein.

   d Wählen Sie **Thin Provision** für Festplattenbereitstellung aus.

3 Beenden Sie die Erstellung der virtuellen Maschine.

Ergebnisse

Sie haben eine virtuelle Maschine mit einer Festplatte im Thin-Format erstellt.

Nächste Schritte

Wenn die virtuelle Festplatte das Thin-Format aufweist, können Sie sie später auf ihre volle Größe vergrößern.

Anzeigen von Speicherressourcen virtueller Maschinen

Sie können anzeigen, wie Speicherplatz von Datenspeichern Ihren virtuellen Maschinen zugeteilt ist.

Verfahren

1 Navigieren Sie zu der virtuellen Maschine.

2 Doppelklicken Sie auf die virtuelle Maschine, und klicken Sie auf die Registerkarte **Übersicht**.

3 Prüfen Sie die Informationen über die Speicherbelegung rechts oben auf der Registerkarte **Übersicht**.

Ergebnisse

Speichernutzung zeigt den Datenspeicherplatz, der von den Dateien der virtuellen Maschine, z. B. Konfigurations- und Protokolldateien, Snapshots, virtuellen Festplatten usw., beansprucht wird. Wenn die virtuelle Maschine läuft, werden im verwendeten Speicherplatz auch die Auslagerungsdateien berücksichtigt.

Für virtuelle Maschinen mit Thin-Festplatten kann der tatsächliche Speichernutzungswert geringer als die Größe der virtuellen Festplatte sein.

Festlegen des Festplattenformats für eine virtuelle Maschine

Sie können festlegen, ob Ihre virtuelle Festplatte im Thick- oder im Schnell-Format vorliegen soll.

Verfahren

1 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

2 Klicken Sie auf die Registerkarte **Virtuelle Hardware**.

3 Klicken Sie auf das Dreieck **Festplatte**, um die Festplattenoptionen zu erweitern.

Im Textfeld **Typ** wird das Format Ihrer virtuellen Festplatte angezeigt.

Nächste Schritte

Wenn die virtuelle Festplatte das Format „Schnell“ aufweist, können Sie sie auf ihre volle Größe vergrößern.

Vergrößern virtueller Thin-Festplatten

Virtuelle Festplatten, die Sie im Thin-Format erstellt haben, können in das Thick-Format konvertiert werden.

Sie können mit dem Datenspeicherbrowser die virtuelle Festplatte im Thin-Format vergrößern.

Voraussetzungen

- Stellen Sie sicher, dass der Datenspeicher, in dem sich die virtuelle Maschine befindet, über ausreichend Speicherplatz verfügt.
- Stellen Sie zudem sicher, dass die virtuelle Festplatte das Thin-Format aufweist.
- Entfernen Sie Snapshots.
- Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie im vSphere Client zum Ordner der virtuellen Festplatte, die Sie vergrößern möchten.

   a Navigieren Sie zu der virtuellen Maschine.

   b Klicken Sie auf die Registerkarte **Datenspeicher**.

   Der Datenspeicher, in dem die Dateien der virtuellen Maschine gespeichert sind, wird angezeigt.

   c Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **Dateien durchsuchen**.

   Der Datenspeicherbrowser zeigt den Inhalt des Datenspeichers an.

2 Erweitern Sie den Ordner der virtuellen Maschine und navigieren Sie zu der Datei der virtuellen Festplatte, die Sie konvertieren möchten.

   Die Datei hat die Erweiterung `.vmdk` und ist durch das Symbol für virtuelle Festplatten () gekennzeichnet.

3 Wählen Sie die virtuelle Festplattendatei aus und klicken Sie auf **Vergrößern**.

   Hinweis Die Option ist möglicherweise nicht verfügbar, wenn die virtuelle Festplatte das Thick-Format aufweist oder wenn die virtuelle Maschine ausgeführt wird.

Ergebnisse

Die vergrößerte virtuelle Festplatte belegt den ganzen Datenspeicherplatz, der ursprünglich für sie bereitgestellt wurde.

Handhabung von Datenspeicher-Überbuchung

Da der für Thin-Festplatten verfügbare Speicherplatz größer sein kann als der übernommene Speicherplatz, kann eine Datenspeicher-Überbuchung auftreten. Dadurch kann der gesamte für die Festplatten der virtuellen Maschine bereitgestellte Speicherplatz die tatsächliche Kapazität überschreiten.

Eine Überbuchung ist möglich, weil normalerweise nicht alle virtuellen Maschinen mit Thin-Festplatten den gesamten für sie bereitgestellten Datenspeicherplatz zur gleichen Zeit benötigen. Sie können jedoch zum Vermeiden einer Datenspeicher-Überbuchung einen Alarm einrichten, der Sie warnt, wenn der bereitgestellte Speicherplatz einen bestimmten Schwellenwert erreicht.

Informationen zum Einstellen von Alarmen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Wenn Ihre virtuellen Maschinen mehr Speicherplatz benötigen, wird der Datenspeicherplatz in der Reihenfolge der Anforderungen zugeteilt. Wenn der Datenspeicherplatz nicht mehr ausreicht, können Sie den physischen Speicher erweitern und den Datenspeicher vergrößern.

Weitere Informationen hierzu finden Sie unter Erhöhen der VMFS-Datenspeicherkapazität.

ESXi und Array-Thin Provisioning

Per Thin Provisioning bereitgestellte Speicher-Arrays können mit ESXi verwendet werden.

Der ESXi-Host wird mit dem blockbasierten Speicher vernetzt und führt die folgenden Aufgaben durch:

- Der Host kann zugrunde liegende per Thin Provisioning bereitgestellte LUNs erkennen und die Speicherplatznutzung überwachen, um zu vermeiden, dass kein physischer Speicherplatz mehr zur Verfügung steht. Der LUN-Speicherplatz kann sich beispielsweise dann ändern, wenn der VMFS-Datenspeicher erweitert wird oder wenn Storage vMotion zum Migrieren von virtuellen Maschinen auf die per Thin Provisioning bereitgestellte LUN verwendet wird. Der Host warnt Sie bei Verletzungen des physischen LUN-Speicherplatzes und bei Speicherplatzknappheit.
- Der Host kann den automatischen T10-Befehl `unmap` von VMFS6- und VM-Gastbetriebssystemen ausgeben, um nicht verwendeten Speicherplatz vom Array zurückzufordern. VMFS5 unterstützt eine manuelle Speicherplatzrückforderungsmethode.

Hinweis ESXi unterstützt die Aktivierung und Deaktivierung von Thin Provisioning auf einem Speichergerät nicht.

Anforderungen

Die folgenden Anforderungen müssen erfüllt sein, damit die Thin Provisioning-Funktionen zur Meldung und Rückforderung von Speicherplatz verwendet werden können:

- Verwenden Sie eine geeignete ESXi-Version.

  Tabelle 25-1. ESXi-Versionen und Thin Provisioning-Unterstützung

Unterstützte Thin Provisioning-Komponenten	ESXi 6.0 und früher	ESXi 6.5 und höher
Thin Provisioning	Ja	Ja
Befehl „Zuordnung aufheben“ von VMFS	Manuell für VMFS5. Verwenden Sie `esxcli storage vmfs unmap`.	Automatisch für VMFS6
Befehl „Zuordnung aufheben“ vom Gastbetriebssystem	Ja. Eingeschränkte Unterstützung.	Ja (VMFS6)

- Verwenden Sie Speichersysteme, die T10-basierte vSphere Storage APIs - Array Integration (VAAI), einschließlich Thin Provisioning und Rückforderung von Speicherplatz, unterstützen. Weitere Informationen erhalten Sie bei Ihrem Speicheranbieter und im *VMware-Kompatibilitätshandbuch*.

Überwachen der Speicherplatznutzung

Die Funktion für die Thin Provisioning-Integration hilft Ihnen, die Speicherplatznutzung auf Thin-bereitgestellten LUNs zu überwachen und zu vermeiden, dass kein Speicherplatz mehr zur Verfügung steht.

Das folgende Datenflussbeispiel zeigt, wie der ESXi-Host und das Speicher-Array interagieren, um Warnungen hinsichtlich Speicherplatzverletzungen und Speicherplatzknappheit für eine Thin-bereitgestellte LUN zu generieren. Derselbe Mechanismus wird angewendet, wenn Sie Storage vMotion zum Migrieren von virtuellen Maschinen auf die Thin-bereitgestellte LUN verwenden.

1 Mithilfe von speicherspezifischen Tools stellt Ihr Speicheradministrator eine Thin-LUN bereit und legt einen Soft-Schwellenwert fest, bei dessen Erreichen ein Alarm ausgelöst wird. Dieser Schritt ist anbieterspezifisch.

2 Mithilfe des vSphere Client erstellen Sie einen VMFS-Datenspeicher auf der Thin-bereitgestellten LUN. Der Datenspeicher umfasst die gesamte logische Größe, die die LUN meldet.

3 Wenn die vom Datenspeicher verwendete Speicherplatzmenge ansteigt und den konfigurierten Soft-Schwellenwert erreicht, finden die folgenden Aktionen statt:

   a Das Speicher-Array meldet die Verletzung Ihrem Host.

   b Ihr Host löst einen Warnungsalarm für den Datenspeicher aus.

      Wenden Sie sich an den Speicheradministrator, um mehr physischen Speicherplatz anzufordern. Alternativ können Sie Storage vMotion verwenden, um Ihre virtuellen Maschinen zu evakuieren, bevor die LUN-Kapazität ausgeht.

4 Wenn kein Speicherplatz mehr zur Verfügung steht, der der Thin-bereitgestellten LUN zugeteilt werden kann, finden die folgenden Aktionen statt:

   a Das Speicher-Array meldet dem Host, dass kein freier Speicherplatz verfügbar ist.

      Vorsicht In einigen Fällen, wenn eine LUN voll wird, kann es offline gehen oder die Zuordnung vom Host entfernen.

   b Der Host hält virtuelle Maschinen an und generiert einen Speicherplatzknappheits-Alarm.

      Sie können das dauerhafte Problem der Speicherplatzknappheit beheben, indem Sie vom Speicheradministrator mehr physischen Speicherplatz anfordern.

Identifizieren von Thin-bereitgestellten Speichergeräten

Verwenden Sie den Befehl `esxcli`, um festzustellen, ob ein bestimmtes Speichergerät Thin-bereitgestellt ist.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- Führen Sie den folgenden Befehl aus: **esxcli storage core device list -d=*device_ID***.

Ergebnisse

Der folgende Thin Provisioning-Status gibt an, dass das Speichergerät Thin-bereitgestellt ist.

```
# esxcli storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 ---------------------
 Thin Provisioning Status: yes
 ---------------------
```

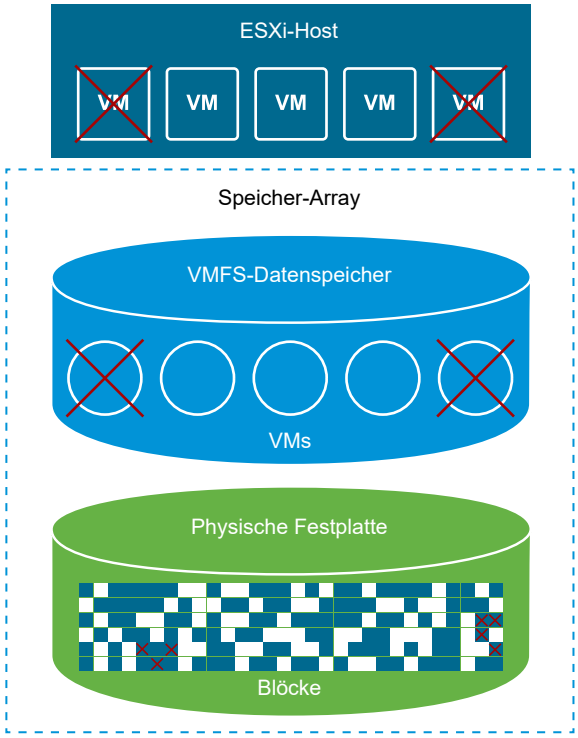
Ein unbekannter Status gibt an, dass ein Speichergerät Thick ist.

Hinweis Einige Speichersysteme präsentieren alle Geräte als Thin-bereitgestellt, egal ob die Geräte Thin oder Thick sind. Ihr Thin Provisioning-Status lautet immer `Ja`. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

Speicherplatzrückforderung

ESXi unterstützt den Befehl zur Speicherplatzrückforderung (auch als SCSI-UNMAP-Befehl bezeichnet), der von einem VMFS-Datenspeicher oder einem VM-Gastbetriebssystem stammt. Dieser Befehl unterstützt per Thin Provisioning bereitgestellte Speicher-Arrays bei der Rückgewinnung von nicht genutztem Speicherplatz vom VMFS-Datenspeicher und den im Datenspeicher enthaltenen virtuellen Festplatten im Thin-Format. Der VMFS6-Datenspeicher kann den Befehl zur Speicherplatzrückforderung automatisch senden. Bei Verwendung des VMFS5-Datenspeichers können Sie den Speicherplatz manuell zurückfordern.

Sie geben Speicherplatz innerhalb des VMFS-Datenspeichers frei, wenn Sie die VM löschen oder migrieren, einen Snapshot konsolidieren usw. Innerhalb der virtuellen Maschine wird Speicherplatz freigegeben, wenn Sie Dateien auf der virtuellen Festplatte im Thin-Format löschen. Bei diesen Vorgängen verbleiben Blöcke mit nicht genutztem Speicher im Speicher-Array. Wenn im Array jedoch nicht erkannt wird, dass die Daten aus den Blöcken gelöscht wurden, bleiben die Blöcke so lange vom Array zugeteilt, bis sie vom Datenspeicher freigegeben werden. VMFS verwendet den SCSI-UNMAP-Befehl, um dem Array mitzuteilen, dass die Speicherblöcke gelöschte Daten enthalten, damit das Array die Zuteilung dieser Blöcke aufheben kann.



Der Befehl kann auch direkt vom Gastbetriebssystem aus ausgegeben werden. Sowohl VMFS5- als auch VMFS6-Datenspeicher können den über das Gastbetriebssystem ausgegebenen Befehl „Zuordnung aufheben“ unterstützen. Die Unterstützung ist jedoch auf VMFS5 beschränkt.

Je nach Typ des VMFS-Datenspeichers verwenden Sie verschiedene Methoden zum Konfigurieren der Speicherplatzrückforderung für den Datenspeicher und Ihre virtuellen Maschinen.

Im nachfolgenden Video erhalten Sie weitere Informationen zur Funktionsweise der Speicherplatzrückforderung.

(Speicherplatzrückforderung mit VMFS)

- Anforderungen zur Speicherplatzrückforderung von VMFS-Datenspeichern

  Durch das Löschen oder Entfernen von Dateien aus einem VMFS-Datenspeicher wird Speicherplatz im Dateisystem freigegeben. Dieser freie Speicherplatz wird einem Speichergerät zugewiesen, bis er vom Dateisystem freigegeben oder die Zuordnung aufgehoben wird. ESXi unterstützt die Rückforderung von freiem Speicherplatz, die auch als Aufhebung der Zuordnung bezeichnet wird.

- Speicherplatzrückforderungen von Gastbetriebssystemen

  ESXi unterstützt die Befehle vom Typ „Zuordnung aufheben“, die direkt von einem Gastbetriebssystem ausgegeben werden, um Speicherplatz zurückzufordern. Der Grad der Unterstützung und die Anforderungen richten sich nach dem Typ des Datenspeichers, in dem sich die virtuelle Maschine befindet.

Anforderungen zur Speicherplatzrückforderung von VMFS-Datenspeichern

Durch das Löschen oder Entfernen von Dateien aus einem VMFS-Datenspeicher wird Speicherplatz im Dateisystem freigegeben. Dieser freie Speicherplatz wird einem Speichergerät zugewiesen, bis er vom Dateisystem freigegeben oder die Zuordnung aufgehoben wird. ESXi unterstützt die Rückforderung von freiem Speicherplatz, die auch als Aufhebung der Zuordnung bezeichnet wird.

Dieser Vorgang ermöglicht dem Speicher-Array, nicht verwendeten Speicherplatz zurückzufordern. Nicht zugeordneter Speicherplatz kann dann für andere Anforderungen zur Speicherzuteilung und zur Erfüllung anderer Bedürfnisse verwendet werden.

Asynchrone Rückforderung von freiem Speicherplatz im VMFS6-Datenspeicher

In VMFS6-Datenspeichern unterstützt ESXi die automatische asynchrone Rückforderung von freiem Speicherplatz. VMFS6 kann den Befehl „Zuordnung aufheben“ ausführen, um auf per Thin Provisioning bereitgestellten Speicher-Arrays, die Vorgänge zum Aufheben der Zuordnung unterstützen, im Hintergrund freien Speicherplatz freizugeben.

Die asynchrone Aufhebung der Zuordnung hat zahlreiche Nachteile:

- Anforderungen zum Aufheben der Zuordnung werden mit einer konstanten Häufigkeit gesendet. So lässt sich jegliche sofortige Belastung auf dem stützenden Array vermeiden.
- Die Aufhebung der Zuordnung und die Bündelung erfolgt für freigegebene Regionen gemeinsam.
- Die E/A-Leistung anderer Arbeitslasten wird durch den Befehl „Zuordnung aufheben“ nicht beeinträchtigt.

Für VMFS6-Datenspeicher können Sie die folgenden Parameter für die Speicherplatzrückforderung konfigurieren.

Granularität der Speicherplatzrückforderung

Die Granularität definiert die Mindestgröße eines freigegebenen Speicherplatzsektors, den zugrunde liegender Speicher zurückfordern kann. Sektoren, die kleiner sind als die angegebene Granularität, können vom Speicher nicht zurückgefordert werden.

Bei VMFS6 entspricht die Granularität der Rückforderung der Blockgröße. Wenn Sie als Blockgröße 1 MB angeben, ist die Granularität ebenfalls 1 MB. Speichersektoren, die kleiner als 1 MB sind, werden nicht zurückgefordert.

Hinweis Bei bestimmten Speicher-Arrays wird die optimale Granularität für die Aufhebung der Zuordnung empfohlen. ESXi unterstützt die automatische Aufhebung der Zuordnung der Verarbeitung auf Arrays mit der empfohlenen Granularität der Zuordnungsaufhebung von 1 MB oder höher, zum Beispiel 16 MB. In den Arrays mit der optimalen Granularität von 1 MB und weniger wird die Aufhebung der Zuordnung unterstützt, wenn die Granularität ein Faktor von 1 MB ist. Beispiel: 1 MB kann durch 512 Byte, 4 KB, 64 KB usw. geteilt werden.

Speicherplatzrückforderungsmethode

Die Methode kann entweder „Priorität“ oder „Fest“ sein. Wenn die eingesetzte Methode „Priorität“ ist, konfigurieren Sie die Prioritätsrate. Für die feste Methode müssen Sie die Bandbreite in MB pro Sekunde angeben.

Priorität der Speicherplatzrückforderung

Dieser Parameter definiert die Rate, mit der die Speicherplatzrückforderung durchgeführt wird, wenn Sie die Rückforderungsmethode Priorität verwenden. In der Regel sendet VMFS6 die Befehle zum Aufheben der Zuordnung entweder in Bursts oder sporadisch, je nach Arbeitslast und Konfiguration. Für VMFS6 können Sie eine der folgenden Optionen angeben.

Priorität der Speicherplatzrückforderung	Beschreibung	Konfiguration
Keine	Deaktiviert die Vorgänge zum Aufheben der Zuordnung für den Datenspeicher.	vSphere Client Befehl `esxcli`
Niedrig (Standard)	Sendet den Befehl „Zuordnung aufheben“ mit einer weniger häufigen Rate: 25–50 MB pro Sekunde.	vSphere Client Befehl `esxcli`
Mittel	Sendet den Befehl mit einer Rate, die doppelt so schnell wie die niedrige Rate ist: 50–100 MB pro Sekunde.	Befehl `esxcli`
Hoch	Sendet den Befehl mit einer Rate, die drei Mal so schnell wie die niedrige Rate ist: über 100 MB pro Sekunde.	Befehl `esxcli`

Hinweis Der ESXi-Host der Version 6.5 erkennt keine Raten mittlerer und hoher Priorität. Wenn Sie die VMs auf die Hostversion 6.5 migrieren, wird die Rate standardmäßig auf niedrig gesetzt.

Nach der Aktivierung der Speicherplatzrückforderung kann der VMFS6-Datenspeicher mit der Freigabe der Blöcke nicht genutzten Speicherplatzes nur dann beginnen, wenn er über mindestens eine geöffnete Datei verfügt. Diese Bedingung kann erfüllt werden, wenn Sie beispielsweise eine der VMs im Datenspeicher einschalten.

Manuelle Rückforderung von freiem Speicherplatz im VMFS5-Datenspeicher

VMFS5 und frühere Dateisysteme führen keine automatische Aufhebung der Zuordnung von freiem Speicherplatz durch. Sie können Speicherplatz jedoch manuell mit dem Befehl `esxcli storage vmfs unmap` zurückfordern. Denken Sie bei der Verwendung dieses Befehls daran, dass er möglicherweise viele Anforderungen zur Aufhebung der Zuordnung auf einmal sendet. Dadurch werden während des Vorgangs ggf. einige Ressourcen gesperrt.

Konfigurieren der Speicherplatzrückforderung für einen VMFS6-Datenspeicher

Wenn Sie einen VMFS6-Datenspeicher erstellen, können Sie die Standardparameter für die automatische Speicherplatzrückforderung ändern.

Zum Zeitpunkt der Erstellung des VMFS6-Datenspeichers ist als einzige Methode für die Speicherplatzrückforderung „Priorität“ verfügbar. Um die Methode „Fest“ zu verwenden, müssen Sie die Einstellungen für die Speicherplatzrückforderung für den Datenspeicher bearbeiten.

Verfahren

1. Navigieren Sie im vSphere Client-Objektnavigator zu einem Host, Cluster oder Datencenter.
2. Wählen Sie im Kontextmenü **Speicher > Neuer Datenspeicher** aus.
3. Führen Sie die Schritte zum Erstellen eines VMFS6-Datenspeichers durch.

4 Geben Sie auf der Seite **Partitionskonfiguration** die Parameter für die Speicherplatzrückforderung an.

Die Parameter definieren die Granularität und die Prioritätsrate, mit der die Vorgänge zur Speicherplatzrückforderung durchgeführt werden. Auf dieser Seite können Sie die Speicherplatzrückforderung für den Datenspeicher auch deaktivieren.

Option	Beschreibung
Blockgröße	Die Blockgröße in einem VMFS-Datenspeicher bestimmt die maximale Dateigröße und den Speicherplatz, den die Datei einnimmt. VMFS6 unterstützt eine Blockgröße von 1 MB.
Granularität der Speicherplatzrückforderung	Gibt die Granularität des Vorgangs zum Aufheben der Zuordnung an. Die Granularität der Aufhebung der Zuordnung entspricht der Blockgröße, d. h. 1 MB. Speichersektoren, die kleiner als 1 MB sind, werden nicht zurückgefordert.
Priorität der Speicherplatzrückforderung	Wählen Sie eine der folgenden Optionen aus. ■ Niedrig (Standard) Verwenden Sie die Prioritätsmethode für die Speicherplatzrückforderung. Aktivieren Sie den Vorgang zum Aufheben mit niedriger Prioritätsrate. ■ Keine. Wählen Sie diese Option aus, wenn Sie die Vorgänge zur Speicherplatzrückforderung für den Datenspeicher deaktivieren möchten.

Hinweis Im vSphere Client sind für die Priorität der Speicherrückforderung nur zwei Optionen verfügbar: „Niedrig“ und „Keine“. Um die Einstellungen in „Mittel“ oder „Hoch“ zu ändern, müssen Sie den Befehl `esxcli` verwenden. Weitere Informationen hierzu finden Sie unter Verwenden des ESXCLI-Befehls zum Ändern von Speicherplatzrückforderungsparametern.

5 Schließen Sie das Erstellen des Datenspeichers ab.

Ergebnisse

Nach der Aktivierung der Speicherplatzrückforderung kann der VMFS6-Datenspeicher mit der Freigabe der Blöcke nicht genutzten Speicherplatzes nur dann beginnen, wenn er über mindestens eine geöffnete Datei verfügt. Diese Bedingung kann erfüllt werden, wenn Sie beispielsweise eine der VMs im Datenspeicher einschalten.

Ändern der Einstellungen für die Speicherplatzrückforderung

Wenn Sie einen VMFS6-Datenspeicher in vSphere Client erstellen, können Sie als einzige Methode für die Speicherplatzrückforderung „Priorität“ angeben. Um die Methode „Fest“ zu aktivieren, müssen Sie die Einstellungen für die Speicherplatzrückforderung für den bestehenden Datenspeicher ändern.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

2 Wählen Sie im Kontextmenü die Option **Speicherplatzrückforderung bearbeiten** aus.

3 Geben Sie die Einstellung für die Speicherplatzrückforderung an.

Option	Beschreibung
Automatische Speicherplatzrückforderung zu fester Rate aktivieren	Verwenden Sie die feste Methode für die Speicherplatzrückforderung. Geben Sie Rückforderungsbandbreite in MB pro Sekunde an.
Automatische Speicherplatzrückforderung deaktivieren	Gelöschte oder nicht zugeordnete Blöcke werden nicht zurückgefordert.

4 Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.

5 Führen Sie den Datenspeicher aus, damit die Änderungen durchgeführt werden.

a Unmounten von Datenspeichern.

b Mounten von Datenspeichern.

6 Wiederholen Sie diesen Vorgang für alle ESXi-Hosts, die auf den Datenspeicher zugreifen.

Ergebnisse

Der geänderte Wert für die Priorität der Speicherplatzrückforderung wird auf der Seite **Allgemein** des Datenspeichers angezeigt.

Verwenden des ESXCLI-Befehls zum Ändern von Speicherplatzrückforderungsparametern

Sie können die standardmäßige Priorität der Speicherplatzrückforderung, die Granularität und andere Parameter ändern.

Verfahren

1 Verwenden Sie für den ESXi-Host folgenden Befehl zum Festlegen von Rückforderungsparametern.

```
esxcli storage vmfs reclaim config set
```

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
-b|--reclaim-bandwidth	Feste Bandbreite zur Speicherplatzrückforderung in MB pro Sekunde.
-g|--reclaim-granularity	Minimale Granularität der automatischen Speicherplatzrückforderung in Byte.
-m|--reclaim-method	Die Methode der automatischen Speicherplatzrückforderung. Unterstützte Optionen: ■ priority ■ Fest

Option	Beschreibung
-p|--reclaim-priority	Priorität der automatische Speicherplatzrückforderung. Unterstützte Optionen: ■ keine ■ low ■ medium ■ high
-l|--volume-label	Die Bezeichnung des VMFS-Ziel-Volumes.
-u|--volume-uuid	Die UUID des VMFS-Ziel-Volumes.

Sie können die folgenden Beispiele verwenden.

- Legen Sie die Rückforderungsmethode auf „Fest“ und die Rate auf 100 MB/s fest.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-method
fixed -b 100
```

- Deaktivieren Sie die automatische Speicherplatzrückforderung für VMFS.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-
priority none
```

2 Unmounten Sie den VMFS6-Datenspeicher von allen anderen ESXi-Hosts, auf denen der Datenspeicher gemountet ist, und mounten Sie ihn dann erneut.

a Unmounten von Datenspeichern.

b Mounten von Datenspeichern.

Dieser Schritt stellt sicher, dass alle ESXi-Hosts, auf denen der VMFS6-Datenspeicher gemountet wurde, zur Rückforderungsmethode „Fest“ für den Datenspeicher wechseln.

Überprüfen der Einstellungen für die automatische Speicherplatzrückforderung

Nachdem Sie die Parameter der Speicherplatzrückforderung für einen VMFS6-Datenspeicher konfiguriert oder bearbeitet haben, können Sie Ihre Einstellungen überprüfen.

Verfahren

1 Navigieren Sie im vSphere Client zum Datenspeicher.

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

3 Klicken Sie auf **Allgemein** und überprüfen Sie die Einstellungen für die Speicherplatzrückforderung.

a Erweitern Sie unter „Eigenschaften“ den Eintrag **Dateisystem** und überprüfen Sie den Wert für die Granularität der Speicherplatzrückforderung.

b Überprüfen Sie unter „Speicherplatzrückforderung“ die Einstellung für die Priorität der Speicherplatzrückforderung.

Wenn Sie Werte über den Befehl `esxcli` konfiguriert haben, z. B. Medium oder High für die Priorität der Speicherplatzrückforderung, werden diese Werte auch im vSphere Client angezeigt.

Beispiel: Abrufen von Parametern für die VMFS6-Speicherplatzrückforderung

Mit dem Befehl **`esxcli storage vmfs reclaim config get -l=VMFS_bezeichnung|-u=VMFS_uuid`** können Sie ebenfalls Informationen für die Konfiguration der Speicherplatzrückforderung abrufen.

```
# esxcli storage vmfs reclaim config get -l my_datastore
Reclaim Granularity: 1048576 Bytes
Reclaim Priority: low
```

Manuelles Rückfordern von angesammeltem Speicherplatz

Auf VMFS-Datenspeichern, die die automatische Speicherplatzrückforderung nicht unterstützen, können Sie den Befehl `esxcli` verwenden, um nicht genutzten Speicherplatz manuell zurückzufordern.

Voraussetzungen

Installieren Sie ESXCLI. Siehe *Erste Schritte mit ESXCLI*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Führen Sie den folgenden Befehl aus, um nicht genutzte Speicherblöcke auf dem per Thin Provisioning bereitgestellten Gerät zurückzufordern:

`esxcli storage vmfs unmap`

Der Befehl verfügt über diese Optionen:

Option	Beschreibung
`-l|--volume-label=volume_bezeichnung`	Die Bezeichnung des VMFS-Volumes, dessen Zuordnung aufgehoben werden soll. Dies ist ein erforderliches Argument. Verwenden Sie bei Angabe dieses Arguments nicht **`-u|--volume-uuid=volume_uuid`**.
`-u|--volume-uuid=volume_uuid`	Die UUID des VMFS-Volumes, dessen Zuordnung aufgehoben werden soll. Dies ist ein erforderliches Argument. Verwenden Sie bei Angabe dieses Arguments nicht **`-l|--volume-label=volume_bezeichnung`**.
`-n|--reclaim-unit=anzahl`	Die Anzahl der VMFS-Blöcke, deren Zuordnung pro Iteration aufgehoben werden soll. Dies ist ein optionales Argument. Wenn es nicht angegeben wird, verwendet der Befehl den Standardwert 200.

2 Um zu überprüfen, ob die Aufhebung der Zuordnung abgeschlossen ist, suchen Sie in der Datei `vmkernel.log` nach „unmap“.

Speicherplatzrückforderungen von Gastbetriebssystemen

ESXi unterstützt die Befehle vom Typ „Zuordnung aufheben“, die direkt von einem Gastbetriebssystem ausgegeben werden, um Speicherplatz zurückzufordern. Der Grad der Unterstützung und die Anforderungen richten sich nach dem Typ des Datenspeichers, in dem sich die virtuelle Maschine befindet.

Innerhalb einer virtuellen Maschine wird Speicherplatz freigegeben, wenn Sie beispielsweise Dateien auf der virtuellen Festplatte im Thin-Format löschen. Das Gastbetriebssystem benachrichtigt VMFS über den freigegebenen Speicherplatz, indem der Befehl „Zuordnung aufheben“ gesendet wird. Durch den vom Gastbetriebssystem gesendeten Befehl „Zuordnung aufheben“ wird Speicherplatz im VMFS-Datenspeicher freigegeben. Der Befehl wird dann für das Array ausgeführt, sodass das Array die freigegebenen Speicherplatzblöcke zurückfordern kann.

Speicherplatzrückforderung für virtuelle VMFS6-Maschinen

VMFS6 unterstützt grundsätzlich die von Gastbetriebssystemen generierte automatische Speicherplatzrückforderung und übergibt diese Anforderungen an das Array. Viele Gastbetriebssysteme können den Befehl „Zuordnung aufheben“ senden und benötigen keinerlei weitere Konfiguration. Bei Gastbetriebssystemen, die keine automatische Aufhebung der Zuordnung unterstützen, muss möglicherweise der Benutzer eingreifen. Informationen über Gastbetriebssysteme, die die automatische Speicherplatzrückforderung auf VMFS6 unterstützen, erhalten Sie bei Ihrem Anbieter.

Generell sendet das Gastbetriebssystem die Befehle zum Aufheben der Zuordnung basierend auf ihrer entsprechenden Granularität. Nähere Informationen finden Sie in der Dokumentation zum Gastbetriebssystem.

Bei der Verwendung der Speicherplatzrückforderung mit VMFS6 muss Folgendes beachtet werden:

- VMFS6 verarbeitet die Anforderung zum Aufheben der Zuordnung vom Gastbetriebssystem nur dann, wenn der zurückzufordernde Speicherplatz 1 MB oder ein Mehrfaches von 1 MB beträgt. Wenn der Speicherplatz weniger als 1 MB beträgt oder kein Mehrfaches von 1 MB ist, werden die Anforderungen zur Aufhebung der Zuordnung nicht verarbeitet.
- Bei virtuellen Maschinen mit Snapshots im standardmäßigen SEsparse-Format unterstützt VMFS6 die automatische Speicherplatzrückforderung nur auf ESXi-Hosts der Version 6.7 oder höher.

  Die Speicherplatzrückforderung betrifft nur den obersten Snapshot und funktioniert, wenn die virtuelle Maschine eingeschaltet ist.

Speicherplatzrückforderung für virtuelle VMFS5-Maschinen

In der Regel kann der vom Gastbetriebssystem in VMFS5 generierte Befehl „Zuordnung aufheben“ nicht direkt an das Array übergeben werden. Sie müssen den Befehl `esxcli storage vmfs unmap` ausführen, um Zuordnungsaufhebungen für das Array auszulösen.

Für eine begrenzte Anzahl von Gastbetriebssystemen unterstützt VMFS5 jedoch Anforderungen zur automatischen Speicherplatzrückforderung.

Um die Anforderungen zum Aufheben der Zuordnung vom Gastbetriebssystem an das Array zu senden, muss die virtuelle Maschine die folgenden Voraussetzungen erfüllen:

- Die virtuelle Festplatte muss per Thin Provisioning bereitgestellt werden.
- Die virtuelle Maschine muss über die Hardwareversion 11 (ESXi 6.0) oder höher verfügen.
- Die erweiterte Einstellung „EnableBlockDelete“ muss auf „1“ gesetzt werden.
- Das Gastbetriebssystem muss die virtuelle Festplatte als Thin-Festplatte identifizieren können.

Erste Schritte mit Cloud Native Storage

26

Bei Cloud Native Storage handelt es sich um eine Lösung, die umfassende Datenverwaltung für statusbehaftete Anwendungen bereitstellt. Mithilfe von Cloud Native Storage können Sie statusbehaftete Containeranwendungen erstellen, die bei Neustarts und Ausfällen bestehen bleiben. Statusbehaftete Container nutzen von vSphere bereitgestellten Speicher, während sie Primitive wie Standarddatenträger, persistentes Volume und dynamische Bereitstellung verwenden.

Mit Cloud Native Storage können Sie persistente Container-Volumes unabhängig vom Lebenszyklus der virtuellen Maschine oder des Containers erstellen. vSphere Storage unterstützt die Volumes, und Sie können eine Speicherrichtlinie direkt auf den Volumes festlegen. Nach der Erstellung der Volumes können Sie diese und die unterstützenden Speicherobjekte im vSphere Client überprüfen und überwachen, ob sie die Speicherrichtlinie einhalten.

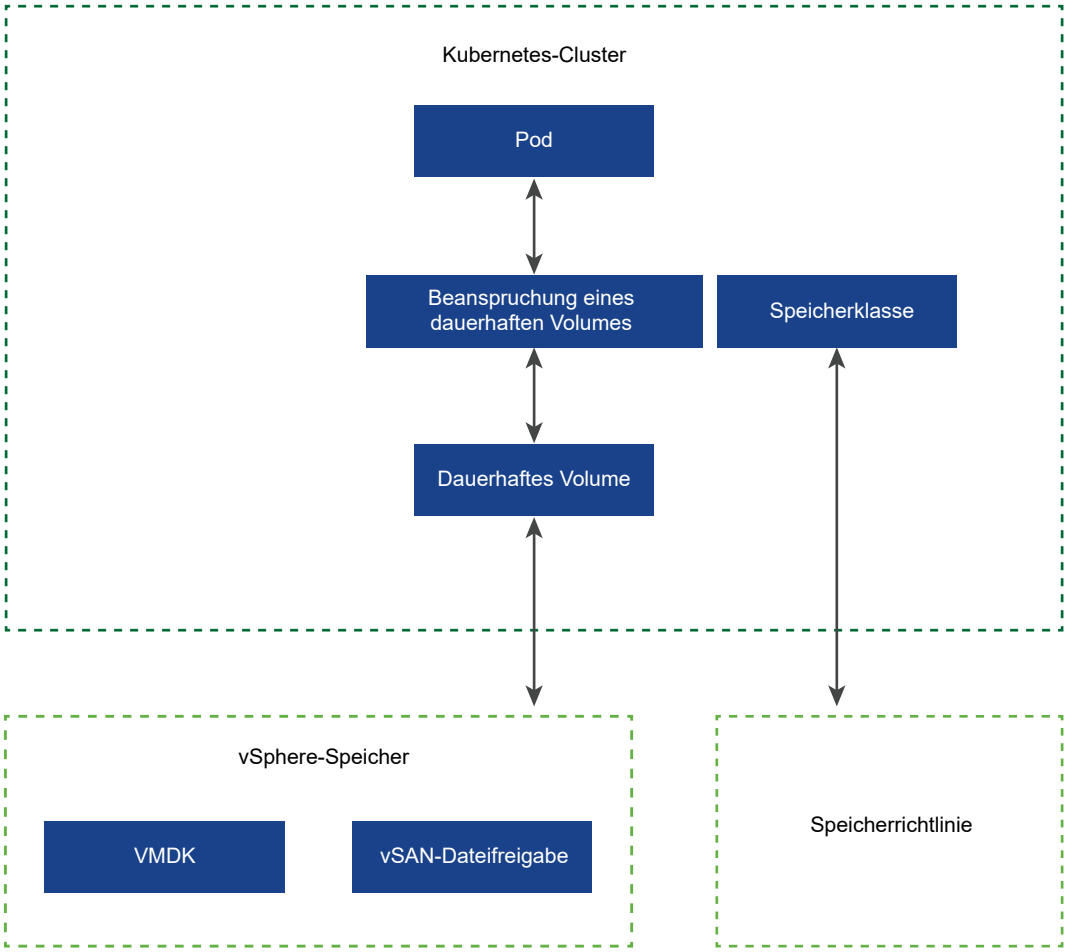
vSphere Cloud Native Storage unterstützt persistente Volumes in den folgenden Kubernetes-Distributionen:

- Generisches Kubernetes, auch als „Vanilla“ bezeichnet, das über die offiziellen Repositorys installiert wird. Diese Dokumentation zu *vSphere-Speicher* beschäftigt sich ausschließlich mit generischem Kubernetes.
- vSphere with Tanzu. Weitere Informationen finden Sie in der Dokumentation *vSphere with Tanzu-Konfiguration und -Verwaltung*.

Dieses Kapitel enthält die folgenden Themen:

Cloud Native Storage – Konzepte und Terminologie

Machen Sie sich mit verschiedenen Konzepten vertraut, die für vSphere Cloud Native Storage-Umgebungen unerlässlich sind.



Kubernetes-Cluster

In der Cloud Native Storage-Umgebung können Sie einen generischen Kubernetes-Cluster in einem VM-Cluster bereitstellen. Zusätzlich zum Kubernetes-Cluster stellen Sie Ihre Containeranwendungen bereit. Anwendungen können statusbehaftet und statusfrei sein.

Hinweis Informationen zu Supervisor- und TKG-Clustern, die in vSphere with Tanzu ausgeführt werden können, finden Sie in der Dokumentation zu *vSphere with Tanzu-Konfiguration und -Verwaltung*.

Pod

Bei einem Pod handelt es sich um eine Gruppe aus einer oder mehreren Containeranwendungen, die Ressourcen wie Speicher und Netzwerk gemeinsam nutzen. Container in einem Pod werden als Gruppe gestartet, angehalten und repliziert.

Container-Orchestrator

Open-Source-Plattformen, wie beispielsweise Kubernetes, für die Bereitstellung, Skalierung und Verwaltung von Containeranwendungen zwischen Hostclustern. Die Plattformen stellen eine containerorientierte Infrastruktur bereit.

Statusbehaftete Anwendung

Da sich Containeranwendungen von statusbehaftet zu statusfrei entwickeln, benötigen sie persistenten Speicher. Im Gegensatz zu statusfreien Anwendungen, die keine Daten zwischen Sitzungen speichern, speichern statusbehaftete Anwendungen Daten im persistenten Speicher. Die gespeicherten Daten werden als Anwendungsstatus bezeichnet. Sie können die Daten später abrufen und in der nächsten Sitzung verwenden. Die meisten Anwendungen sind statusbehaftet. Eine Datenbank ist ein Beispiel für eine statusbehaftete Anwendung.

PersistentVolume

Statusbehaftete Anwendungen verwenden PersistentVolumes zum Speichern der Daten. Bei einem PersistentVolume handelt es sich um ein Kubernetes-Volume, das seinen Status und seine Daten beibehalten kann. Es ist unabhängig von einem Pod und kann auch dann weiterhin bestehen, wenn der Pod gelöscht oder neu konfiguriert wird. In der vSphere-Umgebung verwenden die PersistentVolume-Objekte virtuelle vSphere-Festplatten vom Typ FCD (First Class Disk) oder vSAN-Dateifreigaben als Hintergrundspeicher. First Class Disks werden auch als verbesserte virtuelle Festplatten (Improved Virtual Disk, IVD) oder verwaltete virtuelle Festplatten bezeichnet.

- Virtuelle Festplatten unterstützen Volumes, die als ReadWriteOnce gemountet sind. Diese Volumes können nur von einem einzelnen Pod in Kubernetes verwendet werden.

  Ab vSphere 7.0 können Sie die vSphere-Verschlüsselungstechnologie verwenden, um virtuelle FCD-Festplatten zu schützen, die persistente Volumes sichern. Weitere Informationen finden Sie unter Verwenden der Verschlüsselung mit cloudnativem Speicher.

- vSAN-Dateifreigaben unterstützen ReadWriteMany-Volumes, die von vielen Knoten gemountet werden. Diese Volumes können von mehreren Pods oder Anwendungen gemeinsam genutzt werden, die über Kubernetes-Knoten oder über Kubernetes-Cluster hinweg ausgeführt werden. Informationen zu möglichen Konfigurationen mit Dateifreigaben finden Sie unter Verwenden des vSAN-Dateidiensts zur Bereitstellung von Datei-Volumes.

StorageClass

Kubernetes verwendet eine StorageClass, um verschiedene Speicherebenen zu definieren und verschiedene Arten von Anforderungen für Speicher-Backing des PersistentVolume zu beschreiben. In der vSphere-Umgebung kann eine Speicherklasse mit einer Speicherrichtlinie verknüpft werden. Als vSphere-Administrator erstellen Sie Speicherrichtlinien, die verschiedene Speicheranforderungen beschreiben. Die VM-Speicherrichtlinien können als Teil der Speicherklassendefinition für die Bereitstellung dynamischer Volumes verwendet werden.

Die folgende YAML-Datei referenziert die Speicherrichtlinie **`Gold`**, die Sie zuvor mithilfe des vSphere Client erstellt haben. Die resultierende VMDK des persistenten Volumes wird auf einem kompatiblen Datenspeicher platziert, der den Anforderungen der Speicherrichtlinie **`Gold`** entspricht.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gold-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.vsphere.vmware.com
parameters:
  storagepolicyname: "Gold"
```

PersistentVolumeClaim

In der Regel können Anwendungen oder Pods persistenten Speicher über einen PersistentVolumeClaim anfordern. PersistentVolumeClaim gibt Typ und Speicherklasse, den Zugriffsmodus (entweder ReadWriteOnce oder ReadWriteMany) und andere Parameter für den PersistentVolume an. Die Anforderung kann das entsprechende PersistentVolume-Objekt und die zugrunde liegende virtuelle Festplatte oder vSAN-Dateifreigabe dann dynamisch in der vSphere-Umgebung bereitstellen.

Nach Erstellung des Anspruchs ist das PersistentVolume automatisch an den Anspruch gebunden. Pods verwenden den Anspruch zum Mounten des PersistentVolume und für den Zugriff auf den Speicher.

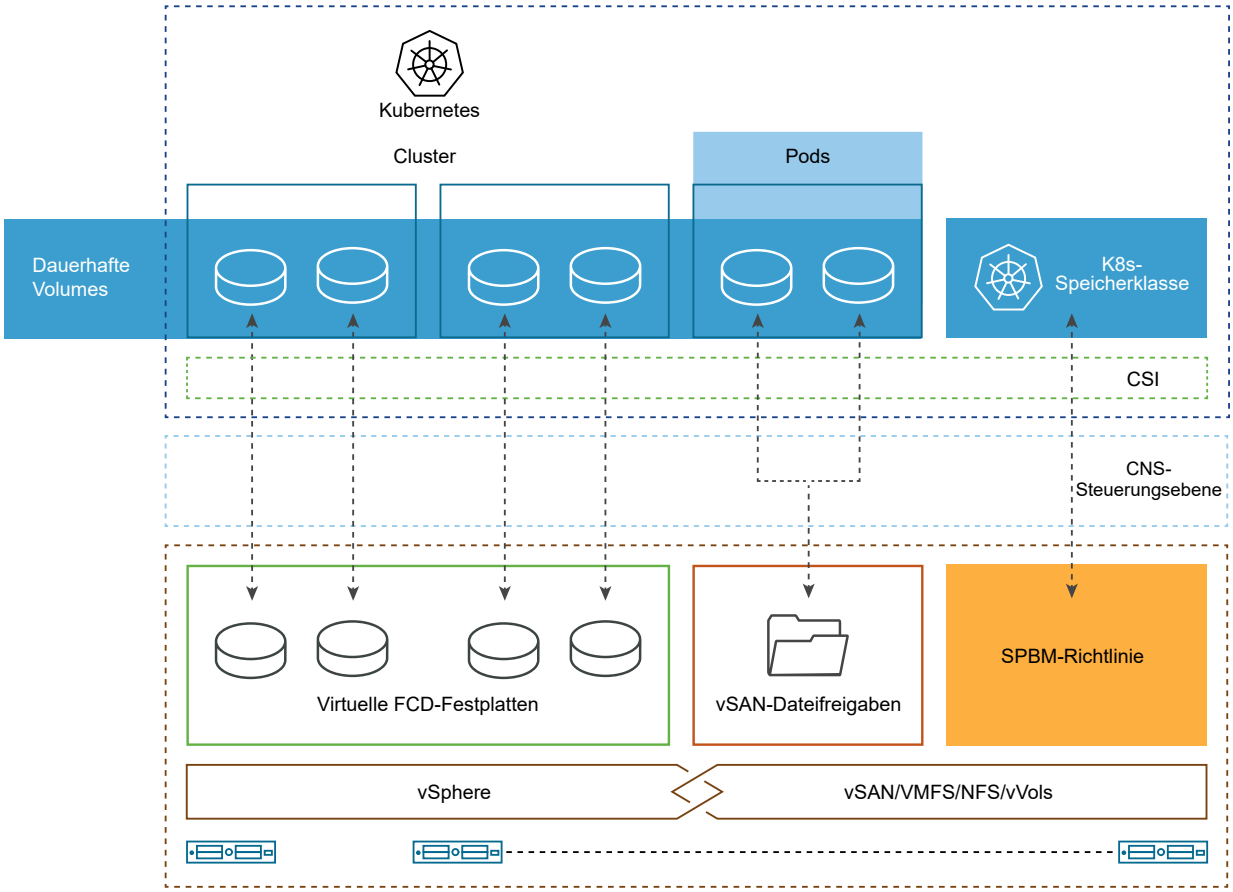
Wenn Sie diesen Anspruch löschen, werden das entsprechende PersistentVolume-Objekt und der zugrunde liegende Speicher gelöscht.

```
kind: PersistentVolumeClaim
metadata:
 name: persistent-VMDK
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 5Gi
 storageClassName: gold-sc
```

Komponenten für Cloud Native Storage

Cloud Native Storage verwendet mehrere Komponenten für die Integration in vSphere Storage.

Die folgende Abbildung zeigt die Interaktion zwischen diesen Komponenten.



Kubernetes-Cluster

In der Cloud Native Storage-Umgebung wird ein generischer Kubernetes-Cluster in einem VM-Cluster oder auf Knoten bereitgestellt, die in vSphere ausgeführt werden. Ein Kubernetes-Benutzer interagiert direkt mit dem Cluster, wenn er zusätzlich statusbehaftete Anwendungen bereitstellt.

Hinweis Informationen zu Supervisor- und TKG-Clustern, die in vSphere with Tanzu ausgeführt werden können, finden Sie in der Dokumentation zu *vSphere with Tanzu-Konfiguration und -Verwaltung*.

Container Storage Interface (CSI) für vSphere

Um zugrunde liegende Infrastrukturressourcen zu nutzen, benötigt der Cluster einen CSI-Treiber.

Die vSphere CSI ist ein Out-of-Tree-Plug-In, das die vSphere-Speicher für containerbasierte Arbeitslasten auf Container-Orchestratoren wie z. B. Kubernetes bereitstellt. Das Plug-In aktiviert vSAN und andere Arten von vSphere-Speicher.

vSphere-CSI kommuniziert für alle Speicherbereitstellungsvorgänge mit der CNS-Steuerungsebene in vCenter Server. Die vSphere CSI unterstützt die folgenden Funktionen:

- Dynamische Bereitstellung von Container-Volumes.

- Die FCD-Funktion (First Class Disk, Erstklassige Festplatte) von vSphere.
- Kubernetes-Zonen.
- Herkömmliche und Raw-Mounts.
- Einzelne vCenter Server und mehrere Datencenter und Cluster.
- Bereitstellung aus mehreren Datenspeichern oder Datenspeicher-Clustern.
- vSAN-Dateidienst

Auf Kubernetes wird der CSI-Treiber mit der Out-of-Tree-CPI (Cloud Provider Interface) von vSphere verwendet. Der CSI-Treiber wird als Container-Image ausgeliefert und muss vom Clusteradministrator bereitgestellt werden. Weitere Informationen finden Sie im Abschnitt Driver Deployment der Dokumentation mit dem Namen Kubernetes vSphere CSI Driver in GitHub.

Informationen zu den in Supervisor- und TKG-Clustern verwendeten CSI-Varianten, die in vSphere with Tanzu ausgeführt werden können, finden Sie in der Dokumentation zu *vSphere with Tanzu-Konfiguration und -Verwaltung*.

Cloud Native Storage-Serverkomponente

Die CNS-Serverkomponente oder die CNS-Steuerungsebene befindet sich in vCenter Server. Es handelt sich um eine Erweiterung der vCenter Server-Verwaltung, die die Bereitstellungs- und Lebenszyklusvorgänge für die Container-Volumes implementiert.

Bei der Bereitstellung von Container-Volumes interagiert die Komponente mit vCenter Server, um Speicherobjekte zur Unterstützung der Volumes zu erstellen. Die Funktion „Speicherrichtlinienbasierte Verwaltung“ gewährleistet die erforderliche Dienstebene für die Volumes.

Der CNS führt auch Abfragevorgänge aus, mit denen Sie Container-Volumes und deren unterstützende Speicherobjekte über vCenter Server verwalten und überwachen können.

Erstklassige Festplatte (First Class Disk, FCD)

Wird auch als verbesserte virtuelle Festplatte (Improved Virtual Disk, IVD) oder verwaltete virtuelle Festplatte bezeichnet. Es handelt sich um eine benannte virtuelle Festplatte, die mit keiner VM verknüpft ist. Diese Festplatten befinden sich auf einem vSAN-, VMFS-, NFS- oder vVols-Datenspeicher und unterstützen ReadWriteOnce-Container-Volumes.

Mit der FCD-Technologie können Lebenszyklusvorgänge im Zusammenhang mit dauerhaften Volumes außerhalb des VM- oder Pod-Lebenszyklus durchgeführt werden. Wenn es sich bei der VM um einen Kubernetes-Knoten handelt, der mehrere containerbasierte Anwendungen ausführt und dauerhafte Volumes und virtuelle Festplatten für viele Anwendungen verwendet, vereinfacht CNS die Lebenszyklusvorgänge im Container und die Granularität des dauerhaften Volumes.

vSAN-Dateidienst

Es handelt sich um eine vSAN-Ebene, die Dateifreigaben bereitstellt. Aktuell werden NFSv3- und NFSv4.1-Dateifreigaben unterstützt. Cloud Native Storage verwendet vSAN-Dateifreigaben für persistente Volumes vom Typ „ReadWriteMany“. Ein einzelnes ReadWriteMany-Volume kann von mehreren Knoten gemountet werden. Das Volume kann zwischen mehreren Pods oder Anwendungen freigegeben werden, die auf Kubernetes-Knoten oder Kubernetes-Clustern ausgeführt werden.

Speicherrichtlinienbasierte Verwaltung

Bei der speicherrichtlinienbasierten Verwaltung handelt es sich um einen vCenter Server-Dienst, der die Bereitstellung persistenter Volumes gemäß den angegebenen Speicheranforderungen unterstützt. Nach der Bereitstellung überwacht der Dienst, ob das Volume die erforderlichen Richtlinieneigenschaften einhält.

Verwenden des vSAN-Dateidiensts zur Bereitstellung von Datei-Volumes

Der vSAN-Dateidienst bietet vSAN-Dateifreigaben an, die von dauerhaften Volumes des Typs ReadWriteMany (RWM) verbraucht werden. Ein einzelnes RWM-Volume kann von mehreren Knoten bereitgestellt werden. Das Volume kann zwischen mehreren Pods oder Anwendungen freigegeben werden, die auf Kubernetes-Knoten oder Kubernetes-Clustern ausgeführt werden.

Wenn ein Kubernetes-Pod ein RWM-Volume anfordert, kommuniziert Cloud Native Storage mit dem vSAN-Dateidienst, um eine auf NFS basierte Dateifreigabe der angeforderten Größe und Speicherklasse zu erstellen. Cloud Native Storage stellt dann das RWM-Volume an den Kubernetes-Worker-Knoten bereit, auf dem der Pod ausgeführt wird. Wenn mehrere Knoten Zugriff auf das RWM-Volume anfordern, bestimmt Cloud Native Storage, dass das RWM-Volume für diese bestimmte Bereitstellung bereits vorhanden ist, und stellt das vorhandene Volume in den Knoten bereit.

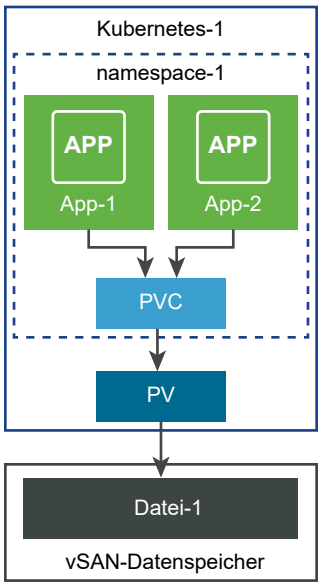
Damit RWM-Volumes unterstützt werden, muss Ihre Umgebung die folgenden Elemente enthalten.

- vSphere 7.0 und höher mit vSAN
- vSAN-Dateidienst aktiviert. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.
- Kubernetes Version 1.14 und höher
- Kompatible Version von CSI. Weitere Informationen finden Sie in der Dokumentation zum Kubernetes vSphere CSI-Treiber in GitHub.

Sie können verschiedene Konfigurationen für Datei-Volumes verwenden.

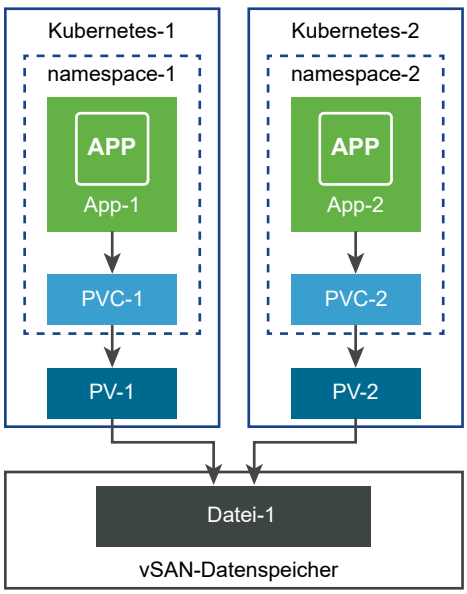
Einzelnes Datei-Volume, das von mehreren Anwendungen im selben Namespace gemeinsam genutzt wird

In diesem Beispiel wird ein einzelnes Datei-Volume als gemeinsam genutzter Speicher für verschiedene Anwendungen im selben Namespace verwendet. Sie verwenden einen einzelnen Anspruch für einen dauerhaften Datenträger, um das Datei-Volume bereitzustellen.



Einzelnes Datei-Volume, das für Anwendungen und Namespaces gemeinsam genutzt wird

In diesem Beispiel wird ein einzelnes Datei-Volume als gemeinsam genutzter Speicher für verschiedene Anwendungen und verschiedene Namespaces verwendet. Für jeden Namespace erstellen Sie einen separaten Anspruch für einen dauerhaften Datenträger, um dasselbe Datei-Volume bereitzustellen.



Cloud Native Storage-Benutzer

Die Benutzertypen, die an der Erstellung und Überwachung von Kubernetes-Volumes in der vSphere Cloud Native Storage-Umgebung beteiligt sind, werden in der Regel in zwei Kategorien

unterteilt: Kubernetes-Benutzer und vSphere-Administrator. Beide Benutzertypen haben Zugriff auf verschiedene Tools und führen verschiedene Aufgaben aus.

CNS-Kubernetes-Benutzer

Der Kubernetes-Benutzer kann als Kubernetes-Entwickler und Anwendungsbesitzer oder als Kubernetes-Administrator fungieren. Eine Kombination beider Funktionen ist auch möglich. Zu den Aufgaben, die vom Kubernetes-Benutzer in der Cloud Native Storage-Umgebung ausgeführt werden, gehören:

- Stellen Sie die vSphere-CSI bereit und verwalten Sie sie. Weitere Informationen finden Sie im Abschnitt vSphere Container Storage Plug-in Deployment der Dokumentation Getting Started with VMware vSphere Container Storage Plug-in.
- Bereitstellen persistenter Volumes. Informationen zu Block-Volumes finden Sie unter vSphere-CSI-Treiber - Block-Volume. Informationen zu Datei-Volumes finden Sie unter vSphere-CSI-Treiber - Datei-Volume.
- Durchführen von Lebenszyklusvorgängen für persistente Volumes.
- Durchführen von Lebenszyklusvorgängen für Speicherklassen.

CNS-vSphere-Benutzer

Ein CNS-vSphere-Benutzer oder ein vSphere-Administrator hat Zugriff auf den vSphere Client, um die folgenden Aufgaben durchzuführen:

- Durchführen von Lebenszyklusvorgängen für die VM-Speicherrichtlinien. Erstellen Sie beispielsweise eine VM-Speicherrichtlinie, die für eine Kubernetes-Speicherklasse verwendet werden soll, und übermitteln Sie den Namen der Richtlinie an den Kubernetes-Benutzer. Weitere Informationen hierzu finden Sie unter Erstellen einer Speicherrichtlinie für Kubernetes.
- Verwenden Sie den Abschnitt „Cloud Native Storage“ des vSphere Client, um die Einhaltung der Speicherrichtlinien für die Container-Volumes und den Zustand der Volumes in den Kubernetes-Clustern zu überwachen. Weitere Informationen hierzu finden Sie unter Überwachen von Container-Volumes in Kubernetes-Clustern.

Cloud Native Storage für vSphere-Administratoren

Ein vSphere-Administrator stellt Speicherressourcen für das Kubernetes-Team bereit und erstellt VM-Speicherrichtlinien, die unterschiedliche Speicheranforderungen und Dienstklassen beschreiben. Nachdem die Arbeitslasten von Kubernetes mit persistentem Speicher bereitgestellt wurden, kann der vSphere-Administrator den Lebenszyklus der zugrundeliegenden Speicherressourcen und deren Konformität mit den Anforderungen überwachen.

Anforderungen für Cloud Native Storage

Ihre Cloud Native Storage-Umgebung und die virtuellen Maschinen, die zum Kubernetes-Cluster gehören, müssen mehrere Anforderungen erfüllen.

Anforderungen für Cloud Native Storage

- vSphere 6.7 Update 3 oder höher.
- Eine kompatible Version von Kubernetes.
- Ein auf den virtuellen Maschinen bereitgestellter Kubernetes-Cluster. Ausführliche Informationen zum Bereitstellen des vSphere-CSI-Plug-Ins sowie zum Ausführen des Kubernetes-Clusters unter vSphere finden Sie im Abschnitt Driver Deployment der Dokumentation in GitHub.

Anforderungen für virtuelle Maschinen des Kubernetes-Clusters

- Virtuelle Maschinen mit Hardware Version 15 oder höher. Installieren Sie VMware Tools auf jeder Knoten-VM.
- VM-Hardwareempfehlungen
  - Legen Sie die CPU und den Arbeitsspeicher basierend auf den Arbeitslastanforderungen angemessen fest.
  - Verwenden Sie den VMware Paravirtual SCSI-Controller für die primäre Festplatte auf der Knoten-VM.
- Alle virtuellen Maschinen müssen Zugriff auf einen gemeinsam genutzten Datenspeicher haben, wie z. B. vSAN.
- Legen Sie den Parameter `disk.EnableUUID` auf jeder Knoten-VM fest. Weitere Informationen hierzu finden Sie unter Konfigurieren der virtuellen Maschinen des Kubernetes-Clusters.
- Um Fehler und unvorhersehbares Verhalten zu vermeiden, sollten Sie keine Snapshots von CNS-Knoten-VMs erstellen.

Anforderungen für das CNS-Datei-Volume

- Verwenden Sie vSphere 7.0 oder höher mit einer kompatiblen Kubernetes-Version.
- Verwenden Sie eine kompatible Version von CSI. Weitere Informationen finden Sie in der Dokumentation zum Kubernetes vSphere CSI-Treiber in GitHub.
- Aktivieren und konfigurieren Sie den vSAN-Dateidienst. Sie müssen u. a. die erforderlichen Dateidienstdomänen, IP-Adressen und das Netzwerk konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.
- Befolgen Sie die spezifischen Richtlinien zum Konfigurieren des Netzwerkzugriffs von einem Gastbetriebssystem im Kubernetes-Knoten auf eine vSAN-Dateifreigabe. Weitere Informationen hierzu finden Sie unter Konfigurieren von Netzwerkzugriff auf die vSAN-Dateifreigabe.

Konfigurieren von Netzwerkzugriff auf die vSAN-Dateifreigabe

Um dauerhafte ReadWriteMany-Volumes in Ihrer generischen vSphere Kubernetes-Umgebung bereitstellen zu können, konfigurieren Sie die notwendigen Netzwerke, Switches und Router von den Kubernetes-Knoten zum Netzwerk des vSAN-Dateidiensts.

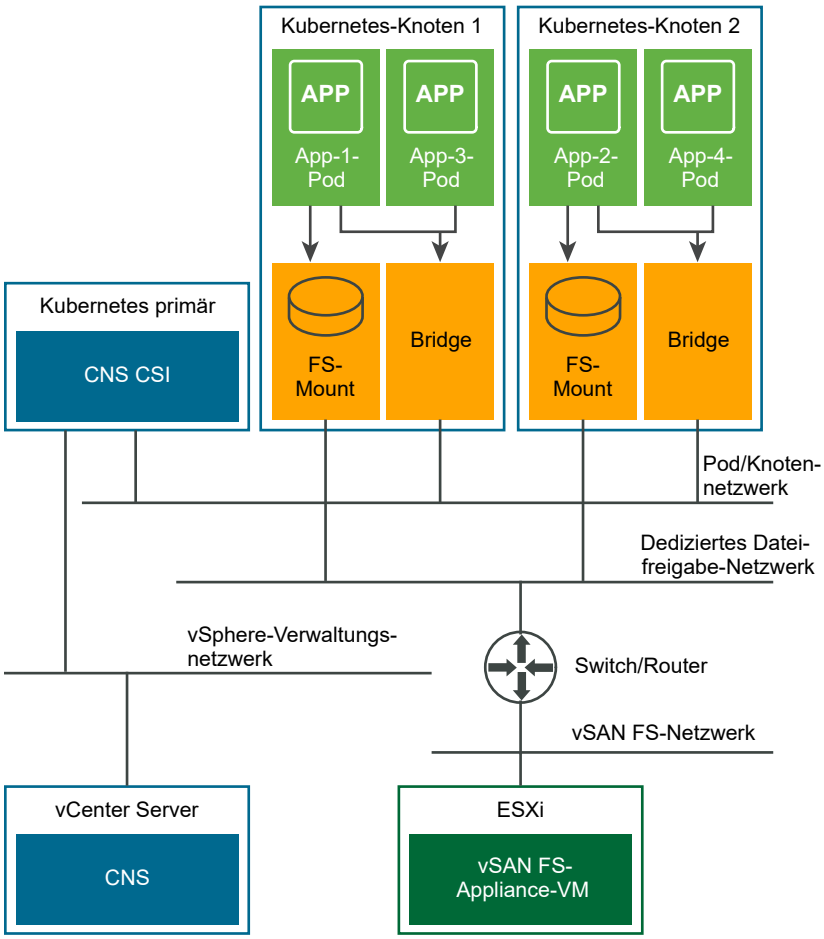
Einrichten des Netzwerks

Beachten Sie beim Konfigurieren der Netzwerke die folgenden Anforderungen:

- Auf jedem Kubernetes-Knoten können Sie eine dedizierte vNIC für den Datenverkehr der vSAN-Dateifreigabe verwenden. Diese Option ist nur erforderlich, wenn Sie einen sicheren Datenverkehrspfad für Ihre Datei-Volumes verwenden möchten.
- Wenn Sie eine dedizierte vNIC verwenden, stellen Sie sicher, dass der Datenverkehr über die dedizierte vNIC zu einem oder mehreren vSAN-Dateidienst-Netzwerken geleitet werden kann.
- Stellen Sie sicher, dass nur das Gastbetriebssystem auf jedem Kubernetes-Knoten direkt auf die vSAN-Dateifreigabe über die IP-Adresse der Dateifreigabe zugreifen kann. Die Pods im Knoten können vSAN-Dateifreigabe nicht über die zugehörige IP-Adresse anpingen bzw. nicht auf diese zugreifen.

  Der CNS-CSI-Treiber stellt sicher, dass nur die Pods, die für die Verwendung des CNS-Datei-Volumes konfiguriert sind, auf die vSAN-Dateifreigabe zugreifen können, indem Sie einen Mount-Punkt im Gastbetriebssystem erstellen.
- Vermeiden Sie das Entstehen eines IP-Adressenkonflikts zwischen den Knoten-VMs und vSAN-Dateifreigaben.

Die folgende Abbildung ist ein Beispiel für die CNS-Netzwerkkonfiguration mit dem vSAN-Dateifreigabedienst.



Die Beispiel-Netzwerkkonfiguration in der Abbildung folgt diesen Richtlinien.

- Bei der Konfiguration werden separate Netzwerke für verschiedene Elemente in der CNS-Umgebung verwendet.

Netzwerk	Beschreibung
vSphere-Verwaltungsnetzwerk	In einem generischen Kubernetes-Cluster hat üblicherweise jeder Knoten Zugriff auf dieses Netzwerk.
Pod oder Knotennetzwerk	Kubernetes verwendet dieses Netzwerk für die Knoten-zu-Knoten- oder Pod-zu-Pod-Kommunikation.
Dediziertes Dateifreigabe-Netzwerk	Dieses Netzwerk wird für den Datenverkehr dieses CNS-Datei-Volumes verwendet.
vSAN-Dateifreigabe-Netzwerk	Netzwerk, in dem die vSAN-Dateifreigabe aktiviert ist und in dem Dateifreigaben verfügbar sind.

- Jeder Kubernetes-Knoten verfügt über eine dedizierte vNIC für den Dateidatenverkehr. Diese vNIC ist von der vNIC getrennt, die für die Knoten-zu-Knoten- oder Pod-zu-Pod-Kommunikation verwendet wird. Diese Konfiguration wird nur als Beispiel verwendet und ist nicht obligatorisch.

- Nur diejenigen Anwendungen, die für die Verwendung der CNS-Dateifreigabe konfiguriert sind, können über den Mount-Punkt im Gastbetriebssystem des Knotens auf vSAN-Dateifreigaben zugreifen. In der Abbildung findet beispielsweise Folgendes statt:
  - Die Pods App-1 und App-2 sind für die Verwendung eines Datei-Volumes konfiguriert und haben Zugriff auf die Dateifreigabe über den vom CSI-Treiber erstellten Mount-Punkt.
  - App-3 und App-4 sind nicht mit einem Datei-Volume konfiguriert und können nicht auf Dateifreigaben zugreifen.
- Die vSAN-Dateifreigaben werden als Container in einer vSAN-Dateifreigabe-Appliance-VM auf dem ESXi-Host bereitgestellt. Ein Kubernetes-Deployer, d. h. eine Software oder ein Dienst, der Kubernetes-Cluster konfigurieren, bereitstellen und verwalten kann, konfiguriert die erforderlichen Router und Switches, sodass das Gastbetriebssystem im Kubernetes-Knoten auf die vSAN-Dateifreigaben zugreifen kann.

Sicherheitseinschränkungen

Obwohl eine dedizierte vNIC verhindert, dass ein nicht autorisierter Pod direkt auf die Dateifreigaben zugreift, gibt es bestimmte Sicherheitseinschränkungen:

- Die CNS-Dateifunktion setzt voraus, dass jeder, der über die CNS-Datei-Volume-ID verfügt, ein autorisierter Benutzer des Volumes ist. Jeder Benutzer, der über die CNS-Datei-Volume-ID verfügt, kann auf die im Volume gespeicherten Daten zugreifen.
- Das CNS-Datei-Volume unterstützt nur die AUTH_SYS-Authentifizierung, die eine auf einer Benutzer-ID basierende Authentifizierung ist. Um den Zugriff auf die Daten im CNS-Datei-Volume zu schützen, müssen Sie geeignete Benutzer-IDs für die Container verwenden, die auf das CNS-Datei-Volume zugreifen.
- Ein ungebundenes persistentes ReadWriteMany-Volume, dass sich auf ein CNS-Datei-Volume bezieht, kann durch einen persistenten Volume-Anspruch gebunden werden, der von einem beliebigen Kubernetes-Benutzer in einem beliebigen Namespace erstellt wurde. Stellen Sie sicher, dass nur autorisierte Benutzer Zugriff auf Kubernetes haben, um Sicherheitsprobleme zu vermeiden.

Konfigurieren des CSI-Treibers für den Zugriff auf vSAN-Dateidienst-Cluster

Je nach Konfiguration kann der CSI-Treiber Datei-Volumes in einem oder mehreren vSAN-Clustern, in denen der Dateidienst aktiviert ist, bereitstellen.

Sie können den Zugriff nur auf bestimmte vSAN-Cluster beschränken, bei denen der Dateidienst aktiviert ist. Konfigurieren Sie bei der Bereitstellung der Kubernetes-Cluster den CSI-Treiber mit Zugriff auf bestimmte Dateidienst-vSAN-Cluster. Dies führt dazu, dass der CSI-Treiber die Datei-Volumes nur in diesen vSAN-Clustern bereitstellen kann.

In der Standardkonfiguration verwendet der CSI-Treiber für die Bereitstellung von Datei-Volumes einen beliebigen Dateidienst-vSAN-Cluster in vCenter Server. Der CSI-Treiber überprüft nicht, auf welchen vSAN-Cluster während der Bereitstellung von Datei-Volumes zugegriffen werden kann.

Rollen und Rechte für Cloud Native Storage

Der CNS vSphere-Benutzer muss bestimmte Berechtigungen aufweisen, um Vorgänge durchzuführen, die sich auf Cloud Native Storage beziehen.

Sie können mehrere Rollen erstellen, um zur Cloud Native Storage-Umgebung gehörenden Objekten Berechtigungssätze zuzuweisen.

Hinweis Diese Rollen müssen nur für generische Kubernetes-Cluster erstellt werden. Wenn Sie in der vSphere with Tanzu-Umgebung arbeiten, verwenden Sie die Rolle „Arbeitslastspeicher-Manager“ für Speichervorgänge.

Weitere Informationen zu Rollen und Berechtigungen in vSphere und zum Erstellen einer Rolle finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Rollenname	Rechtename	Beschreibung	Erforderlich bei
CNS-Datenspeicher	Datenspeicher > Dateivorgänge auf niedriger Ebene	Ermöglicht die Durchführung von Lese-, Schreib-, Lösch- und Umbenennungsvorgängen im Datenspeicherbrowser.	Gemeinsam genutzter Datenspeicher, in dem sich persistente Volumes befinden.
CNS-HOST-CONFIG-STORAGE	Host > Konfiguration > Konfiguration für Speicherpartition	Ermöglicht die Verwaltung des vSAN-Datenspeichers.	Erforderlich auf einem vSAN-Cluster mit vSAN-Dateidienst. Nur für Datei-Volume erforderlich.
CNS-VM	Virtuelle Maschine > Konfiguration ändern > Vorhandene Festplatte hinzufügen	Ermöglicht das Hinzufügen einer vorhandenen virtuellen Festplatte zu einer virtuellen Maschine.	Alle Cluster-Knoten-VMs
	Virtuelle Maschine > Konfiguration ändern > Gerät hinzufügen oder entfernen	Ermöglicht das Hinzufügen oder Entfernen von Geräten (ausgenommen Festplatten).	
CNS-SEARCH-AND-SPBM	CNS > Durchsuchbar	Ermöglicht dem Speicheradministrator das Anzeigen der Benutzeroberfläche des nativen Cloud-Speichers.	Root-vCenter Server.

Rollenname	Rechtename	Beschreibung	Erforderlich bei
	Profile-Driven Storage > Ansicht des Profile-Driven Storage	Ermöglicht die Anzeige festgelegter Speicherrichtlinien.	
Nur Lesen	Standardrolle	Benutzer mit der Rolle „Nur Lesen“ für ein Objekt können den Status des Objekts und Details zum Objekt anzeigen. Benutzer mit dieser Rolle können beispielsweise nach dem freigegebenen Datenspeicher suchen, auf den alle Knoten-VMs zugreifen können. Bei zonen- und topologiefähigen Umgebungen müssen alle Vorgänger der Knoten-VMs, wie z. B. Hosts, Clusters und Datencenter, über die Rolle „Schreibgeschützt“ für den vSphere-Benutzer verfügen, der für die Verwendung des CCM und CSI-Treibers konfiguriert ist. Dies ist erforderlich, um das Lesen von Tags und Kategorien zur Vorbereitung der Knotentopologie zuzulassen.	Alle Hosts, auf denen sich die VMs der Knoten befinden Datencenter

Erstellen einer Speicherrichtlinie für Kubernetes

Das vSphere-Speicherobjekt, das die Kubernetes-Containeranwendung unterstützt, muss bestimmte Speicheranforderungen erfüllen. Als vSphere-Benutzer erstellen Sie eine VM-Speicherrichtlinie basierend auf den Anforderungen, die Ihnen vom Kubernetes-Benutzer zur Verfügung gestellt werden.

Die Speicherrichtlinie wird mit der virtuellen Festplatte oder vSAN-Dateinutzung verknüpft, die den Kubernetes-Container sichern.

Enthält Ihre Umgebung mehrere vCenter Server-Instanzen, erstellen Sie die VM-Speicherrichtlinie für jede Instanz. Verwenden Sie denselben Richtliniennamen für alle Instanzen.

Voraussetzungen

- Der Kubernetes-Benutzer gibt den Kubernetes-Cluster an, auf dem die statusbehaftete Containeranwendung bereitgestellt wird.

- Der Kubernetes-Benutzer erfasst Speicheranforderungen für die Containeranwendung und gibt diese an den vSphere-Benutzer weiter.
- Erforderliche Rechte: **VM-Speicherrichtlinien. Aktualisieren** und **VM-Speicherrichtlinien. Anzeigen**.

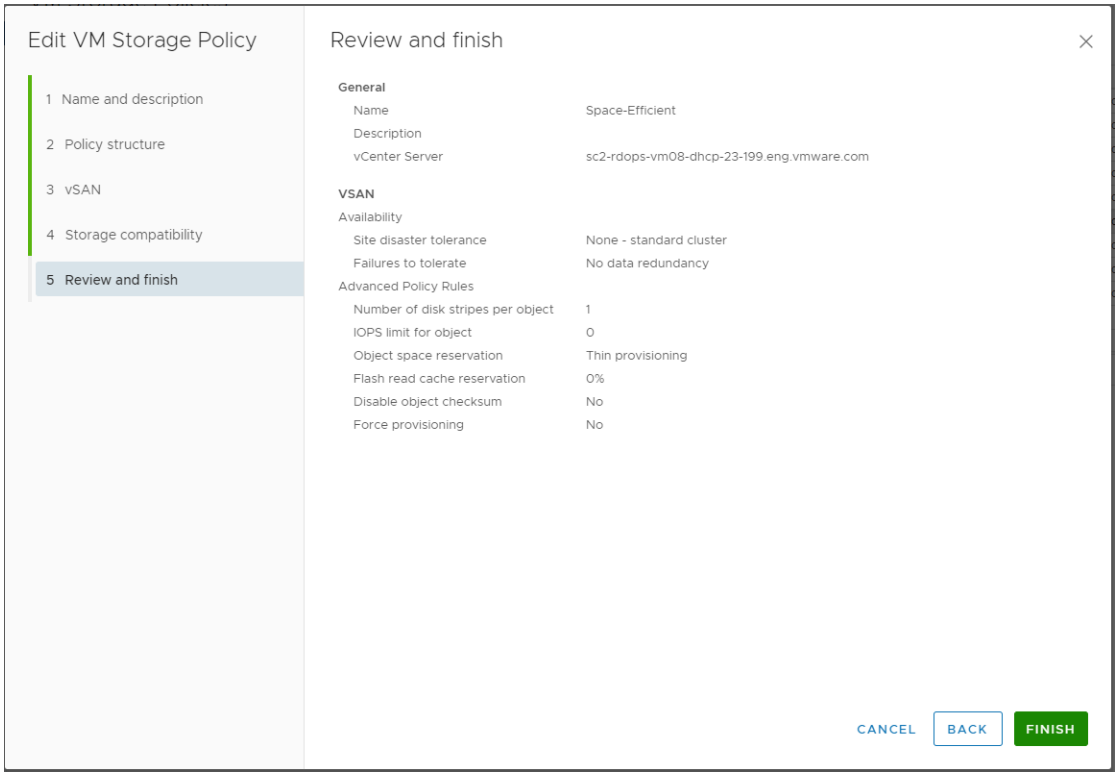
Verfahren

1 Öffnen Sie im vSphere Client den Assistenten **VM-Speicherrichtlinie erstellen**.
   a Klicken Sie auf **Menü > Richtlinien und Profile**.
   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
   c Klicken Sie auf **Erstellen**.
2 Geben Sie den Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.

Option	Aktion
vCenter Server	Wählen Sie die vCenter Server-Instanz aus.
Name	Geben Sie den Namen der Speicherrichtlinie ein, z. B. **`Speichereffizient`**.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Wählen Sie auf der Seite **Richtlinienstruktur** unter „Datenspeicherspezifische Regeln“ die Option **Regeln für vSAN-Speicher aktivieren** aus und klicken Sie auf **Weiter**.
4 Definieren Sie auf der Seite **vSAN** den Satz an Richtlinienregeln und klicken Sie auf **Weiter**.
   a Definieren Sie auf der Registerkarte **Verfügbarkeit** die **Site-Ausfalltoleranz** und die **Anzahl der zu tolerierenden Fehler**.
   b Legen Sie auf der Registerkarte **Erweiterte Richtlinienregeln** erweiterte Richtlinienregeln fest, wie z. B. die Anzahl der Datenträger-Stripes pro Objekt und Flash Read Cache-Reservierungen.
5 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der vSAN-Datenspeicher, die mit dieser Richtlinie übereinstimmen, und klicken Sie auf **Weiter**.

6 Überprüfen Sie auf der Seite **Überprüfen und beenden** die Richtlinieneinstellungen und klicken Sie auf **Beenden**.



Nächste Schritte

Sie können dem Kubernetes-Benutzer nun den Namen der Speicherrichtlinie mitteilen. Die von Ihnen erstellte VM-Speicherrichtlinie wird als Teil der Speicherklassendefinition für die Bereitstellung dynamischer Volumes verwendet.

Konfigurieren der virtuellen Maschinen des Kubernetes-Clusters

Aktivieren Sie auf jeder Knoten-VM den Parameter disk.EnableUUID, damit die VMs die virtuellen Festplatten erfolgreich mounten können.

Führen Sie diese Schritte für alle VM-Knoten aus, die zum Cluster gehören.

Voraussetzungen

- Erstellen Sie mehrere VMs für Ihren Kubernetes-Cluster. Informationen zu den VM-Anforderungen finden Sie unter Anforderungen für Cloud Native Storage.
- Notwendige Berechtigung: **Virtuelle Maschine. Konfiguration. Einstellungen**.

Hinweis Um Fehler und unvorhersehbares Verhalten zu vermeiden, sollten Sie keine Snapshots von CNS-Knoten-VMs erstellen.

Verfahren

1 Klicken Sie im vSphere Client mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.

2 Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie das Menü **Erweitert**.

3 Klicken Sie neben „Konfigurationsparameter“ auf **Konfiguration bearbeiten**.

4 Konfigurieren Sie den Parameter **`disk.EnableUUID`**.

   Wenn der Parameter vorhanden ist, stellen Sie sicher, dass sein Wert auf „True“ festgelegt ist. Wenn der Parameter nicht vorhanden ist, können Sie ihn hinzufügen und den Wert auf „True“ setzen.

Name	Wert
`disk.EnableUUID`	True

Überwachen von Container-Volumes in Kubernetes-Clustern

Nachdem eine statusbehaftete Anwendung in Kubernetes bereitgestellt wurde, werden die Volumes und die sie stützenden vSphere-Speicherobjekte im vSphere Client sichtbar. Sie können die Volumes anzeigen und überwachen und mögliche Speicherprobleme beheben.

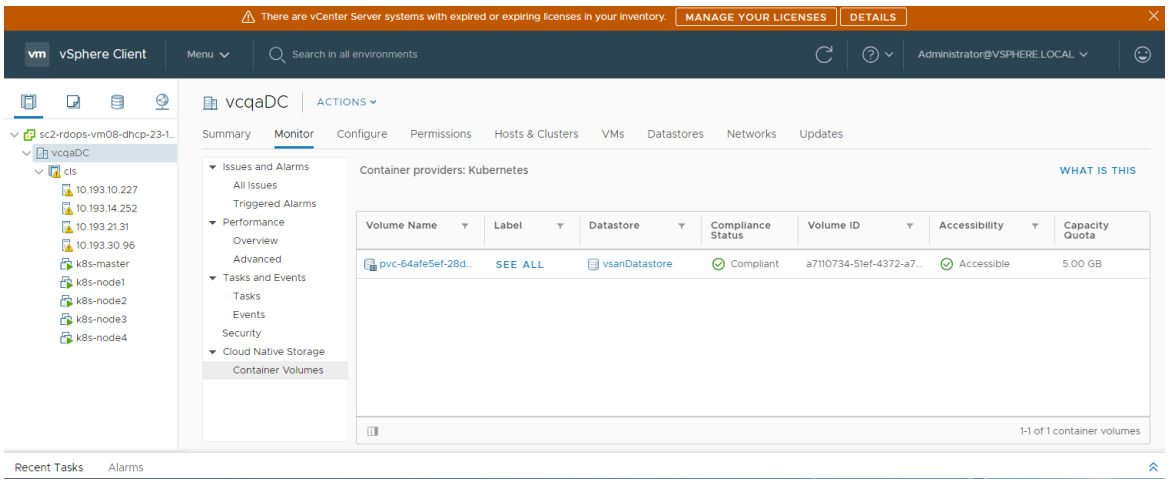
Hinweis Bei Fehlern auf dem Kubernetes-CNS-Server werden die CNS-Objekte im vSphere Client unter Umständen erst dann ordnungsgemäß angezeigt, wenn eine vollständige Synchronisierung stattfindet.

Verfahren

1 Navigieren Sie zur vCenter Server-Instanz, zu einem Datencenter oder Datenspeicher.

2 Klicken Sie auf die Registerkarte **Überwachen** und dann auf **Container-Volumes** unter **Cloudnativer Speicher**.

3 Beobachten Sie die in Ihrer Umgebung verfügbaren Container-Volumes und überwachen Sie den Compliance-Status der zugehörigen Speicherrichtlinie.

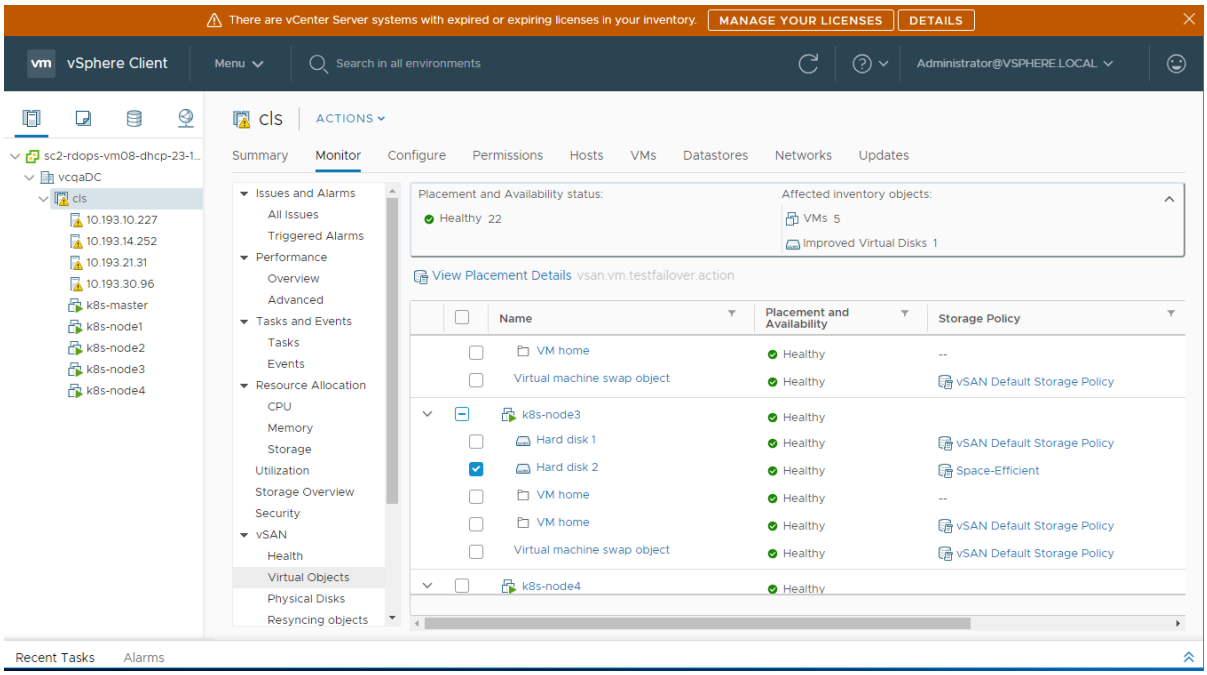


4 Klicken Sie in der Spalte „Bezeichnung“ auf den Link **ALLE ANZEIGEN**, um weitere Details anzuzeigen.

   Die Details beinhalten den Namen von „PersistentVolumeClaim“, „StorageClass“ usw. Sie helfen Ihnen, das Volume den damit verbundenen Kubernetes-Objekten zuzuordnen.

5 Klicken Sie auf den Link in der Spalte **Volume-Name**, um die verschiedenen Komponenten zu überprüfen, die das Volume und Details wie Platzierung, Konformität und Speicherrichtlinie unterstützen.

Hinweis Der Bildschirm **Virtuelles Objekt** ist nur verfügbar, wenn der zugrunde liegende Datenspeicher vSAN ist.



Verwenden der Verschlüsselung mit cloudnativem Speicher

Ab vSphere 7.0 können Sie die vSphere-Verschlüsselungstechnologie verwenden, um virtuelle FCD-Festplatten zu schützen, die persistente Volumes sichern.

Die Verwendung der Verschlüsselung in Ihrer vSphere-Umgebung erfordert eine gewisse Vorbereitung und beinhaltet die Einrichtung einer vertrauenswürdigen Verbindung zwischen vCenter Server und einem Schlüsselanbieter. vCenter Server kann dann nach Bedarf Schlüssel beim Schlüsselanbieter abrufen. Informationen zu Komponenten, die am vSphere-Verschlüsselungsprozess beteiligt sind, finden Sie unter vSphere Virtual Machine Encryption-Komponenten in der *vSphere-Sicherheit*-Dokumentation.

Verfahren

1 Richten Sie den Schlüsselanbieter in Ihrer vSphere-Umgebung ein.

   Weitere Informationen finden Sie unter Einrichten des Schlüsselmanagementserver-Clusters.

2 Verschlüsseln Sie alle Knoten-VMs im Kubernetes-Cluster.

Verwenden Sie für diesen Schritt den vSphere Client.

a Navigieren Sie zu einer Knoten-VM.

b Wählen Sie im Kontextmenü **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten** aus.

c Wählen Sie im Dropdown-Menü **VM-Speicherrichtlinie** die Option **VM-Speicherrichtlinie** aus und klicken Sie auf **OK**.

Um den Verschlüsselungsprozess der Knoten-VMs zu beschleunigen, können Sie nur VM-Home verschlüsseln.

3 Erstellen Sie verschlüsselte persistente Volumes im Kubernetes-Cluster mit der vSphere-CSI-Konfiguration.

a Erstellen Sie eine StorageClass, die auf die Speicherrichtlinie für die VM-Verschlüsselung verweist.

Verwenden Sie die folgende YAML-Datei als Beispiel.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: encryption
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: "VM Encryption Policy"
  datastore: vsanDatastore
```

b Verwenden Sie „PersistentVolumeClaim“, um das persistente Volume bereitzustellen.

„PersistentVolumeClaim“ muss den Namen der Verschlüsselungsspeicherklasse im Feld `storageClassName` enthalten.

Verwenden von „vmkfstools“ 27

`vmkfstools` ist einer der ESXi Shell-Befehle zum Verwalten von VMFS-Volumes, Speichergeräten und virtuellen Festplatten. Mit dem `vmkfstools`-Befehl können Sie viele Speichervorgänge durchführen. Beispielsweise können Sie VMFS-Datenspeicher auf einer physischen Partition erstellen und verwalten oder virtuelle Festplattendateien bearbeiten, die auf VMFS- oder NFS-Datenspeichern abgelegt sind.

Hinweis Nachdem Sie mit `vmkfstools` eine Änderung vorgenommen haben, wird der vSphere Client möglicherweise nicht sofort aktualisiert. Führen Sie vom Client aus eine Aktualisierung oder eine erneute Prüfung durch.

Weitere Informationen zur ESXi Shell finden Sie unter *Erste Schritte mit ESXCLI*.

Dieses Kapitel enthält die folgenden Themen:

Syntax des vmkfstools-Befehls

Normalerweise müssen Sie sich nicht als Root-Benutzer anmelden, um die `vmkfstools`-Befehle auszuführen. Für einige Befehle, wie beispielsweise die Dateisystembefehle, ist jedoch eine Anmeldung als Root-Benutzer erforderlich.

Der `vmkfstools`-Befehl unterstützt die folgende Befehlssyntax:

`vmkfstools` *Optionen Ziel*.

Als Ziel wird eine Partition, ein Gerät oder ein Pfad angegeben, auf den die Befehlsoption angewendet wird.

Tabelle 27-1. Befehlsargumente für `vmkfstools`

Argument	Beschreibung
Optionen	Eine oder mehrere Befehlszeilenoptionen und die zugehörigen Argumente, mit denen Sie die Aktivität angeben, die `vmkfstools` ausführen soll. Hierzu gehört beispielsweise die Auswahl des Festplattenformats beim Erstellen einer neuen virtuellen Festplatte. Geben Sie nach Eingabe der Option ein Ziel an, für das der Vorgang ausgeführt werden soll. Als Ziel kann eine Partition, ein Gerät oder ein Pfad angegeben werden.
Partition	Gibt Festplattenpartitionen an. Dieses Argument wird im Format *disk_ID:P* angegeben. Dabei ist *disk_ID* die vom Speicher-Array zurückgegebene Geräte-ID und *P* eine Ganzzahl, die die Partitionsnummer darstellt. Die Ziffer der Partition muss größer als null (0) sein und einer gültigen VMFS-Partition entsprechen.
Gerät	Gibt Geräte oder logische Volumes an. Bei diesem Argument wird ein Pfadname im Dateisystem des ESXi-Geräts verwendet. Der Pfadname beginnt mit `/vmfs/devices`. Dies ist der Mount-Punkt des Dateisystems des Geräts. Verwenden Sie die folgenden Formate zur Angabe von verschiedenen Arten von Geräten: ■ `/vmfs/devices/disks` für lokale oder SAN-basierte Festplatten. ■ `/vmfs/devices/lvm` für logische ESXi-Volumes. ■ `/vmfs/devices/generic` für generische SCSI-Geräte.

Pfad	Gibt ein VMFS-Dateisystem oder eine VMFS-Datei an. Dieses Argument ist ein absoluter oder relativer Pfad, mit dem ein symbolischer Links eines Verzeichnisses, eine Raw-Gerätezuordnung oder eine Datei unter `/vmfs` benannt wird.
	■ Geben Sie ein VMFS-Dateisystem im folgenden Format an:
	`/vmfs/volumes/file_system_UUID`
	oder
	`/vmfs/volumes/file_system_label`
	■ Geben Sie eine Datei in einem VMFS-Datenspeicher im folgenden Format an:
	`/vmfs/volumes/file_system_label|file_system_UUID/[dir]/myDisk.vmdk`
	Wenn das aktuelle Arbeitsverzeichnis gleichzeitig das übergeordnete Verzeichnis von `myDisk.vmdk` ist, geben Sie nicht den gesamten Pfad an.

vmkfstools-Befehlsoptionen

Der `vmkfstools`-Befehl verfügt über verschiedene Optionen. Einige der Optionen werden nur für fortgeschrittene Benutzer empfohlen.

Die lange Form und die aus einem Buchstaben bestehende Form der Optionen sind gleichwertig. Die folgenden Befehle sind beispielsweise identisch.

```
vmkfstools --createfs vmfs6 --blocksize 1m disk_ID:P
vmkfstools -C vmfs6 -b 1m disk_ID:P
```

Unteroption -v

Die Unteroption `-v` bestimmt die Ausführlichkeit der Meldungen in der Befehlsausgabe.

Das Format für diese Unteroption lautet wie folgt:

```
-v --verbose number
```

Der Wert *Zahl* wird als ganze Zahl von 1 bis 10 angegeben.

Sie können die Unteroption `-v` für alle `vmkfstools`-Optionen verwenden. Wenn die Unteroption `-v` für die Ausgabe einer Option nicht vorgesehen ist, ignoriert `vmkfstools` den Teil `-v` der Befehlszeile.

Hinweis Da Sie die Unteroption `-v` in jeder `vmkfstools`-Befehlszeile verwenden können, wird sie in den Beschreibungen der einzelnen Optionen nicht als Unteroption verwendet.

Dateisystemoptionen

Mithilfe von Dateisystemoptionen können Sie einen VMFS-Datenspeicher erstellen und verwalten. Diese Optionen gelten nicht für NFS. Sie können viele dieser Aufgaben auch über den vSphere Client ausführen.

Auflisten der Attribute eines VMFS-Datenspeichers

Verwenden Sie zum Auflisten der Attribute eines VMFS-Datenspeichers den Befehl `vmkfstools`.

```
-P|--queryfs
      -h|--humanreadable
```

Diese Option listet bei Anwendung auf eine Datei oder ein Verzeichnis auf einem VMFS-Datenspeicher die Attribute des angegebenen Datenspeichers auf. Zu den aufgelisteten Attributen zählen in der Regel die Dateisystembezeichnung, die Anzahl der Erweiterungen für den Datenspeicher, die UUID und eine Liste der Geräte, auf denen sich die einzelnen Erweiterungen befinden.

Hinweis Wenn ein Gerät zur Sicherung des VMFS-Dateisystems offline geschaltet wird, ändert sich die Anzahl der Erweiterungen und des verfügbaren Speichers entsprechend.

Sie können die Unteroption `-h|--humanreadable` für die Option `-P` verwenden. In diesem Fall listet `vmkfstools` die Kapazität des Volumes in verständlicherer Form auf.

Beispiel: Beispiel für die Auflistung von VMFS-Attributen

```
~ vmkfstools -P -h /vmfs/volumes/my_vmfs
VMFS-5.81 (Raw Major Version: 14) file system spanning 1 partitions.
File system label (if any): my_vmfs
Mode: public
Capacity 99.8 GB, 97.5 GB available, file block size 1 MB, max supported file size 62.9 TB
UUID: 571fe2fb-ec4b8d6c-d375-XXXXXXXXXXXX
Partitions spanned (on "lvm"):
        eui.3863316131XXXXXX:1
Is Native Snapshot Capable: YES
```

Erstellen eines VMFS-Datenspeichers oder einer Scratch-Partition

Verwenden Sie den Befehl `vmkfstools`, um einen VMFS-Datenspeicher oder eine Scratch-Partition zu erstellen.

```
-C|--createfs [vmfs5|vmfs6|vfat]
```

Mit dieser Option wird ein VMFS-Datenspeicher auf der angegebenen SCSI-Partition erstellt, z. B. *disk_ID:P*. Die Partition wird zur Head-Partition des Datenspeichers. Für VMFS5 und VMFS6 steht nur die Blockgröße 1 MB zur Verfügung.

Für die Option `-C` können Sie folgende Unteroptionen angeben.

- `-S|--setfsname` – Definieren Sie die Volume-Bezeichnung des VMFS-Datenspeichers, den Sie erstellen. Verwenden Sie diese Unteroption nur mit der Option `-C`. Die Bezeichnung kann bis zu 128 Zeichen lang sein und darf keine Leerstellen am Anfang oder Ende enthalten.

  Hinweis vCenter Server unterstützt die Längenbeschränkung von 80 Zeichen für alle Einträge. Wenn ein Datenspeichername diese Länge überschreitet, wird der Name beim Hinzufügen dieses Datenspeichers zu vCenter Server gekürzt.

  Nachdem Sie die Volume-Bezeichnung festgelegt haben, können Sie sie bei der Angabe des VMFS-Datenspeichers im Befehl `vmkfstools` verwenden. Die Volume-Bezeichnung erscheint auch in den Auflistungen, die mit dem Linux-Befehl `ls -l` generiert werden, und als symbolische Verknüpfung zum VMFS-Volume im Verzeichnis `/vmfs/volumes`.

  Verwenden Sie den Befehl `ln -sf`, wenn Sie die VMFS-Volume-Bezeichnung ändern möchten. Beispiel:

  ```
  ln -sf /vmfs/volumes/UUID /vmfs/volumes/Datenspeicher
  ```

  Datenspeicher ist die neue Volume-Bezeichnung, die für das VMFS mit der *UUID* zu verwenden ist.

  Hinweis Wenn der Host bei vCenter Server registriert ist, werden alle Änderungen, die Sie an der VMFS-Volume-Bezeichnung vornehmen, von vCenter Server überschrieben. Dieser Vorgang stellt sicher, dass die VMFS-Bezeichnung über alle vCenter Server-Hosts hinweg einheitlich ist.

- `-Y|--unmapGranularity #[bBsSkKmMgGtT]` – Diese Unteroption gilt nur für VMFS6. Definieren Sie die Granularität für den Vorgang zum Aufheben der Zuordnung. Die Standardgranularität ist 1 MB. Geben Sie wie bei der Blockgröße die Einheit ein.
- `-O|--unmapPriority <none|low|medium|high>` – Diese Unteroption gilt nur für VMFS6. Definieren Sie die Priorität für den Vorgang zum Aufheben der Zuordnung.

Beispiel: Erstellen eines VMFS-Dateisystems – Beispiel

Dieses Beispiel veranschaulicht die Erstellung eines neuen VMFS6-Datenspeichers mit dem Namen „my_vmfs“ auf der Partition `naa.ID:1`.

```
~ vmkfstools -C vmfs6 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

Hinzufügen einer Erweiterung zu einem VMFS-Datenspeicher

Mit dem `vmkfstools`-Befehl können Sie dem VMFS-Datenspeicher eine Erweiterung hinzufügen.

Wenn Sie eine Erweiterung hinzufügen, erstreckt sich der VMFS-Datenspeicher von der Head-Partition bis zu der von *span_partition* angegebenen Partition.

```
-Z|--spanfs span_partitionhead_partition
```

Sie müssen den vollständigen Pfad für die Head- und Span-Partitionen angeben, zum Beispiel `/vmfs/devices/disks/disk_ID:1`. Bei jeder Verwendung dieser Option fügen Sie dem VMFS-Datenspeicher eine Erweiterung hinzu, sodass der Datenspeicher mehrere Partitionen umfasst.

Vorsicht Bei Ausführung dieser Option werden alle Daten gelöscht, die zuvor auf dem in *span_partition* angegebenen SCSI-Gerät vorhanden waren.

Beispiel: Beispiel für die Erweiterung eines VMFS-Datenspeichers

In diesem Beispiel erweitern Sie die vorhandene Head-Partition des VMFS-Datenspeichers über eine neue Partition.

```
~ vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

Der erweiterte Datenspeicher umfasst zwei Partitionen: `naa.disk_ID_1:1` und `naa.disk_ID_2:1`. In diesem Beispiel ist `naa.disk_ID_1:1` der Name der Head-Partition.

Erweitern eines VMFS-Datenspeichers

Anstatt einem VMFS-Datenspeicher eine Erweiterung hinzufügen, können Sie einen vorhandenen Datenspeicher vergrößern. Verwenden Sie den Befehl `vmkfstools -G`.

Sie können den Datenspeicher vergrößern, nachdem die Kapazität des zugrunde liegenden Speichers erhöht wurde.

Der Befehl verwendet die folgende Option:

```
-G|--growfs devicedevice
```

Mit dieser Option wird der VMFS-Datenspeicher oder seine spezielle Erweiterung erweitert. Beispiel:

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

Optionen für virtuelle Festplatten

Mithilfe von Optionen für virtuelle Festplatten können Sie in Ihren Datenspeichern gespeicherte virtuelle Festplatten einrichten, migrieren und verwalten. Sie können die meisten dieser Aufgaben auch über den vSphere Client ausführen.

Unterstützte Festplattenformate

Beim Erstellen oder Klonen einer virtuellen Festplatte können Sie mit der Unteroption `-d|--diskformat` das Format der Festplatte festlegen.

Wählen Sie eines der folgenden Formate:

- `zeroedthick` (Standard) – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Erstellvorgangs zugewiesen. Alle Daten, die auf dem physischen Gerät verbleiben, werden beim Erstellvorgang nicht gelöscht, sondern bei Bedarf beim ersten Schreiben von der virtuellen Maschine durch Nullbyte ersetzt. Die virtuelle Maschine liest keine veralteten Daten von der Festplatte.
- `eagerzeroedthick` – Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum `zeroedthick`-Format werden die auf dem physischen Gerät verbleibenden Daten während des Erstellvorgangs durch Nullen ersetzt. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.
- `thin` – Per Thin Provisioning bereitgestellte virtuelle Festplatte. Anders als beim `thick`-Format wird der für die virtuelle Festplatte benötigte Speicherplatz nicht während des Erstellvorgangs zugewiesen, sondern wird bei Bedarf durch Nullen ersetzt.
- `rdm:`*Gerät* – Rohfestplattenzuordnung im virtuellen Kompatibilitätsmodus.
- `rdmp:`*Gerät* – Rohfestplattenzuordnung im physischen Kompatibilitätsmodus (Passthrough).
- `2gbsparse` – Eine Festplatte mit geringer Datendichte mit einer maximalen Erweiterung von 2 GB. Festplatten mit diesem Format können mit gehosteten VMware-Produkten wie VMware Fusion verwendet werden. Eine Festplatte mit geringer Datendichte kann auf einem ESXi-Host jedoch erst eingeschaltet werden, nachdem sie zunächst mit dem Befehl `vmkfstools` in einem kompatiblen Format wie `thick` oder `thin` erneut importiert wurde.

Festplattenformate in NFS-Datenspeichern

Für NFS können ausschließlich die Festplattenformate `thin`, `thick`, `zeroedthick` und `2gbsparse` verwendet werden.

Die Formate `Thick`, `zeroedthick` und `thin` verhalten sich üblicherweise auf die gleiche Weise, da der NFS-Server und nicht der ESXi-Host die Zuteilungsrichtlinie bestimmt. Die standardmäßige Zuteilungsrichtlinie auf den meisten NFS-Servern ist `thin`. Auf NFS-Servern, die Storage APIs - Array Integration unterstützen, können Sie jedoch virtuelle Festplatten im `zeroedthick`-Format erstellen. Durch den Vorgang zur Reservierung von Speicherplatz erhalten NFS-Server die Möglichkeit, Speicherplatz zuzuteilen und zu garantieren.

Weitere Informationen zu APIs für die Array-Integration finden Sie unter Kapitel 24 Speicherhardware-Beschleunigung.

Erstellen eines virtuellen Laufwerks

Verwenden Sie zum Erstellen einer virtuellen Festplatte den Befehl `vmkfstools`.

```
-c|--createvirtualdisk size[bB|sS|kK|mM|gG]
      -d|--diskformat [thin|zeroedthick|eagerzeroedthick]
      -W|--objecttype [file|vsan|vvol]
      --policyFile fileName
```

Diese Option erstellt eine virtuelle Festplatte im angegebenen Pfad auf einem Datenspeicher. Legen Sie die Größe der virtuellen Festplatte fest. Wenn Sie einen Wert für die *Größe* angeben, können Sie die Einheit festlegen, indem Sie entweder das Suffix `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) angeben. Bei der Größeneinheit wird die Groß-/Kleinschreibung nicht berücksichtigt. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit angeben, ist die Standardeinstellung für `vmkfstools` Byte.

Für die Option `-c` können Sie folgende Unteroptionen angeben.

- `-d|--diskformat` bezeichnet die Festplattenformate.
- `-W|--objecttype` gibt an, ob es sich bei der virtuellen Festplatte um eine Datei in einem VMFS- oder NFS-Datenspeicher oder um ein Objekt in einem vSAN- oder einem Virtual Volumes-Datenspeicher handelt.
- `--policyFile` *`fileName`* gibt die VM-Speicherrichtlinie für die Festplatte an.

Beispiel: Beispiel für das Erstellen einer virtuellen Festplatte

Dieses Beispiel zeigt, wie eine virtuelle Festplattendatei mit 2 GB mit der Bezeichnung `disk.vmdk` erstellt wird. Sie erstellen die Festplatte im VMFS-Datenspeicher namens `myVMFS`. Die Festplattendatei stellt eine leere virtuelle Festplatte dar, auf die virtuelle Maschinen zugreifen können.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/disk.vmdk
```

Initialisieren einer virtuellen Festplatte

Mit dem `vmkfstools`-Befehl können Sie eine virtuelle Festplatte initialisieren.

```
-w|--writezeros
```

Mit dieser Option wird die virtuelle Festplatte bereinigt, indem sämtlichen Daten auf ihr mit Nullen überschrieben werden. Je nach Größe der virtuellen Festplatte und der E/A-Bandbreite des Geräts, das die virtuelle Festplatte hostet, kann die Ausführung dieses Befehls viel Zeit in Anspruch nehmen.

Vorsicht Bei Verwendung dieses Befehls werden alle vorhandenen Daten auf der virtuellen Festplatte gelöscht.

Vergrößern virtueller Festplatten im Thin-Format

Mit dem `vmkfstools`-Befehl können Sie eine virtuelle Festplatte im Thin-Format vergrößern.

```
-j|--inflatedisk
```

Mit dieser Option wird eine virtuelle Festplatte im `thin`-Format unter Beibehaltung aller vorhandenen Daten in das `eagerzeroedthick`-Format konvertiert. Durch die Option werden alle noch nicht zugeteilten Blöcke zugeteilt und durch Nullbyte ersetzt.

Konvertieren einer virtuellen Zeroedthick-Festplatte in eine Eagerzeroedthick-Festplatte

Mit dem Befehl `vmkfstools` können Sie eine beliebige virtuelle Zeroedthick-Festplatte in eine Eagerzeroedthick-Festplatte konvertieren.

```
-k|--eagerzero
```

Während die Konvertierung durchgeführt wird, werden durch diese Option alle Daten auf der virtuellen Festplatte beibehalten.

Gehen Sie wie im folgenden Beispiel vor:

```
vmkfstools --eagerzero /vmfs/volumes/myVMFS/VMName/disk.vmdk
```

Entfernen von auf Null gesetzten Blöcken

Mit dem `vmkfstools`-Befehl können Sie auf Null gesetzte Blöcke entfernen.

```
-K|--punchzero
```

Mit dieser Option wird die Zuteilung aller auf Null gesetzten Blöcke aufgehoben und es werden nur diejenigen Blöcke beibehalten, die zuvor zugeteilt wurden und gültige Daten enthalten. Die resultierende virtuelle Festplatte weist das Thin-Format auf.

Löschen einer virtuellen Festplatte

Mit dem vmkfstools-Befehl können Sie eine virtuelle Festplatte im angegebenen Pfad auf dem VMFS-Volume löschen.

Verwenden Sie die folgende Option:

```
-U|--deletevirtualdisk
```

Umbenennen einer virtuellen Festplatte

Mit dem vmkfstools-Befehl können Sie eine virtuelle Festplatte im angegebenen Pfad auf dem VMFS-Volume umbenennen.

Sie müssen den ursprünglichen Dateinamen oder Dateipfad *oldName* und den neuen Dateinamen oder Dateipfad *newName* angeben.

```
-E|--renamevirtualdisk oldNamenewName
```

Klonen oder Konvertieren einer virtuellen Festplatte oder einer RDM-Festplatte

Mit dem vmkfstools-Befehl können Sie eine Kopie einer von Ihnen angegebenen virtuellen Festplatte oder Rohfestplatte erstellen.

Ein Nicht-Root-Benutzer kann keine virtuelle Festplatte oder RDM klonen. Sie müssen den ursprünglichen Dateinamen oder Dateipfad *oldName* und den neuen Dateinamen oder Dateipfad *newName* angeben.

```
-i|--clonevirtualdisk oldName newName
     -d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device|2gbsparse]
     -W|--objecttype [file|vsan|vvol]
     --policyFile fileName
     -N|--avoidnativeclone
```

Mit den folgenden Unteroptionen können Sie die entsprechenden Parameter für die von Ihnen erstellte Kopie ändern.

- `-d|--diskformat` bezeichnet die Festplattenformate.
- `-W|--objecttype` gibt an, ob es sich bei der virtuellen Festplatte um eine Datei in einem VMFS- oder NFS-Datenspeicher oder um ein Objekt in einem vSAN- oder einem Virtual Volumes-Datenspeicher handelt.
- `--policyFile` *`fileName`* gibt die VM-Speicherrichtlinie für die Festplatte an.

Standardmäßig verwendet ESXi die nativen Methoden zur Ausführung der Klonvorgänge. Wenn das Array die Klontechnologien unterstützt, können Sie die Vorgänge an das Array auslagern. Um natives Klonen von ESXi zu verhindern, geben Sie die Option `-N|--avoidnativeclone` an.

Beispiel: Beispiel für das Klonen oder Konvertieren einer virtuellen Festplatte

In diesem Beispiel wird das Klonen der Inhalte einer virtuellen primären Festplatte aus dem Repository `templates` in eine virtuelle Festplattendatei mit der Bezeichnung `myOS.vmdk` im Dateisystem `myVMFS` veranschaulicht.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Sie können eine virtuelle Maschine für die Verwendung dieser virtuellen Festplatte konfigurieren, indem Sie der Konfigurationsdatei der virtuellen Maschine Zeilen hinzufügen, wie im folgenden Beispiel gezeigt:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Wenn Sie das Format der Festplatte konvertieren möchten, verwenden Sie hierfür die Unteroption `-d|--diskformat`.

Diese Unteroption ist nützlich, wenn Sie virtuelle Festplatten in einem Format importieren möchten, das nicht mit ESXi kompatibel ist, wie beispielsweise das 2gbsparse-Format. Nachdem die Festplatte konvertiert wurde, können Sie diese Festplatte einer neuen virtuellen Maschine hinzufügen, die Sie in ESXi erstellen.

Beispiel:

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/
myOS.vmdk  -d thin
```

Erweitern einer virtuellen Festplatte

Nachdem Sie eine virtuelle Maschine erstellt haben, können Sie mit dem vmkfstools-Befehl eine der virtuellen Maschine zugewiesene Festplatte vergrößern.

```
-X|--extendvirtualdisk newSize[bBsSkKmMgGtT]
```

Geben Sie den Parameter `newSize` an und fügen Sie ein entsprechendes Suffix für die Einheit hinzu. Bei der Größeneinheit wird die Groß-/Kleinschreibung nicht berücksichtigt. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit angeben, ist die Standardeinstellung für `vmkfstools` Kilobyte.

Der Parameter `newSize` beschreibt die gesamte neue Größe und nicht nur die beabsichtigte Erweiterung der Festplatte.

Um beispielsweise eine virtuelle Festplatte mit 4 GB um 1 GB zu erweitern, geben Sie Folgendes ein: `vmkfstools -X 5g`*disk name*.

Mithilfe der Option `-d eagerzeroedthick` können Sie die virtuelle Festplatte auf das Format „eagerzeroedthick“ erweitern.

Wenn Sie die Option `-X` verwenden, ist Folgendes zu beachten:

- Erweitern Sie nicht die Basisfestplatte einer virtuellen Maschine, der Snapshots zugeordnet sind. Falls doch, können Sie den Snapshot nicht länger übergeben oder die Basisfestplatte auf ihre ursprüngliche Größe zurücksetzen.
- Nach der Erweiterung der Festplatte müssen Sie möglicherweise das Dateisystem auf der Festplatte aktualisieren. Dies führt dazu, dass das Gastbetriebssystem die neue Größe der Festplatte erkennt und diese nutzen kann.

Aktualisieren von virtuellen Festplatten

Mit dieser Option wird die angegebene virtuelle Festplattendatei von ESX Server 2-Formaten in das ESXi-Format konvertiert.

Verwenden Sie diese Option, um virtuelle Festplatten vom Typ LEGACYSPARSE, LEGACYPLAIN, LEGACYVMFS, LEGACYVMFS_SPARSE und LEGACYVMFS_RDM zu konvertieren.

```
-M|--migratevirtualdisk
```

Erstellen einer Raw-Gerätezuordnung (Raw Device Mapping, RDM) im virtuellen Kompatibilitätsmodus

Mit dem vmkfstools-Befehl können Sie eine RDM-Datei (Raw Device Mapping) auf einem VMFS-Volume erstellen und dieser Datei eine Roh-LUN zuordnen. Nachdem die Zuordnung eingerichtet wurde, können Sie auf die LUN genauso zugreifen wie auf eine normale virtuelle VMFS-Festplatte. Die Dateilänge der Zuordnung ist mit der Größe der Roh-LUN, auf die sie verweist, identisch.

```
-r|--createrdm device
```

Geben Sie den Parameter *device* in folgendem Format an:

```
/vmfs/devices/disks/disk_ID:P
```

Beispiel: Beispiel für das Erstellen einer RDM im Kompatibilitätsmodus

In diesem Beispiel erstellen Sie eine RDM-Datei mit der Bezeichnung *my_rdm.vmdk* und ordnen die Rohfestplatte *disk_ID* dieser Datei zu.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

Sie können eine virtuelle Maschine für die Verwendung der Zuordnungsdatei `my_rdm.vmdk` konfigurieren, indem Sie der Konfigurationsdatei der virtuellen Maschine die folgenden Zeilen hinzufügen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Erstellen einer Raw-Gerätezuordnung (Raw Device Mapping, RDM) im physischen Kompatibilitätsmodus

Mit dem vmkfstools-Befehl können Sie ein Passthrough-Raw-Gerät einer Datei auf einem VMFS-Volume zuordnen. Durch diese Zuordnung kann eine virtuelle Maschine die SCSI-Befehlsfilterung von ESXi beim Zugriff auf die virtuelle Festplatte umgehen. Dieser Zuordnungstyp ist nützlich, wenn die virtuelle Maschine proprietäre SCSI-Befehle senden muss, beispielsweise wenn SAN-fähige Software auf der virtuellen Maschine ausgeführt wird.

```
-z|--createrdmpassthru deviceexample.vmdk
```

Nachdem Sie diesen Zuordnungstyp eingerichtet haben, können Sie damit auf die Rohfestplatte genauso wie auf jede andere virtuelle VMFS-Festplatte zugreifen.

Geben Sie den Pfad für *device* in folgendem Format an:

```
/vmfs/devices/disks/device_ID
```

Verwenden Sie für den Namen der VMDK-Datei folgendes Format. Erstellen Sie den Datenspeicher unbedingt, bevor Sie diesen Befehl verwenden.

```
/vmfs/volumes/datastore_name/example.vmdk
```

Beispiel:

```
vmkfstools -z /vmfs/devices/disks/naa.600a0000000000000... /vmfs/volumes/datastore1/
mydisk.vmdk
```

Auflisten von RDM-Attributen

Mit dem vmkfstools-Befehl können die Attribute einer Rohfestplattenzuordnung aufgelistet werden. Anhand dieser Attribute können Sie das Speichergerät ermitteln, dem die RDM-Dateien zugeordnet sind.

```
-q|--querydrm my_rdm.vmdk
```

Mit dieser Option wird der Name einer RDM-Rohfestplatte gedruckt. Darüber hinaus werden weitere Identifikationsdaten, beispielsweise die Festplatten-ID, für die Rohfestplatte gedruckt.

Beispiel: Beispiel für die Auflistung von RDM-Attributen

```
# vmkfstools -q /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk

Disk /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk is a Passthrough Raw Device Mapping

Maps to: vml.02000000006005076801900207700000000000000005323134352020
```

Anzeigen der Geometrie der virtuellen Festplatte

Mit dem vmkfstools-Befehl können Sie Informationen über die Geometrie einer virtuellen Festplatte abrufen.

```
-g|--geometry
```

Die Ausgabe erfolgt im folgenden Format: `Geometry information C/H/S`, wobei `C` die Anzahl der Zylinder, `H` die Anzahl der Köpfe und `S` die Anzahl der Sektoren darstellt.

Hinweis Wenn Sie virtuelle Festplatten von gehosteten VMware-Produkten auf dem ESXi-Host importieren, wird möglicherweise eine Fehlermeldung aufgrund der nicht übereinstimmenden Geometrie der Festplatte angezeigt. Eine nicht übereinstimmende Festplattengeometrie kann auch Probleme beim Laden eines Gastbetriebssystems oder Ausführen einer neu erstellten virtuellen Maschine verursachen.

Überprüfen und Reparieren von virtuellen Festplatten

Mit dem vmkfstools-Befehl können Sie überprüfen, ob eine virtuelle Festplatte beschädigt ist, und diese reparieren.

```
-x|--fix [check|repair]
```

Beispiel:

```
vmkfstools -x check /vmfs/volumes/my_datastore/my_disk.vmdk
```

Überprüfen einer Festplattenkette auf Konsistenz

Mit dem vmkfstools-Befehl können Sie die gesamte Snapshot-Kette überprüfen. Sie können ermitteln, ob Links in der Kette beschädigt sind oder ob ungültige Beziehungen zwischen übergeordneten und untergeordneten Elementen bestehen.

```
-e|--chainConsistent
```

Speichergeräteoptionen

Sie können die Geräteoptionen des Befehls „vmkfstools“ verwenden, um administrative Aufgaben für physische Speichergeräte durchzuführen.

Verwalten von SCSI-Reservierungen für LUNs

Mit dem vmkfstools-Befehl kann eine SCSI-LUN zur ausschließlichen Verwendung durch den ESXi-Host reserviert werden. Sie können eine Reservierung auch freigeben, sodass andere Hosts auf die LUN zugreifen können, und eine Reservierung zurücksetzen, sodass die Freigabe aller Reservierungen des Ziels erzwungen wird.

```
-L|--lock [reserve|release|lunreset|targetreset|busreset|readkeys|readresv] device
```

Vorsicht Mit der Option `-L` können die Vorgänge anderer Server in einem SAN unterbrochen werden. Verwenden Sie die Option `-L` nur bei der Behebung von Fehlern in Cluster-Setups.

Verwenden Sie diese Option niemals für eine LUN, die ein VMFS-Volume hostet, sofern Sie nicht von VMware dazu aufgefordert werden.

Die Option `-L` kann auf verschiedene Arten angegeben werden:

- `-L reserve` – Reserviert die angegebene LUN. Nach der Reservierung kann nur der Server, der diese LUN reserviert hat, darauf zugreifen. Wenn andere Server versuchen, auf diese LUN zuzugreifen, wird ein Reservierungsfehler angezeigt.
- `-L release` – Gibt die Reservierung für die angegebene LUN frei. Andere Server können nun wieder auf die LUN zugreifen.
- `-L lunreset` – Setzt die angegebene LUN zurück, indem alle Reservierungen für die LUN gelöscht werden und die LUN wieder für alle Server zur Verfügung gestellt wird. Die Rücksetzung wirkt sich auf keine der anderen LUNs auf dem Gerät aus. Falls noch eine andere LUN auf dem Gerät reserviert ist, bleibt sie reserviert.
- `-L targetreset` – Setzt das gesamte Ziel zurück. Durch die Rücksetzung werden alle Reservierungen für alle diesem Ziel zugeordneten LUNs gelöscht und die LUNs werden wieder für alle Server zur Verfügung gestellt.
- `-L busreset` – Setzt alle Ziele, auf die zugegriffen werden kann, auf dem Bus zurück. Durch die Rücksetzung werden alle Reservierungen für alle LUNs, auf die über den Bus zugegriffen werden kann, zurückgesetzt. Außerdem werden sie für alle Server wieder zur Verfügung gestellt.
- `-L readkeys` – Liest die mit einer LUN registrierten Reservierungsschlüssel. Dies betrifft SCSI-III-persistente Gruppenreservierungsfunktionalität.
- `-L readresv` – Liest den Reservierungsstatus in einer LUN. Dies betrifft SCSI-III-persistente Gruppenreservierungsfunktionalität.

Verwenden Sie bei der Eingabe des Parameters *device* das folgende Format:

```
/vmfs/devices/disks/disk_ID:P
```

Aufheben von Gerätesperren

Mit dem vmkfstools-Befehl können Sie die Gerätesperre für eine bestimmte Partition aufheben.

```
-B|--breaklock device
```

Verwenden Sie bei der Eingabe des Parameters *device* das folgende Format:

```
/vmfs/devices/disks/disk_ID:P
```

Diesen Befehl können Sie verwenden, wenn ein Host inmitten eines Datenspeichervorgangs (beispielsweise Erweitern des Datenspeichers, Hinzufügen einer Erweiterung oder Neusignierung) ausfällt. Vergewissern Sie sich, dass kein anderer Host die Sperre hält, wenn Sie diesen Befehl ausführen.