# Verwalten von VMware vSAN

VMware vSphere 6.5
VMware vSAN 6.6.1

vmware®

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

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

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

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

docfeedback@vmware.com



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

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

# Inhalt

# Informationen zu VMware vSAN

In *Verwalten von VMware vSAN* wird beschrieben, wie Sie einen VMware vSAN-Cluster in einer VMware vSphere®-Umgebung konfigurieren, verwalten und überwachen. In *Verwalten von VMware vSAN* wird außerdem erläutert, wie Sie die lokalen physischen Speicherressourcen, die als Speicherkapazitätsgeräte in einem vSAN-Cluster dienen, organisieren, Speicherrichtlinien für virtuelle Maschinen definieren, die für Datenspeicher für vSAN bereitgestellt wurden, und Fehler in einem vSAN-Cluster handhaben.

## Zielgruppe

Diese Informationen sind für erfahrene Virtualisierungsadministratoren bestimmt, die mit der Virtualisierungstechnologie, mit den üblichen Vorgängen in Datencentern und mit vSAN-Konzepten vertraut sind.

## vSphere Client-HTML5 für vSAN

**vSphere Client**

Der vSphere Client ist ein neuer Client auf HTML5-Basis, der zusammen mit dem vSphere Web Client im Lieferumfang von vCenter Server enthalten ist. Der neue vSphere Client verwendet viele Schnittstellenterminologien, -topologien und Workflows, die auch der vSphere Web Client verwendet. Allerdings bietet vSphere Client keine Unterstützung für vSAN. Benutzer von vSAN sollten weiterhin den vSphere Web Client für entsprechende Prozesse verwenden.

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

# Einführung in vSAN 1

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

vSAN unterstützt VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, wie etwa HA, vMotion und DRS. Dadurch wird ein externer gemeinsam genutzter Speicher überflüssig, und außerdem werden die Speicherkonfiguration und Aktivitäten zum Bereitstellen von virtuellen Maschinen vereinfacht.

Dieses Kapitel behandelt die folgenden Themen:



## vSAN -Konzepte

VMware vSAN verwendet einen softwaredefinierten Ansatz zum Erstellen von gemeinsam genutztem Speicher für virtuelle Maschinen. Mit VMware Virtual SAN werden die lokalen physischen Speicherressourcen von ESXi-Hosts virtualisiert und in Speicherpools verwandelt, die unterteilt und virtuellen Maschinen und Anwendungen gemäß ihren Servicequalitätsanforderungen zugewiesen werden können. vSAN ist direkt im ESXi-Hypervisor implementiert.

Sie können vSAN so konfigurieren, dass es als Hybrid- oder All-Flash-Cluster verwendet wird. In Hybrid-Clustern werden Flash-Geräte für die Cache-Ebene verwendet. Magnetische Festplatten werden hingegen für die Speicherkapazitätsschicht verwendet. In Alle-Flash-Clustern werden Flash-Geräte als Zwischenspeicher und Kapazität verwendet.

Sie können vSAN auf Ihren vorhandenen Host-Clustern und beim Erstellen neuer Cluster aktivieren. vSAN fasst alle verfügbaren lokalen Kapazitätsgeräte zu einem einzelnen, von allen Hosts im vSAN-Cluster gemeinsam genutzten Datenspeicher zusammen. Sie können den Datenspeicher erweitern, indem Sie dem Cluster Kapazitätsgeräte oder Hosts mit Kapazitätsgeräten hinzufügen. vSAN funktioniert am besten, wenn alle ESXi-Hosts im Cluster bei allen Clustermitgliedern ähnliche oder identische Konfigurationen zu verwenden, einschließlich ähnlicher oder identischer Speicherkonfigurationen. Mit dieser konsistenten Konfiguration werden ausgeglichene Speicherkomponenten der virtuellen Maschine auf allen Geräten und Hosts im Cluster sichergestellt. Die Hosts ohne lokale Geräte können auch teilnehmen und ihre virtuellen Maschinen im Datenspeicher von vSAN ausführen.

Wenn ein Host seine lokalen Speichergeräte zum vSAN-Datenspeicher beiträgt, muss der Host mindestens ein Gerät für Flash-Cache und mindestens ein Gerät für Kapazität bereitstellen. Kapazitätsgeräte werden auch als Datenfestplatten bezeichnet.

Die Geräte auf dem beitragenden Host bilden eine oder mehrere Festplattengruppen. Jede Festplattengruppe enthält ein Flash-Zwischenspeichergerät und ein oder mehrere Kapazitätsgeräte für dauerhaften Speicher. Jeder Host kann für die Verwendung mehrerer Festplattengruppen konfiguriert werden.

Informationen zu Best Practices, Überlegungen zur Kapazität und allgemeine Empfehlungen in Bezug auf das Entwerfen und Dimensionieren eines vSAN-Clusters finden Sie im *Handbuch für VMware Virtual SAN Design und Sizing*.

## Merkmale von vSAN

In diesem Kapitel werden die Merkmale von vSAN, den zugehörigen Clustern und Datenspeichern zusammengefasst.

vSAN bietet zahlreiche Vorteile für Ihre Umgebung.

**Tabelle 1-1.** Funktionen von vSAN

| Unterstützte Funktionen | Beschreibung |
|---|---|
| Unterstützung von gemeinsam genutztem Speicher | vSAN unterstützt VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, wie HA, vMotion und DRS. Beispiel: Wenn ein Host überlastet wird, kann DRS die virtuellen Maschinen zu anderen Hosts im Cluster migrieren. |
| Just a Bunch Of Disks (JBOD) | vSAN unterstützt JBOD zur Verwendung in einer Blade-Server-Umgebung. Wenn Ihr Cluster Blade-Server enthält, können Sie die Kapazität des Datenspeichers mit JBOD-Speicher, der an die Blade-Server angeschlossen ist, erweitern. |
| On-Disk-Format | vSAN 6.6 unterstützt das Format 5.0 für virtuelle Festplattendateien, das für jeden vSAN-Cluster Unterstützung für eine stark skalierbare Snapshot- und Klonverwaltung bietet. Informationen zur Anzahl der je vSAN-Cluster unterstützten VM-Snapshots und -Klone finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*. |
| Reine Flash- und Hybrid-Konfigurationen | vSAN kann für reine Flash- oder Hybrid-Cluster konfiguriert werden. |
| Fault Domains | vSAN unterstützt das Konfigurieren von Fault Domains, um Hosts vor Rack- oder Gehäuseausfällen zu schützen, wenn der vSAN-Cluster sich über mehrere Racks oder Blade-Server-Gehäuse in einem Datencenter erstreckt. |
| Ausgeweiteter Cluster | vSAN unterstützt ausgeweitete Cluster, die sich über zwei geografische Standorte erstrecken. |
| vSAN-Integritätsdienst | Der vSAN-Integritätsdienst enthält vorkonfigurierte Tests zur Systemdiagnoseprüfung, um die Ursache von Problemen bei Clusterkomponenten zu überwachen, zu beheben und zu diagnostizieren und um potenzielle Risiken zu erkennen. |
| vSAN-Leistungsdienst | Der vSAN-Leistungsdienst beinhaltet statistische Diagramme, die zum Überwachen von IOPS, Durchsatz, Latenz und Überlastung verwendet werden. Sie können die Leistung eines Clusters, Hosts, einer Festplattengruppe, einer Festplatte und von VMs von vSAN überwachen. |
| Integration in vSphere-Speicherfunktionen | vSAN ist in den vSphere-Datenverwaltungsfunktionen integriert, die ursprünglich mit dem VMFS- und NFS-Speicher verwendet wurden. Diese Funktionen beinhalten Snapshots, verknüpfte Klone, vSphere Replication und vSphere APIs für den Datenschutz. |

**Tabelle 1-1.** Funktionen von vSAN (Fortsetzung)

| Unterstützte Funktionen | Beschreibung |
|---|---|
| VM-Speicherrichtlinien | vSAN arbeitet mit VM-Speicherrichtlinien, um einen VM-zentrierten Ansatz für die Speicherverwaltung zu unterstützen.<br>Wenn Sie während der Bereitstellung keine Speicherrichtlinie zuweisen, wird der VM automatisch die Standardspeicherrichtlinie für vSAN zugewiesen. |
| Schnelle Bereitstellung | vSAN ermöglicht eine schnelle Bereitstellung von Speicher in vCenter Server® während der Erstellung und Bereitstellung einer virtuellen Maschine. |

# vSAN -Begriffe und -Definitionen

vSAN führt bestimmte wichtige Begriffe und Definitionen ein.

Bevor Sie mit vSAN beginnen, überprüfen Sie die vSAN-Schlüsselbegriffe und -Definitionen.

## Festplattengruppe

Eine Festplattengruppe ist eine Einheit physischer Speicherkapazität auf einem Host und eine Gruppe physischer Geräte, die dem vSAN-Cluster Leistung und Kapazität bereitstellen. Auf jedem ESXi-Host, der mit seinen lokalen Geräten zu einem vSAN-Cluster beiträgt, sind die Geräte in Festplattengruppen organisiert.

Jede Festplattengruppe muss über ein Flash-Cache-Gerät und mindestens ein Kapazitätsgerät verfügen. Die für das Caching verwendeten Geräte können nicht über Festplattengruppen hinweg oder für andere Verwendungszwecke freigegeben werden. Jedes einzelne Caching-Gerät muss für eine einzige Festplattengruppe dediziert sein. In Hybrid-Clustern werden Flash-Geräte für die Cache-Ebene verwendet. Magnetische Festplatten werden hingegen für die Speicherkapazitätsschicht verwendet. In einem reinen Flash-Cluster werden Flash-Geräte für Cache und Kapazität verwendet. Informationen zum Erstellen und Verwalten von Festplattengruppen finden Sie unter Kapitel 10, „Geräteverwaltung in einem vSAN-Cluster“, auf Seite 111.

## Benötigte Kapazität

Menge an physischer Kapazität, die von einer oder mehreren virtuellen Maschinen zu einem bestimmten Zeitpunkt benötigt wird. Viele Faktoren bestimmen die benötigte Kapazität, unter anderem die benötigte Größe Ihrer VMDKs oder Schutzreplikate. Die für die Schutzreplikate verwendete Kapazität ist bei der Berechnung der Cachegröße nicht zu berücksichtigen.

## Objektbasierter Speicher

vSAN speichert und verwaltet Daten in Form von flexiblen Datencontainern, die als Objekte bezeichnet werden. Ein Objekt ist ein logisches Volume, dessen Daten und Metadaten über den Cluster verteilt sind. Jede VMDK ist beispielsweise ein Objekt, genauso wie jeder Snapshot. Wenn Sie eine virtuelle Maschine auf einem vSAN-Datenspeicher bereitstellen, erstellt vSAN eine Gruppe von Objekten aus mehreren Komponenten für jede virtuelle Festplatte. Außerdem wird der VM-Start-Namespace erstellt, ein Containerobjekt, in dem alle Metadatendateien der virtuellen Maschine gespeichert werden. Basierend auf der zugewiesenen VM-Speicherrichtlinie wird von vSAN jedes Objekt einzeln bereitgestellt und verwaltet. Dies kann auch das Erstellen einer RAID-Konfiguration für jedes Objekt umfassen.

Wenn vSAN ein Objekt für eine virtuelle Festplatte erstellt und festlegt, wie das Objekt im Cluster verteilt werden soll, werden die folgenden Parameter berücksichtigt:

- vSAN stellt sicher, dass die Anforderungen an die virtuelle Festplatte entsprechend den festgelegten VM-Speicherrichtlinieneinstellungen angewendet werden.

- vSAN überprüft, ob zum Zeitpunkt der Bereitstellung die richtigen Clusterressourcen verwendet werden. Beispielsweise bestimmt vSAN anhand der Schutzrichtlinie die Anzahl der zu erstellenden Replikate. Die Leistungsrichtlinie ermittelt die Menge des jedem Replikat zugeordneten Flash-Lesecache und bestimmt, wie viele Stripes für jedes Replikat erstellt und wo diese im Cluster gespeichert werden.
- vSAN überwacht ständig den Status der Richtlinieneinhaltung der virtuellen Festplatte und erstellt Berichte dazu. Wenn Sie einen nicht konformen Richtlinienstatus finden, müssen Sie das zugrunde liegende Problem diagnostizieren und beheben.

  **Hinweis** Falls erforderlich, können Sie die VM-Speicherrichtlinieneinstellungen bearbeiten. Die Bearbeitung der Speicherrichtlinieneinstellungen hat keine Auswirkungen auf den VM-Zugriff. vSAN sorgt aktiv für eine Drosselung der für die Neukonfiguration verwendeten Speicher- und Netzwerkressourcen, um die Auswirkungen der Neukonfiguration von Objekten auf die normale Arbeitslast auf ein Minimum zu beschränken. Wenn Sie die VM-Speicherrichtlinieneinstellungen ändern, kann vSAN einen Objektneuerstellungsvorgang und eine nachfolgende Neusynchronisierung initiieren. Siehe „Informationen zur Neusynchronisierung eines vSAN-Clusters“, auf Seite 149.

- vSAN stellt sicher, dass die erforderlichen Schutzkomponenten, z. B. Spiegel und Zeugen, sich auf getrennten Hosts oder in unterschiedlichen Fault Domains befinden. Um z. B. Komponenten während eines Ausfalls neu zu erstellen, sucht vSAN nach ESXi-Hosts, die die Platzierungsregeln erfüllen, wobei die Komponenten der VM-Objekte auf zwei verschiedenen Hosts oder in Fault Domains platziert werden müssen.

## vSAN -Datenspeicher

Nachdem Sie vSAN auf einem Cluster aktiviert haben, wird ein einzelner vSAN-Datenspeicher erstellt. Er wird in der Liste der möglicherweise verfügbaren Datenspeicher als eine andere Art von Datenspeicher, beispielsweise als virtuelles Volume, VMFS oder NFS, angezeigt. Ein einzelner vSAN-Datenspeicher kann für jede virtuelle Maschine oder jede virtuelle Festplatte verschiedene Service-Level bieten. In vCenter Server® werden Speichermerkmale des vSAN-Datenspeichers als Funktionssatz angezeigt. Sie können diese Funktionen beim Definieren einer Speicherrichtlinie für virtuelle Maschinen referenzieren. Wenn Sie später virtuelle Maschinen bereitstellen, verwendet vSAN diese Richtlinie, um virtuelle Maschinen basierend auf den Anforderungen Ihrer virtuellen Maschine optimal zu platzieren. Allgemeine Informationen zum Verwenden von Speicherrichtlinien finden Sie in der Dokumentation zu *vSphere Storage*.

Bei einem vSAN-Datenspeicher müssen die folgenden Merkmale beachtet werden.

- vSAN erstellt einen einzelnen vSAN-Datenspeicher, auf den alle Hosts im Cluster zugreifen können, unabhängig davon, ob sie dem Cluster Speicher bereitstellen. Alle Hosts können zudem beliebige weitere Datenspeicher mounten, z. B. virtuelle Volumes, VMFS oder NFS.
- Sie können Storage vMotion zum Verschieben von virtuellen Maschinen zwischen vSAN-, NFS- und VMFS-Datenspeichern verwenden.
- Nur Magnetfestplatten und Flash-Geräte, die für Kapazität verwendet werden, können zur Datenspeicherkapazität beitragen. Die für Flash-Cache verwendete Geräte werden nicht als Teil des Datenspeichers betrachtet.

## Objekte und Komponenten

Jedes Objekt besteht aus einem Satz von Komponenten, die durch die in der VM-Speicherrichtlinie verwendeten Funktionen bestimmt werden. Wenn z. B. die Richtlinie für **Primäre Ebene von zu tolerierenden Fehlern** auf 1 eingestellt ist, stellt vSAN sicher, dass die Schutzkomponenten, beispielsweise Replikate und Zeugen, auf getrennten Hosts im vSAN-Cluster platziert werden, wobei jedes Replikat eine Objektkomponente ist. Wenn darüber hinaus in derselben Richtlinie die **Anzahl der Festplatten-Stripes pro Objekt** auf zwei oder mehr konfiguriert ist, verteilt vSAN das Objekt außerdem per Striping auf mehrere Kapazitätsgeräte und jeder Stripe wird als Komponente des jeweiligen Objekts betrachtet. Bei Bedarf kann vSAN zudem große Objekte in mehrere Komponenten aufteilen.

Ein vSAN-Datenspeicher enthält die folgenden Objekttypen:

| | |
|---|---|
| **VM-Home-Namespace** | Das Startverzeichnis der virtuellen Maschine, in dem alle VM-Konfigurationsdateien gespeichert sind, z. B. `.vmx`-Dateien, Protokolldateien, VMDKs, und Snapshot-Delta-Beschreibungsdateien. |
| **VMDK** | Eine Festplattendatei für eine virtuelle Maschine oder `.vmdk` speichert die Inhalte eines Festplattenlaufwerks einer virtuellen Maschine. |
| **VM-Auslagerungsobjekt** | Wird beim Einschalten einer virtuellen Maschine erstellt. |
| **Snapshot-Delta-VMDKs** | Werden beim Erstellen von VM-Snapshots angelegt. |
| **Arbeitsspeicherobjekt** | Wird beim Erstellen oder Anhalten einer virtuellen Maschine erstellt, wenn die Arbeitsspeicher-Snapshot-Option aktiviert ist. |

## Übereinstimmungsstatus der virtuellen Maschine: „Übereinstimmung“ und „Nicht übereinstimmend“.

Eine virtuelle Maschine wird als „Nicht übereinstimmend“ betrachtet, wenn mindestens eines ihrer Objekte die Anforderungen der zugewiesenen Speicherrichtlinie nicht erfüllt. Der Status wechselt beispielsweise in „Nicht übereinstimmend“, wenn auf eine der Spiegelkopien nicht zugegriffen werden kann. Erfüllen Ihre virtuellen Maschinen die in der Speicherrichtlinie definierten Anforderungen, lautet ihr Status „Übereinstimmung“. Auf der Registerkarte **Platzierung physischer Festplatten** auf der Seite Virtuelle Festplatten können Sie den Übereinstimmungsstatus des VM-Objekts überprüfen. Informationen zur Fehlerbehebung für vSAN-Cluster finden Sie unter „Behandeln von Fehlern in vSAN“, auf Seite 172.

## Komponentenzustand: Die Zustände „Herabgestuft“ und „Abwesend“

vSAN erkennt die folgenden Fehlerzustände für Komponenten:

- Herabgestuft. Eine Komponente befindet sich im Zustand „Herabgestuft“, wenn vSAN einen dauerhaften Ausfall einer Komponente feststellt und davon ausgeht, dass die ausgefallene Komponente nicht in den ursprünglichen Zustand wiederhergestellt werden kann. Daraufhin beginnt vSAN sofort, die herabgestufte Komponente neu zu erstellen. Dieser Zustand kann auftreten, wenn sich eine Komponente auf einem ausgefallenen Gerät befindet.
- Abwesend. Eine Komponente befindet sich im Zustand „Abwesend“, wenn vSAN einen temporären Ausfall einer Komponente feststellt und die Komponenten, einschließlich all ihrer Daten, wiederhergestellt werden können und vSAN in den ursprünglichen Zustand zurückgesetzt werden kann. Dieser Zustand kann eintreten, wenn Sie Hosts neu starten oder ein Gerät vom vSAN-Host trennen. vSAN beginnt mit dem Neuerstellen der abwesenden Komponenten, wenn dieser Status länger als 60 Minuten anhält.

## Objektzustand: „Ordnungsgemäß“ und „Nicht ordnungsgemäß“

Je nach Typ und Anzahl der Fehler im Cluster kann ein Objekt einen der folgenden Zustände aufweisen:

- Ordnungsgemäß. Wenn mindestens eine vollständige RAID 1-Spiegelung oder die Mindestzahl der benötigten Datensegmente verfügbar ist, wird das Objekt als in einem ordnungsgemäßen Zustand befindlich betrachtet.
- Nicht ordnungsgemäß. Ein Objekt gilt als nicht ordnungsgemäß, wenn kein vollständiger Spiegel verfügbar ist oder die mindestens erforderliche Anzahl von Datensegmenten für RAID 5- oder RAID 6-Objekte nicht verfügbar ist. Wenn weniger als 50 Prozent der Stimmen eines Objekts verfügbar sind, ist das Objekt nicht ordnungsgemäß. Mehrerer Ausfälle im Cluster können dazu führen, dass Objekte nicht ordnungsgemäß sind. Wenn der Betriebsstatus eines Objekts als nicht ordnungsgemäß betrachtet wird, hat dies Auswirkungen auf die Verfügbarkeit der zugeordneten VM.

## Zeuge

Ein Zeuge ist eine Komponente, die nur Metadaten und keine eigentlichen Anwendungsdaten enthält. Wenn eine Entscheidung hinsichtlich der Verfügbarkeit der verbleibenden Datenspeicherkomponenten nach einem potenziellen Ausfall getroffen werden muss, dient der Zeuge als Entscheidungskriterium. Ein Zeuge verbraucht etwa 2 MB Speicherplatz für Metadaten im vSAN-Datenspeicher bei Verwendung des Festplattenformats der Version 1.0 bzw. 4 MB für das Festplattenformat der Version 2.0 und höher.

vSAN 6.0 und höhere Versionen sorgen mit einem asymmetrischen Abstimmungssystem für das Quorum, wobei jede Komponente möglicherweise mehrere Stimmen für die Entscheidung über die Verfügbarkeit von Objekten hat. Der Zugriff auf mehr als 50 % der Stimmen, die das Speicherobjekt einer VM ausmachen, muss jederzeit möglich sein, damit das Objekt als verfügbar betrachtet wird. Wenn 50 % oder weniger Stimmen für alle Hosts zugänglich sind, kann der vSAN-Datenspeicher nicht mehr auf das Objekt zugreifen. Objekte, auf die kein Zugriff möglich ist, können die Verfügbarkeit der zugeordneten VM beeinträchtigen.

## Speicherrichtlinienbasierte Verwaltung (SPBM)

Wenn Sie vSAN verwenden, können Sie Speicheranforderungen für virtuelle Maschinen wie Leistung und Verfügbarkeit in Form einer Richtlinie definieren. vSAN sorgt dafür, dass den in vSAN-Datenspeichern bereitgestellten virtuellen Maschinen mindestens eine VM-Speicherrichtlinie zugewiesen wird. Wenn Sie die Speicheranforderungen Ihrer virtuellen Maschinen kennen, können Sie benutzerdefinierte Speicherrichtlinien definieren und diese Ihren virtuellen Maschinen zuweisen. Wenn Sie bei der Bereitstellung virtueller Maschinen keine Speicherrichtlinie anwenden, weist vSAN automatisch eine vSAN-Standardrichtlinie zu, die Folgendes festlegt: **Primäre Ebene von zu tolerierenden Fehlern** ist 1, ein einziger Festplatten-Stripe für jedes Objekt und eine schnell („thin“) bereitgestellte virtuelle Festplatte. Um die besten Ergebnisse zu erzielen, definieren Sie Ihre eigenen VM-Speicherrichtlinien, selbst wenn die Anforderungen der Richtlinie denjenigen entsprechen, die in der Standardspeicherrichtlinie definiert sind. Informationen zur Arbeit mit vSAN-Speicherrichtlinien finden Sie unter Kapitel 12, „Verwenden von vSAN-Speicherrichtlinien“, auf Seite 137.

## Ruby vSphere Console (RVC)

Ruby vSphere Console (RVC) ist eine Befehlszeilenschnittstelle, die zum Verwalten des vSAN-Clusters und für die Fehlerbehebung verwendet wird. RVC stellt anstelle der hostzentrierten Ansicht von `esxcli` eine clusterweite Ansicht bereit. Da RVC im Lieferumfang von vCenter Server Appliance und vCenter Server für Windows enthalten ist, brauchen Sie es nicht separat zu installieren. Informationen zu den RVC-Befehlen finden Sie im *Referenzhandbuch zu RVC-Befehlen*.

## vSphere PowerCLI

VMware vSphere PowerCLI fügt Befehlszeilenskriptunterstützung für vSAN hinzu, um Sie bei der Automatisierung von Konfigurations- und Verwaltungsaufgaben zu unterstützen. vSphere PowerCLI ist eine Windows PowerShell-Schnittstelle zur vSphere API. PowerCLI enthält Cmdlets zur Verwaltung von vSAN-Komponenten. Informationen zur Verwendung von vSphere PowerCLI finden Sie in der *vSphere PowerCLI-Dokumentation*.

## vSAN Observer

VMware vSAN Observer ist ein webbasiertes Tool, das auf RVC ausgeführt wird und zur umfassenden Leistungsanalyse und Überwachung des vSAN-Clusters dient. Verwenden Sie vSAN Observer zum Anzeigen der Leistungsstatistiken der Kapazitätsschicht, von statistischen Informationen über physische Festplattengruppen, der aktuellen Auslastung der CPU, der Nutzung von vSAN-Speicherpools und der physischen und arbeitsspeicherinternen Objektverteilung in vSAN-Clustern.

Informationen zum Konfigurieren, Starten und Verwenden von RVC und vSAN Observer finden Sie im *Referenzhandbuch zur vSAN-Fehlerbehebung*.

# vSAN und herkömmlicher Speicher

vSAN weist zwar viele gemeinsame Merkmale mit herkömmlichen Speicher-Arrays auf, aber das Verhalten und die Funktionsweise von vSAN sind insgesamt unterschiedlich. Beispielsweise kann vSAN nur ESXi-Hosts verwalten und verwenden, und eine einzelne vSAN-Instanz kann nur einen einzigen Cluster unterstützen.

vSAN und herkömmlicher Speicher unterscheiden sich auch in den folgenden wichtigen Aspekten:

- vSAN benötigt keinen externen Netzwerkspeicher für die Remotespeicherung von VM-Dateien, wie beispielsweise auf einem Fibre Channel (FC) oder einem Storage Area Network (SAN).
- Bei Verwendung von herkömmlichem Speicher teilt der Speicheradministrator vorab Speicherplatz auf unterschiedlichen Speichersystemen zu. vSAN konvertiert die lokalen physischen Speicherressourcen der ESXi-Hosts automatisch in einen einzelnen Speicherpool. Diese Pools können unterteilt und virtuellen Maschinen und Anwendungen gemäß ihren Servicequalitätsanforderungen zugewiesen werden.
- vSAN hat kein Konzept für herkömmliche Speichervolumes auf Basis von LUNs oder NFS-Freigaben, obwohl der iSCSI-Zieldienst LUNs verwendet, damit ein Initiator auf einem Remotehost Blockebenendaten auf ein Speichergerät im vSAN-Cluster übertragen kann.
- Einige Standardspeicherprotokolle, z. B. FCP, gelten für vSAN nicht.
- vSAN ist nahtlos in vSphere integriert. Im Gegensatz zu herkömmlichem Speicher benötigen Sie für vSAN keine separaten Plug-Ins bzw. keine Speicherkonsole. vSAN können Sie mit dem vSphere Web Client bereitstellen, verwalten und überwachen.
- vSAN muss nicht von einem eigens dafür vorgesehenen Speicheradministrator verwaltet werden. Stattdessen kann ein vSphere-Administrator eine vSAN-Umgebung verwalten.
- Bei Verwendung von vSAN werden automatisch VM-Speicherrichtlinien zugewiesen, wenn Sie neue VMs bereitstellen. Die Speicherrichtlinien können bei Bedarf dynamisch geändert werden.

# Erstellen eines vSAN -Clusters

Wenn Sie vSAN verwenden möchten, haben Sie die Auswahl unter mehreren Konfigurationslösungen für die Bereitstellung eines vSAN-Clusters.

In Abhängigkeit von Ihren Anforderungen können Sie vSAN mithilfe einer der folgenden Methoden bereitstellen.

## vSAN Ready Node

Bei vSAN Ready Node handelt es sich um eine vorkonfigurierte Lösung der vSAN-Software, die von VMware-Partner wie beispielsweise Cisco, Dell, Fujitsu, IBM und Supermicro bereitgestellt wird. Diese Lösung beinhaltet validierte Serverkonfiguration in Form von getesteter, zertifizierter Hardware für die vSAN-Bereitstellung, die vom Server-OEM und von VMware empfohlen wird. Informationen zur vSAN Ready Node-Lösung für einen bestimmten Partner finden Sie auf der VMware-Partner-Website.

## Benutzerdefinierter vSAN -Cluster

Sie können einen vSAN-Cluster erstellen, indem Sie einzelne Software- und Hardwarekomponenten wie Treiber, Firmware und Speicher-E/A-Controller auswählen, die auf der VMware-Kompatibilitätshandbuch-Website (vSAN Compatibility Guide, VCG) unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind. Sie können beliebige Server, Speicher-E/A-Controller, Kapazitäts- und Flash-Cache-Geräte, Arbeitsspeicher, eine beliebige Anzahl von erforderlichen Kernen pro CPU usw. auswählen, die auf der VCG-Website zertifiziert und aufgelistet sind. Lesen Sie die Kompatibilitätsinformationen auf der VCG-Website durch, bevor Sie Software- und Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller, die von vSAN unterstützt werden, auswäh-

len. Verwenden Sie beim Entwerfen eines vSAN-Clusters nur Geräte, Firmware und Treiber, die auf der VCG-Website aufgelistet sind. Die Verwendung von Software- und Hardwareversionen, die nicht auf der VCG-Website aufgelistet sind, kann zu Clusterfehlern oder unerwarteten Datenverlusten führen. Informationen zum Entwerfen eines vSAN-Clusters finden Sie in Kapitel 3, „Entwerfen und Dimensionieren eines vSAN-Clusters“, auf Seite 21.

# Integrieren in andere VMware-Software

Wenn vSAN betriebsbereit ist, erfolgt die Integration in den restlichen VMware-Software-Stack. Mithilfe der vSphere-Komponenten und -Funktionen wie etwa vSphere vMotion, Snapshots, Klone, Distributed Resource Scheduler (DRS), vSphere High Availability, vCenter Site Recovery Manager usw. können Sie weitgehend dieselben Aufgaben wie mit herkömmlichen Speicherlösungen ausführen.

## Integrieren in vSphere HA

Sie können vSphere HA und vSAN auf demselben Cluster aktivieren. Wie herkömmliche Datenspeicher gewährleistet vSphere HA denselben Schutz für virtuelle Maschinen auf vSAN-Datenspeichern. Dieser Schutz bedeutet Einschränkungen bei der Interaktion von vSphere HA und vSAN. Spezifische Überlegungen zur Integration von vSphere HA und vSAN finden Sie unter „Verwenden von vSAN und vSphere HA“, auf Seite 56.

## Integrieren in VMware Horizon View

vSAN kann in VMware Horizon View integriert werden. Durch die Integration bietet vSAN die folgenden Vorteile für virtuelle Desktop-Umgebungen:

- Hochleistungsspeicher mit automatischer Zwischenspeicherung
- Speicherrichtlinienbasierte Verwaltung für die automatische Wartung

Informationen zum Integrieren von vSAN in VMware Horizon finden Sie in der Dokumentation zu *VMware Horizon with View*. Informationen zum Design und zur Skalierung von VMware Horizon View für vSAN finden Sie im *Handbuch für Design und Sizing für Horizon View*.

# Einschränkungen von vSAN

In diesem Thema werden die Einschränkungen von vSAN behandelt.

Wenn Sie mit vSAN arbeiten, beachten Sie folgende Einschränkungen:

- vSAN unterstützt keine Hosts, die zu mehreren vSAN-Clustern gehören. Ein vSAN-Host kann jedoch auf andere externe Speicherressourcen zugreifen, die über Cluster hinweg gemeinsam genutzt werden.
- vSAN unterstützt vSphere DPM und Storage I/O Control nicht.
- vSAN unterstützt SCSI-Reservierungen nicht.
- vSAN unterstützt RDM, VMFS, Diagnosepartitionen und andere Gerätezugriffsfunktionen nicht.

# Anforderungen für die Aktivierung von vSAN 2

Bevor Sie das vSAN aktivieren, überprüfen Sie, ob Ihre Umgebung alle Anforderungen erfüllt.

Dieses Kapitel behandelt die folgenden Themen:



## Hardwareanforderungen für vSAN

Stellen Sie sicher, dass die ESXi-Hosts in Ihrer Organisation die vSAN-Hardwareanforderungen erfüllen.

### Anforderungen an Speichergeräte

Alle Kapazitätsgeräte, Treiber und Firmware-Versionen in Ihrer vSAN-Konfiguration müssen zertifiziert sein und im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch* aufgeführt werden.

**Tabelle 2-1.** Anforderungen an Speichergeräte für vSAN -Hosts

| Speicherkomponente | Anforderungen |
|---|---|
| Cache | ■ Ein SAS- oder SATA-SSD-Laufwerk oder PCIe-Flash-Gerät.<br>■ Bevor Sie den Wert für **Primäre Ebene von zu tolerierenden Fehlern** berechnen, überprüfen Sie die Größe des Flash-Caching-Geräts in jeder Festplattengruppe. Überprüfen Sie, dass mindestens 10 Prozent des Speichers, der voraussichtlich auf dem Kapazitätsgerät verbraucht wird, zur Verfügung gestellt wird – und zwar ohne Replikate wie beispielsweise Spiegel.<br>■ vSphere Flash Read Cache darf keine Flash-Geräte nutzen, die für vSAN-Cache reserviert sind.<br>■ Die Flash-Cache-Geräte dürfen nicht mit VMFS oder einem anderen Dateisystem formatiert sein. |
| VM-Datenspeicher | ■ Stellen Sie bei Konfigurationen mit Hybrid-Gruppen sicher, dass mindestens eine SAS-, NL-SAS- oder SATA-Magnetfestplatte vorhanden ist.<br>■ Stellen Sie bei Konfigurationen mit reinen Flash-Festplattengruppen sicher, dass mindestens ein SAS- oder SATA-SSD-Laufwerk oder PCIe-Flash-Gerät vorhanden ist. |
| Speicher-Controller | Ein SAS- oder SATA-HBA (Hostbusadapter) oder ein RAID-Controller im Passthrough- oder RAID 0-Modus. |

### Arbeitsspeicher

Die Anforderungen an den Arbeitsspeicher für vSAN hängen von der Anzahl der Festplattengruppen und Geräte ab, die der ESXi-Hypervisor verwalten muss. Jeder Host muss über mindestens 32 GB Arbeitsspeicher verfügen, um die Höchstanzahl von 5 Festplattengruppen und 7 Kapazitätsgeräten pro Festplattengruppe aufnehmen zu können.

### Flash-Startgeräte

Während des Installationsvorgangs erstellt das ESXi-Installationsprogramm eine Core-Dump-Partition auf dem Startgerät. Die Standardgröße der Core-Dump-Partition erfüllt die meisten Installationsanforderungen.

- Wenn der Arbeitsspeicher des ESXi-Hosts 512 GB oder weniger beträgt, können Sie den Host von einem USB-, SD- oder SATADOM-Gerät aus starten. Wenn Sie einen vSAN-Host von einem USB-Gerät aus oder über eine SD-Karte starten, muss die Größe des Startgeräts mindestens 4 GB betragen.
- Ist der Arbeitsspeicher des ESXi-Hosts größer als 512 GB, müssen Sie den Host von einem SATADOM- oder Festplattengerät aus starten. Wenn Sie einen vSAN-Host von einem SATADOM-Gerät aus starten, müssen Sie ein SLC-Gerät (Single-Level Cell) verwenden. Die Größe des Startgeräts muss mindestens 16 GB betragen.

**Hinweis** In vSAN 6.5 und höher können Sie die Größe einer vorhandenen Core-Dump-Partition auf einem ESXi-Host in einem vSAN-Cluster ändern und somit von USB-/SD-Geräten aus starten. Weitere Informationen finden Sie in dem VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2147881.

Wenn Sie einen ESXi 6.0-Host oder höher von einem USB-Gerät oder von einer SD-Karte starten, werden die vSAN-Nachverfolgungsprotokolle auf RAMDisk geschrieben. Diese Protokolle werden beim Herunterfahren oder bei einem Systemabsturz (PANIC) automatisch per Offload an dauerhafte Medien übertragen. Dies ist die einzige Unterstützungsmethode für die Verarbeitung von vSAN-Traces beim Starten eines ESXi-Hosts über einen USB-Stick oder eine SD-Karte. Bei einem Stromausfall werden vSAN-Trace-Protokolle nicht beibehalten.

Wenn Sie einen ESXi 6.0-Host oder höher über ein SATADOM-Gerät starten, werden die vSAN-Nachverfolgungsprotokolle direkt auf ein SATADOM-Gerät geschrieben. Daher ist es wichtig, dass das SATADOM-Gerät die in diesem Handbuch aufgeführten Spezifikationen erfüllt.

## Cluster-Anforderungen für vSAN

Vergewissern Sie sich, dass ein Host-Cluster die Anforderungen für die Aktivierung von vSAN erfüllt.

- Alle Kapazitätsgeräte, Treiber und Firmware-Versionen in Ihrer vSAN-Konfiguration müssen zertifiziert sein und im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch* aufgeführt werden.
- Ein vSAN-Cluster muss mindestens drei Hosts aufweisen, die Kapazität zum Cluster beitragen. Informationen zu den Überlegungen für einen Cluster mit drei Hosts finden Sie unter „Design-Überlegungen für einen Cluster vSAN“, auf Seite 29.
- Ein Host, der sich in einem vSAN-Cluster befindet, darf nicht an anderen Clustern beteiligt sein.

## Softwareanforderungen für vSAN

Stellen Sie sicher, dass die vSphere-Komponenten in Ihrer Umgebung die Anforderungen an die Softwareversion zur Verwendung von vSAN erfüllen.

Um den vollständigen Satz von vSAN-Funktionen verwenden zu können, müssen die ESXi-Hosts in vSAN-Clustern die Version 6.5 oder höher aufweisen. Während des vSAN-Upgrades von vorherigen Versionen können Sie die aktuelle Version des Festplattenformats beibehalten, können dann aber viele der neuen Funktionen nicht verwenden. vSAN 6.6 und höher unterstützt alle Festplattenformate.

# Netzwerkanforderungen für vSAN

Stellen Sie sicher, dass die Netzwerkinfrastruktur und die Netzwerkkonfiguration auf den ESXi-Hosts die Mindestnetzwerkanforderungen für vSAN erfüllen.

**Tabelle 2-2.** Netzwerkanforderungen für vSAN

| Netzwerkkomponente | Anforderung |
|---|---|
| Hostbandbreite | Bei jedem Host muss eine Mindestbandbreite für vSAN reserviert sein.<br>■ 1 Gbit/s reserviert für Hybridkonfigurationen<br>■ 10 Gbit/s für Alle-Flash-Konfigurationen reserviert oder gemeinsam genutzt<br>Informationen zu Netzwerküberlegungen in vSAN finden Sie unter „Entwerfen des vSAN-Netzwerks“, auf Seite 30. |
| Verbindung zwischen Hosts | Jeder Host im vSAN-Cluster muss unabhängig davon, ob er Kapazität beiträgt, über einen VMkernel-Netzwerkadapter für vSAN-Datenverkehr verfügen. Siehe „Einrichten eines VMkernel-Netzwerks für vSAN“, auf Seite 50. |
| Hostnetzwerk | Alle Hosts in Ihrem vSAN-Cluster müssen mit einem vSAN-Netzwerk der Schicht 2 oder Schicht 3 verbunden sein. |
| IPv4- und IPv6-Unterstützung | Das vSAN-Netzwerk unterstützt IPv4 und IPv6. |

# Lizenzanforderungen

Prüfen Sie, ob Sie über eine gültige Lizenz für vSAN verfügen.

Die Verwendung von vSAN in Produktionsumgebungen erfordert eine spezielle Lizenz, die Sie den vSAN-Clustern zuweisen.

Sie können dem Cluster eine vSAN-Standardlizenz oder eine Lizenz für erweiterten Funktionsumfang zuweisen. Zu den erweiterten Funktionen gehören RAID 5/6 Erasure Coding sowie Deduplizierung und Komprimierung. Für IOPS-Grenzwerte und ausgeweitete Cluster ist eine Enterprise-Lizenz erforderlich. Informationen zum Zuweisen von Lizenzen finden Sie unter „Konfigurieren von Lizenzeinstellungen für einen vSAN-Cluster“, auf Seite 54.

Die Kapazität der Lizenz muss die Gesamtanzahl von CPUs im Cluster abdecken.

# Entwerfen und Dimensionieren eines vSAN -Clusters 3

Um die besten Ergebnisse hinsichtlich Leistung und Verwendung zu erzielen, planen Sie vor dem Bereitstellen von vSAN in einer vSphere-Umgebung die Funktionen und die Konfiguration von Hosts und zugehörigen Speichergeräten. Berücksichtigen Sie sorgfältig bestimmte Host- und Netzwerkkonfigurationen innerhalb des vSAN-Clusters.

Die Dokumentation zu *Verwalten von VMware vSAN* beleuchtet die wichtigsten Punkte bezüglich Entwurf und Dimensionierung eines vSAN-Clusters. Detaillierte Anweisungen zu Entwurf und Dimensionierung eines vSAN-Clusters finden Sie unter *Handbuch für VMware vSAN Design und Sizing*.

Dieses Kapitel behandelt die folgenden Themen:



## Entwerfen und Dimensionieren von vSAN -Speicherkomponenten

Planen Sie Kapazität und Zwischenspeicher auf der Grundlage der erwarteten Nutzung. Berücksichtigen Sie die Anforderungen in Bezug auf Verfügbarkeit und Belastungsfähigkeit.

- Design-Überlegungen für Magnetfestplatten in vSAN auf Seite 26

  Berücksichtigen Sie beim Planen der Größe und Anzahl magnetischer Festplatten für Kapazität in Hybridkonfigurationen die folgenden Anforderungen in Bezug auf Speicherplatz und Leistungsfähigkeit.

- Überlegungen zum Design für Speicher-Controllern in vSAN auf Seite 27

  Verwenden Sie auf den Hosts eines vSAN-Clusters Speicher-Controller, die die Anforderungen an Leistung und Verfügbarkeit am besten erfüllen.

## Kapazitätsplanung in vSAN

Sie können die Kapazität eines vSAN-Datenspeichers festlegen, damit die VM-Dateien im Cluster sowie Fehler und Wartungsvorgänge verarbeitet werden.

### Rohkapazität

Um die Rohkapazität eines vSAN-Datenspeichers zu bestimmen, addieren Sie alle Festplattengruppen im Cluster mit der Größe der Kapazitätsgeräte in diesen Festplattengruppen, abzüglich des Overheads durch das vSAN-Festplattenformat.

### Primäre Ebene von zu tolerierenden Fehlern

Bei der Planung der Kapazität des vSAN-Datenspeichers (ohne die Anzahl virtueller Maschinen und die Größe der VMDK-Dateien) müssen Sie die Attribute **Primäre Ebene von zu tolerierenden Fehlern** und **Fehlertoleranzmethode** der VM-Speicherrichtlinien für den Cluster berücksichtigen.

**Primäre Ebene von zu tolerierenden Fehlern** spielt eine wichtige Rolle bei der Planung und Größenanpassung der Speicherkapazität für vSAN. Basierend auf den Verfügbarkeitsanforderungen einer virtuellen Maschine kann diese Einstellung im Vergleich zum Verbrauch einer virtuellen Maschine und von deren Einzelgeräten mindestens zur Verdoppelung des Verbrauchs führen.

Beispiel: Wenn **Fehlertoleranzmethode** auf **RAID-1 (Spiegelung) - Leistung** und **Primäre Ebene von zu tolerierenden Fehlern** (PFTT) auf 1 festgelegt ist, können virtuelle Maschinen etwa 50 Prozent der Rohkapazität nutzen. Wenn der PFTT-Wert auf 2 festgelegt ist, beträgt die nutzbare Kapazität etwa 33 Prozent. Wenn der PFTT-Wert auf 3 festgelegt ist, beträgt die nutzbare Kapazität etwa 25 Prozent.

Wenn allerdings **Fehlertoleranzmethode** auf **RAID-5/6 (Erasure Coding) - Kapazität** und der PFTT-Wert auf 1 festgelegt ist, können virtuelle Maschinen etwa 75 Prozent der Rohkapazität nutzen. Wenn der PFTT-Wert auf 2 festgelegt ist, beträgt die nutzbare Kapazität etwa 67 Prozent. Weitere Informationen zu RAID 5/6 finden Sie unter „Verwenden von RAID 5- oder RAID 6-Erasure Coding“, auf Seite 80.

Informationen zu den Attributen in einer vSAN-Speicherrichtlinie finden Sie in Kapitel 12, „Verwenden von vSAN-Speicherrichtlinien“, auf Seite 137.

### Berechnen der erforderlichen Kapazität

Die für die VMs in einem Cluster mit RAID 1-Spiegelung benötigte Kapazität basiert auf den folgenden Kriterien:

1 Berechnen Sie den Speicherplatz, den die virtuellen Maschinen im vSAN-Cluster voraussichtlich verbrauchen werden.

```
expected overall consumption = number of VMs in the cluster * expected percentage of consumption per VMDK
```

2 Berücksichtigen Sie das Attribut **Primäre Ebene von zu tolerierenden Fehlern**, das in den Speicherrichtlinien für die virtuellen Maschinen im Cluster konfiguriert ist. Dieses Attribut hat direkte Auswirkungen auf die Anzahl der Replikate einer VMDK-Datei auf den Hosts im Cluster.

```
datastore capacity = expected overall consumption * (PFTT + 1)
```

3 Schätzen Sie die Overhead-Anforderung des vSAN-Festplattenformats.

- Version 3.0 und höher des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät. Deduplizierung und Komprimierung mit aktivierter Software-Prüfsumme benötigt zusätzlichen Overhead von ungefähr 6,2 Prozent Kapazität pro Gerät.
- Version 2.0 des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät.
- Version 1.0 des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise 1 GB pro Kapazitätsgerät.

## Richtlinien für die Größenanpassung der Kapazität

- Lassen Sie mindestens 30 Prozent des Speicherplatzes ungenutzt, um zu verhindern, dass vSAN eine Neuverteilung der Speicherlast vornimmt. vSAN führt eine Neuverteilung der Komponenten im Cluster durch, falls der Verbrauch auf einem physischen Kapazitätsgerät 80 Prozent übersteigt. Der Neuverteilungsvorgang führt möglicherweise zu einer Leistungsbeeinträchtigung der Anwendungen. Zur Vermeidung dieser Probleme sollte die Speicherbelegung weniger als 70 Prozent betragen.
- Planen Sie zusätzliche Kapazität für potenzielle Fehler oder den Austausch von Kapazitätsgeräten, Festplattengruppen und Hosts ein. Wenn ein Kapazitätsgerät nicht erreichbar ist, stellt vSAN die Komponenten auf einem anderen Gerät im Cluster wieder her. Wenn ein Flash-Cache-Gerät ausfällt oder entfernt wird, stellt vSAN die Komponenten von der gesamten Festplattengruppe wieder her.
- Reservieren Sie zusätzliche Kapazität, um sicherzustellen, dass vSAN Komponenten wiederherstellt, wenn ein Hostfehler auftritt oder wenn ein Host in den Wartungsmodus wechselt. Stellen Sie beispielsweise für Hosts ausreichende Kapazität bereit, sodass genügend freie Kapazität für Komponenten vorhanden ist, damit sie nach einem Hostfehler oder während der Wartung erfolgreich neu erstellt werden können. Dies ist bei mehr als drei Hosts wichtig, damit Sie genügend freie Kapazität haben, um die fehlgeschlagenen Komponenten wiederherzustellen. Wenn ein Host fehlschlägt, findet die Neuerstellung auf dem auf einem anderen Host verfügbaren Speicher statt, sodass kein anderer Ausfall toleriert werden kann. In einem Cluster mit drei Hosts führt vSAN jedoch den Neuerstellungsvorgang nicht aus, falls für **Primäre Ebene von zu tolerierenden Fehlern** 1 festgelegt ist. Wenn nämlich bei einem Host ein Fehler auftritt, verbleiben im Cluster nur zwei Hosts. Für die Tolerierung einer Neuerstellung nach einem Fehler benötigen Sie mindestens drei Hosts.
- Stellen Sie ausreichend temporären Speicherplatz für Änderungen bei der vSAN-VM-Speicherrichtlinie bereit. Wenn Sie eine VM-Speicherrichtlinie dynamisch ändern, erstellt vSAN möglicherweise ein Layout der Replikate, aus denen ein Objekt besteht. Wenn vSAN diese Replikate mit dem Originalreplikat instanziiert und synchronisiert, muss der Cluster vorübergehend zusätzlichen Speicherplatz bereitstellen.
- Wenn Sie erweiterte Funktionen verwenden möchten, zum Beispiel Software-Prüfsumme oder Deduplizierung und Komprimierung, reservieren Sie zusätzliche Kapazität, um den Betriebs-Overhead zu verarbeiten.

## Überlegungen zu VM-Objekten

Berücksichtigen Sie bei der Planung der Speicherkapazität im vSAN-Datenspeicher den erforderlichen Speicherplatz für die VM-Home-Namespace-Objekte, Snapshots und Auslagerungsdateien im Datenspeicher.

- VM-Home-Namespace. Sie können eine Speicherrichtlinie speziell für das Home-Namespace-Objekt für eine virtuelle Maschine zuweisen. Um eine unnötige Zuteilung von Kapazität und Cache-Speicher zu vermeiden, wendet vSAN nur die Einstellungen **Primäre Ebene von zu tolerierenden Fehlern** und **Bereitstellung erzwingen** aus der Richtlinie im VM-Home-Namespace an. Planen Sie den Speicherplatz so, dass die Anforderungen für eine Speicherrichtlinie erfüllt werden, die einem VM-Home-Namespace zugewiesen ist, dessen Wert für **Primäre Ebene von zu tolerierenden Fehlern** größer 0 ist.

- Snapshots. Delta-Geräte übernehmen die Richtlinie der VMDK-Basisdatei. Planen Sie zusätzlichen Speicherplatz gemäß der erwarteten Größe und Anzahl von Snapshots und gemäß der Einstellungen in den vSAN-Speicherrichtlinien ein.

  Der erforderliche Speicherplatz kann variieren. Die Größe hängt davon ab, wie oft die virtuelle Maschine Daten ändert und wie lange ein Snapshot der virtuellen Maschine zugeordnet ist.

- Auslagerungsdateien. vSAN verwendet für die Auslagerungsdateien von virtuellen Maschinen eine separate Speicherrichtlinie. Diese Richtlinie toleriert einen einzigen Fehler, definiert kein Striping und keine Read Cache-Reservierung und aktiviert das Erzwingen der Bereitstellung.

## Design-Überlegungen für Flash-Caching-Geräte in vSAN

Planen Sie die Konfiguration von Flash-Geräten für vSAN-Cache und reine Flash-Kapazität, um hohe Leistung und den erforderlichen Speicherplatz bereitzustellen, und berücksichtigen Sie dabei zukünftiges Wachstum.

### Auswählen zwischen PCIe- oder SSD-Flash-Geräten

Wählen Sie PCIe- oder SSD-Flash-Geräte entsprechend den Anforderungen in Bezug auf Leistung, Kapazität, Schreibbelastungsfähigkeit und Kosten des vSAN-Speichers aus.

- Kompatibilität. Das Modell der PCIe- oder SSD-Geräte muss im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch* aufgeführt sein.
- Leistung. Die Leistungsfähigkeit von PCIe-Geräten ist im Allgemeinen höher als bei SSD-Geräten.
- Kapazität. Die maximale Kapazität, die für PCIe-Geräte verfügbar ist, ist im Allgemeinen größer als die maximale Kapazität, die für SSD-Geräte für vSAN im *VMware-Kompatibilitätshandbuch* derzeit aufgeführt ist.
- Schreibbelastungsfähigkeit. Die Schreibbelastungsfähigkeit der PCIe- und SSD-Geräte muss in Alle-Flash-Konfigurationen die Anforderungen in Bezug auf Kapazität oder den Zwischenspeicher und in Hybridkonfigurationen in Bezug auf den Zwischenspeicher erfüllen.

  Informationen zu den Anforderungen in Bezug auf Schreibbelastungsfähigkeit für Alle-Flash- und Hybridkonfigurationen finden Sie im *Handbuch für VMware vSAN Design und Sizing*. Informationen zur Schreibbelastungsfähigkeits-Klasse von PCIe- und SSD-Geräten finden Sie im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch*.

- Kosten. PCIe-Geräte verursachen im Allgemeinen höhere Kosten als SSD-Geräte.

### Flash-Geräte als vSAN -Cache

Entwerfen Sie die Konfiguration von Flash-Cache für vSAN im Hinblick auf die Lebensdauer für Schreibvorgänge, Leistung und potenzielles Wachstum basierend auf diesen Überlegungen.

**Tabelle 3-1.** Dimensionieren des vSAN -Cache

| Speicherkonfiguration | Überlegungen |
|---|---|
| Reine Flash- und Hybrid-Konfigurationen | ■ Die Kapazität des Flash-Zwischenspeichergeräts muss mindestens 10 Prozent des Speichers betragen, der voraussichtlich auf den virtuellen Maschinen verbraucht wird, und zwar ohne Replikate wie beispielsweise Spiegel.<br><br>Das Attribut **Anzahl der zu tolerierenden Fehler** aus der VM-Speicherrichtlinie hat keine Auswirkungen auf die Cachegröße.<br>■ Ein höheres Verhältnis von Cache zu Kapazität erleichtert zukünftiges Kapazitätswachstum. Das Überdimensionieren des Cache erleichtert das Hinzufügen weiterer Kapazität zu vorhandenen Festplattengruppen, ohne den Cache vergrößern zu müssen.<br>■ Flash-Caching-Geräte müssen eine hohe Lebensdauer für Schreibvorgänge aufweisen.<br>■ Wenn ein Flash-Caching-Gerät das Ende seiner Lebensdauer erreicht hat, ist das Austauschen komplizierter als bei Kapazitätsgeräten, weil ein solcher Vorgang Auswirkungen auf die gesamte Festplattengruppe hat.<br>■ Wenn Sie zusätzliche Flash-Geräte hinzufügen, um den Cache zu vergrößern, müssen Sie weitere Festplattengruppen erstellen. Das Verhältnis zwischen Flash-Cache-Geräten und Festplattengruppen beträgt immer 1:1.<br><br>Eine Konfiguration mehrerer Festplattengruppen bietet folgende Vorteile:<br>■ Geringeres Ausfallrisiko, weil weniger Kapazitätsgeräte betroffen sind, wenn ein einzelnes Zwischenspeichergerät ausfällt<br>■ Potenziell verbesserte Leistung, wenn Sie mehrere Festplattengruppen bereitstellen, die kleinere Flash-Zwischenspeichergeräte enthalten.<br><br>Wenn Sie jedoch mehrere Festplattengruppen konfigurieren, steigt der Arbeitsspeicherverbrauch der Hosts. |
| Reine Flash-Konfigurationen | In reinen Flash-Konfigurationen verwendet vSAN die Cache-Ebene nur für das Schreib-Caching. Der Schreibcache muss in der Lage sein, eine sehr hohe Schreibaktivität zu verarbeiten. Dieser Ansatz erweitert die Lebensdauer von Kapazitäts-Flash, der möglicherweise kostengünstiger ist und eine geringere Lebensdauer für Schreibvorgänge aufweist. |
| Hybrid-Konfigurationen | Wenn in der aktiven VM-Speicherrichtlinie aus Leistungsgründen die Lesecache-Reservierung konfiguriert wird, müssen die Hosts im vSAN-Cluster über ausreichend Cache verfügen, um den Ressourcenbedarf für die Reservierung während einer Neuerstellung nach einem Fehler oder während eines Wartungsvorgangs zu erfüllen.<br>Wenn der verfügbare Lesecache für die Reservierung nicht ausreicht, schlägt der Neuerstellungs- oder Wartungsvorgang fehl. Verwenden Sie die Lesecache-Reservierung nur, wenn Sie eine bestimmte, bekannte Leistungsanforderung für eine spezielle Arbeitslast erfüllen müssen.<br>Die Verwendung von Snapshots verbraucht Cache-Ressourcen. Wenn Sie die Verwendung mehrerer Snapshots planen, ziehen Sie in Betracht, mehr Cache als das übliche Verhältnis zwischen Cache und benötigter Kapazität in Höhe von 10 Prozent bereitzustellen. |

# Design-Überlegungen für Flash-Kapazitätsgeräte in vSAN

Planen Sie die Konfiguration von Flash-Kapazitätsgeräten für reine vSAN-Flash-Konfigurationen, um hohe Leistung und den erforderlichen Speicherplatz bereitzustellen, und berücksichtigen Sie dabei zukünftiges Wachstum.

## Auswählen zwischen PCIe- oder SSD-Flash-Geräten

Wählen Sie PCIe- oder SSD-Flash-Geräte entsprechend den Anforderungen in Bezug auf Leistung, Kapazität, Schreibbelastungsfähigkeit und Kosten des vSAN-Speichers aus.

- Kompatibilität. Das Modell der PCIe- oder SSD-Geräte muss im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch* aufgeführt sein.
- Leistung. Die Leistungsfähigkeit von PCIe-Geräten ist im Allgemeinen höher als bei SSD-Geräten.
- Kapazität. Die maximale Kapazität, die für PCIe-Geräte verfügbar ist, ist im Allgemeinen größer als die maximale Kapazität, die für SSD-Geräte für vSAN im *VMware-Kompatibilitätshandbuch* derzeit aufgeführt ist.
- Schreibbelastungsfähigkeit. Die Schreibbelastungsfähigkeit der PCIe- und SSD-Geräte muss in Alle-Flash-Konfigurationen die Anforderungen in Bezug auf Kapazität oder den Zwischenspeicher und in Hybridkonfigurationen in Bezug auf den Zwischenspeicher erfüllen.

  Informationen zu den Anforderungen in Bezug auf Schreibbelastungsfähigkeit für Alle-Flash- und Hybridkonfigurationen finden Sie im *Handbuch für VMware vSAN Design und Sizing*. Informationen zur Schreibbelastungsfähigkeits-Klasse von PCIe- und SSD-Geräten finden Sie im vSAN-Abschnitt des *VMware-Kompatibilitätshandbuch*.
- Kosten. PCIe-Geräte verursachen im Allgemeinen höhere Kosten als SSD-Geräte.

## Flash-Geräte als vSAN -Kapazität

In All-Flash-Konfigurationen verwendet vSAN keinen Cache für Lesevorgänge und wendet die Einstellung für die Lesecache-Reservierung aus der VM-Speicherrichtlinie nicht an. Für Cache können Sie eine kleine Menge des teureren Flash verwenden, der eine hohe Lebensdauer für Schreibvorgänge aufweist. Für Kapazität können Sie kostengünstigeren Flash verwenden, der eine geringere Lebensdauer für Schreibvorgänge aufweist.

Berücksichtigen Sie bei der Planung einer Konfiguration von Flash-Kapazitätsgeräten die folgenden Richtlinien:

- Eine bessere Leistung von vSAN erreichen Sie durch mehr Festplattengruppen aus kleineren Flash-Kapazitätsgeräten.
- Eine ausgeglichene Leistung und vorhersehbares Verhalten erreichen Sie durch Verwendung von Flash-Kapazitätsgeräten desselben Typs und Modells.

# Design-Überlegungen für Magnetfestplatten in vSAN

Berücksichtigen Sie beim Planen der Größe und Anzahl magnetischer Festplatten für Kapazität in Hybridkonfigurationen die folgenden Anforderungen in Bezug auf Speicherplatz und Leistungsfähigkeit.

## Magnetische Geräte des Typs SAS, NL-SAS und SATA

Verwenden Sie magnetische Geräte des Typs SAS, NL-SAS oder SATA entsprechend den Anforderungen in Bezug auf Leistung, Kapazität und Kosten des vSAN-Speichers.

- Kompatibilität. Das Modell der magnetischen Festplatte muss zertifiziert sein und im vSAN-Abschnitt im *VMware-Kompatibilitätshandbuch* aufgeführt werden.

- Leistung. SAS- und NL-SAS-Geräte sind leistungsfähiger als SATA-Festplatten.
- Kapazität. Die Kapazität von magnetischen SAS-, NL-SAS- und SATA-Festplatten für vSAN ist im Abschnitt „vSAN“ im *VMware-Kompatibilitätshandbuch* aufgeführt. Verwenden Sie eine größere Anzahl kleinerer Geräte anstatt einer kleineren Anzahl größerer Geräte.
- Kosten. SAS- und NL-SAS-Geräte sind teurer als SATA-Festplatten.

Die Verwendung von SATA-Festplatten anstelle von SAS- und NL-SAS-Geräten lässt sich in Umgebungen rechtfertigen, in denen Kapazität und reduzierte Kosten wichtiger als die Leistungsfähigkeit sind.

### Magnetfestplatten als vSAN Kapazität

Berücksichtigen Sie beim Planen einer Konfiguration magnetischer Festplatten folgende Richtlinien:

- Verwenden Sie für eine höhere Leistung von vSAN viele magnetische Festplatten kleinerer Kapazität.

  Sie müssen genug magnetische Festplatten haben, die zusammengefasst eine angemessene Leistung beim Übertragen von Daten zwischen Zwischenspeicher und Kapazität gewährleisten. Mit vielen kleinen Geräten erhalten Sie eine höhere Leistung als mit wenigen großen Geräten. Mit mehreren Spindeln magnetischer Festplatten kann der Destaging-Prozess beschleunigt werden.

  In Umgebungen mit vielen virtuellen Maschinen ist die Anzahl magnetischer Festplatten auch für Lesevorgänge wichtig, wenn Daten im Lesezwischenspeicher nicht verfügbar sind und vSAN die Daten von der magnetischen Festplatte liest. In Umgebungen mit wenigen virtuellen Maschinen wirkt sich die Anzahl der Festplatten auf Lesevorgänge aus, wenn die **Anzahl der Festplatten-Stripes pro Objekt** in der aktiven VM-Speicherrichtlinie größer als 1 ist.
- Um eine ausgewogene Leistung und ein vorhersehbares Verhalten zu erhalten, sollten Sie in einem Datenspeicher für vSAN denselben Typ und dasselbe Modell von magnetischen Festplatten verwenden.
- Stellen Sie genug magnetische Festplatten bereit, um die in den definierten Speicherrichtlinien festgelegten Werte für die Attribute **Primäre Ebene von zu tolerierenden Fehlern** und **Anzahl der Festplatten-Stripes pro Objekt** zu erfüllen. Informationen zu den VM-Speicherrichtlinien für vSAN finden Sie unter Kapitel 12, „Verwenden von vSAN-Speicherrichtlinien“, auf Seite 137.

## Überlegungen zum Design für Speicher-Controllern in vSAN

Verwenden Sie auf den Hosts eines vSAN-Clusters Speicher-Controller, die die Anforderungen an Leistung und Verfügbarkeit am besten erfüllen.

- Verwenden Sie Speicher-Controller-Modelle sowie Treiber- und Firmware-Versionen, die im *VMware-Kompatibilitätshandbuch* aufgelistet sind. Suchen Sie nach vSAN im *VMware-Kompatibilitätshandbuch*.
- Verwenden Sie nach Möglichkeit mehrere Speicher-Controller, um die Leistung zu verbessern und einen potenziellen Controller-Fehler auf bestimmte Festplattengruppen zu beschränken.
- Verwenden Sie Speicher-Controller, die im *VMware-Kompatibilitätshandbuch* die höchsten Warteschlangentiefen aufweisen. Bei Verwendung von Controllern mit einer hohen Warteschlangentiefe wird die Leistung verbessert. Beispiele: Wenn vSAN Komponenten nach einem Ausfall neu erstellt, oder wenn ein Host in den Wartungsmodus versetzt wird.
- Verwenden Sie Speicher-Controller im Passthrough-Modus für die optimale Leistung von vSAN. Speicher-Controller im RAID 0-Modus erfordern im Vergleich zu Speicher-Controllern im Passthrough-Modus einen höheren Konfigurations- und Wartungsaufwand.

# Entwerfen und Dimensionieren von vSAN -Hosts

Planen Sie die Konfiguration der Hosts im vSAN-Cluster im Hinblick auf optimale Leistung und Verfügbarkeit.

## Arbeitsspeicher und CPU

Legen Sie die Größe von Arbeitsspeicher und CPU der Hosts im vSAN-Cluster anhand der folgenden Überlegungen fest.

**Tabelle 3-2.** Festlegen der Größe des Arbeitsspeichers und der CPU von vSAN -Hosts

| Computing-Ressource | Überlegungen |
|---|---|
| Arbeitsspeicher | ■ Arbeitsspeicher pro virtueller Maschine<br>■ Arbeitsspeicher pro Host basierend auf der erwarteten Anzahl virtueller Maschinen<br>■ Mindestens 32 GB Arbeitsspeicher für voll funktionsfähiges vSAN mit fünf Festplattengruppen pro Host und sieben Kapazitätsgeräten pro Festplattengruppe<br>Hosts mit einem Arbeitsspeicher von 512 GB oder weniger können von einem USB-, SD- oder SATADOM-Gerät gestartet werden. Wenn der Arbeitsspeicher des Hosts größer als 512 GB ist, starten Sie den Host von einem SATADOM- oder Festplattengerät. |
| CPU | ■ Sockets pro Host<br>■ Cores pro Socket<br>■ Anzahl an vCPUs basierend auf der erwarteten Anzahl virtueller Maschinen<br>■ Verhältnis vCPU zu Core<br>■ 10 % CPU-Overhead für vSAN |

## Hostnetzwerk

Stellen Sie für vSAN-Datenverkehr mehr Bandbreite bereit, um die Leistung zu verbessern.

- Wenn Sie Hosts mit 1-GbE-Adaptern verwenden möchten, nutzen Sie Adapter ausschließlich für vSAN. Planen Sie für All-Flash-Konfigurationen Hosts mit reservierten oder gemeinsam genutzten 10-GbE-Adaptern.
- Wenn Sie 10-GbE-Adapter verwenden möchten, können diese gemeinsam mit anderen Datenverkehrstypen sowohl für Hybrid- als auch All-Flash-Konfigurationen genutzt werden.
- Wenn ein 10-GbE-Adapter gemeinsam mit anderen Datenverkehrstypen genutzt wird, verwenden Sie einen vSphere Distributed Switch für vSAN-Datenverkehr, um den Datenverkehr mithilfe von Network I/O Control und VLANs zu isolieren.
- Erstellen Sie aus Gründen der Redundanz eine Gruppe von physischen Adaptern für vSAN-Datenverkehr.

## Mehrere Festplattengruppen

Wenn der Flash-Cache oder der Speicher-Controller nicht mehr reagiert, kann eine komplette Festplattengruppe fehlschlagen. Demzufolge erstellt vSAN alle Komponenten für die ausgefallene Festplattengruppe an einer anderen Position im Cluster neu.

Die Verwendung von mehreren Festplattengruppen mit weniger Kapazität bietet die folgenden Vor- und Nachteile:

- Vorteile
  - Die Leistung wird verbessert, da der Datenspeicher mehr zusammengeführten Cache aufweist und die E/A-Vorgänge schneller sind.
  - Das Ausfallrisiko wird auf mehrere Festplattengruppen verteilt.
  - Beim Ausfall einer Festplattengruppe erstellt vSAN weniger Komponenten neu, damit die Leistung verbessert wird.
- Nachteile
  - Die Kosten sind höher, weil zwei oder mehr Zwischenspeichergeräte benötigt werden.
  - Für die Verarbeitung von mehr Festplattengruppen ist mehr Arbeitsspeicher erforderlich.
  - Es werden mehrere Speichercontroller benötigt, um das Risiko einer einzelnen Fehlerquelle zu verringern.

### Laufwerkschächte

Zur Vereinfachung der Wartung sollten Sie Hosts verwenden, deren Laufwerkschächte und PCIe-Steckplätze sich an der Vorderseite des Servergehäuses befinden.

### Blade-Server und externer Speicher

Die Kapazität von Blade-Servern wird in einem vSAN-Datenspeicher gewöhnlich nicht skaliert, da es eine begrenzte Anzahl von Festplattensteckplätzen gibt. Verwenden Sie zur Erweiterung der geplanten Kapazität von Blade-Servern externe Speichergehäuse. Informationen zu den unterstützten Modellen externer Speichergehäuse finden Sie im *VMware-Kompatibilitätshandbuch*.

### Hotplug und Hot-Swap von Geräten

Den Passthrough-Modus des Speicher-Controllers können Sie für das einfache Hot-Plugging bzw. den einfachen Austausch von Magnetfestplatten und Flash-Kapazitätsgeräten auf einem Host verwenden. Wenn ein Controller im RAID 0-Modus arbeitet, müssen Sie zusätzliche Schritte ausführen, damit der Host das neue Laufwerk erkennt.

## Design-Überlegungen für einen Cluster vSAN

Konfigurieren Sie Hosts und Verwaltungsknoten für optimale Verfügbarkeit und Toleranz in Bezug auf zunehmende Nutzung.

### Dimensionierung des vSAN -Clusters zum Tolerieren von Fehlern

Sie konfigurieren das Attribut **Primäre Ebene von zu tolerierenden Fehlern** (PFTT) in den VM-Speicherrichtlinien zum Handhaben von Hostausfällen. Die Anzahl der für den Cluster erforderlichen Hosts lautet wie folgt: `2 * PFTT + 1`. Je mehr Fehler der Cluster toleriert, desto mehr Kapazitätshosts sind erforderlich.

Wenn die Clusterhosts in Rack-Servern verbunden sind, können Sie die Hosts in Fault Domains anordnen, um die Fehlerverwaltung zu verbessern. Siehe „Entwerfen und Dimensionieren von vSAN-Fault Domains“, auf Seite 33.

### Einschränkungen in einer Clusterkonfiguration mit zwei oder drei Hosts

In einer Konfiguration mit zwei oder drei Hosts können Sie nur einen Hostfehler tolerieren, indem Sie **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festlegen. vSAN speichert jedes der beiden erforderlichen Replikate der VM-Daten auf getrennten Hosts. Das Zeugenobjekt ist auf einem dritten Host. Wegen der geringen Anzahl der Hosts im Cluster bestehen die folgenden Einschränkungen:

- Wenn ein Host ausfällt, kann vSAN nicht die Daten auf einem anderen Host neu erstellen, um sie vor einem weiteren Ausfall zu schützen.
- Wenn ein Host in den Wartungsmodus wechseln muss, kann vSAN die entfernten Daten nicht neu schützen. Die Daten sind einem potenziellen Fehler ausgesetzt, während der Host sich im Wartungsmodus befindet.

  Sie können nur die Datenevakuierungsoption **Datenzugriff sicherstellen** verwenden. Die Option **Alle Daten evakuieren** ist nicht verfügbar, weil der Cluster nicht über einen Ersatzhost verfügt, den er zum Evakuieren der Daten verwenden könnte.

  Folglich sind virtuelle Maschinen in Gefahr, weil sie bei einem weiteren Ausfall unzugänglich werden.

### Ausgeglichene und unausgeglichene Clusterkonfiguration

vSAN funktioniert am besten auf Hosts mit einheitlichen Konfigurationen.

Die Verwendung von Hosts mit verschiedenen Konfigurationen hat die folgenden Nachteile in einem vSAN-Cluster:

- Verringerte Prognostizierbarkeit der Speicherleistung, weil vSAN nicht dieselbe Anzahl von Komponenten auf jedem Host speichert.
- Verschiedene Wartungsverfahren.
- Verringerte Leistung auf Hosts im Cluster, die über kleinere oder verschiedenartige Cache-Geräte verfügen.

### Bereitstellen von vCenter Server auf vSAN

Wenn Sie vCenter Server auf dem Datenspeicher für vSAN bereitstellen, können Sie vCenter Server möglicherweise nicht zur Fehlerbehebung verwenden, wenn ein Problem im vSAN-Cluster auftritt.

## Entwerfen des vSAN -Netzwerks

Sie sollten Netzwerkfunktionen verwenden, die die Verfügbarkeit, Sicherheit und Bandbreite in einem vSAN-Cluster garantieren können.

Ausführliche Informationen zur Konfiguration des vSAN-Netzwerks finden Sie im *Handbuch für VMware vSAN Design und Sizing* und *Handbuch für vSAN-Netzwerkdesign*.

### Failover und Lastausgleich für das Netzwerk

vSAN verwendet die Gruppierungs- und Failover-Richtlinie, die auf dem unterstützenden virtuellen Switch konfiguriert ist, nur zur Netzwerkredundanz. vSAN verwendet die NIC-Gruppierung nicht für den Lastausgleich.

Wenn Sie ein NIC-Team für die Verfügbarkeit planen möchten, sollten Sie die folgenden Failover-Konfigurationen berücksichtigen.

| Gruppierungsalgorithmus | Failover-Konfiguration der Adapter im Team |
|---|---|
| Anhand des ursprünglichen virtuellen Ports routen | Aktiv/Passiv |
| Anhand des IP-Hashs routen | Aktiv/Aktiv mit statischem EtherChannel für den Standard-Switch und LACP-Portkanal für den Distributed Switch |
| Anhand der physischen Netzwerkkartenauslastung routen | Aktiv/Aktiv |

vSAN unterstützt den IP-Hash-Lastausgleich, kann aber keine Leistungsverbesserung für alle Konfigurationen garantieren. Sie können von IP-Hash profitieren, wenn vSAN unter den zahlreichen Konsumenten ist. In diesem Fall führt IP-Hash den Lastausgleich durch. Wenn vSAN der einzige Konsument ist, bemerken Sie möglicherweise keine Verbesserung. Dieses Verhalten gilt insbesondere für 1-GbE-Umgebungen. Wenn Sie z. B. vier physische 1-GbE-Adapter mit IP-Hash für vSAN verwenden, können Sie möglicherweise nicht mehr als 1 GBit/s verwenden. Dieses Verhalten gilt auch für alle von VMware unterstützten NIC-Gruppierungsrichtlinien.

## Verwenden von Unicast im vSAN -Netzwerk

In vSAN 6.6 und höheren Versionen ist Multicast auf den physischen Switches, die den vSAN-Cluster unterstützen, nicht erforderlich. Sie können für vSAN ein einfaches Unicast-Netzwerk entwerfen. Frühere Versionen von vSAN stützen sich auf Multicast, um Taktsignale zu aktivieren und um Metadaten zwischen Hosts im Cluster auszutauschen. Wenn einige Hosts in Ihrem vSAN-Cluster frühere Softwareversionen ausführen, ist dennoch ein Multicast-Netzwerk erforderlich. Weitere Informationen zur Verwendung von Multicast in einem vSAN-Cluster finden Sie in einer früheren Version von *Verwalten von VMware vSAN*.

**Hinweis** Die folgende Konfiguration wird nicht unterstützt: vCenter Server, der auf einem vSAN 6.6-Cluster bereitgestellt wird, der IP-Adressen von DHCP ohne Reservierungen verwendet. Sie können DHCP mit Reservierungen verwenden, da die zugewiesenen IP-Adressen an die MAC-Adressen der VMkernel-Ports gebunden sind.

## Zuteilen von Bandbreite für vSAN mithilfe von Network I/O Control

Falls vSAN-Datenverkehr physische 10-GbE-Netzwerkadapter verwendet, die gemeinsam mit anderen Systemdatenverkehrstypen genutzt werden, wie z. B. vSphere vMotion-Datenverkehr, vSphere HA-Datenverkehr, VM-Datenverkehr usw., können Sie mithilfe von vSphere Network I/O Control für den vSphere Distributed Switch garantieren, dass die erforderliche Bandbreite für vSAN verfügbar ist.

In vSphere Network I/O Control können Sie Reservierungen und Anteile für den ausgehenden vSAN-Datenverkehr konfigurieren.

- Nehmen Sie eine Reservierung vor, damit Network I/O Control auf dem physischen Adapter die Mindestbandbreite für vSAN garantiert.
- Legen Sie Anteile fest, damit bei einer Sättigung des für vSAN zugewiesenen physischen Adapters eine gewisse Bandbreite für vSAN verfügbar ist und um zu verhindern, dass vSAN die gesamte Kapazität des physischen Adapters während Neuerstellungs- und Synchronisierungsvorgängen belegt. Beispielsweise könnte der physische Adapter gesättigt sein, wenn ein anderer physischer Adapter im Team fehlschlägt und der gesamte Datenverkehr in der Portgruppe an die anderen Adapter im Team übertragen wird.

Beispielsweise können Sie auf einem physischen 10-GbE-Adapter, der den Datenverkehr für vSAN, vSphere vMotion und virtuelle Maschinen verarbeitet, bestimmte Bandbreiten und Anteile konfigurieren.

**Tabelle 3-3.** Beispiel für eine Network I/O Control-Konfiguration für einen physischen Adapter, der Datenverkehr für vSAN verarbeitet

| Art des Datenverkehrs | Reservierung, GBit/s | Anteile |
|---|---|---|
| vSAN | 1 | 100 |
| vSphere vMotion | 0,5 | 70 |
| Virtuelle Maschine | 0,5 | 30 |

Falls der 10-GbE-Adapter gesättigt ist, werden vSAN auf dem physischen Adapter 5 GBit/s von Network I/O Control zugeteilt.

Informationen zum Konfigurieren der Bandbreitenzuteilung für vSAN-Datenverkehr mithilfe von vSphere Network I/O Control finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

## Markieren des vSAN -Datenverkehrs

Das Prioritäts-Tagging ist ein Mechanismus, um die verbundenen Netzwerkgeräte darauf hinzuweisen, dass vSAN-Datenverkehr höhere QoS (Quality of Service)-Anforderungen hat. Sie können vSAN-Datenverkehr einer bestimmten Klasse zuweisen und den Datenverkehr mithilfe der Richtlinie zum Filtern und Markieren des Datenverkehrs von vSphere Distributed Switch entsprechend mit einem Dienstklassenwert (Class of Service, CoS) zwischen 0 (niedrige Priorität) und 7 (hohe Priorität) markieren.

## Segmentieren des vSAN -Datenverkehrs in einem VLAN

Sie können den vSAN-Datenverkehr in einem VLAN isolieren, um die Sicherheit und Leistung zu verbessern, insbesondere wenn Sie die Kapazität des unterstützenden physischen Adapters auf mehrere Datenverkehrstypen aufteilen.

## Jumbo-Frames

Wenn Sie Jumbo-Frames zusammen mit vSAN verwenden möchten, um die CPU-Leistung zu verbessern, vergewissern Sie sich, dass Jumbo-Frames auf allen Netzwerkgeräten und Hosts im Cluster aktiviert sind.

Standardmäßig sind der TCP-Segmentierungs-Offload (TCP Segmentation Offload, TSO) und der Large Receive Offload (LRO) für ESXi aktiviert. Sie sollten sich überlegen, ob die Verwendung von Jumbo-Frames die Leistung ausreichend verbessert, um die Kosten für die Aktivierung dieser Funktionen auf allen Knoten im Netzwerk zu rechtfertigen.

## Erstellen von statischen Routen für vSAN -Netzwerke

Sie müssen in Ihrer vSAN-Umgebung möglicherweise statische Routen erstellen.

In traditionellen Konfigurationen, in denen vSphere ein einziges Standard-Gateway verwendet, versucht der gesamte geroutete Datenverkehr, sein Ziel über dieses Gateway zu erreichen.

In bestimmten vSAN-Bereitstellungen kann jedoch statisches Routing erforderlich sein. Beispiele sind Bereitstellungen, bei denen sich der Zeuge in einem anderen Netzwerk befindet, oder die Bereitstellung eines ausgeweiteten Clusters, bei der sich die Daten-Sites und der Zeugen-Host auf unterschiedlichen Sites befinden.

Verwenden Sie den Befehl „esxcli“, um statisches Routing auf Ihren ESXi-Hosts zu konfigurieren:

```
esxcli network ip route ipv4 add -n Remotenetzwerk -g Zu-verwendendes-Gateway
```

*Remotenetzwerk* ist das Remotenetzwerk, auf das Ihr Host zugreifen muss, und *Zu-verwendendes-Gateway* ist die Schnittstelle, die zum Senden des Datenverkehrs an das Remotenetzwerk verwendet wird.

Weitere Informationen finden Sie unter „Netzwerkplanung für ausgeweitete Cluster“, auf Seite 67.

# Empfohlene Vorgehensweisen für vSAN -Netzwerke

Beachten Sie die Best Practices für Netzwerke für vSAN, um die Leistung und den Durchsatz zu optimieren.

- Reservieren Sie für Hybridkonfigurationen mindestens einen physischen 1-GbE-Netzwerkadapter. Platzieren Sie für die optimale Netzwerkleistung vSAN-Datenverkehr auf einem reservierten oder gemeinsam genutzten physischen 10-GbE-Adapter.
- Verwenden Sie für All-Flash-Konfigurationen einen reservierten oder gemeinsam genutzten physischen 10-GbE-Netzwerkadapter.
- Stellen Sie eine zusätzliche physische Netzwerkkarte als Failover-Netzwerkkarte bereit.
- Falls Sie einen gemeinsam genutzten 10-GbE-Netzwerkadapter verwenden, platzieren Sie den vSAN-Datenverkehr auf einem Distributed Switch und konfigurieren Sie Network I/O Control, um Bandbreite für vSAN zu garantieren.

# Entwerfen und Dimensionieren von vSAN -Fault Domains

Die Funktion der vSAN-Fault Domains weist vSAN an, Redundanzkomponenten auf die Server in separaten Computing-Racks zu verteilen. Auf diese Weise können Sie die Umgebung vor einem Rack-Ausfall schützen, z. B. bei einem Stromausfall oder Verbindungsverlust.

## Fault Domain-Konstrukte

vSAN benötigt mindestens zwei Fault Domains, von denen jede aus einem oder mehreren Hosts bestehen kann. Fault Domain-Definitionen müssen physische Hardware-Konstrukte berücksichtigen, die eine potenzielle Fehlerzone darstellen, z. B. ein einzelnes Computing-Rack-Gehäuse.

Falls möglich, sollten Sie mindestens vier Fault Domains verwenden. Bei Verwendung von drei Domänen können bestimmte Evakuierungsmodi nicht verwendet werden und die Daten können nach einem Ausfall von vSAN nicht erneut geschützt werden. In diesem Fall benötigen Sie eine zusätzliche Fault Domain mit Kapazität für die Neuerstellung, die Sie mit der Konfiguration mit drei Domänen nicht bereitstellen können.

Werden Fault Domains aktiviert, wendet vSAN die aktive VM-Speicherrichtlinie nicht auf die einzelnen Hosts, sondern auf die Fault Domains an.

Berechnen Sie die Anzahl der Fehlerdomänen in einem Cluster basierend auf dem Attribut **Primäre Ebene von zu tolerierenden Fehlern** (PFTT) in den Speicherrichtlinien, die Sie den virtuellen Maschinen zuzuweisen beabsichtigen.

```
number of fault domains = 2 * PFTT + 1
```

Wenn ein Host kein Mitglied einer Fault Domain ist, interpretiert vSAN diesen als eine eigenständige Fault Domain.

## Verwenden von Fault Domains gegen den Ausfall mehrerer Hosts

Ziehen Sie einen Cluster mit vier Server-Racks und jeweils zwei Hosts in Betracht. Wenn der Wert für **Primäre Ebene von zu tolerierenden Fehlern** 1 beträgt und Fault Domains nicht aktiviert sind, kann vSAN beide Replikate eines Objekts bei Hosts im selben Rack-Gehäuse speichern. Dadurch sind Anwendungen bei einem Ausfall auf Rack-Ebene einem möglichen Datenverlustrisiko ausgesetzt. Wenn Sie Hosts, die potenziell gleichzeitig ausfallen können, in separaten Fault Domains konfigurieren, stellt vSAN sicher, dass alle Schutzkomponenten (Replikate und Zeugen) in separaten Fault Domains platziert werden.

Wenn Sie Hosts und Kapazität hinzufügen, können Sie die vorhandene Fault Domain-Konfiguration verwenden bzw. Fault Domains definieren.

Um eine ausgeglichene Speicherlast und Fehlertoleranz unter Verwendung von Fault Domains zu erreichen, ziehen Sie die folgenden Richtlinien in Betracht:

- Stellen Sie genügend Fehlerdomänen für die in den Speicherrichtlinien konfigurierte **Primäre Ebene von zu tolerierenden Fehlern** bereit.

  Definieren Sie mindestens drei Fault Domains. Definieren Sie mindestens vier Domänen, um optimalen Schutz zu gewährleisten.

- Weisen Sie jeder Fault Domain dieselbe Anzahl von Hosts zu.
- Verwenden Sie Hosts mit einheitlichen Konfigurationen.
- Dedizieren Sie, falls möglich, eine Fault Domain mit freier Kapazität zum Neuerstellen der Daten nach einem Ausfall.

# Verwenden von Startgeräten und vSAN

Beim Starten einer ESXi-Installation, die Teil eines vSAN-Clusters ist, von einem Flash-Gerät aus bestehen bestimmte Einschränkungen.

Wenn Sie einen vSAN-Host über ein USB-/SD-Gerät starten, müssen Sie ein qualitativ hochwertiges USB- oder SD-Flash-Laufwerk mit mindestens 4 GB verwenden.

Wenn Sie einen vSAN-Host von einem SATADOM-Gerät aus starten, müssen Sie ein SLC-Gerät (Single-Level Cell) verwenden. Die Größe des Startgeräts muss mindestens 16 GB betragen.

Während des Installationsvorgangs erstellt das ESXi-Installationsprogramm eine Core-Dump-Partition auf dem Startgerät. Die Standardgröße der Core-Dump-Partition erfüllt die meisten Installationsanforderungen.

Wenn der Arbeitsspeicher des ESXi-Hosts 512 GB oder weniger beträgt, können Sie den Host von einem USB-, SD- oder SATADOM-Gerät aus starten. Ist der Arbeitsspeicher des ESXi-Hosts größer als 512 GB, müssen Sie den Host von einem SATADOM- oder Festplattengerät aus starten.

**Hinweis** In vSAN 6.5 und höher können Sie die Größe einer vorhandenen Core-Dump-Partition auf einem ESXi-Host in einem vSAN-Cluster ändern und somit von USB-/SD-Geräten aus starten. Weitere Informationen finden Sie in dem VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2147881.

Hosts, die von einer Festplatte aus gestartet werden, verfügen über ein lokales VMFS. Falls Sie über eine Festplatte mit VMFS verfügen, die VMs ausführt, müssen Sie sie für einen ESXi-Start, der nicht vSAN gilt, separieren. In diesem Fall benötigen Sie separate Controller.

## Protokollinformationen und Startgeräte in vSAN

Wenn Sie ESXi von einem USB- oder SD-Gerät aus starten, gehen die Protokollinformationen und Stack-Traces beim Neustart des Hosts verloren. Sie gehen deshalb verloren, weil sich die Scratch-Partition auf einem RAM-Laufwerk befindet. Verwenden Sie dauerhaften Speicher für Protokolle, Stack-Traces und Arbeitsspeicher-Dumps.

Speichern Sie keine Protokolldaten auf dem Datenspeicher für vSAN. Diese Konfiguration wird nicht unterstützt, da sich ein Fehler im vSAN-Cluster auf die Zugänglichkeit von Protokolldaten auswirken könnte.

Ziehen Sie die folgenden Optionen für dauerhaften Protokollspeicher in Betracht:

- Verwenden Sie ein Speichergerät, das nicht für vSAN verwendet wird und mit VMFS oder NFS formatiert ist.
- Konfigurieren Sie den ESXi Dump Collector und den vSphere Syslog Collector auf dem Host so, dass Arbeitsspeicher-Dumps und Systemprotokolle zu vCenter Server gesendet werden.

Informationen zur Einrichtung der Scratch-Partition mit einem dauerhaften Speicherort finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

# Dauerhafte Protokollierung in einem vSAN -Cluster

Stellen Sie Speicher für Persistenz der Protokolle von den Hosts im vSAN-Cluster bereit.

Wenn Sie ESXi auf einem USB- oder SD-Gerät installieren und vSAN lokalen Speicher zuweisen, verfügen Sie möglicherweise nicht mehr über ausreichend lokalen Speicher oder Datenspeicherplatz für das dauerhafte Protokollieren.

Um einen potenziellen Verlust von Protokollinformationen zu verhindern, konfigurieren Sie den ESXi Dump Collector und den vSphere Syslog Collector so, dass ESXi-Arbeitsspeicher-Dumps und Systemprotokolle auf einen Netzwerkserver umgeleitet werden. Informationen finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

# Vorbereiten eines neuen oder vorhandenen Clusters für vSAN 4

Bevor Sie vSAN in einem Cluster aktivieren und als VM-Speicher verwenden, stellen Sie die für einen ordnungsgemäßen Betrieb von vSAN erforderliche Infrastruktur bereit.

Dieses Kapitel behandelt die folgenden Themen:



## Auswählen oder Überprüfen der Kompatibilität von Speichergeräten

Vor der Bereitstellung von vSAN ist es wichtig, mithilfe des *VMware-Kompatibilitätshandbuch* zu prüfen, ob Ihre Speichergeräte, Treiber und Firmware zu vSAN kompatibel sind.

Sie können verschiedene Optionen in Bezug auf die vSAN-Kompatibilität auswählen.

- Verwenden Sie einen für vSAN vorbereiteten Knoten-Server, einen physischen Server, den OEM-Anbieter und VMware für vSAN-Kompatibilität validieren.
- Erstellen Sie einen Knoten durch Auswählen einzelner Komponenten von validierten Gerätemodellen.

| ***VMware-Kompatibilitätshandbuch* Abschnitt** | **Komponententyp für Verifizierung** |
|---|---|
| ***DELETE*** | Physischer Server, der ESXi ausführt. |
| vSAN | ■ SAS- oder SATA-Modell mit magnetischer Festplatte für Hybridkonfigurationen.<br>■ Flash-Gerätemodell, das im *VMware-Kompatibilitätshandbuch* aufgeführt ist. Bestimmte Modelle von PCIe Flash-Geräten können auch mit vSAN arbeiten. Ziehen Sie auch die Schreibbeanspruchung und Leistungsklasse in Betracht.<br>■ Speicher-Controller-Modell, das Passthrough unterstützt.<br>vSAN kann mit Speicher-Controllern arbeiten, die für den RAID 0-Modus konfiguriert sind, wenn jedes Speichergerät als einzelne RAID 0-Gruppe dargestellt ist. |

# Vorbereiten von Speicher

Stellen Sie ausreichend Speicherplatz für vSAN und die virtualisierten Arbeitslasten bereit, die den vSAN-Datenspeicher verwenden.

## Vorbereiten von Speichergeräten

Verwenden Sie Flash-Geräte und magnetische Festplatten entsprechend den Anforderungen für vSAN.

Stellen Sie sicher, dass der Cluster über genug Kapazität für die erwartete Nutzung der virtuellen Maschine verfügt, und prüfen Sie die Einstellung **Primäre Ebene von zu tolerierenden Fehlern** in der Speicherrichtlinie für die virtuellen Maschinen.

Die Speichergeräte müssen die folgenden Voraussetzungen erfüllen, damit sie von vSAN beansprucht werden können:

- Die Speichergeräte sind lokal für die ESXi-Hosts. vSAN kann keine Remotegeräte beanspruchen.
- Auf den Speichergeräten befinden sich keine Partitionsdaten.
- Alle-Flash- und Hybrid-Festplattengruppen können nicht gleichzeitig demselben Host zugewiesen sein.

### Vorbereiten von Geräten für Festplattengruppen

Jede Festplattengruppe stellt ein Flash-Zwischenspeichergerät und mindestens eine magnetische Festplatte oder ein Flash-Kapazitätsgerät bereit. Die Kapazität des Flash-Zwischenspeichergeräts muss mindestens 10 Prozent des erwarteten genutzten Speichers auf dem Kapazitätsgerät betragen, ohne Berücksichtigung der Schutzkopien.

vSAN benötigt mindestens eine Festplattengruppe auf einem Host, der für einen aus mindestens drei Hosts bestehenden Cluster Speicher bereitstellt. Verwenden Sie Hosts mit einer einheitlichen Konfiguration, um vSAN optimal zu nutzen.

### Rohkapazität und nutzbare Kapazität

Stellen Sie eine Rohspeicherkapazität bereit, die größer als die Kapazität für virtuelle Maschinen ist, um bestimmte Fälle handhaben zu können.

- Beziehen Sie die Größe der Flash-Zwischenspeichergeräte nicht als Kapazität mit ein. Diese Geräte tragen nicht zum Speicher bei, sondern werden als Zwischenspeicher verwendet, es sei denn, Sie haben Flash-Geräte als Speicher hinzugefügt.
- Stellen Sie genug Speicherplatz bereit, um den in einer VM-Speicherrichtlinie festgelegten Wert für **Primäre Ebene von zu tolerierenden Fehlern** (PFTT) handhaben zu können. Ein PFTT-Wert größer als 0 erhöht den Speicherplatzbedarf des Geräts. Wenn der PFTT-Wert gleich 1 ist, verdoppelt sich der Speicherplatzbedarf. Wenn der PFTT-Wert gleich 2 ist, verdreifacht sich der Speicherplatzbedarf usw.
- Prüfen Sie, ob der Datenspeicher für vSAN über genug Speicherplatz für einen Vorgang verfügt. Prüfen Sie dazu den Speicherplatz auf den einzelnen Hosts und nicht auf dem konsolidierten vSAN-Datenspeicherobjekt. Beispiel: Wenn Sie einen Host entfernen, ist der gesamte freie Speicherplatz im Datenspeicher eventuell auf dem Host, den Sie entfernen. Der Cluster kann die Auslagerung auf einen anderen Host nicht ermöglichen.
- Stellen Sie genug Speicherplatz bereit, damit ausreichend Kapazität für den Datenspeicher verfügbar ist, wenn Arbeitslasten mit schnell („thin“) bereitgestelltem Speicher beginnen, einen großen Teil des Speichers zu nutzen.
- Stellen Sie sicher, dass der physische Speicher den erneuten Schutz und Wartungsmodus der Hosts im vSAN-Cluster ermöglichen kann.

- Berücksichtigen Sie den vSAN-Overhead für den nutzbaren Speicherplatz.
  - Version 1.0 des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise 1 GB pro Kapazitätsgerät.
  - Version 2.0 des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät.
  - Version 3.0 und höher des Festplattenformats fügt zusätzlichen Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät. Deduplizierung und Komprimierung mit aktivierter Software-Prüfsumme benötigt zusätzlichen Overhead von ungefähr 6,2 Prozent Kapazität pro Gerät.

Weitere Informationen zur Planung der Kapazität von Datenspeichern für vSAN finden Sie unter *Handbuch für VMware vSAN Design und Sizing*.

### Auswirkungen der vSAN -Richtlinie auf die Kapazität

Die vSAN-Speicherrichtlinie für virtuelle Maschinen wirkt sich auf verschiedene Weisen auf die Kapazitätsgeräte aus.

**Tabelle 4-1.** VM-Richtlinie und Rohkapazität von vSAN

| Aspekte des Richtlinieneinflusses | Beschreibung |
|---|---|
| Richtlinienänderungen | ■ **Primäre Ebene von zu tolerierenden Fehlern** (PFTT) wirkt sich auf den physischen Speicherplatz aus, den Sie für virtuelle Maschinen bereitstellen müssen. Je größer der PFTT-Wert für höhere Verfügbarkeit ist, desto mehr Speicherplatz müssen Sie bereitstellen.<br><br>Wenn der PFTT-Wert auf 1 festgelegt ist, sind zwei Replikate der VMDK-Datei einer virtuellen Maschine erforderlich. Wenn der PFTT-Wert auf 1 festgelegt ist, sind für eine 50 GB große VMDK-Datei 100 GB Speicherplatz auf verschiedenen Hosts erforderlich. Wenn der PFTT-Wert auf 2 geändert wird, müssen Sie genug Speicherplatz haben, um drei Replikate der VMDK auf den Hosts im Cluster zu unterstützen, also 150 GB.<br>■ Bei einigen Richtlinienänderungen, z. B. durch eine neue Anzahl der Festplatten-Stripes pro Objekt, sind temporäre Ressourcen erforderlich. vSAN erstellt die Objekte neu, die von der Änderung betroffen sind. Der physische Speicher muss für eine bestimmte Zeit die alten und neuen Objekte aufnehmen. |
| Verfügbarer Speicherplatz für neues Schützen oder den Wartungsmodus | Wenn Sie einen Host in den Wartungsmodus versetzen oder eine virtuelle Maschine klonen, kann der Datenspeicher die VM-Objekte möglicherweise nicht evakuieren, obwohl der vSAN-Datenspeicher anzeigt, dass ausreichend Speicherplatz vorhanden ist. Diese Mangel an Speicherplatz kann auftreten, wenn sich der freie Speicherplatz auf dem Host befindet, der in den Wartungsmodus versetzt wird. |

## Markieren von Flash-Geräten mithilfe von ESXCLI als Kapazitätsgeräte

Mit dem esxcli-Befehl können Sie die Flash-Geräte auf jedem Host manuell als Kapazitätsgeräte markieren.

#### Voraussetzungen

Stellen Sie sicher, dass Sie vSAN 6.5 oder höher verwenden.

### Vorgehensweise

1 Führen Sie den folgenden Befehl auf jedem Host aus, um den Namen des Flash-Geräts anzuzeigen, das Sie als Kapazitätsgerät markieren möchten.

   a Führen Sie in der ESXi Shell den Befehl `esxcli storage core device list` aus.

   b Suchen Sie oben in der Befehlsausgabe nach dem Gerätenamen und notieren Sie sich den Namen.

   Der Befehl verfügt über die folgenden Optionen:

**Tabelle 4-2.** Befehlsoptionen

| Optionen | Beschreibung |
|---|---|
| `-d\|--disk=str` | Der Name des Geräts, das Sie als Kapazitätsgerät kennzeichnen möchten. Beispielsweise `mpx.vmhba1:C0:T4:L0` |
| `-t\|--tag=str` | Geben Sie das Tag an, das Sie hinzufügen oder entfernen möchten. Beispielsweise wird mit dem Tag `capacityFlash` ein Flash-Gerät als Kapazitätsgerät markiert. |

   Dieser Befehl listet alle durch ESXi identifizierten Geräteinformationen auf.

2 Überprüfen Sie in der Ausgabe, ob das Attribut `Is SSD` für das Gerät `true` ist.

3 Führen Sie den Befehl `esxcli vsan storage tag add -d <device name> -t capacityFlash` aus, um ein Flash-Gerät als Kapazitätsgerät zu kennzeichnen.

   Befehlsbeispiel: `esxcli vsan storage tag add -t capacityFlash -d mpx.vmhba1:C0:T4:L0`; dabei ist `mpx.vmhba1:C0:T4:L0` der Gerätename.

4 Überprüfen Sie, ob das Flash-Gerät als Kapazitätsgerät markiert ist.

   a Bestimmen Sie in der Ausgabe, ob das Attribut `IsCapacityFlash` für das Gerät auf `1` festgelegt ist.

## Beispiel: Befehlsausgabe

Sie können den Befehl `vdq -q -d <device name>` ausführen, um das Attribut `IsCapacityFlash` zu überprüfen. Beispielsweise wird durch Ausführen des Befehls `vdq -q -d mpx.vmhba1:C0:T4:L0` die folgende Ausgabe zurückgegeben.

```
\{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "1",
"IsPDL"    : "0",
    \},
```

## Kennzeichnung mithilfe von ESXCLI von Flash-Geräten entfernen, die als Kapazität verwendet werden

Sie können die Kennzeichnung von Flash-Geräten, die als Kapazitätsgeräte verwendet werden, entfernen, sodass sie als Zwischenspeicher verfügbar sind.

### Vorgehensweise

1 Um die Kennzeichnung von einem als Kapazität markierten Flash-Gerät zu entfernen, führen Sie den Befehl `esxcli vsan storage tag remove –d <device name> –t capacityFlash` aus. Befehlsbeispiel: `esxcli vsan storage tag remove –t capacityFlash –d mpx.vmhba1:C0:T4:L0`; dabei ist `mpx.vmhba1:C0:T4:L0` der Gerätename.

2 Prüfen Sie, ob die Kennzeichnung des Flash-Geräts entfernt ist.

   a Bestimmen Sie in der Ausgabe, ob das Attribut `IsCapacityFlash` für das Gerät auf `0` festgelegt ist.

### Beispiel: Befehlsausgabe

Sie können den Befehl `vdq –q –d <device name>` ausführen, um das Attribut `IsCapacityFlash` zu überprüfen. Beispielsweise wird durch Ausführen des Befehls `vdq –q –d mpx.vmhba1:C0:T4:L0` die folgende Ausgabe zurückgegeben.

```
[
    \{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "0",
"IsPDL"    : "0",
    \},
```

## Markieren von Flash-Geräten mithilfe von RVC als Kapazitätsgeräte

Führen Sie den RVC-Befehl `vsan.host_claim_disks_differently` aus, um Speichergeräte als Flash, Kapazitäts-Flash oder Magnetfestplatte (HDD) zu markieren.

Mit dem RVC-Tool können Sie Flash-Geräte einzeln oder stapelweise als Kapazitätsgeräte kennzeichnen, indem Sie das Modell des Geräts angeben. Wenn Sie Flash-Geräte als Kapazitätsgeräte kennzeichnen möchten, können Sie sie einer All-Flash-Festplattengruppe hinzufügen.

---

**Hinweis** Mit dem Befehl `vsan.host_claim_disks_differently` wird vor der Kennzeichnung nicht der Gerätetyp überprüft. Jedes Gerät, dem Sie die Befehlsoption `capacity_flash` anhängen, wird mit diesem Befehl gekennzeichnet, einschließlich der bereits verwendeten Magnetfestplatten und Geräte. Überprüfen Sie vor dem Kennzeichnen unbedingt den Gerätestatus.

---

Informationen zu den RVC-Befehlen für die vSAN-Verwaltung finden Sie im *Referenzhandbuch zu den RVC-Befehlen (RVC Command Reference Guide)*.

### Voraussetzungen

- Stellen Sie sicher, dass Sie vSAN Version 6.5 oder höher verwenden.
- Vergewissern Sie sich, dass SSH für die vCenter Server Appliance aktiviert ist.

### Vorgehensweise

1 Stellen Sie eine SSH-Verbindung mit der vCenter Server Appliance her.

2 Melden Sie sich bei der Appliance mithilfe eines lokalen Kontos mit Administratorrechten an.

3 Starten Sie RVC, indem Sie den folgenden Befehl ausführen.

```
rvc local_user_name@target_vCenter_Server
```

Um beispielsweise dieselbe vCenter Server Appliance als Root-Benutzer zum Markieren von Flash-Geräten als Kapazitätsgeräte zu verwenden, führen Sie den folgenden Befehl aus:

```
rvc root@localhost
```

4 Geben Sie das Kennwort für den Benutzernamen ein.

5 Navigieren Sie in der vSphere-Infrastruktur zum Verzeichnis `vcenter_server/data_center/computers/cluster/hosts`.

6 Führen Sie den Befehl `vsan.host_claim_disks_differently` mit den Optionen `--claim-type capacity_flash --model` *Modellname* aus, um alle Flash-Geräte desselben Modells auf allen Hosts im Cluster als Kapazitätsgeräte zu markieren.

```
vsan.host_claim_disks_differently --claim-type capacity_flash --model model_name *
```

### Weiter

Aktivieren Sie vSAN auf dem Cluster und beanspruchen Sie Kapazitätsgeräte.

## Bereitstellen von Arbeitsspeicher für vSAN

Sie müssen Hosts Arbeitsspeicher entsprechend der maximalen Anzahl von Geräten und Festplattengruppen bereitstellen, die Sie vSAN zuzuweisen beabsichtigen.

Damit die maximale Anzahl von Geräten und Festplattengruppen unterstützt wird, müssen Sie Hosts mit 32 GB Arbeitsspeicher für Systemvorgänge bereitstellen. Informationen zur Konfiguration mit der maximalen Geräteanzahl finden Sie in der Dokumentation *Maximalwerte für die Konfiguration von vSphere*.

## Vorbereiten Ihrer Hosts für vSAN

Im Rahmen der Vorbereitung für die Aktivierung von vSAN sollten Sie die Anforderungen und Empfehlungen zur Konfiguration von Hosts für den Cluster berücksichtigen.

- Vergewissern Sie sich, dass die Speichergeräte auf den Hosts sowie die Treiber- und Firmware-Versionen im vSAN-Abschnitt im *VMware-Kompatibilitätshandbuch* aufgelistet sind.
- Stellen Sie sicher, dass mindestens drei Hosts Speicher für den vSAN-Datenspeicher bereitstellen.
- Für Wartungsvorgänge im Falle eines Fehlers sollten Sie dem Cluster mindestens vier Hosts hinzufügen.
- Legen Sie Hosts mit einer einheitlichen Konfiguration fest, um ein optimales Gleichgewicht des Speichers im Cluster sicherzustellen.
- Fügen Sie dem Cluster keine Hosts hinzu, die nur Computing-Ressourcen aufweisen, um die ungleichmäßige Verteilung von Speicherkomponenten auf den Hosts zu vermeiden, die Speicher bereitstellen. Virtuelle Maschinen, die viel Speicherplatz benötigen und auf reinen Computing-Hosts ausgeführt werden, speichern möglicherweise sehr viele Komponenten auf Einzelkapazitätshosts. Dadurch ist die Speicherleistung im Cluster möglicherweise niedriger.

- Konfigurieren Sie auf den Hosts keine aggressiven CPU-Energieverwaltungsrichtlinien zur Einsparung von Energie. Die Leistung bestimmter Anwendungen, die sensibel auf Wartezeiten bei der CPU-Geschwindigkeit reagieren, ist möglicherweise sehr stark beeinträchtigt. Informationen zu CPU-Energieverwaltungsrichtlinien finden Sie in der Dokumentation zur *Handbuch zur vSphere-Ressourcenverwaltung*.
- Falls Ihr Cluster Blade-Server enthält, sollten Sie eventuell die Kapazität des Datenspeichers durch externen Speicher erweitern, der mit den Blade-Servern verbunden ist und im vSAN-Abschnitt im *VMware-Kompatibilitätshandbuch* aufgelistet ist.
- Berücksichtigen Sie die Konfiguration der Arbeitslasten für eine Hybrid- oder All-Flash-Festplattenkonfiguration.
  - Für eine gut prognostizierbare Leistung sollten Sie einen Cluster mit All-Flash-Festplattengruppen bereitstellen.
  - Für das Gleichgewicht zwischen Leistung und Kosten sollten Sie einen Cluster mit Hybridfestplattengruppen bereitstellen.

## vSAN - und vCenter Server -Kompatibilität

Synchronisieren Sie die Versionen von vCenter Server und ESXi, um potenzielle Fehler aufgrund von Unterschieden bei der Unterstützung von vSAN in vCenter Server und ESXi zu vermeiden.

Für die optimale Integration zwischen vSAN-Komponenten in vCenter Server und ESXi sollten Sie die neueste Version der beiden vSphere-Komponenten bereitstellen. Weitere Hinweise finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere* und *vSphere-Upgrade*.

## Vorbereiten von Speicher-Controllern

Konfigurieren Sie den Speicher-Controller auf einem Host gemäß den Anforderungen von vSAN.

Vergewissern Sie sich, dass die Speicher-Controller auf den vSAN-Hosts bestimmte Anforderungen im Hinblick auf Modus, Treiber- und Firmware-Version, Warteschlangentiefe, Zwischenspeicherung und erweiterte Funktionen erfüllen.

**Tabelle 4-3.** Analysieren der Speicher-Controller-Konfiguration für vSAN

| Storage-Controller-Funktion | Storage-Controller-Anforderung |
|---|---|
| Erforderlicher Modus | ■ Prüfen Sie die vSAN-Anforderungen im *VMware-Kompatibilitätshandbuch* im Hinblick auf den erforderlichen Modus (Passthrough oder RAID 0) des Controllers.<br>■ Wenn der Passthrough- und der RAID 0-Modus unterstützt werden, konfigurieren Sie den Passthrough-Modus anstelle von RAID 0. Bei RAID 0 ist der Festplattenaustausch kompliziert. |
| RAID-Modus | ■ Erstellen Sie für RAID 0 ein RAID-Volume pro physischem Festplattengerät.<br>■ Aktivieren Sie nur den im *VMware-Kompatibilitätshandbuch* aufgeführten RAID-Modus.<br>■ Aktivieren Sie nicht die Controller-Aufteilung. |
| Treiber- und Firmware-Version | ■ Verwenden Sie für den Controller die neueste Treiber- und Firmware-Version gemäß dem *VMware-Kompatibilitätshandbuch*.<br>■ Überprüfen Sie bei Verwendung des mitgelieferten Controller-Treibers, ob der Treiber für vSAN zertifiziert ist.<br>OEM-Versionen von ESXi enthalten möglicherweise Treiber, die nicht zertifiziert und nicht im *VMware-Kompatibilitätshandbuch* aufgeführt sind. |
| Warteschlangentiefe | Vergewissern Sie sich, dass der Controller eine Warteschlangentiefe von mindestens 256 aufweist. Durch eine höhere Warteschlangentiefe wird die Leistung verbessert. |

**Tabelle 4-3.** Analysieren der Speicher-Controller-Konfiguration für vSAN (Fortsetzung)

| Storage-Controller-Funktion | Storage-Controller-Anforderung |
|---|---|
| Cache | Deaktivieren Sie den Speicher-Controller-Cache oder legen Sie ihn auf 100 Prozent fest, falls die Deaktivierung des Caches nicht möglich ist. |
| Erweiterte Funktionen | Deaktivieren Sie erweiterte Funktionen wie beispielsweise HP SSD Smart Path. |

# Konfigurieren eines vSAN -Netzwerks

Bevor Sie vSAN in einem Cluster und auf ESXi-Hosts aktivieren, müssen Sie das erforderliche Netzwerk für die vSAN-Kommunikation erstellen.

vSAN stellt eine verteilte Speicherlösung bereit, die den Datenaustausch über ESXi-Hosts im Cluster hinweg umfasst. Zum Vorbereiten des Netzwerks für die Installation von vSAN sind bestimmte Konfigurationsaspekte zu berücksichtigen.

Informationen zu den Richtlinien für das Netzwerkdesign finden Sie unter „Entwerfen des vSAN-Netzwerks“, auf Seite 30.

## Platzieren von Hosts im selben Subnetz

Die Hosts müssen sich im selben Subnetz befinden, um eine optimale Netzwerkleistung zu erzielen. In vSAN 6.0 und höher können Sie, falls erforderlich, auch Hosts im selben Layer 3-Netzwerk verbinden.

## Dedizieren von Netzwerkbandbreite auf einem physischen Adapter

Reservieren Sie mindestens 1 Gbit/s Bandbreite für vSAN. Sie können hierzu eine der folgenden Optionen verwenden:

- Dedizieren Sie physische 1-GbE-Adapter für eine Hybrid-Hostkonfiguration.
- Verwenden Sie dedizierte oder gemeinsam genutzte physische 10-GbE-Adapter für reine Flash-Konfigurationen.
- Verwenden Sie dedizierte oder gemeinsam genutzte physische 10-GbE-Adapter für Hybrid-Konfigurationen, falls möglich.
- Leiten Sie vSAN-Datenverkehr an einen physischen 10-GbE-Adapter, der anderen Systemdatenverkehr verarbeitet, und verwenden Sie vSphere Network I/O Control auf einem Distributed Switch, um Bandbreite für vSAN zu reservieren.

## Konfigurieren einer Portgruppe für den virtuellen Switch

Konfigurieren Sie eine Portgruppe auf einem virtuellen Switch für vSAN.

- Weisen Sie der Portgruppe den physischen Adapter für vSAN als einen aktiven Uplink zu.

  Falls die Netzwerkverfügbarkeit durch eine Gruppe von Netzwerkkarten gewährleistet wird, wählen Sie einen auf der Verbindung der physischen Adapter mit dem Switch basierenden Gruppierungsalgorithmus.
- Falls gemäß Design vorgesehen, weisen Sie den vSAN-Datenverkehr einem VLAN zu, indem Sie das Tagging auf dem virtuellen Switch aktivieren.

## Untersuchen der Firewall auf einem Host für vSAN

vSAN sendet Meldungen an bestimmte Ports auf jedem Host im Cluster. Stellen Sie sicher, dass die Firewalls der Hosts Datenverkehr über diese Ports zulassen.

**Tabelle 4-4.** Ports auf den Hosts in vSAN

| vSAN-Dienst | Datenverkehrsrichtung | Kommunizierende Knoten | Transportprotokoll | Port |
|---|---|---|---|---|
| vSAN-Anbieter-Provider (Vsanvp) | Eingehend und ausgehend | vCenter Server und ESXi | TCP | 8080 |
| vSAN-Clusterdienst | | ESXi | UDP | 12345, 23451 |
| vSAN-Transport | | ESXi | TCP | 2233 |
| Unicast-Agent | | ESXi | UDP | 12321 |

# Überlegungen zur vSAN -Lizenz

Wenn Sie Ihren Cluster für vSAN vorbereiten, überprüfen Sie die Anforderungen der vSAN-Lizenz.

- Stellen Sie sicher, dass Sie eine gültige Lizenz für eine komplette Hostkonfigurationssteuerung im Cluster erhalten haben. Die Lizenz sollte verschieden von der Lizenz sein, die Sie für Testphasenzwecke verwendet haben.

  Wenn die Lizenz oder die Testphase von vSAN abgelaufen ist, können Sie die aktuelle Konfiguration der vSAN-Ressourcen weiterhin verwenden. Sie können jedoch einer Festplattengruppe keine Kapazität hinzufügen oder Festplattengruppen erstellen.

- Wenn der Cluster aus All-Flash-Festplattengruppen besteht, stellen Sie sicher, dass die All-Flash-Funktion unter Ihrer Lizenz verfügbar ist.

- Wenn das vSAN-Cluster erweiterte Funktionen wie Deduplizierung und Komprimierung oder erweiterter Cluster verwendet, stellen Sie sicher, dass die Funktion unter Ihrer Lizenz verfügbar ist.

- Berücksichtigen Sie die CPU-Kapazität der vSAN-Lizenz im Cluster, wenn Sie dem Cluster Hosts hinzufügen oder Hosts aus dem Cluster entfernen.

  Die Kapazität der vSAN-Lizenzen wird pro CPU angegeben. Wenn Sie einem Cluster eine vSAN-Lizenz zuweisen, entspricht die Menge der verbrauchten Lizenzkapazität der Gesamtanzahl der CPUs auf den Hosts im Cluster.

# Erstellen eines vSAN -Clusters 5

Sie können vSAN aktivieren, wenn Sie einen Cluster erstellen, oder Sie können vSAN für Ihre vorhandenen Cluster aktivieren.

Dieses Kapitel behandelt die folgenden Themen:



## Merkmale eines vSAN -Clusters

Vor dem Arbeiten an einer vSAN-Umgebung sollten Sie die Merkmale eines Clusters für vSAN beachten.

Ein vSAN-Cluster weist die folgenden Merkmale auf:

- Sie können mehrere vSAN-Cluster für jede vCenter Server-Instanz haben. Sie können einen einzelnen vCenter Server zum Verwalten mehrerer vSAN-Cluster verwenden.
- vSAN nutzt alle Geräte, einschließlich Flash-Zwischenspeicher- und Kapazitätsgeräte, und nutzt die Geräte nicht gemeinsam mit anderen Funktionen.
- Cluster für vSAN können Hosts mit oder ohne Kapazitätsgeräte beinhalten. Es werden mindestens drei Hosts mit Kapazitätsgeräten benötigt. Um optimale Ergebnisse zu erzielen, erstellen Sie ein Cluster für vSAN mit gleich konfigurierten Hosts.
- Wenn ein Host Kapazität bereitstellt, muss er mindestens ein Flash-Zwischenspeichergerät und ein Kapazitätsgerät haben.
- In Hybrid-Clustern werden die magnetischen Festplatten für Kapazität und Flash-Geräte als Zwischenspeicher zum Lesen und Schreiben verwendet. vSAN weist 70 Prozent des gesamten verfügbaren Zwischenspeichers für Lesevorgänge und 30 Prozent für den Schreibpuffer zu. In diesen Konfigurationen dienen die Flash-Geräte als Lesezwischenspeicher und Schreibpuffer.
- In einem Alle-Flash-Cluster werden ein ausgewiesenes Flash-Gerät als Schreibzwischenspeicher und weitere Flash-Geräte für Kapazität verwendet. In Alle-Flash-Clustern kommen alle Leseanforderungen direkt von der Flash-Pool-Kapazität.
- Nur lokal oder direkt angeschlossene Kapazitätsgeräte können in einem Cluster für vSAN verwendet werden. vSAN kann keine anderen mit dem Cluster verbundenen externen Speicher wie SAN oder NAS verwenden.

Empfohlene Vorgehensweisen beim Planen und Dimensionieren eines vSAN-Clusters finden Sie unter Kapitel 3, „Entwerfen und Dimensionieren eines vSAN-Clusters“, auf Seite 21.

# Vor dem Erstellen eines vSAN -Clusters

In diesem Thema finden Sie eine Checkliste der Software- und Hardwareanforderungen für die Erstellung eines vSAN-Clusters. Sie können mit der Checkliste auch prüfen, ob der Cluster die Richtlinien und grundlegenden Anforderungen erfüllt.

## Anforderungen für ein vSAN -Cluster

Prüfen Sie zuerst die Kompatibilität der Hardwaregeräte, Treiberversionen und Firmware im VMware-Kompatibilitätshandbuch auf der Website unter http://www.vmware.com/resources/compatibility/search.php. Die folgende Tabelle enthält die wichtigsten Anforderungen zu der von vSAN unterstützten Software und Hardware.

**Vorsicht** Die Verwendung von nicht zertifizierten Software- und Hardwarekomponenten, Treibern, Controllern und nicht zertifizierter Firmware kann zu unerwartetem Datenverlust und Leistungsproblemen führen.

**Tabelle 5-1.** vSAN -Clusteranforderungen

| Anforderungen | Beschreibung |
|---|---|
| ESXi-Hosts | ■ Stellen Sie sicher, dass Sie die neueste Version von ESXi auf Ihren Hosts verwenden.<br>■ Stellen Sie sicher, dass mindestens drei ESXi-Hosts mit unterstützten Speicherkonfigurationen verfügbar sind, um sie dem vSAN-Cluster zuzuweisen. Um optimale Ergebnisse zu erzielen, sollten Sie den Cluster für vSAN mit mindestens vier Hosts konfigurieren. |
| Arbeitsspeicher | ■ Stellen Sie sicher, dass jeder Host über einen Arbeitsspeicher von mindestens 8 GB verfügt.<br>■ Bei größeren Konfigurationen und für höhere Leistungen benötigen Sie einen Arbeitsspeicher von mindestens 32 GB im Cluster. Siehe „Entwerfen und Dimensionieren von vSAN-Hosts“, auf Seite 28. |
| E/A-Speichercontroller, Treiber, Firmware | ■ Stellen Sie sicher, dass die E/A-Speichercontroller, Treiber- und Firmwareversionen zertifiziert sind und im VMware-Kompatibilitätshandbuch auf der Website unter http://www.vmware.com/resources/compatibility/search.php aufgeführt werden.<br>■ Stellen Sie sicher, dass der Controller für Passthrough oder den Modus RAID 0 konfiguriert ist.<br>■ Stellen Sie sicher, dass der Controllerzwischenspeicher und die erweiterten Funktionen deaktiviert sind. Wenn Sie den Zwischenspeicher nicht deaktivieren können, müssen Sie den Lesezwischenspeicher auf 100 Prozent setzen.<br>■ Prüfen Sie, ob Sie Controller mit höheren Warteschlangentiefen verwenden. Die Verwendung von Controllern mit Warteschlangentiefen kleiner als 256 kann sich während der Wartung oder bei Fehlern merklich auf die Leistung der virtuellen Maschinen auswirken. |
| Zwischenspeicher und Kapazität | ■ Stellen Sie sicher, dass vSAN-Hosts, die dem Cluster Speicher zur Verfügung stellen, über mindestens einen Zwischenspeicher und ein Kapazitätsgerät verfügen. Für vSAN ist Exklusivzugriff auf den lokalen Zwischenspeicher und die Kapazitätsgeräte der Hosts im vSAN-Cluster erforderlich. Sie können diese Geräte nicht mit anderen Verwendungen wie Virtual Flash File System (VFFS), VMFS-Partitionen oder einer ESXi-Boot-Partition teilen.<br>■ Um optimale Ergebnisse zu erzielen, erstellen Sie ein Cluster für vSAN mit gleich konfigurierten Hosts. |

**Tabelle 5-1.** vSAN -Clusteranforderungen (Fortsetzung)

| Anforderungen | Beschreibung |
|---|---|
| Netzwerkkonnektivität | ■ Stellen Sie sicher, dass jeder Host mit mindestens einem Netzwerkadapter konfiguriert ist.<br>■ Stellen Sie bei Hybridkonfigurationen sicher, dass für vSAN-Hosts eine Mindestbandbreite von 1 GbE reserviert ist.<br>■ Stellen Sie bei Alle-Flash-Konfigurationen sicher, dass für vSAN-Hosts eine Mindestbandbreite von 10 GbE verfügbar ist.<br>Informationen zu empfohlenen Vorgehensweisen und Überlegungen beim Planen eines vSAN-Netzwerks finden Sie unter „Entwerfen des vSAN-Netzwerks“, auf Seite 30 und „Netzwerkanforderungen für vSAN“, auf Seite 19. |
| vSAN- und vCenter Server-Kompatibilität | Stellen Sie sicher, dass Sie die neueste Version von vCenter Server verwenden. |
| Lizenzschlüssel | ■ Stellen Sie sicher, dass Sie über einen gültigen Lizenzschlüssel für vSAN verfügen.<br>■ Um die All-Flash-Funktion verwenden zu können, muss Ihre Lizenz diese Funktionalität unterstützen.<br>■ Um erweiterte Funktionen, z. B. ausgeweitete Cluster oder Deduplizierung und Komprimierung, verwenden zu können, muss Ihre Lizenz diese Funktionen unterstützen.<br>■ Stellen Sie sicher, dass die Höhe der Lizenzkapazität, die Sie zu verwenden planen, der Gesamtzahl der CPUs in den Hosts entspricht, die Teil des vSAN-Clusters sind. Stellen Sie Lizenzkapazitäten nicht nur für Hosts bereit, die dem Cluster Kapazität zur Verfügung stellen. Informationen über die Lizenzierung für vSAN finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*. |

Ausführliche Informationen zu den Anforderungen für vSAN-Cluster finden Sie unter Kapitel 2, „Anforderungen für die Aktivierung von vSAN“, auf Seite 17.

Ausführliche Informationen zum Planen und Dimensionieren eines vSAN-Clusters finden Sie im *Handbuch für VMware vSAN Design und Sizing*.

## Aktivieren von vSAN

Um vSAN verwenden zu können, müssen Sie einen Hostcluster erstellen und vSAN auf dem Cluster aktivieren.

Ein Cluster für vSAN kann Hosts mit Kapazität sowie Hosts ohne Kapazität beinhalten. Halten Sie sich beim Erstellen eines Clusters für vSAN an diese Richtlinien.

- Ein Cluster für vSAN muss aus mindestens drei ESXi-Hosts bestehen. Mindestens drei Hosts, die dem Cluster für vSAN beitreten, müssen Kapazität für den Cluster zur Verfügung stellen, damit der Cluster für vSAN Host- und Gerätefehler toleriert. Fügen Sie vier oder mehr Hosts hinzu, die dem Cluster Kapazität zur Verfügung stellen, um optimale Ergebnisse zu erhalten.
- Nur ESXi 5.5 Update 1-Hosts (oder höher) können dem vSAN-Cluster beitreten.
- Alle Hosts im vSAN-Cluster müssen dasselbe Festplattenformat aufweisen.
- Bevor Sie einen Host von einem vSAN-Cluster in einen anderen Cluster verschieben, stellen Sie sicher, dass der Zielcluster für vSAN aktiviert ist.
- Für den Zugriff auf den Datenspeicher für vSAN muss ein ESXi-Host zum Cluster für vSAN gehören.

Nach der Aktivierung von vSAN wird der vSAN-Speicheranbieter automatisch bei vCenter Server und der vSAN-Datenspeicher wird erstellt. Informationen zu Speicheranbietern finden Sie in der Dokumentation *vSphere-Speicher*.

## Einrichten eines VMkernel-Netzwerks für vSAN

Um den Austausch von Daten im Cluster für vSAN zu ermöglichen, müssen Sie auf jedem ESXi-Host einen VMkernel-Netzwerkadapter für den Datenverkehr auf vSAN bereitstellen.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum Host.

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

3 Wählen Sie unter **Netzwerk** die Option **VMkernel-Adapter** aus.

4 Klicken Sie auf das Symbol **Hostnetzwerk hinzufügen** (  ), um den Assistenten zum Hinzufügen eines Netzwerks zu öffnen.

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

6 Konfigurieren Sie das Zielwechselgerät.

7 Wählen Sie auf der Seite Porteigenschaften die Option **vSAN-Datenverkehr** aus.

8 Schließen Sie die VMkernel-Adapterkonfiguration ab.

9 Stellen Sie auf der Seite Bereit zum Abschließen sicher, dass vSAN im Status für den VMkernel-Adapter aktiviert ist, und klicken Sie auf **Beenden**.

vSAN-Netzwerk wird für den Host aktiviert.

### Weiter

Nun können Sie vSAN auf dem Host-Cluster aktivieren.

## Erstellen eines vSAN Clusters

vSAN kann beim Erstellen eines Clusters aktiviert werden.

### Vorgehensweise

1 Klicken Sie mit der rechten Maustaste auf ein Datencenter im vSphere Web Client und wählen Sie **Neuer Cluster** aus.

2 Geben Sie einen Namen für den Cluster in das Textfeld **Name** ein.

Dieser Name wird im Navigator von vSphere Web Client angezeigt.

3 Aktivieren Sie das Kontrollkästchen **Einschalten** für vSAN und klicken Sie auf **OK**.

Der Cluster wird in der Bestandsliste angezeigt.

4 Fügen Sie dem vSAN-Cluster Hosts hinzu. Siehe „Hinzufügen eines Hosts zu einem vSAN-Cluster“, auf Seite 122.

Cluster für vSAN können Hosts mit oder ohne Kapazitätsgeräte beinhalten. Fügen Sie Hosts mit Kapazität hinzu, um optimale Ergebnisse zu erzielen.

Beim Aktivieren von vSAN wird ein vSAN-Datenspeicher erstellt und der vSANSpeicheranbieter registriert. vSAN-Speicheranbieter sind integrierte Softwarekomponenten, die die Speicherfunktionen des Datenspeichers an vCenter Server übermitteln.

### Weiter

Vergewissern Sie sich, dass der Datenspeicher für vSAN erstellt wurde. Siehe „Anzeigen des vSAN-Datenspeichers“, auf Seite 55.

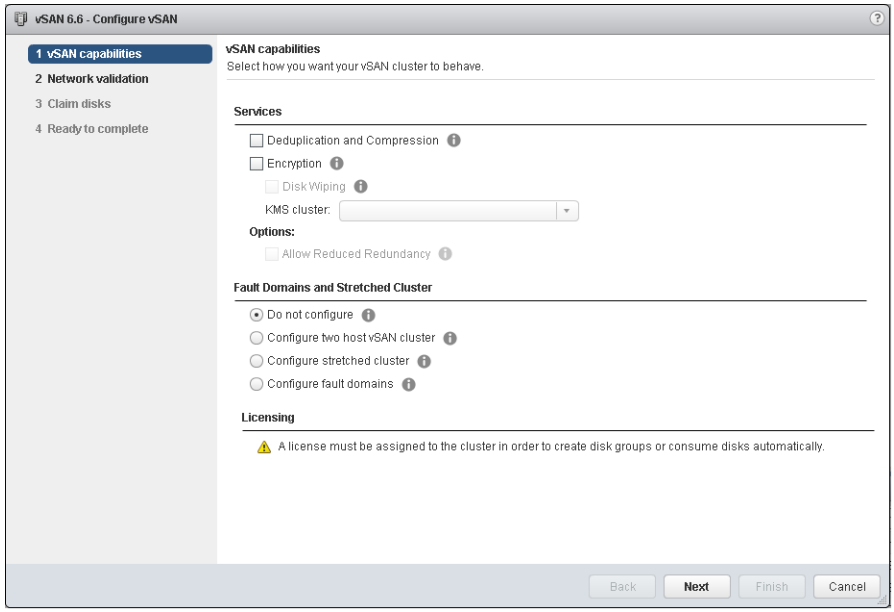
Vergewissern Sie sich, dass der Speicheranbieter für vSAN registriert ist. Siehe „Anzeigen von vSAN-Speicheranbietern“, auf Seite 141.

Beanspruchen Sie die Speichergeräte oder erstellen Sie Festplattegruppen. Siehe Kapitel 10, „Geräteverwaltung in einem vSAN-Cluster“, auf Seite 111.

Konfigurieren Sie den vSAN-Cluster. Siehe „Konfigurieren eines Clusters für vSAN“, auf Seite 51.

## Konfigurieren eines Clusters für vSAN

Sie können den Assistenten zum Konfigurieren von vSAN für die grundlegende Konfiguration Ihres vSAN-Clusters verwenden.




### Voraussetzungen

Bevor Sie den Assistenten zum Konfigurieren von vSAN verwenden, müssen Sie einen Cluster erstellen und diesem Hosts zuweisen, um die grundlegende Konfiguration abzuschließen.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu einem vorhandenen Cluster.

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

3 Wählen Sie unter „vSAN“ die Option **Allgemein** aus und klicken Sie auf die Schaltfläche **Konfigurieren**.

4 Wählen Sie **vSAN-Funktionen** aus.

   a (Optional) Wählen Sie das Kontrollkästchen **Deduplizierung und Komprimierung** aus, wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren möchten.

   Sie können das Kontrollkästchen **Verringerte Redundanz zulassen** aktivieren, um Deduplizierung und Komprimierung auf einem vSAN-Cluster zu aktivieren, das begrenzte Ressourcen aufweist (zum Beispiel ein Cluster mit drei Hosts, auf dem **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt ist). Wenn Sie verringerte Redundanz zulassen, sind Ihre Daten bei der Neuformatierung der Festplatte möglicherweise gefährdet.

   b (Optional) Aktivieren Sie das Kontrollkästchen **Verschlüsselung**, falls Sie die Verschlüsselung für nicht verwendete Daten aktivieren möchten, und wählen Sie einen KMS aus.

c Wählen Sie den Fault Tolerance-Modus für den Cluster aus.

| Option | Beschreibung |
|---|---|
| **Nicht konfigurieren** | Für einen vSAN-Cluster an einem einzelnen Standort verwendete Standardeinstellung. |
| **vSAN-Cluster mit zwei Hosts konfigurieren** | Bietet Fault Tolerance für einen Cluster, der über zwei Hosts an einer Außenstelle und einen Zeugen-Host in der Hauptniederlassung verfügt. Legen Sie die Richtlinie **Primäre Ebene von zu tolerierenden Fehlern** auf 1 fest. |
| **Ausgeweiteten Cluster konfigurieren** | Unterstützt zwei aktive Standorte mit einer gleichmäßigen Anzahl an Hosts und Speichergeräten und einen Zeugen-Host an einem dritten Standort. |
| **Fault Domains konfigurieren** | Unterstützt Fault Domains, die Sie zum Gruppieren von vSAN-Hosts verwenden können, die möglicherweise gemeinsam fehlschlagen. Weisen Sie jeder Fault Domain mindestens einen Host zu. |

d Sie können das Kontrollkästchen **Verringerte Redundanz zulassen** aktivieren, um die Verschlüsselung oder Deduplizierung und Komprimierung auf einem vSAN-Cluster mit begrenzten Ressourcen zu aktivieren. Dies ist beispielsweise sinnvoll, wenn Sie einen Cluster mit drei Hosts haben und die Option **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt ist. Wenn Sie verringerte Redundanz zulassen, sind Ihre Daten bei der Neuformatierung der Festplatte möglicherweise gefährdet.

5 Klicken Sie auf **Weiter**.

6 Überprüfen Sie auf der Seite Netzwerkvalidierung die Einstellung für vSAN-VMkernel-Adapter und klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite Festplatten beanspruchen die Festplatten zur Verwendung durch den Cluster aus und klicken Sie auf **Weiter**.

Wählen Sie für jeden Host, der Speicher bereitstellt, ein Flash-Gerät für die Cache-Schicht und ein oder mehrere Geräte für die Kapazitätsschicht aus.

8 Folgen Sie dem Assistenten, um die Konfiguration des Clusters basierend auf dem Fault Tolerance-Modus abzuschließen.

a Wenn Sie **Virtual SAN-Cluster mit zwei Hosts konfigurieren** festgelegt haben, wählen Sie einen Zeugenhost für den Cluster aus und beanspruchen Sie Festplatten für den Zeugenhost.

b Definieren Sie bei Auswahl von **Ausgeweiteten Cluster konfigurieren** Fault Domains für den Cluster, wählen Sie einen Zeugen-Host aus und beanspruchen Sie Festplatten für den Zeugen-Host.

c Definieren Sie bei Auswahl von **Fault Domains konfigurieren** Fault Domains für den Cluster.

Weitere Informationen zu Fault Domains finden Sie unter „Verwalten von Fault Domains in vSAN-Clustern“, auf Seite 128.

Weitere Informationen zu ausgeweiteten Clustern finden Sie unter Kapitel 6, „Erweitern eines Datenspeichers auf zwei Sites mit ausgeweiteten Clustern“, auf Seite 63.

9 Überprüfen Sie auf der Seite Bereit zum Abschließen die Konfiguration und klicken Sie auf **Beenden**.

## Bearbeiten von vSAN -Einstellungen

Sie können die Einstellungen Ihres vSAN-Clusters bearbeiten, um die Methode für die Beanspruchung von Festplatten zu ändern und um Deduplizierung und Komprimierung zu aktivieren.

Bearbeiten Sie die Einstellungen eines vorhandenen vSAN-Clusters, wenn Sie Deduplizierung und Komprimierung oder die Verschlüsselung aktivieren möchten. Wenn Sie Deduplizierung und Komprimierung oder die Verschlüsselung aktivieren, wird das Festplattenformat des Clusters automatisch auf die aktuelle Version aktualisiert.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSAN-Host-Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein**.

4 Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**.

5 (Optional) Wählen Sie das Kontrollkästchen Deduplizierung und Komprimierung aus, wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren möchten.

   vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt.

6 (Optional) Wenn Sie auf dem Cluster die Verschlüsselung aktivieren möchten, aktivieren Sie das Kontrollkästchen Verschlüsselung und wählen Sie einen KMS-Server aus.

   vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt.

7 Klicken Sie auf **OK**.

## Aktivieren von vSAN für einen vorhandenen Cluster

Sie können Clustereigenschaften bearbeiten, um vSAN für einen vorhandenen Cluster zu aktivieren.

Nachdem Sie vSAN in Ihrem Cluster aktiviert haben, können Sie vSAN-Hosts nicht mehr aus einem für vSAN aktivierten Cluster in einen nicht für vSAN aktivierten Cluster verschieben.

### Voraussetzungen

Vergewissern Sie sich, dass Ihre Umgebung alle Anforderungen erfüllt. Siehe Kapitel 2, „Anforderungen für die Aktivierung von vSAN“, auf Seite 17.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu einem vorhandenen Host-Cluster.

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

3 Wählen Sie unter vSAN **Allgemein** aus und klicken Sie auf **Bearbeiten**, um die Clustereinstellungen zu bearbeiten.

4 Wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren möchten, aktivieren Sie das Kontrollkästchen Deduplizierung und Komprimierung.

   vSAN aktualisiert automatisch das Festplattenformat und löst auf diese Weise eine rollende Neuformatierung aller Festplattengruppen im Cluster aus.

5 (Optional) Wenn Sie auf dem Cluster die Verschlüsselung aktivieren möchten, aktivieren Sie das Kontrollkästchen Verschlüsselung und wählen Sie einen KMS-Server aus.

   vSAN aktualisiert automatisch das Festplattenformat und löst auf diese Weise eine rollende Neuformatierung aller Festplattengruppen im Cluster aus.

6 Klicken Sie auf **OK**.

### Weiter

Beanspruchen Sie die Speichergeräte oder erstellen Sie Festplattegruppen. Siehe Kapitel 10, „Geräteverwaltung in einem vSAN-Cluster“, auf Seite 111.

## Deaktivieren von vSAN

Sie können vSAN für einen Host-Cluster deaktivieren.

Wenn Sie den Cluster für vSAN deaktivieren, kann auf keine der auf dem gemeinsam genutzten Datenspeicher für vSAN platzierten virtuellen Maschinen mehr zugegriffen werden. Wenn Sie beabsichtigen, eine virtuelle Maschine zu verwenden, während vSAN deaktiviert ist, stellen Sie sicher, dass Sie virtuelle Maschinen vor dem Deaktivieren des vSAN-Clusters aus dem vSAN-Datenspeicher in einen anderen Datenspeicher migrieren.

### Voraussetzungen

Stellen Sie sicher, dass sich die Hosts im Wartungsmodus befinden.

### Vorgehensweise

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

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

3 Wählen Sie unter vSAN **Allgemein** aus und klicken Sie auf **Bearbeiten**, um Einstellungen für vSAN zu bearbeiten.

4 Deaktivieren Sie das vSAN-Kontrollkästchen **Einschalten**.

## Konfigurieren von Lizenzeinstellungen für einen vSAN -Cluster

Sie müssen einem vSAN-Cluster nach Ablauf des Testzeitraums oder der Gültigkeit der derzeit zugewiesenen Lizenz eine Lizenz zuweisen.

Wenn Sie für vSAN-Lizenzen ein Upgrade durchführen, sie kombinieren oder teilen, müssen Sie die neuen Lizenzen vSAN-Clustern zuweisen. Wenn Sie einem Cluster eine vSAN-Lizenz zuweisen, entspricht die Menge der verbrauchten Lizenzkapazität der Gesamtanzahl an CPUs in den Hosts im Cluster. Die Lizenznutzung des vSAN-Clusters wird jedes Mal neu berechnet und aktualisiert, wenn Hosts zum Cluster hinzugefügt oder aus diesem entfernt werden. Informationen zum Verwalten von Lizenzen sowie zur Lizenzierungsterminologie und zu Definitionen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Wenn Sie vSAN auf einem Cluster aktivieren, können Sie vSAN im Testmodus ausführen, um die zugehörigen Funktionen auszuprobieren. Der Testzeitraum beginnt, wenn vSAN aktiviert wird, und läuft nach 60 Tagen ab. Um vSAN zu verwenden, müssen Sie den Cluster lizenzieren, bevor die Testphase abgelaufen ist. Ähnlich wie bei vSphere-Lizenzen wird die Kapazität der vSAN-Lizenzen pro CPU angegeben. Einige erweiterte Funktionen wie All-Flash-Konfiguration und ausgeweitete Cluster benötigen eine Lizenz, die diese Funktion unterstützt.

### Voraussetzungen

- Zum Anzeigen und Verwalten von vSAN-Lizenzen müssen Sie über die Berechtigung **Global.Licenses**auf den vCenter Server-Systemen verfügen, auf denen der vSphere Web Client ausgeführt wird.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu einem Cluster, auf dem vSAN aktiviert ist.

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

3 Wählen Sie unter **Konfiguration** die Option **Lizenzierung** aus und klicken Sie auf **Lizenz zuweisen**.

4 Wählen Sie eine Lizenzierungsoption aus.

- Wählen Sie eine vorhandene Lizenz aus und klicken Sie auf **OK**.
- Erstellen Sie eine vSAN-Lizenz.

  a Klicken Sie auf das Symbol **Neue Lizenz erstellen** (Symbol ).

  b Geben Sie im Dialogfeld „Neue Lizenzen“ einen vSAN-Lizenzschlüssel ein bzw. kopieren Sie ihn in das Feld und klicken Sie auf **Weiter**.

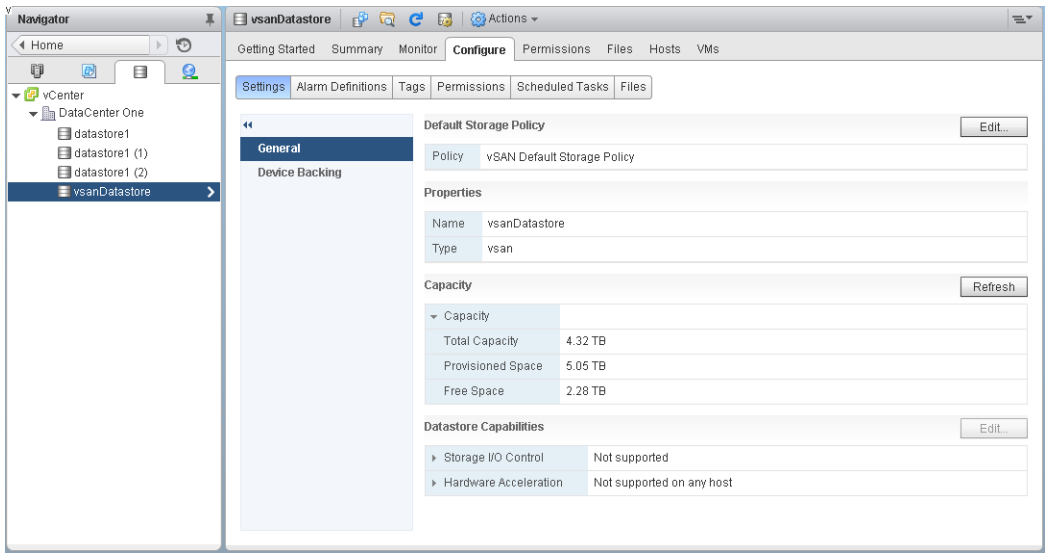
  c Benennen Sie auf der Seite Lizenznamen bearbeiten die neue Lizenz wie gewünscht um und klicken Sie auf **Weiter**.

  d Klicken Sie auf **Beenden**.

  e Wählen Sie im Dialogfeld Lizenz zuweisen die neu erstellte Lizenz aus und klicken Sie auf **OK**.

## Anzeigen des vSAN -Datenspeichers

Nachdem Sie vSAN aktiviert haben, wird ein einzelner Datenspeicher erstellt. Sie können die Kapazität des vSAN-Datenspeichers überprüfen.




### Voraussetzungen

Aktivieren Sie vSAN und konfigurieren Sie Festplattengruppen.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum Speicher.

2 Wählen Sie den vSAN-Datenspeicher aus.

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

4 Überprüfen Sie die Kapazität des vSAN-Datenspeichers.

Die Größe des vSAN-Datenspeichers ist abhängig von der Anzahl der Kapazitätsgeräte pro ESXi-Host und der Anzahl der ESXi-Hosts im Cluster. Angenommen, ein Host weist sieben Kapazitätslaufwerke mit 2 TB auf, und der Cluster besteht aus acht Hosts. In diesem Fall beträgt die Speicherkapazität etwa 7 x 2 TB x 8 = 112 TB. Beachten Sie, dass bei Verwendung der All-Flash-Konfiguration Flash-Geräte für die Kapazität verwendet werden. Für Hybridkonfigurationen werden Magnetfestplatten für die Kapazität verwendet.

Ein Teil der Kapazität wird für Metadaten zugeteilt.

- Version 1.0 des Festplattenformats fügt etwa 1 GB pro Kapazitätsgerät hinzu.
- Version 2.0 des Festplattenformats fügt Kapazitäts-Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät.
- Version 3.0 und höher des Festplattenformats fügt Kapazitäts-Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät. Deduplizierung und Komprimierung mit aktivierter Software-Prüfsumme benötigt zusätzlichen Overhead von ungefähr 6,2 Prozent Kapazität pro Gerät.

**Weiter**

Erstellen Sie mithilfe der Speicherfunktionen des Datenspeichers für vSAN eine Speicherrichtlinie für virtuelle Maschinen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Speicher*.

## Verwenden von vSAN und vSphere HA

Sie können vSphere HA und vSAN auf demselben Cluster aktivieren. Wie herkömmliche Datenspeicher gewährleistet vSphere HA denselben Schutz für virtuelle Maschinen auf vSAN-Datenspeichern. Dieser Schutz bedeutet Einschränkungen bei der Interaktion von vSphere HA und vSAN.

### Anforderungen für ESXi -Hosts

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

- Für die ESXi-Hosts des Clusters ist mindestens Version 5.5 Update 1 erforderlich.
- Der Cluster muss aus mindestens drei ESXi-Hosts bestehen. Um optimale Ergebnisse zu erzielen, sollten Sie den Cluster für vSAN mit mindestens vier Hosts konfigurieren.

### Unterschiede beim Netzwerk

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

**Hinweis** Sie müssen vSphere HA deaktivieren, bevor Sie vSAN auf dem Cluster aktivieren. Anschließend können Sie vSphere HA erneut aktivieren.

Wenn eine virtuelle Maschine in allen Netzwerkpartitionen nur teilweise verfügbar ist, können Sie die virtuelle Maschine nicht einschalten, oder keine Partition hat vollen Zugriff auf sie. Wenn Sie einen Cluster z. B. in die Partitionen „P1“ und „P2“ partitionieren, ist das VM-Namespace-Objekt für die Partition „P1“, aber nicht für „P2“ verfügbar. Die VMDK ist für Partition „P2“, aber nicht für „P1“ verfügbar. In solchen Fällen kann die virtuelle Maschine nicht eingeschaltet werden, und keine Partition hat vollen Zugriff auf sie.

In der folgenden Tabelle werden die Unterschiede beim vSphere HA-Netzwerk erläutert, wenn vSAN verwendet bzw. nicht verwendet wird.

**Tabelle 5-2.** Unterschiede beim vSphere HA-Netzwerk

| | vSAN aktiviert | vSAN deaktiviert |
|---|---|---|
| Von vSphere HA verwendetes Netzwerk | vSAN-Speichernetzwerk | Verwaltungsnetzwerk |
| Taktsignal-Datenspeicher | Jeder für mehrere Hosts gemountete Datenspeicher, nicht jedoch vSAN-Datenspeicher | Jeder für mehrere Hosts gemountete Datenspeicher |
| Als isoliert erklärter Host | Isolationsadressen können nicht angepingt werden, kein Zugriff auf das Speichernetzwerk für vSAN | Isolationsadressen können nicht angepingt werden, kein Zugriff auf das Verwaltungsnetzwerk |

Wenn Sie die vSAN-Netzwerkkonfiguration ändern, übernehmen die vSphere HA-Agenten nicht automatisch die neuen Netzwerkeinstellungen. Um Änderungen am vSAN-Netzwerk vorzunehmen, müssen Sie die Hostüberwachung für den vSphere HA-Cluster unter Verwendung von vSphere Web Client wieder aktivieren:

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

2 Nehmen Sie die Änderungen am vSAN-Netzwerk vor.

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

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

## Einstellungen für die Kapazitätsreservierung

Wenn Sie Kapazität für Ihren vSphere HA-Cluster mit einer Zugangssteuerungsrichtlinie reservieren, muss diese Einstellung mit der entsprechenden Richtlinieneinstellung **Primäre Ebene von zu tolerierenden Fehlern** im vSAN-Regelsatz koordiniert werden und darf nicht niedriger als die durch die Einstellung für die vSphere HA-Zugangssteuerung reservierte Kapazität sein. Wenn beispielsweise der Regelsatz für vSAN nur zwei Fehler zulässt, muss die vSphere HA-Zugangssteuerungsrichtlinie Kapazität reservieren, die nur einem oder zwei Hostfehlern entspricht. Falls Sie die Richtlinie „Prozentsatz der reservierten Clusterressourcen“ für einen Cluster mit acht Hosts verwenden, dürfen Sie nicht mehr als 25 Prozent der Clusterressourcen reservieren. Für denselben Cluster mit der Richtlinie **Primäre Ebene von zu tolerierenden Fehlern** darf die Einstellung nicht höher als zwei Hosts sein. Wenn weniger Kapazität durch vSphere HA reserviert wird, kann die Failover-Aktivität unvorhersehbar sein. Die Reservierung von zu viel Kapazität bedeutet dagegen, dass das Einschalten von virtuellen Maschinen und die vSphere vMotion-Migrationen zwischen Clustern übermäßig belastet werden. Informationen zur Richtlinie „Prozentsatz der reservierten Clusterressourcen“ finden Sie in der Dokumentation zur *Verfügbarkeit in vSphere*.

## Verhalten von vSAN und vSphere HA bei einem Ausfall mehrerer Hosts

Nach dem Ausfall eines vSAN-Clusters mit einem Verlust des Failover-Quorums für ein VM-Objekt kann vSphere HA möglicherweise die virtuelle Maschine nicht neu starten, auch wenn das Cluster-Quorum wiederhergestellt wurde. vSphere HA garantiert den Neustart nur, wenn ein Cluster-Quorum vorhanden ist und auf die neueste Kopie des VM-Objekts zugegriffen werden kann. Die neueste Kopie ist die letzte zu schreibende Kopie.

Nehmen Sie als Beispiel die vSAN-VM, die so bereitgestellt wurde, dass ein Hostausfall toleriert wird. Die virtuelle Maschine wird auf einem vSAN-Cluster ausgeführt, der drei Hosts umfasst, nämlich H1, H2 und H3. Alle drei Hosts fallen nacheinander aus, wobei H3 der letzte Host ist.

Nachdem H1 und H2 wiederhergestellt worden sind, hat der Cluster ein Quorum (ein Hostausfall wird toleriert). Trotz dieses Quorums kann vSphere HA die virtuelle Maschine nicht neu starten, da der letzte ausgefallene Host (H3) die neueste Kopie des VM-Objekts enthält und noch nicht auf ihn zugegriffen werden kann.

In diesem Beispiel müssen alle drei Hosts entweder gleichzeitig wiederhergestellt werden oder das Doppel-Host-Quorum muss H3 enthalten. Wenn keine der beiden Bedingungen erfüllt ist, versucht HA die virtuelle Maschine neu zu starten, sobald der Host H3 wieder online ist.

### Bereitstellen von vSAN mit vCenter Server Appliance

Sie können einen vSAN-Cluster erstellen, wenn Sie einen vCenter Server Appliance bereitstellen und die Appliance dann auf diesem Cluster hosten.

Die vCenter Server Appliance ist eine vorkonfigurierte Linux-VM, die zum Ausführen von VMware vCenter Server auf Linux-Systemen verwendet wird. Mithilfe dieser Funktion können Sie einen vSAN-Cluster auf neuen ESXi-Hosts konfigurieren, ohne vCenter Server verwenden zu müssen.

Wenn Sie das vCenter Server Appliance-Installationsprogramm verwenden, um eine vCenter Server Appliance bereitzustellen, können Sie einen aus einem einzelnen Host bestehenden vSAN-Cluster erstellen und den vCenter Server Appliance auf dem Cluster hosten. Wenn Sie während Phase 1 der Bereitstellung einen Datenspeicher auswählen, klicken Sie auf **Auf einem neuen vSAN-Cluster mit dem Zielhost installieren**. Führen Sie die Schritte im Installationsassistenten aus, um die Bereitstellung abzuschließen.

Das vCenter Server Appliance-Installationsprogramm erstellt einen vSAN-Cluster, der aus einem einzelnen Host mit vom Host beanspruchten Festplatten besteht. vCenter Server Appliance wird auf dem vSAN-Cluster bereitgestellt.

Nach Abschluss der Bereitstellung können Sie den aus einem Host bestehenden vSAN-Cluster mit vCenter Server Appliance verwalten. Sie müssen die Konfiguration des vSAN-Clusters abschließen.

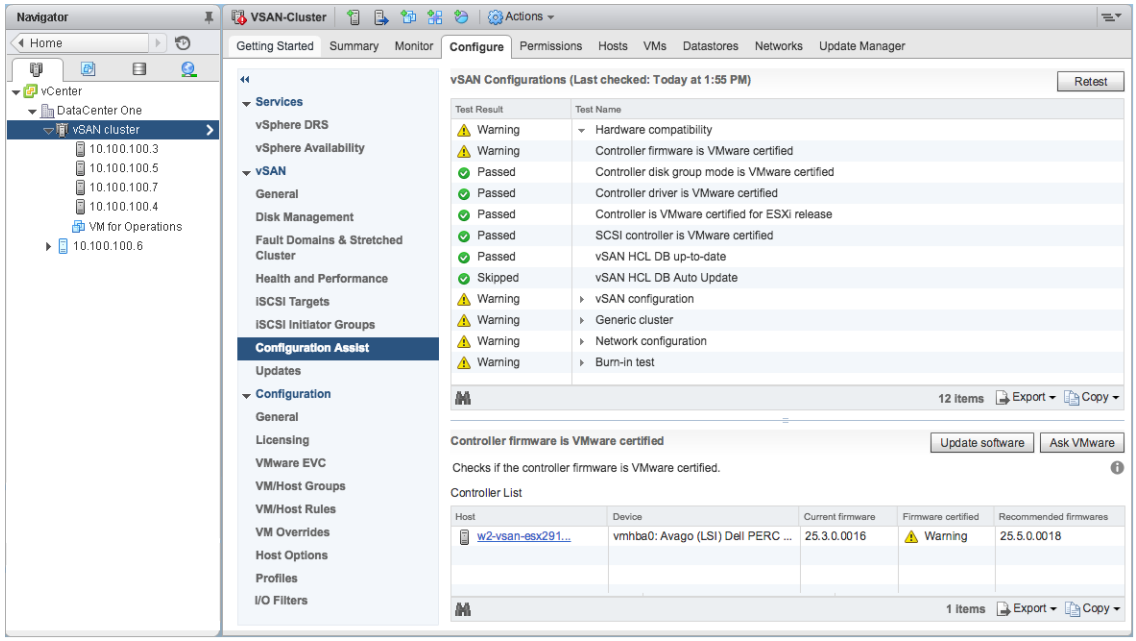
Sie können einen Platform Services Controller und vCenter Server auf demselben vSAN-Cluster oder auf getrennten Clustern bereitstellen.

- Sie können einen Platform Services Controller und vCenter Server auf demselben vSAN-Cluster bereitstellen. Stellen Sie den PSC und vCenter Server auf dem aus einem einzelnen Host bestehenden vSAN-Datenspeicher bereit. Nach Abschluss der Bereitstellung laufen der Platform Services Controller und vCenter Server auf demselben Cluster.
- Sie können einen Platform Services Controller und vCenter Server auf unterschiedlichen vSAN-Clustern bereitstellen. Stellen Sie den Platform Services Controller und vCenter Server auf getrennten, aus einem einzelnen Host bestehenden vSAN-Clustern bereit. Nach Abschluss der Bereitstellung müssen Sie die einzelnen vSAN-Cluster getrennt konfigurieren.

## Verwenden des vSAN -Konfigurationsassistent und Verwenden von Updates

Mit dem Konfigurationsassistenten können Sie die Konfiguration Ihres vSAN-Clusters überprüfen und Probleme beheben.

Mit dem vSAN-Konfigurationsassistenten können Sie die Konfiguration der Clusterkomponenten überprüfen, Probleme beheben und eine Fehlerbehebung durchführen. Die Konfigurationsprüfungen decken Hardwarekompatibilität, Netzwerk und vSAN-Konfigurationsoptionen ab.




Die Prüfungen des Konfigurationsassistenten sind in Kategorien unterteilt. Jede Kategorie enthält individuelle Konfigurationsprüfungen.

**Tabelle 5-3.** Konfigurationsassistent-Kategorien

| Konfigurationskategorie | Beschreibung |
|---|---|
| Hardwarekompatibilität | Überprüft die Hardwarekomponenten für den vSAN-Cluster, um sicherzustellen, dass sie unterstützte Hardware, Software und Treiber verwenden. |
| vSAN-Konfiguration | vSAN-Konfigurationsoptionen werden überprüft. |
| Allgemeiner Cluster | Überprüft die grundlegenden Optionen der Clusterkonfiguration. |
| Netzwerkkonfiguration | vSAN-Netzwerkkonfiguration wird überprüft. |
| Burn-In-Test | Überprüft Burn-In-Testvorgänge. |

Falls die Speicher-Controller-Firmware oder -Treiber nicht die im *VMware-Kompatibilitätshandbuch* aufgeführten Anforderungen erfüllen, können Sie die Controller über die Seite „Updates“ aktualisieren.

## Überprüfen der vSAN -Konfiguration

Sie können den Konfigurationsstatus Ihres vSAN-Clusters anzeigen und Probleme beheben, die den Betrieb Ihres Clusters beeinträchtigen.

### Vorgehensweise

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

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

3 Klicken Sie unter **vSAN** auf **Konfigurationsassistent**, um die vSAN-Konfigurationskategorien zu überprüfen.

Wenn in der Spalte „Testergebnis“ ein Warnsymbol angezeigt wird, erweitern Sie die Kategorie, um die Ergebnisse der einzelnen Konfigurationsprüfungen zu überprüfen.

4 Wählen Sie eine einzelne Konfigurationsprüfung aus und prüfen Sie die detaillierten Informationen unten auf der Seite.

Sie können auf die Schaltfläche **VMware fragen** klicken, um einen Knowledgebase-Artikel zu öffnen, in dem die Prüfung beschrieben wird und Informationen zur Fehlerbehebung bereitgestellt werden.

Einige Konfigurationsprüfungen bieten zusätzliche Schaltflächen, die Ihnen bei der Durchführung der Konfiguration helfen.

## Konfigurieren eines Distributed Switch für vSAN

Mit dem Assistenten „Neuen Distributed Switch für vSAN konfigurieren“ können Sie einen vSphere Distributed Switch zur Unterstützung des vSAN-Datenverkehrs konfigurieren.

Wenn in Ihrem Cluster kein vSphere Distributed Switch zur Unterstützung des vSAN-Datenverkehrs konfiguriert ist, gibt die Seite „Konfigurationsassistent“ eine Warnung für **Netzwerkkonfiguration > vDS für vSAN verwenden** aus.

### Vorgehensweise

1 Navigieren Sie zu Ihrem vSAN-Cluster im vSphere Web Client.

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

3 Wählen Sie unter vSAN **Konfigurationsassistent** und klicken Sie, um die Kategorie **Netzwerkkonfiguration** zu erweitern.

4 Klicken Sie auf **vDS für vSAN verwenden**. Klicken Sie in der unteren Hälfte der Seite auf **vDS erstellen**.

5 Geben Sie unter „Name und Typ“ einen Namen für den neuen Distributed Switch ein und wählen Sie, ob ein neuer Switch erstellt oder ein vorhandener Standard-Switch migriert werden soll.

6 Wählen Sie die nicht verwendeten Adapter aus, die Sie zum neuen Distributed Switch migrieren möchten, und klicken Sie auf **Weiter**.

7 (Optional) Wählen Sie unter „Infrastruktur-VMs migrieren“ die VM aus, die während der Migration als Infrastruktur-VM für einen vorhandenen Standard-Switch behandelt werden soll, und klicken Sie auf **Weiter**.

Dieser Schritt ist nicht erforderlich, wenn Sie einen neuen Distributed Switch erstellen.

8 Überprüfen Sie unter „Bereit zum Abschließen“ die Konfiguration und klicken Sie auf **Beenden**.

## Erstellen eines VMkernel-Netzwerkadapters für vSAN

Mit dem Assistenten „Neue VMkernel-Netzwerkadapter für vSAN“ können Sie vmknics zur Unterstützung des vSAN-Datenverkehrs konfigurieren.

Wenn für ESXi-Hosts in Ihrem Cluster vmknics zur Unterstützung des vSAN-Datenverkehrs nicht konfiguriert ist, gibt die Seite „Konfigurationsassistent“ eine Warnung für **Netzwerkkonfiguration > Für alle Hosts ist vSAN-vmknic konfiguriert** aus.

### Vorgehensweise

1 Navigieren Sie zu Ihrem vSAN-Cluster im vSphere Web Client.

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

3 Wählen Sie unter vSAN **Konfigurationsassistent** und klicken Sie, um die Kategorie **Netzwerkkonfiguration** zu erweitern.

4 Klicken Sie auf **Für alle Hosts ist vSAN-vmknic konfiguriert**. Klicken Sie in der unteren Hälfte der Seite auf **VMkernel-Netzwerkadapter erstellen**.

5 Aktivieren Sie unter „Hosts auswählen“ die Kontrollkästchen für alle Hosts, für die vmknic für vSAN nicht konfiguriert ist, und klicken Sie auf **Weiter**.

Hosts ohne vSAN-vmknic werden auf der Seite „Konfigurationsassistent“ aufgelistet.

6 Wählen Sie unter „Speicherort und Dienste“ einen Distributed Switch aus und aktivieren Sie dann das Kontrollkästchen **vSAN-Datenverkehr**. Klicken Sie auf **Weiter**.

7 Wählen Sie in den vSAN-Adaptereinstellungen eine Portgruppe, IP-Einstellungen und die Konfiguration aus und klicken Sie auf **Weiter**.

8 Überprüfen Sie unter „Bereit zum Abschließen“ die Konfiguration und klicken Sie auf **Beenden**.

## Installieren von Controller-Verwaltungstools für Treiber- und Firmware-Updates

Anbieter von Speicher-Controllern stellen ein Software-Verwaltungstool zur Verfügung, das vSAN zum Aktualisieren von Controller-Treiber und -Firmware nutzen kann. Falls das Verwaltungstool auf ESXi-Hosts nicht zur Verfügung steht, können Sie es herunterladen.

Auf der Seite Updates werden nur bestimmte Speicher-Controller-Modelle ausgewählter Anbieter unterstützt.

### Voraussetzungen

- Überprüfen Sie auf der Seite Konfigurationsassistent die Hardwarekompatibilität.
- DRS muss aktiviert sein, wenn während der Softwareaktualisierung die VMs noch im Betrieb bleiben müssen.

### Vorgehensweise

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

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

3 Klicken Sie unter „vSAN“ auf **Updates**, um die Komponenten zu überprüfen, die fehlen oder zur Installation bereit sind.

4 Wählen Sie das Verwaltungstool für Ihren Controller aus und klicken Sie auf das Symbol **Herunterladen**.

Das Verwaltungstool wird auf vCenter Server heruntergeladen.

5 Klicken Sie auf das Symbol **Alle aktualisieren**, um das Verwaltungstool auf den ESXi-Hosts in Ihrem Cluster zu installieren.

Geben Sie an, ob Sie alle Hosts auf einmal oder nach und nach aktualisieren möchten.

6 Klicken Sie auf das Symbol **Aktualisieren**.

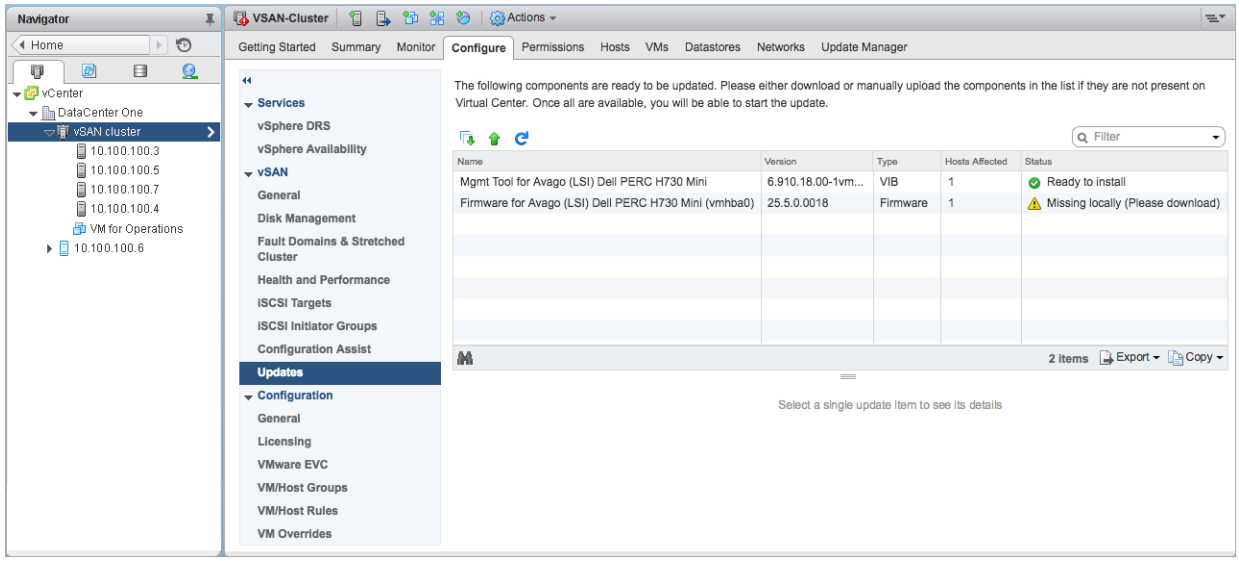
Auf der Seite „Updates“ werden die Controller-Komponenten aufgeführt, die aktualisiert werden müssen.

### Weiter

Wenn das Speicher-Controller-Verwaltungstool nicht zur Verfügung steht, werden auf der Seite „Updates“ alle fehlenden Treiber bzw. die fehlende Firmware aufgeführt. Sie können diese fehlenden Komponenten aktualisieren.

## Aktualisieren der Speicher-Controller-Treiber und -Firmware

Mit vSAN können Sie alte oder falsche Treiber und Firmware auf Speicher-Controllern aktualisieren.




Der Konfigurationsassistent überprüft, ob Ihre Speicher-Controller die neueste Treiber- und Firmware-Version verwenden, wie im *VMware-Kompatibilitätshandbuch* aufgeführt. Falls die Controller-Treiber oder die Controller-Firmware nicht die Anforderungen erfüllen, führen Sie über die Seite „Updates“ Treiber- und Firmware-Updates durch.

### Voraussetzungen

Die Controller-Verwaltungstools für Ihre Speichergeräte müssen auf dem ESXi-Host vorhanden sein.

### Vorgehensweise

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

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

3 Klicken Sie unter „vSAN“ auf **Updates**, um die Komponenten zu überprüfen, die fehlen oder zur Installation bereit sind.

Die Seite „Updates“ listet die fehlende Firmware und die fehlenden Treiberkomponenten auf.

---

**Hinweis** Wenn das Controller-Verwaltungtool (Mgmt) nicht verfügbar ist, werden Sie aufgefordert, das Verwaltungstool herunterzuladen und zu installieren. Wenn das Verwaltungtool verfügbar ist, werden die fehlenden Treiber bzw. die fehlende Firmware aufgelistet.

---

4 Wählen Sie die Komponente aus, die Sie aktualisieren möchten, und klicken Sie auf das **Update**-Symbol, um die Komponente auf den ESXi-Hosts im Cluster zu aktualisieren. Oder klicken Sie auf das Symbol **Alles aktualisieren**, um alle fehlenden Komponenten zu aktualisieren.

Geben Sie an, ob Sie alle Hosts auf einmal oder nach und nach aktualisieren möchten.

---

**Hinweis** Bei einigen Verwaltungtools und Treibern umgeht der Update-Vorgang den Wartungsmodus und führt einen Neustart auf Basis des Installationsergebnisses durch. In diesen Fällen sind die Felder **MM erforderlich** und **Neustart erforderlich** leer.

---

5 Klicken Sie auf das Symbol **Aktualisieren**.

Die aktualisierten Komponenten werden aus der Anzeige entfernt.

# Erweitern eines Datenspeichers auf zwei Sites mit ausgeweiteten Clustern

6

Sie können einen ausgeweiteten Cluster erstellen, der sich über zwei geografische Standorte (oder Sites) erstreckt. Mit ausgeweiteten Clustern können Sie den vSAN-Datenspeicher auf zwei Sites zwecks Verwendung als ausgeweiteten Speicher erweitern. Der ausgeweitete Cluster ist weiterhin funktionsbereit, wenn ein Fehler auftritt oder eine geplante Wartung auf einer Site vorgenommen wird.

Dieses Kapitel behandelt die folgenden Themen:



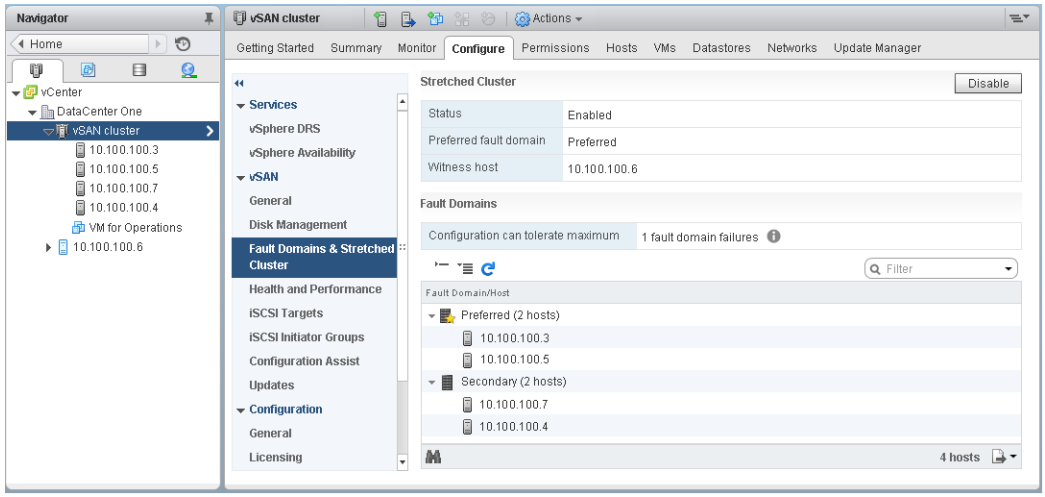
## Einführung in ausgeweitete Cluster

Ausgeweitete Cluster erweitern den vSAN-Cluster von einer Site auf zwei Sites und bieten somit eine höhere Verfügbarkeit und verbesserten Lastausgleich zwischen den einzelnen Sites. Ausgeweitete Cluster werden normalerweise in Umgebungen bereitgestellt, bei denen die Entfernung zwischen den Datencentern gering ist, zum Beispiel in Großstädten oder Universitäten.

Sie können ausgeweitete Cluster zum Verwalten geplanter Wartungsvorgänge und zum Vermeiden von Notfallszenarien verwenden, da sich die Wartung oder der Verlust einer Site nicht auf den Gesamtbetrieb des Clusters auswirken. In einer Konfiguration mit ausgeweiteten Clustern können beide Sites aktive Sites sein. Wenn eine der beiden Sites fehlschlägt, verwendet vSAN den Speicherplatz auf der anderen Site. vSphere HA startet alle VMs neu, die auf der verbleibenden aktiven Site neu gestartet werden müssen.

Sie müssen eine Site als bevorzugte Site festlegen. Die andere Site wird zu einer sekundären oder nicht bevorzugten Site. Das System verwendet die bevorzugte Site nur in Fällen, in denen ein Verlust der Netzwerkverbindung zwischen den beiden aktiven Sites aufgetreten ist. Die als bevorzugte Site festgelegte Site ist also die Site, deren Betrieb aufrecht erhalten bleibt.

Ein ausgeweiteter vSAN-Cluster kann jeweils einen Verbindungsausfall tolerieren, wobei die Verfügbarkeit der Daten gewährleistet ist. Ein Verbindungsausfall ist der Verlust der Netzwerkverbindung zwischen den beiden Sites oder zwischen einer Site und dem Zeugen-Host. Während eines Siteausfalls oder eines Verlusts der Netzwerkverbindung wechselt vSAN automatisch zu voll funktionsfähigen Sites.




Weitere Informationen zum Arbeiten mit ausgeweiteten Clustern finden Sie im *vSAN Stretched Cluster Guide* (Handbuch für ausgeweitete vSAN-Cluster).

## Zeugen-Host

Jeder ausgeweitete Cluster besteht aus zwei Sites und einem Zeugen-Host. Der Zeugen-Host befindet sich auf einer dritten Site und enthält die Zeugen-Komponenten der VM-Objekte. Er enthält nur Metadaten und ist an keinen Speichervorgängen beteiligt.

Der Zeugen-Host dient als Entscheidungskriterium, wenn eine Entscheidung hinsichtlich der Verfügbarkeit der Datenspeicherkomponenten bei Verlust der Netzwerkverbindung zwischen den beiden Sites getroffen werden muss. In diesem Fall bildet der Zeugen-Host normalerweise einen vSAN-Cluster mit der bevorzugten Site. Wenn allerdings die bevorzugte Site von der sekundären Site und dem Zeugen-Host getrennt wird, bildet der Zeugen-Host einen Cluster unter Verwendung der sekundären Site. Wenn die bevorzugte Site erneut online geschaltet wird, werden die Daten neu synchronisiert, um sicherzustellen, dass beide Sites über die aktuellsten Kopien aller Daten verfügen.

Wenn der Zeugen-Host ausfällt, sind alle zugehörigen Objekte nicht mehr kompatibel, der Zugriff auf die Objekte ist jedoch weiterhin möglich.

Der Zeugen-Host verfügt über die folgenden Eigenschaften:

- Der Zeugen-Host kann Verbindungen mit geringer Bandbreite und hoher Latenz verwenden.
- Der Zeugen-Host kann keine VMs ausführen.
- Der Zeugen-Host kann nur ausgeweitete vSAN-Cluster unterstützen.
- Der Zeugen-Host muss über einen VMkernel-Adapter mit aktiviertem vSAN-Datenverkehr mit Verbindungen zu allen Hosts im Cluster verfügen. Der Zeugen-Host verwendet einen VMkernel-Adapter für die Verwaltung und einen VMkernel-Adapter für den vSAN-Datenverkehr. Der Zeugen-Host darf nur einen für vSAN reservierten VMkernel-Adapter aufweisen.
- Der Zeugen-Host muss ein eigenständiger für den ausgeweiteten Cluster reservierter Host sein. Er kann keinem anderen Cluster hinzugefügt oder über vCenter Server in die Bestandsliste verschoben werden.

Der Zeugen-Host kann ein physischer Host oder ein innerhalb einer VM ausgeführter ESXi-Host sein. Der VM-Zeugen-Host bietet keine anderen Funktionen, wie zum Beispiel das Speichern oder Ausführen von VMs. Mehrere Zeugen-Hosts können als VMs auf einem einzelnen physischen Server ausgeführt werden. Für die Patching-Konfiguration und die grundlegende Netzwerk- und Überwachungskonfiguration arbeitet der VM-Zeugen-Host genau wie ein typischer ESXi-Host. Sie können ihn mit vCenter Server verwalten, unter Verwendung von `esxcli` oder vSphere Update Manager patchen und aktualisieren und mit Standardtools überwachen, die mit ESXi-Hosts interagieren.

Sie können eine virtuelle Zeugen-Appliance als Zeugen-Host in einem ausgeweiteten Cluster verwenden. Die virtuelle Zeugen-Appliance ist ein ESXi-Host in einer VM, die als OVF oder OVA gepackt ist. Die Appliance ist basierend auf dem Umfang der Bereitstellung mit verschiedenen Optionen verfügbar.

### Ausgeweitete Cluster im Vergleich zu Fault Domains

Ausgeweitete Cluster bieten Redundanz und Ausfallschutz für Datencenter an zwei geografischen Standorten. Fault Domains bieten Schutz vor Ausfall auf Rack-Ebene innerhalb derselben Site. Jede Site in einem ausgeweiteten Cluster befindet sich auf einer separaten Fault Domain.

Ein ausgeweiteter Cluster benötigt drei Fault Domains: die bevorzugte Site, die sekundäre Site und einen Zeugen-Host.

Sie können in vSAN 6.6 und höheren Versionen eine zusätzliche Ebene von lokalem Fehlerschutz für VM-Objekte in ausgeweiteten Clustern bereitstellen. Wenn Sie einen ausgeweiteten Cluster mit vier oder mehr Hosts an jeder Site konfigurieren, stehen die folgenden Richtlinienregeln für Objekte im Cluster zur Verfügung:

- **Primäre Ebene von zu tolerierenden Fehlern (PFTT)**. Diese Regel definiert die Anzahl von Host- und Gerätefehlern, die ein VM-Objekt über die zwei Sites hinweg tolerieren kann. Der Standardwert ist 1 und der Maximalwert ist 3.
- **Sekundäre Ebene von zu tolerierenden Fehlern** Definiert die Anzahl von Host- und Objektfehlern, die ein VM-Objekt innerhalb einer einzelnen Site tolerieren kann. Der Standardwert ist 0 und der Maximalwert ist 3.
- **Affinität**. Diese Regel ist nur dann verfügbar, wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist. Sie können die Affinitätsregel auf „Keine“, „Bevorzugt“ oder „Sekundär“ festlegen. Diese Regel ermöglicht es Ihnen, die VM-Objekte auf eine ausgewählte Site im ausgeweiteten Cluster zu begrenzen. Der Standardwert ist „Keine“.

---

**Hinweis** Wenn Sie für den ausgeweiteten Cluster die **Sekundäre Ebene von zu tolerierenden Fehlern** konfigurieren, gilt die Regel **Fault Tolerance-Methode** für die **Sekundäre Ebene von zu tolerierenden Fehlern**. Der Standardwert für die für **Primäre Ebene von zu tolerierenden Fehlern (PFTT)** verwendete Fehlertoleranzmethode ist RAID 1.

---

In einem ausgeweiteten Cluster mit lokalem Fehlerschutz kann der Cluster Reparaturen an fehlenden oder beschädigten Komponenten an der vorhandenen Site auch dann durchführen, wenn eine Site nicht verfügbar ist.

## Design-Überlegungen für ausgeweitete Cluster

Halten Sie sich beim Erstellen eines ausgeweiteten vSAN-Clusters an diese Richtlinien.

- Konfigurieren Sie DRS-Einstellungen für den ausgeweiteten Cluster.
  - DRS muss auf dem Cluster aktiviert sein. Wenn Sie DRS in den teilweise automatisierten Modus versetzen, können Sie steuern, welche VMs auf jede Site migriert werden.
  - Erstellen Sie zwei Hostgruppen, eine für die bevorzugte Site und eine für die sekundäre Site.
  - Erstellen Sie zwei VM-Gruppen, eine zum Aufnehmen der VMs auf der bevorzugten Site und eine zum Aufnehmen der VMs auf der sekundären Site.

- Erstellen Sie zwei Affinitätsregeln für VM-Hosts, die VMs zu Hostgruppen zuweisen, und geben Sie an, welche VMs und Hosts sich auf der bevorzugten Site befinden und welche VMs und Hosts sich auf der sekundären Site befinden.
- Konfigurieren Sie Affinitätsregeln für VM-Hosts, um die anfängliche Platzierung von VMs im Cluster durchzuführen.

- Konfigurieren Sie HA-Einstellungen für den ausgeweiteten Cluster.
  - HA muss auf dem Cluster aktiviert sein.
  - Einstellungen für HA-Regeln müssen Affinitätsregeln für VM-Hosts während des Failovers einhalten.
  - Deaktivieren Sie HA-Datenspeicher-Taktsignale.
- Für ausgeweitete Cluster ist das Festplattenformat 2.0 oder höher erforderlich. Führen Sie bei Bedarf ein Upgrade des Festplattenformats durch, bevor Sie einen ausgeweiteten Cluster konfigurieren. Siehe „Upgrade des vSAN-Festplattenformats mit dem vSphere Web Client“, auf Seite 104.
- Legen Sie die **Primäre Ebene von zu tolerierenden Fehlern** für ausgeweitete Cluster auf 1 fest.
- Ausgeweitete vSAN-Cluster unterstützen keine symmetrische Multiprozessor-Fault Tolerance (SMP-FT).
- Wenn ein Host getrennt wird oder nicht antwortet, können Sie den Zeugen-Host nicht hinzufügen oder entfernen. Mit dieser Einschränkung wird sichergestellt, dass vSAN genügend Informationen von allen Hosts sammelt, bevor Neukonfigurationsvorgänge durchgeführt werden.
- Die Verwendung von `esxcli` zum Hinzufügen oder Entfernen von Hosts wird für ausgeweitete Cluster nicht unterstützt.

## Best Practices für das Arbeiten mit ausgeweiteten Clustern

Halten Sie sich beim Arbeiten mit ausgeweiteten vSAN-Clustern an die folgenden Empfehlungen, um gute Leistungen zu erzielen.

- Wenn der Zugriff auf eine der Sites (Fault Domains) in einem ausgeweiteten Cluster nicht möglich ist, können neue VMs nach wie vor im Unter-Cluster bereitgestellt werden, in dem die anderen beiden Sites vorhanden sind. Die Bereitstellung dieser neuen VMs wird implizit erzwungen und die VMs sind erst wieder kompatibel, wenn die partitionierte Site dem Cluster wieder beitritt. Diese implizit erzwungene Bereitstellung wird nur durchgeführt, wenn zwei der drei Sites verfügbar sind. Eine Site verweist hier entweder auf eine Datensite oder auf einen Zeugen-Host.
- Wenn eine komplette Site wegen Stromausfall oder Verlust der Netzwerkverbindung in den Offline-Modus geschaltet wird, starten Sie die Site sofort ohne viel Verzögerung neu. Starten Sie nicht jeden vSAN-Host einzeln neu, sondern schalten Sie alle Hosts ungefähr gleichzeitig in den Online-Modus, idealerweise innerhalb von 10 Minuten. Mit diesem Verfahren können Sie die erneute Synchronisierung von großen Datenmengen über Sites hinweg vermeiden.
- Wenn ein Host permanent nicht verfügbar ist, entfernen Sie den Host aus dem Cluster, bevor Sie Neukonfigurationsaufgaben durchführen.
- Wenn Sie einen VM-Zeugen-Host zur Unterstützung mehrerer ausgeweiteter Cluster klonen möchten, konfigurieren Sie die VM vor dem Klonen nicht als Zeugen-Host. Stellen Sie zunächst die VM über die OVF-Datei bereit, klonen Sie die VM und konfigurieren Sie dann jeden Klon als einen Zeugen-Host für einen anderen Cluster. Über die OVF können Sie unbegrenzt viele VMs bereitstellen und jede als einen Zeugen-Host für einen anderen Cluster konfigurieren.

# Netzwerkplanung für ausgeweitete Cluster

Alle drei Sites in einem ausgeweiteten Cluster kommunizieren über das Verwaltungsnetzwerk und das vSAN-Netzwerk hinweg. Die VMs in beiden Datensites kommunizieren über ein gemeinsames Netzwerk von virtuellen Maschinen hinweg.

Ein ausgeweiteter vSAN-Cluster muss bestimmte grundsätzliche Netzwerkanforderungen erfüllen.

- Das Verwaltungsnetzwerk benötigt Konnektivität über alle drei Sites hinweg und verwendet dabei ein ausgeweitetes Layer 2-Netzwerk oder ein Layer 3-Netzwerk.
- Das vSAN-Netzwerk benötigt Konnektivität über alle drei Sites hinweg. VMware empfiehlt die Verwendung eines ausgeweiteten Layer 2-Netzwerks zwischen den beiden Datensites und ein Layer 3-Netzwerk zwischen den Datensites und dem Zeugenhost.
- Das VM-Netzwerk benötigt Konnektivität zwischen den Datensites, aber nicht mit dem Zeugenhost. VMware empfiehlt die Verwendung eines ausgeweiteten Layer 2-Netzwerks zwischen den Datensites. Bei einem Ausfall benötigen die VMs keine neue IP-Adresse, damit sie auf der ortsfernen Site eingesetzt werden können.
- Das vMotion-Netzwerk benötigt Konnektivität zwischen den Datensites, aber nicht mit dem Zeugenhost. VMware unterstützt die Verwendung eines ausgeweiteten Layer 2- oder eines Layer 3-Netzwerks zwischen Datensites.

## Verwenden von statischen Routen auf ESXi -Hosts

Falls Sie ein einzelnes Standard-Gateway auf ESXi-Hosts verwenden, beachten Sie, dass jeder ESXi-Host einen standardmäßigen TCP/IP-Stapel enthält, der über einen einzelnen Standard-Gateway verfügt. Die Standardroute ist typischerweise mit dem TCP/IP-Stapel des Verwaltungsnetzwerks verknüpft.

Das Verwaltungsnetzwerk und das vSAN-Netzwerk sind möglicherweise voneinander getrennt. Als Beispiel verwendet das Verwaltungsnetzwerk möglicherweise vmk0 auf der physischen Netzwerkkarte 0, während das vSAN-Netzwerk vmk2 auf der physischen Netzwerkkarte 1 verwendet (getrennte Netzwerkadapter für zwei unterschiedliche TCP/IP-Stapel). Diese Konfiguration setzt voraus, dass das vSAN-Netzwerk kein Standard-Gateway hat.

Betrachten Sie als Beispiel ein vSAN-Netzwerk, das über zwei Datensites auf einer Layer 2-Broadcast-Domäne verteilt ist (beispielsweise 172.10.0.0), und den Zeugenhost, der auf einer anderen Broadcast-Domäne sitzt (beispielsweise 172.30.0.0). Falls die VMkernel-Adapter auf einer Datensite versuchen, eine Verbindung zum vSAN-Netzwerk auf dem Zeugenhost herzustellen, schlägt die Verbindung fehl, da das Standard-Gateway auf dem ESXi-Host mit dem Verwaltungsnetzwerk verknüpft ist und es keine Route vom Verwaltungsnetzwerk zum vSAN-Netzwerk gibt.

Sie können statische Routen zur Behebung dieses Problems verwenden. Definieren Sie einen neuen Routeneintrag, der angibt, welchem Pfad gefolgt werden muss, um ein bestimmtes Netzwerk zu erreichen. Für ein vSAN-Netzwerk auf einem ausgeweiteten Cluster können Sie statische Routen hinzufügen, um eine ordnungsgemäße Kommunikation über alle Hosts hinweg sicherzustellen.

Beispielsweise können Sie eine statische Route zu den Hosts auf jeder Datensite hinzufügen, sodass Anfragen zum Erreichen des 172.30.0.0-Zeugennetzwerks über die 172.10.0.0-Schnittstelle geleitet werden. Fügen Sie auch eine statische Route zum Zeugenhost hinzu, sodass Anfragen zum Erreichen des 172.10.0.0-Netzwerks für die Datensites über die 172.30.0.0-Schnittstelle geleitet werden.

**Hinweis** Falls Sie statische Routen verwenden, müssen Sie sie für neue ESXi-Hosts, die zu einem der Sites hinzufügt wurden, manuell hinzufügen, bevor diese Hosts über den Cluster hinweg kommunizieren können. Falls Sie den Zeugenhost ersetzen, müssen Sie die Konfiguration für statische Routen aktualisieren.

Verwenden Sie den Befehl `esxcli network ip route`, um statische Routen hinzuzufügen.

# Konfigurieren eines ausgeweiteten vSAN -Clusters

Konfigurieren Sie ein vSAN-Cluster, der sich über zwei geografische Standorte erstreckt.

### Voraussetzungen

- Stellen Sie sicher, dass Sie mindestens über drei Hosts verfügen: einen für den bevorzugten Standort, einen für den sekundären Standort und einen Host, der als Zeugen-Host eingesetzt wird.
- Stellen Sie sicher, dass Sie einen Host als Zeugen-Host für den ausgeweiteten Cluster konfiguriert haben. Vergewissern Sie sich, dass der Zeugen-Host nicht Teil des vSAN-Clusters ist und dass er nur einen VMkernel-Adapter aufweist, der für vSAN-Datenverkehr konfiguriert ist.
- Stellen Sie sicher, dass der Zeugen-Host leer ist und keine Komponenten enthält. Um einen vorhandenen vSAN-Host als Zeugen-Host zu konfigurieren, evakuieren Sie zunächst alle Daten vom Host und löschen Sie die Datenträgergruppe.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.
4. Klicken Sie auf die Schaltfläche **Konfigurieren** des ausgeweiteten Clusters, um den Konfigurationsassistenten für den ausgeweiteten Cluster zu öffnen.
5. Wählen Sie die Fault Domain aus, die Sie dem sekundären Standort zuweisen möchten, und klicken Sie auf >>.

   Die Hosts, die unter der bevorzugten Fault Domain aufgelistet sind, befinden sich am bevorzugten Standort.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie einen Zeugen-Host aus, der nicht Mitglied eines ausgeweiteten vSAN-Clusters ist, und klicken Sie auf **Weiter**.
8. Beanspruchen Sie Speichergeräte auf dem Zeugenhost und klicken Sie auf **Weiter**.

   Beanspruchen Sie Speichergeräte auf dem Zeugenhost. Wählen Sie ein Flash-Gerät für die Cache-Schicht und ein oder mehrere Geräte für die Kapazitätsschicht aus.
9. Überprüfen Sie auf der Seite Bereit zum Abschließen die Konfiguration und klicken Sie auf **Beenden**.

# Ändern der bevorzugten Fault Domain

Sie können die sekundäre Site als bevorzugte Site konfigurieren. Die aktuelle bevorzugte Site wird zur sekundären Site.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.
4. Wählen Sie die sekundäre Fault Domain aus und klicken Sie auf das Symbol **Fault Domain als bevorzugt für ausgeweiteten Cluster markieren** (  ).

5 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Die ausgewählte Fault Domain ist als bevorzugte Fault Domain gekennzeichnet.

# Ändern des Zeugenhosts

Sie können den Zeugenhost für einen ausgeweiteten vSAN-Cluster ändern.

Ändern Sie den ESXi-Host, der als Zeugenhost für Ihren ausgeweiteten vSAN-Cluster verwendet wird.

### Voraussetzungen

Stellen Sie sicher, dass der Zeugen-Host nicht verwendet wird.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Klicken Sie auf die Schaltfläche **Zeugenhost ändern**.

5 Wählen Sie einen neuen Host aus, der als Zeugenhost verwendet werden soll, und klicken Sie auf **Weiter**.

6 Beanspruchen Sie Festplatten auf dem neuen Zeugenhost und klicken Sie auf **Weiter**.

7 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Konfiguration und klicken Sie auf **Beenden**.

# Bereitstellen einer vSAN -Zeugen-Appliance

Bestimmte vSAN-Konfigurationen, wie etwa ein ausgeweiteter Cluster, erfordern einen Zeugen-Host. Anstatt einen dedizierten physischen ESXi-Host als Zeugen-Host zu verwenden, können Sie die vSAN-Zeugen-Appliance bereitstellen. Die Appliance ist eine vorkonfigurierte virtuelle Maschine, auf der ESXi ausgeführt wird, und wird als OVA-Datei verteilt.

Im Gegensatz zu einem allgemeinen ESXi-Host führt die Zeugen-Appliance keine virtuellen Maschinen aus. Sie dient ausschließlich als vSAN-Zeuge.

Für den Workflow zum Bereitstellen und Konfigurieren der vSAN-Zeugen-Appliance gehen Sie wie folgt vor:

1 Laden Sie die Appliance von der VMware-Website herunter.

2 Stellen Sie die Appliance auf einem vSAN-Host oder -Cluster bereit. Weitere Informationen finden Sie unter „Bereitstellen von OVF-Vorlagen“ in der Dokumentation zur *vSphere-Administratorhandbuch für virtuelle Maschinen*.

3 Konfigurieren Sie das vSAN-Netzwerk auf der Zeugen-Appliance.

4 Konfigurieren Sie das Verwaltungsnetzwerk auf der Zeugen-Appliance.

5 Fügen Sie vCenter Server die Appliance als ESXi-Zeugen-Host hinzu. Stellen Sie sicher, dass Sie die vSAN-VMkernel-Schnittstelle auf dem Host konfigurieren.

## Einrichten des vSAN -Netzwerks auf der Zeugen-Appliance

Die vSAN-Zeugen-Appliance enthält zwei vorkonfigurierte Netzwerkadapter. Sie müssen die Konfiguration des zweiten Adapters ändern, sodass die Appliance eine Verbindung zum vSAN-Netzwerk herstellen kann.

### Vorgehensweise

1 Wechseln Sie im vSphere Web Client zur virtuellen Appliance, die den Zeugenhost enthält.

2 Klicken Sie mit der rechten Maustaste auf die Appliance und wählen Sie **Einstellungen bearbeiten** aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** den zweiten Netzwerkadapter.

4 Wählen Sie aus dem Dropdown-Menü die vSAN-Portgruppe aus und klicken Sie auf **OK**.

### Konfigurieren des Verwaltungsnetzwerks

Konfigurieren Sie die Zeugen-Appliance, sodass sie im Netzwerk erreichbar ist.

Standardmäßig kann die Appliance automatisch Netzwerkparameter abrufen, wenn Ihr Netzwerk einen DHCP-Server umfasst. Ist dies nicht der Fall, müssen Sie die Einstellungen in geeigneter Weise konfigurieren.

#### Vorgehensweise

1 Schalten Sie die Zeugen-Appliance ein und öffnen Sie ihre Konsole.

Da Ihre Appliance ein ESXi-Host ist, sehen Sie die Direct Console User Interface (DCUI).

2 Drücken Sie F2 und navigieren Sie zur Seite „Netzwerkadapter“.

3 Vergewissern Sie sich auf der Seite „Netzwerkadapter“, dass mindestens eine vmnic für den Transport ausgewählt ist.

4 Konfigurieren Sie die IPv4-Parameter für das Verwaltungsnetzwerk.

a Navigieren Sie zum Abschnitt „IPv4-Konfiguration“ und ändern Sie die standardmäßige DHCP-Einstellung in „statisch“.

b Geben Sie die folgenden Einstellungen ein:

- IP-Adresse
- Subnetzmaske
- Standard-Gateway

5 Konfigurieren Sie die DNS-Parameter.

- Primärer DNS-Server
- Alternativer DNS-Server
- Hostname

## Konfigurieren der Netzwerkschnittstelle für Zeugen-Datenverkehr

vSAN-Datenverkehr erfordert eine Verbindung mit niedriger Latenz und hoher Bandbreite. Für den Zeugen-Datenverkehr kann eine Verbindung mit hoher Latenz, geringer Bandbreite und eine routingfähige Verbindung verwendet werden. Zur Trennung des allgemeinen Datenverkehrs vom Zeugen-Datenverkehr können Sie einen dedizierten VMkernel-Netzwerkadapter für vSAN-Zeugen-Datenverkehr konfigurieren.

In unterstützten Konfigurationen mit ausgeweitetem Cluster kann der allgemeine Datenverkehr vom Zeugen-Datenverkehr getrennt werden. Der für den vSAN-Datenverkehr verwendete VMkernel-Adapter und der für den Zeugen-Datenverkehr verwendete VMkernel-Adapter müssen mit demselben physischen Switch verbunden sein.

Sie können Unterstützung für eine direkte netzwerkübergreifende Verbindung hinzufügen, um vSAN-Datenverkehr in einem ausgeweiteten vSAN-Cluster mit zwei Hosts zu übertragen. Sie können eine separate Netzwerkverbindung für Zeugen-Datenverkehr konfigurieren. Konfigurieren Sie auf jedem Datenhost im Cluster den VMkernel-Netzwerkadapter für die Verwaltung, um auch Zeugen-Datenverkehr zu übertragen. Konfigurieren Sie die Art des Zeugen-Datenverkehrs nicht auf dem Zeugen-Host.

### Voraussetzungen

- Vergewissern Sie sich, dass die Verbindung für den Datenverkehr von Daten-Site zu Zeuge mindestens eine Bandbreite von 100 MBit/s und eine Latenz von weniger als 200 ms RTT aufweist.
- Vergewissern Sie sich, dass der vSAN-Datenverkehr über eine direkte Ethernet-Kabelverbindung mit einer Geschwindigkeit von 10 GBit/s übertragen werden kann.
- Vergewissern Sie sich, dass der allgemeine Datenverkehr und der Zeugen-Datenverkehr dieselbe IP-Version verwenden.

### Vorgehensweise

1 Stellen Sie eine SSH-Verbindung mit dem ESXi-Host her.

2 Verwenden Sie den Befehl `esxcli network ip interface list` zum Ermitteln, welcher VMkernel-Netzwerkadapter für den Verwaltungsdatenverkehr verwendet wird.

Beispiel:

```
esxcli network  ip interface list
vmk0
   Name: vmk0
   MAC Address: e4:11:5b:11:8c:16
   Enabled: true
   Portset: vSwitch0
   Portgroup: Verwaltungsnetzwerk
   Netstack Instance: defaultTcpipStack
   VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1500
   TSO MSS: 65535
   Port ID: 33554437

vmk1
   Name: vmk1
   MAC Address: 00:50:56:6a:3a:74
   Enabled: true
   Portset: vSwitch1
   Portgroup: vsandata
   Netstack Instance: defaultTcpipStack
  VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 9000
   TSO MSS: 65535
   Port ID: 50331660
```

**Hinweis** Zum Zwecke der Abwärtskompatibilität sind Multicast-Informationen enthalten. vSAN 6.6 und höhere Versionen benötigen kein Multicast.

3 Verwenden Sie den Befehl `esxcli vsan network ip add` zum Konfigurieren des VMkernel-Netzwerkadapters für die Verwaltung so, dass er Zeugen-Datenverkehr unterstützt.

```
esxcli vsan network ip add –i vmkx –T=witness
```

4 Verwenden Sie den Befehl `esxcli vsan network list` zum Überprüfen der neuen Netzwerkkonfiguration.

Beispiel:

```
esxcli vsan network list
Interface
   VmkNic Name: vmk0
   IP Protocol: IP
   Interface UUID: 8cf3ec57–c9ea–148b–56e1–a0369f56dcc0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: Zeuge

Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: 6df3ec57–4fb6–5722–da3d–a0369f56dcc0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

Im vSphere Web Client ist die VMkernel-Netzwerkschnittstelle für die Verwaltung nicht für vSAN-Datenverkehr ausgewählt. Aktivieren Sie die Schnittstelle im vSphere Web Client nicht erneut.

# Konvertieren eines ausgeweiteten Clusters in einen standardmäßigen vSAN -Cluster

Sie können einen ausgeweiteten Cluster außer Betrieb nehmen und ihn in einen standardmäßigen vSAN-Cluster konvertieren.

Wenn Sie einen ausgeweiteten Cluster deaktivieren, wird der Zeugen-Host entfernt, aber die Fehlerdomänen-Konfiguration bleibt erhalten. Da der Zeugen-Host nicht verfügbar ist, fehlen alle Zeugen-Komponenten für Ihre virtuellen Maschinen. Um eine uneingeschränkte Verfügbarkeit für Ihre VMs sicherzustellen, reparieren Sie die Clusterobjekte umgehend.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum ausgeweiteten vSAN-Cluster.

2 Deaktivieren Sie den ausgeweiteten Cluster.

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

   b Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

   c Klicken Sie auf die Schaltfläche **Konfigurieren** für den ausgeweiteten Cluster.

   Der Konfigurationsassistent für den ausgeweiteten Cluster wird angezeigt.

   d Klicken Sie auf **Deaktivieren** und dann zum Bestätigen auf **Ja**.

3 Entfernen Sie die Fehlerdomänen-Konfiguration.

   a Wählen Sie eine Fehlerdomäne aus und klicken Sie auf das Symbol **Ausgewählte Fehlerdomänen entfernen** (✖). Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

   b Wählen Sie die andere Fehlerdomäne aus und klicken Sie auf das Symbol **Ausgewählte Fehlerdomänen entfernen** (✖). Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

4 Reparieren Sie die Objekte im Cluster.

   a Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.

   b Klicken Sie unter „vSAN“ auf **Integrität** und dann auf **vSAN-Objektintegrität**.

   c Klicken Sie auf **Objekt sofort reparieren**.

   vSAN erstellt die Zeugenkomponenten innerhalb des Clusters neu.

# Erhöhen der Speichereffizienz in einem vSAN -Cluster

7

Mit den Speichereffizienztechniken können Sie den Speicherplatz zum Speichern von Daten verringern. Diese Techniken reduzieren den zum Erfüllen Ihrer Anforderungen benötigten Gesamtspeicherplatz.

Dieses Kapitel behandelt die folgenden Themen:



## Einführung in die vSAN -Speicherplatzeffizienz

Mit den Speichereffizienztechniken können Sie den Speicherplatz zum Speichern von Daten verringern. Diese Techniken reduzieren die zum Erfüllen Ihrer Anforderungen benötigte Gesamtspeicherkapazität.

Sie können Deduplizierung und Komprimierung auf einem vSAN-Cluster aktivieren, um doppelt vorhandene Daten zu vermeiden und den zum Speichern der Daten erforderlichen Speicherplatz zu verringern.

Sie können das Richtlinienattribut **Fehlertoleranzmethode** auf VMs zur Verwendung von RAID 5- oder RAID 6-Erasure Coding festlegen. Mit Erasure Coding können Sie Ihre Daten schützen und im Vergleich zur standardmäßigen RAID 1-Spiegelung weniger Speicherplatz verwenden.

Sie können Deduplizierung und Komprimierung sowie RAID 5- oder RAID 6-Erasure Coding verwenden, um noch mehr Speicherplatz zu gewinnen. RAID 5 und RAID 6 bieten gegenüber RAID 1 klar definierte Speicherplatzeinsparungen. Mit Deduplizierung und Komprimierung sind weitere Einsparungen möglich.

## Verwenden von Deduplizierung und Komprimierung

vSAN kann Deduplizierung und Komprimierung auf Blockebene durchführen, um Speicherplatz zu sparen. Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-All-Flash-Cluster aktivieren, werden redundante Daten innerhalb jeder Festplattengruppe reduziert.

Bei der Deduplizierung werden redundante Datenblöcke entfernt, wohingegen bei der Komprimierung zusätzliche redundante in allen Datenblöcken entfernt werden. Diese Techniken arbeiten zusammen, um den zum Speichern der Daten erforderlichen Speicherplatz zu reduzieren. vSAN wendet Deduplizierung und Komprimierung beim Verschieben von Daten aus der Cache-Schicht in die Kapazitätsschicht an.

Sie können Deduplizierung und Komprimierung als clusterweite Einstellung aktivieren, die Anwendung findet jedoch auf einer Festplattengruppenbasis statt. Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-Cluster aktivieren, werden redundante Daten innerhalb jeder Festplattengruppe auf eine einzelne Kopie reduziert.

Sie können Deduplizierung und Komprimierung beim Erstellen eines neuen vSAN-All-Flash-Clusters oder beim Bearbeiten eines vorhandenen vSAN-All-Flash-Clusters aktivieren. Weitere Informationen zum Erstellen und Bearbeiten eines vSAN-Clusters finden Sie unter „Aktivieren von vSAN“, auf Seite 49.

Wenn Sie Deduplizierung und Komprimierung aktivieren oder deaktivieren, führt vSAN eine rollende Neuformatierung aller Festplattengruppen auf jedem Host durch. Je nach den im vSAN-Datenspeicher gespeicherten Daten kann dieser Vorgang sehr lange dauern. Es wird empfohlen, diesen Vorgang nicht häufig durchzuführen. Wenn Sie Deduplizierung und Komprimierung deaktivieren möchten, müssen Sie zunächst sicherstellen, dass genügend physische Speicherkapazität für Ihre Daten vorhanden ist.

**Hinweis** Die Deduplizierung und Komprimierung haben möglicherweise keinen Einfluss auf verschlüsselte VMs, da die VM-Verschlüsselung Daten auf dem Host verschlüsselt, bevor sie in den Speicher geschrieben werden. Nehmen Sie Speichereinbußen in Kauf, wenn VM-Verschlüsselung verwendet wird.

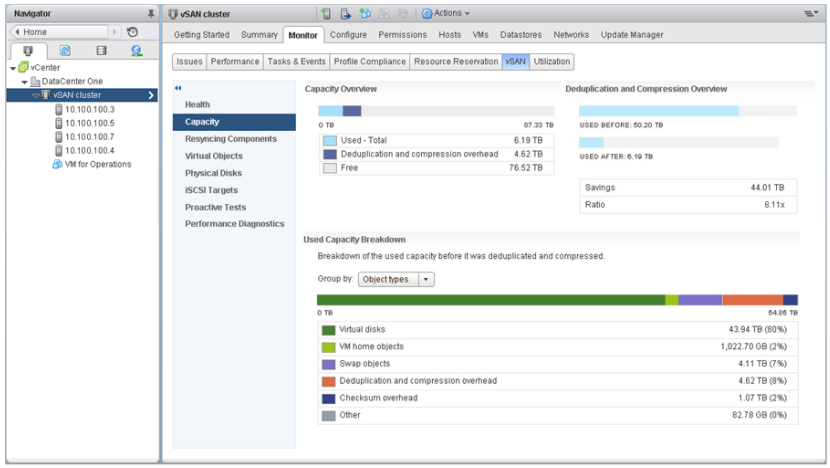
## Verwalten von Festplatten in einem Cluster mit Deduplizierung und Komprimierung

Beachten Sie beim Verwalten von Festplatten in einem Cluster mit aktivierter Deduplizierung und Komprimierung die folgenden Richtlinien.

- Fügen Sie einer Festplattengruppe keine Festplatten hinzu. Um die Deduplizierung und Komprimierung effizienter zu gestalten, fügen Sie eine neue Festplatte hinzu, um die Speicherkapazität des Clusters zu erhöhen.
- Wenn Sie eine neue Festplattengruppe manuell hinzufügen, fügen Sie alle Kapazitätsfestplatten gleichzeitig hinzu.
- Sie können eine einzelne Festplatte nicht aus einer Festplattengruppe entfernen. Sie müssen die gesamte Festplattengruppe entfernen, um Änderungen vorzunehmen.
- Der Ausfall einer einzelnen Festplatte führt dazu, dass die gesamte Festplattengruppe ausfällt.

## Überprüfen der Speichereinsparungen aus Deduplizierung und Komprimierung

Die Reduzierung des Speichers aufgrund von Deduplizierung und Komprimierung hängt von vielen Faktoren ab, wie zum Beispiel vom Typ der gespeicherten Daten und der Anzahl der doppelten Blöcke. Größere Festplattengruppen neigen dazu, ein höheres Deduplizierungsverhältnis bereitzustellen. Sie können die Ergebnisse von Deduplizierung und Komprimierung überprüfen, indem Sie die Übersicht für Deduplizierung und Komprimierung in der vSAN-Kapazitätsüberwachung anzeigen.



Sie können die Übersicht für Deduplizierung und Komprimierung anzeigen, wenn Sie die vSAN-Kapazität im vSphere Web Client überwachen. Es werden Informationen zu den Ergebnissen der Deduplizierung und Komprimierung angezeigt. Die Speicherplatzangabe „Verwendung vorher“ zeigt den vor der Anwendung der Deduplizierung und Komprimierung erforderlichen logischen Speicherplatz an, wohingegen die Speicherplatzangabe „Verwendung nachher“ den nach der Anwendung der Deduplizierung und Komprimierung verwendeten physischen Speicherplatz anzeigt. Die Speicherplatzangabe „Verwendung nachher“ zeigt ebenfalls eine Übersicht über den eingesparten Speicherplatz sowie das Verhältnis von Deduplizierung und Komprimierung an.

Das Verhältnis von Deduplizierung und Komprimierung basiert auf dem Verhältnis von logischem („Verwendung vorher“) Speicherplatz, der zum Speichern der Daten vor der Anwendung von Deduplizierung und Komprimierung erforderliche ist, und dem physischen („Verwendung nachher“) Speicherplatz nach der Anwendung von Deduplizierung und Komprimierung. Das Verhältnis wird wie folgt berechnet: Speicherplatz „Verwendung vorher“ geteilt durch den Speicherplatz „Verwendung nachher“. Wenn beispielsweise der Speicherplatz „Verwendung vorher“ 3 GB beträgt, der physische Speicherplatz „Verwendung nachher“ aber nur 1 GB aufweist, ist das Verhältnis von Deduplizierung und Komprimierung 3x.

Bei Aktivierung von Deduplizierung und Komprimierung auf dem vSAN-Cluster kann es einige Minuten dauern, bis Aktualisierungen der Kapazität in der Kapazitätsüberwachung angezeigt werden, da Festplattenspeicher in Anspruch genommen und neu zugeteilt wird.

## Design-Überlegungen für Deduplizierung und Komprimierung

Beachten Sie bei der Konfiguration von Deduplizierung und Komprimierung in einem vSAN-Cluster die folgenden Richtlinien.

- Deduplizierung und Komprimierung sind nur auf All-Flash-Festplattengruppen verfügbar.
- Festplattenformat Version 3.0 oder höher ist für die Unterstützung von Deduplizierung und Komprimierung erforderlich.
- Sie müssen über eine gültige Lizenz verfügen, um Deduplizierung und Komprimierung auf einem Cluster zu aktivieren.
- Sie können Deduplizierung und Komprimierung nur aktivieren, wenn die Methode zur Beanspruchung von Speicher auf den manuellen Modus eingestellt ist. Nach der Aktivierung von Deduplizierung und Komprimierung können Sie die Methode zur Beanspruchung von Speicher auf den automatischen Modus einstellen.
- Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-Cluster aktivieren, sind alle Festplattengruppen über die Deduplizierung und Komprimierung von der Reduzierung von Daten betroffen.
- vSAN kann doppelte Datenblöcke innerhalb jeder einzelnen Festplattengruppe entfernen, aber nicht über Festplattengruppen hinweg.
- Der Kapazitäts-Overhead für Deduplizierung und Komprimierung beträgt ungefähr fünf Prozent der gesamten Rohkapazität.
- Richtlinien müssen entweder 0 % oder 100 % reservierten Objektspeicherplatz aufweisen. Richtlinien mit 100 % reserviertem Objektspeicherplatz werden immer berücksichtigt. Dies kann jedoch dazu führen, dass Deduplizierung und Komprimierung weniger effizient sind.

## Aktivieren von Deduplizierung und Komprimierung auf einem neuen vSAN -Cluster

Sie können die Deduplizierung und Komprimierung aktivieren, wenn Sie einen neuen vSAN-All-Flash-Cluster konfigurieren.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu einem vorhandenen Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein** aus und klicken Sie auf die Schaltfläche **vSAN konfigurieren**.

4 Konfigurieren Sie die Deduplizierung und Komprimierung auf dem Cluster.

   a Aktivieren Sie auf der Seite **vSAN-Funktionen** das Kontrollkästchen **Aktivieren** unter „Deduplizierung und Komprimierung“.

   b (Optional) Aktivieren Sie verringerte Redundanz für Ihre VMs.

   Siehe „Reduzieren der VM-Redundanz für vSAN-Cluster“, auf Seite 79.

5 Geben Sie auf der Seite **Festplatten beanspruchen** an, welche Festplatten für den vSAN-Cluster beansprucht werden sollen.

   a Wählen Sie ein Flash-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf das Symbol **Für Kapazitätsschicht beanspruchen** (  ).

   b Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf das Symbol **Für Cache-Schicht beanspruchen** (  ).

6 Schließen Sie die Clusterkonfiguration ab.

## Aktivieren von Deduplizierung und Komprimierung auf einem vorhandenen vSAN -Cluster

Sie können Deduplizierung und Komprimierung aktivieren, indem Sie Konfigurationsparameter auf einem vorhandenen vSAN-Cluster bearbeiten.

### Voraussetzungen

Erstellen Sie einen vSAN-Cluster.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSAN-Host-Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein** aus.

4 Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**.

5 Konfigurieren Sie die Deduplizierung und Komprimierung.

   a Legen Sie die Deduplizierung und Komprimierung auf **Aktiviert** fest.

   b (Optional) Aktivieren Sie verringerte Redundanz für Ihre VMs.

   Siehe „Reduzieren der VM-Redundanz für vSAN-Cluster“, auf Seite 79.

   c Klicken Sie auf **OK**, um Ihre Konfigurationsänderungen zu speichern.

Während des Aktivierens der Deduplizierung und Komprimierung ändert sich das Festplattenformat für vSAN in jeder Festplattengruppe des Clusters. Zur Ausführung dieser Änderung evakuiert vSAN die Daten aus der Festplattengruppe, entfernt die Festplattengruppe und erstellt sie mit einem neuen Format, das Deduplizierung und Komprimierung unterstützt, neu.

Der Aktivierungsvorgang erfordert kein Migrieren von virtuellen Maschinen und keinen DRS. Die für diesen Vorgang erforderliche Zeit hängt von der Anzahl von Hosts im Cluster und der Datenmenge ab. Sie können den Fortschritt auf der Registerkarte **Aufgaben und Ereignisse** überwachen.

## Deaktivieren von Deduplizierung und Komprimierung

Sie können Deduplizierung und Komprimierung auf Ihrem vSAN-Cluster deaktivieren.

Wenn Deduplizierung und Komprimierung auf dem vSAN-Cluster deaktiviert werden, kann sich die verwendete Kapazität im Cluster (je nach Deduplizierungsverhältnis) vergrößern. Vergewissern Sie sich vor dem Deaktivieren der Deduplizierung und Komprimierung, dass der Cluster genügend Kapazität zum Verarbeiten der Größe der erweiterten Daten aufweist.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSAN-Host-Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein**.

4 Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**.

5 Deaktivieren Sie die Deduplizierung und Komprimierung.

   a Legen Sie den Modus für das Beanspruchen von Festplatten auf **Manuell** fest.

   b Legen Sie die Deduplizierung und Komprimierung auf **Deaktiviert** fest.

   c Klicken Sie auf **OK**, um Ihre Konfigurationsänderungen zu speichern.

Während des Deaktivierens der Deduplizierung und Komprimierung ändert sich das Festplattenformat für vSAN in jeder Festplattengruppe des Clusters. vSAN evakuiert die Daten aus der Festplattengruppe, entfernt die Festplattengruppe und erstellt sie mit einem Format, das Deduplizierung und Komprimierung nicht unterstützt, neu.

Die für diesen Vorgang erforderliche Zeit hängt von der Anzahl von Hosts im Cluster und der Datenmenge ab. Sie können den Fortschritt auf der Registerkarte **Aufgaben und Ereignisse** überwachen.

## Reduzieren der VM-Redundanz für vSAN -Cluster

Wenn Sie Deduplizierung und Komprimierung aktivieren, müssen Sie in bestimmten Fällen möglicherweise die Schutzebene für Ihre virtuellen Maschinen verringern.

Für die Aktivierung der Deduplizierung und Komprimierung ist ein Formatwechsel für Festplattengruppen notwendig. Zur Ausführung dieser Änderung evakuiert vSAN die Daten aus der Festplattengruppe, entfernt die Festplattengruppe und erstellt sie mit einem neuen Format, das Deduplizierung und Komprimierung unterstützt, neu.

In bestimmten Umgebungen verfügt Ihr vSAN-Cluster möglicherweise nicht über genügend Ressourcen, um die Festplattengruppe vollständig zu evakuieren. Zu den Beispielen für solche Bereitstellungen gehört ein Cluster mit 3 Knoten ohne Ressourcen zur Evakuierung des Replikats oder Zeugen bei gleichzeitiger Beibehaltung des vollständigen Schutzes oder ein Cluster mit vier Knoten mit bereits bereitgestellten RAID-5-Objekten. Im letzteren Fall steht kein Platz zur Verfügung, um einen Teil des RAID-5-Stripes zu verschieben, da RAID-5-Objekte mindestens vier Knoten benötigen.

Sie können nach wie vor die Deduplizierung und Komprimierung aktivieren und die Option „Verringerte Redundanz zulassen“ verwenden. Mit dieser Option werden die VMs weiter ausgeführt, diese können aber möglicherweise nicht die volle Anzahl an Fehlern tolerieren, die in der VM-Speicherrichtlinie festgelegt ist. Als Folge sind Ihre virtuellen Maschinen vorübergehend während des Formatwechsels für die Deduplizierung und Komprimierung möglicherweise dem Risiko von Datenverlust ausgesetzt. vSAN stellt die vollständige Übereinstimmung und Redundanz nach Abschluss der Formatkonvertierung wieder her.

### Hinzufügen oder Entfernen von Festplatten mit aktivierter Deduplizierung und Komprimierung

Wenn Sie einem vSAN-Cluster mit aktivierter Deduplizierung und Komprimierung Festplatten hinzufügen, sind bestimmte Aspekte zu beachten.

- Sie können einer Festplattengruppe mit aktivierter Deduplizierung und Komprimierung eine Kapazitätsfestplatte hinzufügen. Um die Deduplizierung und Komprimierung jedoch effizienter zu gestalten, erstellen Sie zur Erhöhung der Speicherkapazität des Clusters eine neue Festplattengruppe, anstatt Kapazitätsfestplatten hinzuzufügen.
- Wenn Sie eine Festplatte aus einer Cache-Schicht entfernen, wird die gesamte Festplattengruppe entfernt. Das Entfernen einer Festplatte auf der Cache-Schicht bei aktivierter Deduplizierung und Komprimierung löst eine Evakuierung der Daten aus.
- Deduplizierung und Komprimierung sind auf der Ebene der Festplattengruppe implementiert. Sie können eine Kapazitätsfestplatte nicht aus einem Cluster mit aktivierter Deduplizierung und Komprimierung entfernen. Sie müssen die gesamte Festplattengruppe entfernen.
- Wenn eine Kapazitätsfestplatte ausfällt, ist die gesamte Festplattengruppe nicht mehr verfügbar. Beheben Sie dieses Problem, indem Sie die fehlerhafte Komponente sofort identifizieren und ersetzen. Verwenden Sie beim Entfernen der fehlerhaften Festplattengruppe die Option „Keine Datenmigration“.

## Verwenden von RAID 5- oder RAID 6-Erasure Coding

Sie können RAID 5- oder RAID 6-Erasure Coding für den Schutz vor Datenverlust und zum Erhöhen der Speichereffizienz verwenden. Mit Erasure Coding kann derselbe Datenschutz wie bei der Spiegelung (RAID 1) erzielt werden, es wird jedoch weniger Speicherkapazität benötigt.

Mit RAID 5- oder RAID 6-Erasure Coding kann vSAN einen Ausfall von bis zu zwei Kapazitätsgeräten im Datenspeicher tolerieren. Sie können RAID 5 auf All-Flash-Clustern mit mindestens vier Fault Domains konfigurieren. Sie können RAID 5 oder RAID 6 auf All-Flash-Clustern mit mindestens sechs Fault Domains konfigurieren.

Im Vergleich zur RAID-1-Spiegelung benötigt RAID 5- oder RAID 6-Erasure Coding weniger zusätzliche Speicherkapazität für den Schutz Ihrer Daten. Beispiel: Eine VM mit RAID 1, die durch die Festlegung der Option **Primäre Ebene von zu tolerierenden Fehlern** auf 1 geschützt ist, benötigt die zweifache virtuelle Festplattengröße. Mit RAID 5 hingegen ist nur eine 1,33-fache Größe erforderlich. Die folgende Tabelle zeigt einen allgemeinen Vergleich zwischen RAID 1 und RAID 5 oder RAID 6.

**Tabelle 7-1.** Zum Speichern und Schützen von Daten auf verschiedenen RAID-Ebenen erforderliche Kapazität

| RAID-Konfiguration | Primäre Ebene von zu tolerierenden Fehlern | Datengröße | Benötigte Kapazität |
|---|---|---|---|
| RAID 1 (Spiegelung) | 1 | 100 GB | 200 GB |
| RAID 5 oder RAID 6 (Erasure Coding) mit vier Fault Domains | 1 | 100 GB | 133 GB |
| RAID 1 (Spiegelung) | 2 | 100 GB | 300 GB |
| RAID 5 oder RAID 6 (Erasure Coding) mit sechs Fault Domains | 2 | 100 GB | 150 GB |

RAID 5- oder RAID 6-Erasure Coding ist ein Richtlinienattribut, dass Sie auf VM-Komponenten anwenden können. Um RAID 5 zu verwenden, legen Sie **Fehlertoleranzmethode** auf **RAID-5/6 (Erasure Coding) - Kapazität** und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 fest. Um RAID 6 zu verwenden, legen Sie die **Fehlertoleranzmethode** auf **RAID-5/6 (Erasure Coding) - Kapazität** und **Primäre Ebene von zu tolerierenden Fehlern** auf 2 fest. RAID 5- oder RAID 6-Erasure Coding unterstützt nicht den Wert 3 für **Primäre Ebene von zu tolerierenden Fehlern**.

Um RAID 1 zu verwenden, legen Sie die **Fehlertoleranzmethode** auf **RAID-1 (Spiegelung) - Leistung** fest. RAID 1-Spiegelung benötigt weniger E/A-Vorgänge zu den Speichergeräten und kann daher bessere Leistung bieten. Beispielsweise kann die Neusynchronisierung eines Clusters mit RAID 1 schneller abgeschlossen werden.

Weitere Informationen zum Konfigurieren von Richtlinien finden Sie unter Kapitel 12, „Verwenden von vSAN-Speicherrichtlinien“, auf Seite 137.

## Design-Überlegungen für RAID 5 oder RAID 6

Beachten Sie bei der Konfiguration von RAID 5 oder RAID 6 Erasure Coding in einem vSAN-Cluster die folgenden Richtlinien.

- RAID 5 oder RAID 6 Erasure Coding ist nur für All-Flash-Festplattengruppen verfügbar.
- Festplattenformat Version 3.0 oder höher ist für die Unterstützung von RAID 5 oder RAID 6 erforderlich.
- Sie müssen über eine gültige Lizenz verfügen, um RAID 5/6 auf einem Cluster zu aktivieren.
- RAID 5/6 wird auf ausgeweiteten Clustern nicht unterstützt.
- Sie können weitere Speichereinsparungen vornehmen, wenn Sie Deduplizierung und Komprimierung auf dem vSAN-Cluster aktivieren.

# Verwenden der Verschlüsselung auf einem vSAN -Cluster

8

Sie können zum Schutz der Daten in Ihrem vSAN-Cluster die Verschlüsselung für nicht verwendete Daten verwenden.

vSAN kann die Verschlüsselung von nicht verwendeten Daten durchführen. Die Daten werden verschlüsselt, nachdem alle anderen Verarbeitungsvorgänge, z. B. die Deduplizierung, durchgeführt wurden. Die Verschlüsselung für nicht verwendete Daten schützt die Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.

Die Verwendung der Verschlüsselung auf Ihrem vSAN-Cluster erfordert einige Vorbereitung. Nachdem Ihre Umgebung eingerichtet wurde, können Sie die Verschlüsselung auf Ihrem vSAN-Cluster aktivieren.

Für die vSAN-Verschlüsselung werden ein externer Schlüsselmanagementserver (KMS), das vCenter Server-System und Ihre ESXi-Hosts benötigt. vCenter Server fordert Verschlüsselungsschlüssel von einem externen KMS an. Der KMS generiert und speichert die Schlüssel und vCenter Server erhält die Schlüssel-IDs vom KMS und verteilt sie auf den ESXi-Hosts.

Der vCenter Server speichert keine KMS-Schlüssel, sondern nur eine Liste mit Schlüssel-IDs.

Dieses Kapitel behandelt die folgenden Themen:



## Funktionsweise der vSAN -Verschlüsselung

Wenn Sie die Verschlüsselung aktivieren, verschlüsselt vSAN alles, was sich im vSAN-Datenspeicher befindet. Alle Dateien werden verschlüsselt, sodass alle virtuellen Maschinen und ihre entsprechenden Daten geschützt sind. Nur Administratoren mit Berechtigungen zum Verschlüsseln können Verschlüsselungs- und Entschlüsselungsaufgaben durchführen.

vSAN verwendet Verschlüsselungsschlüssel wie folgt:

- vCenter Server fordert einen AES-256-KEK vom KMS an. vCenter Server speichert nur die ID des KEK, nicht jedoch den Schlüssel selbst.

- Der ESXi-Host verschlüsselt die Festplattendaten im branchenüblichen AES-256-XTS-Modus. Jede Festplatte verfügt über einen anderen zufällig erzeugten Datenverschlüsselungsschlüssel (Data Encryption Key, DEK).
- Jeder ESXi-Host verwendet den KEK, um seine DEKs zu verschlüsseln, und speichert die verschlüsselten DEKs auf Festplatte. Der Host speichert den KEK nicht auf der Festplatte. Wenn ein Host neu gestartet wird, fordert er vom KMS den KEK mit der entsprechenden ID an. Der Host kann dann seine DEKs nach Bedarf entschlüsseln.
- Ein Hostschlüssel wird zum Verschlüsseln von Core-Dumps, nicht von Daten, verwendet. Alle Hosts im selben Cluster verwenden denselben Hostschlüssel. Beim Erfassen von Support-Paketen wird zur Neuverschlüsselung der Core-Dumps ein Zufallsschlüssel erzeugt. Verwenden Sie ein Kennwort, wenn Sie den Zufallsschlüssel verschlüsseln.

Wenn ein Host neu gestartet wird, werden dessen Festplattengruppen erst dann gemountet, wenn er den KEK erhalten hat. Dieser Vorgang kann einige Minuten oder länger dauern. Sie können im vSAN-Integritätsdienst unter **Physische Festplatten > Softwarezustand-Integrität** den Status der Festplattengruppen überwachen.

## Design-Überlegungen für vSAN -Verschlüsselung

Halten Sie sich beim Arbeiten mit der vSAN-Verschlüsselung an diese Richtlinien.

- Stellen Sie Ihren KMS-Server nicht im selben vSAN-Datenspeicher bereit, den Sie verschlüsseln möchten.
- Die Verschlüsselung ist CPU-intensiv. Mit AES-NI wird die Verschlüsselungsleistung deutlich gesteigert. Aktivieren Sie AES-NI im BIOS.
- Der Zeugenhost in einem ausgeweiteten Cluster ist nicht Teil der vSAN-Verschlüsselung. Auf dem Zeugenhost befinden sich lediglich Metadaten.
- Erstellen Sie eine Richtlinie bezüglich Core-Dumps. Core-Dumps sind verschlüsselt, da sie vertrauliche Informationen wie etwa Schlüssel enthalten können. Gehen Sie sorgfältig mit den vertraulichen Daten um, wenn Sie einen Core-Dump entschlüsseln. ESXi-Core-Dumps können Schlüssel für den ESXi-Host und die sich darauf befindlichen Daten enthalten.
  - Verwenden Sie immer ein Kennwort, wenn Sie ein `vm-support`-Paket erfassen. Sie können das Kennwort angeben, wenn Sie das Support-Paket vom vSphere Web Client generieren oder den `vm-support`-Befehl verwenden.

    Das Kennwort verschlüsselt Core-Dumps erneut, die interne Schlüssel zur Verwendung von auf diesem Kennwort basierenden Schlüsseln verwenden. Sie können das Kennwort zu einem späteren Zeitpunkt zum Entschlüsseln und Verschlüsseln von Core-Dumps verwenden, die möglicherweise im Support-Paket enthalten sind. Nicht verschlüsselte Core-Dumps oder Protokolle sind davon nicht betroffen.
  - Das von Ihnen während der `vm-support`-Paketerstellung angegebene Kennwort wird in vSphere-Komponenten nicht dauerhaft gespeichert. Sie müssen Ihre Kennwörter für Support-Pakete selbst speichern bzw. diese notieren.

## Festlegen des KMS-Clusters

Ein Schlüsselmanagementserver-Cluster (KMS-Cluster) stellt die Schlüssel bereit, die Sie zum Verschlüsseln des vSAN-Datenspeichers verwenden können.

Bevor Sie den vSAN-Datenspeicher verschlüsseln können, müssen Sie einen KMS-Cluster so einrichten, dass er die Verschlüsselung unterstützt. Die Aufgabe umfasst das Hinzufügen des Schlüsselmanagementservers (KMS) zu vCenter Server und das Herstellen des Vertrauens mit dem KMS. vCenter Server stellt Verschlüsselungsschlüssel vom KMS-Cluster bereit.

Der KMS muss den Key Management Interoperability Protocol (KMIP) 1.1-Standard unterstützen.

## Hinzufügen eines KMS zu vCenter Server

Sie fügen Ihrem vCenter Server-System vom vSphere Web Client aus einen Schlüsselmanagementserver (Key Management Server, KMS) hinzu.

vCenter Server erstellt einen KMS-Cluster, wenn Sie die erste KMS-Instanz hinzufügen. stellen Sie sicher, dass Sie denselben KMS-Clusternamen verwenden, wenn Sie den KMS-Cluster auf zwei oder mehreren vCenter Servern konfigurieren.

**Hinweis** Stellen Sie Ihre KMS-Server nicht auf dem vSAN-Cluster bereit, den Sie verschlüsseln möchten. Wenn es zu einem Ausfall kommt, müssen die Hosts im vSAN-Cluster mit dem KMS kommunizieren.

- Wenn Sie den KMS hinzufügen, werden Sie aufgefordert, diesen Cluster als Standard festzulegen. Sie können später den Standard-Cluster explizit ändern.
- Nachdem vCenter Server den ersten Cluster erstellt hat, können Sie KMS-Instanzen des gleichen Anbieters dem Cluster hinzufügen.
- Sie können den Cluster mit nur einer KMS-Instanz einrichten.
- Wenn Ihre Umgebung KMS-Lösungen anderer Anbieter unterstützt, können Sie mehrere KMS-Cluster hinzufügen.

### Voraussetzungen

- Stellen Sie sicher, dass der Schlüsselserver in *vSphere-Kompatibilitätstabellen* und KMIP 1.1-kompatibel ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen: **Cryptographer.ManageKeyServers**
- Das Herstellen einer Verbindung zu einem KMS mit lediglich einer IPv6-Adresse wird nicht unterstützt.
- Das Verbinden mit einem KMS über einen Proxy-Server, der Benutzername und Kennwort benötigt, wird nicht unterstützt.

### Vorgehensweise

1 Melden Sie sich beim vCenter Server-System mit vSphere Web Client an.

2 Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.

3 Klicken Sie auf **Konfigurieren** und dann auf **Schlüsselmanagementserver**.

4 Klicken Sie auf **KMS hinzufügen**, geben Sie im Assistenten die KMS-Informationen an und klicken Sie auf **OK**.

| Option | Wert |
|---|---|
| **KMS-Cluster** | Wählen Sie **Neuen Cluster erstellen**, wenn Sie einen neuen Cluster erstellen möchten. Wenn ein Cluster vorhanden ist, können Sie diesen Cluster auswählen. |
| **Clustername** | Name des KMS-Clusters. Sie können diesen Namen für die Verbindung zum KMS verwenden, wenn Ihre vCenter Server-Instanz ausfällt. |
| **Serveralias** | Alias für den KMS. Sie können diesen Alias für die Verbindung zum KMS verwenden, wenn Ihre vCenter Server-Instanz ausfällt. |
| **Serveradresse** | IP-Adresse oder FQDN des KMS. |
| **Server-Port** | Port, an dem vCenter Server eine Verbindung zum KMS herstellt. |
| **Proxy-Adresse** | Optionale Proxy-Adresse für die Verbindung zum KMS. |
| **Proxy-Port** | Optionaler Proxyport für die Verbindung zum KMS. |

| Option | Wert |
|---|---|
| **Benutzername** | Einige KMS-Anbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann einen Benutzernamen an, wenn Ihr KMS diese Funktion unterstützt und Sie beabsichtigen, sie zu verwenden. |
| **Kennwort** | Einige KMS-Anbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann ein Kennwort an, wenn Ihr KMS diese Funktion unterstützt und Sie beabsichtigen, sie zu verwenden. |

## Herstellen einer vertrauenswürdigen Verbindung durch den Austausch von Zertifikaten

Nach dem Hinzufügen des KMS zum vCenter Server-System können Sie eine vertrauenswürdige Verbindung herstellen. Der spezifische Prozess hängt von den Zertifikaten ab, die der KMS akzeptiert, und von der Unternehmensrichtlinie.

### Voraussetzungen

Fügen Sie den KMS-Cluster hinzu.

### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Klicken Sie auf **vertrauenswürdige Verbindung mit KMS einrichten**.

5 Wählen Sie die entsprechenden Option für den Server aus und durchlaufen Sie die Schritte.

| Option | Informationen hierzu unter |
|---|---|
| **CA-Root-Zertifikat** | „Verwenden der Root-CA-Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung“, auf Seite 86. |
| **Zertifikat** | „Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung“, auf Seite 87. |
| **Neue Zertifikatssignieranforderung** | „Verwenden der Option „Neue Zertifikatsignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung“, auf Seite 88. |
| **Zertifikat und privaten Schlüssel hochladen** | „Verwenden der Option zum Hochladen des Zertifikats und des privaten Schlüssels, um eine vertrauenswürdige Verbindung herzustellen“, auf Seite 88. |

### Verwenden der Root-CA-Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter wie z. B. SafeNet verlangen, dass Sie Ihr Root-CA-Zertifikat auf den KMS hochladen. Alle von Ihrer Root-Zertifizierungsstelle signierten Zertifikate werden dann von diesem KMS als vertrauensvoll angesehen.

Das von der vSphere VM-Verschlüsselung verwendete Root-CA-Zertifikat ist ein selbst signiertes Zertifikat, das in einem separaten Speicher im VECS (VMware Endpoint Certificate Store) auf dem vCenter Server-System gespeichert wird.

**Hinweis** Generieren Sie ein Root-CA-Zertifikat nur dann, wenn Sie vorhandene Zertifikate ersetzen möchten. Wenn Sie das tun, werden andere von dieser Root-Zertifizierungsstelle signierten Zertifikate ungültig. Sie können ein neues Root-CA-Zertifikat als Teil dieses Workflows generieren.

### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Root-CA-Zertifikat** aus und klicken Sie auf **OK**.

Im Dialogfeld „Root-CA-Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

5 Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie das Zertifikat als Datei herunter.

6 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf sein System hochzuladen.

**Hinweis** Einige KMS-Anbieter, z. B. SafeNet, verlangen, dass der KMS-Anbieter den KMS neu startet, um das von Ihnen hochgeladene Root-Zertifikat abzuholen.

### Weiter

Schließen Sie den Zertifikatsaustausch ab. Weitere Informationen hierzu finden Sie unter „Einrichten der vertrauenswürdigen Verbindung“, auf Seite 89.

### Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter wie z. B. Vormetric verlangen, dass Sie das vCenter Server-Zertifikat auf den KMS hochladen. Nach dem Upload akzeptiert der KMS den Datenverkehr, der von einem System mit diesem Zertifikat stammt.

vCenter Server generiert ein Zertifikat, um Verbindungen mit dem KMS zu schützen. Das Zertifikat wird in einem getrennten Keystore im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System gespeichert.

### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Zertifikat** und klicken Sie auf **OK**.

Im Dialogfeld „Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

**Hinweis** Generieren Sie kein neues Zertifikat, es sei denn, Sie möchten vorhandene Zertifikate ersetzen.

5 Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie es als Datei herunter.

6 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf den KMS hochzuladen.

### Weiter

Schließen Sie die Vertrauensbeziehung ab. Siehe „Einrichten der vertrauenswürdigen Verbindung“, auf Seite 89.

### Verwenden der Option „Neue Zertifikatsignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter, z. B. Thales, verlangen, dass vCenter Server eine Zertifikatsignierungsanforderung (CSR) generiert und sie an den KMS übermittelt. Der KMS signiert die Zertifikatsignierungsanforderung und sendet das signierte Zertifikat zurück. Sie können das signierte Zertifikat auf den vCenter Server hochladen.

Bei der Verwendung der Option **Neue Zertifikatsignierungsanforderung** handelt es sich um einen Vorgang mit zwei Schritten. Zuerst generieren Sie die Zertifikatsignierungsanforderung und senden diese an den KMS-Anbieter. Anschließend laden Sie das signierte Zertifikat, das Sie vom KMS-Anbieter erhalten, auf den vCenter Server hoch.

#### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Neue Zertifikatsignierungsanforderung** und klicken Sie auf **OK**.

5 Im Dialogfeld kopieren Sie das vollständige Zertifikat aus dem Textfeld in die Zwischenablage oder laden Sie es als Datei herunter. Klicken Sie anschließend auf **OK**.

   Klicken Sie auf die Schaltfläche **Neue CSR generieren** des Dialogfelds nur dann, wenn Sie explizit eine Zertifikatsignierungsanforderung generieren möchten. Durch die Verwendung dieser Option werden alle signierten Zertifikate ungültig, die auf der alten Zertifikatsignierungsanforderung basieren.

6 Folgen Sie den Anweisungen Ihres KMS-Anbieters zum Einreichen der Zertifikatsignierungsanforderung.

7 Wenn Sie vom KMS-Anbieter das signierte Zertifikat erhalten, klicken Sie erneut auf **Schlüsselmanagementserver** und wählen Sie erneut **Neue Zertifikatsignierungsanforderung**.

8 Fügen Sie das signierte Zertifikat in das untere Textfeld ein oder klicken Sie auf **Datei hochladen** und laden Sie die Datei hoch. Klicken Sie anschließend auf **OK**.

#### Weiter

Schließen Sie die Vertrauensbeziehung ab. Siehe „Einrichten der vertrauenswürdigen Verbindung“, auf Seite 89.

### Verwenden der Option zum Hochladen des Zertifikats und des privaten Schlüssels, um eine vertrauenswürdige Verbindung herzustellen

Einige KMS-Anbieter, z. B. HyTrust, verlangen, dass Sie das KMS-Serverzertifikat und den privaten Schlüssel auf das vCenter Server-System hochladen.

Einige KMS-Anbieter generieren ein Zertifikat und einen privaten Schlüssel für die Verbindung und stellen Ihnen diese zur Verfügung. Sobald Sie die Dateien hochgeladen haben, wird Ihre vCenter Server-Instanz vom KMS für vertrauenswürdig erachtet.

#### Voraussetzungen

- Fordern Sie ein Zertifikat und einen privaten Schlüssel vom KMS-Anbieter an. Bei den Dateien handelt es sich um X509-Dateien im PEM-Format.

#### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Zertifikat und privater Schlüssel hochladen** und klicken Sie auf **OK**.

5 Fügen Sie das Zertifikat, das Sie vom KMS-Anbieter erhalten haben, in das obere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Zertifikatsdatei hochzuladen.

6 Fügen Sie die Schlüsseldatei in das untere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Schlüsseldatei hochzuladen.

7 Klicken Sie auf **OK**.

#### Weiter

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter „Einrichten der vertrauenswürdigen Verbindung“, auf Seite 89.

## Festlegen des Standard-KMS-Clusters

Sie müssen den Standard-KMS-Cluster festlegen, wenn Sie den ersten Cluster nicht als Standard-Cluster festlegen oder wenn es mehrere Cluster in Ihrer Umgebung gibt und Sie den Standard-Cluster entfernen.

#### Voraussetzungen

Als Best Practice stellen Sie sicher, dass auf der Registerkarte Schlüsselmanagementserver der Verbindungsstatus als „Normal“ mit einem grünen Häkchen angezeigt wird.

#### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Mehr** unter **Schlüsselmanagementserver**.

3 Wählen Sie den Cluster aus und klicken Sie auf **KMS-Cluster als Standard festlegen**.

   Wählen Sie den Server nicht aus. Das Menü zum Festlegen des Standard-Clusters steht nur für den Cluster zur Verfügung.

4 Klicken Sie auf **Ja**.

   Das Wort `default` erscheint neben dem Clusternamen.

## Einrichten der vertrauenswürdigen Verbindung

Sofern Sie im Dialogfeld **Server hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS-Server einzurichten, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikataustausch explizit einrichten.

Eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS-Server können Sie einrichten, indem Sie entweder den KMS-Server als vertrauenswürdig einstufen oder ein KMS-Zertifikat hochladen. Die folgenden beiden Möglichkeiten stehen zur Verfügung:

- Legen Sie über die Option **KMS-Zertifikat aktualisieren** das Zertifikat explizit als vertrauenswürdig fest.
- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** in vCenter Server hoch.

**Hinweis** Wenn Sie das CA-Root-Zertifikat oder das Zwischen-CA-Zertifikat hochladen, vertraut vCenter Server allen Zertifikaten, die von dieser Zertifizierungsstelle signiert wurden. Um hohe Sicherheit zu gewährleisten, laden Sie ein untergeordnetes Zertifikat oder ein Zwischen-CA-Zertifikat hoch, das vom KMS-Anbieter kontrolliert wird.

### Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Zum Einrichten der Vertrauensbeziehung aktualisieren Sie das KMS-Zertifikat oder laden Sie es hoch.

| Option | Aktion |
|---|---|
| **KMS-Zertifikat aktualisieren** | a Klicken Sie auf **Alle Aktionen** und wählen Sie **KMS-Zertifikat aktualisieren** aus.<br>b Klicken Sie im daraufhin angezeigten Dialogfeld auf **Vertrauenswürdigkeit**. |
| **KMS-Zertifikat hochladen** | a Klicken Sie auf **Alle Aktionen** und wählen Sie **KMS-Zertifikat hochladen** aus.<br>b Klicken Sie im daraufhin angezeigten Dialogfeld auf **Datei hochladen**, laden Sie eine Zertifikatdatei hoch und klicken Sie auf **OK**. |

# Aktivieren der Verschlüsselung auf einen neuen vSAN -Cluster

Sie können die Verschlüsselung aktivieren, wenn Sie einen neuen vSAN-Cluster konfigurieren.

### Voraussetzungen

- Erforderliche Rechte:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**
- Sie müssen einen KMS-Cluster eingerichtet und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu einem vorhandenen Cluster.

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

3 Wählen Sie unter „vSAN“ die Option **Allgemein** aus und klicken Sie auf die Schaltfläche **vSAN konfigurieren**.

4 Aktivieren Sie auf der Seite **vSAN-Funktionen** das Kontrollkästchen **Verschlüsselung** und wählen Sie einen KMS-Cluster aus.

**Hinweis** Stellen Sie sicher, dass das Kontrollkästchen **Festplatten vor Verwendung löschen** nicht aktiviert ist, es sei denn, Sie möchten vorhandene Daten auf den Speichergeräten löschen, während diese verschlüsselt werden.

5 Geben Sie auf der Seite **Festplatten beanspruchen** an, welche Festplatten für den vSAN-Cluster beansprucht werden sollen.

a Wählen Sie ein Flash-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf das Symbol **Für Kapazitätsschicht beanspruchen** (  ).

b Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf das Symbol **Für Cache-Schicht beanspruchen** (  ).

6 Schließen Sie die Clusterkonfiguration ab.

Das Verschlüsseln von Daten bei der Speicherung ist auf dem vSAN-Cluster aktiviert. vSAN verschlüsselt alle zum vSAN-Datenspeicher hinzugefügten Daten.

## Neue Verschlüsselungsschlüssel generieren

Sie können neue Verschlüsselungsschlüssel generieren, falls ein Schlüssel abläuft oder kompromittiert wird.

Die folgenden Optionen stehen zur Verfügung, wenn Sie neue Verschlüsselungsschlüssel für Ihren vSAN-Cluster generieren.

- Wenn Sie einen neuen KEK generieren, erhalten alle Hosts im vSAN-Cluster den neuen KEK vom KMS. Der DEK eines jeden Hosts wird mit dem neuen KEK neu verschlüsselt.
- Wenn Sie alle Daten mit neuen Schlüsseln neu verschlüsseln möchten, werden ein neuer KEK und neue DEKs generiert. Eine rollierende Neuformatierung der Festplatten ist erforderlich, um die Daten neu zu verschlüsseln.

### Voraussetzungen

- Erforderliche Rechte:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageKeys**
- Sie müssen einen KMS-Cluster eingerichtet und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum vSAN-Host-Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein** aus.

4 Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Neue Verschlüsselungsschlüssel generieren**.

5 Klicken Sie auf **OK**, um einen neuen KEK zu generieren. Die DEKs werden mit dem neuen KEK neu verschlüsselt.
   - Um einen neuen KEK und neue DEKs zu generieren und alle Daten im vSAN-Cluster neu zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Auch alle Daten auf dem Speicher mit neuen Schlüsseln neu verschlüsseln**.
   - Wenn der vSAN-Cluster über beschränkte Ressourcen verfügt, aktivieren Sie das Kontrollkästchen **Verringerte Redundanz zulassen**. Wenn Sie verringerte Redundanz zulassen, sind Ihre Daten bei der Neuformatierung der Festplatte möglicherweise gefährdet.

## Aktivieren der vSAN -Verschlüsselung auf einem vorhandenen vSAN -Cluster

Sie können die Verschlüsselung aktivieren, indem Sie die Konfigurationsparameter eines vorhandenen vSAN-Clusters bearbeiten.

### Voraussetzungen

- Erforderliche Rechte:
  - **Host.Inventory.EditCluster**

- **Cryptographer.ManageEncryptionPolicy**
- **Cryptographer.ManageKMS**
- **Cryptographer.ManageKeys**

- Sie müssen einen KMS-Cluster eingerichtet und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.
- Der Modus für Festplattenbeanspruchung des Clusters muss auf „manuell“ festgelegt sein.

**Vorgehensweise**

1 Navigieren Sie im vSphere Web Client zum vSAN-Host-Cluster.

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

3 Wählen Sie unter vSAN die Option **Allgemein** aus.

4 Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**.

5 Aktivieren Sie im Dialogfeld „vSAN-Einstellungen bearbeiten“ das Kontrollkästchen **Verschlüsselung** und wählen Sie einen KMS-Cluster aus.

6 (Optional) Wenn die Speichergeräte in Ihrem Cluster vertrauliche Daten enthalten, aktivieren Sie das Kontrollkästchen **Festplatten vor Verwendung löschen**.

   Diese Einstellung sorgt dafür, dass vSAN vorhandene Daten von den Speichergeräten löscht, während sie verschlüsselt werden.

7 Klicken Sie auf **OK**.

Eine rollierende Neuformatierung aller Festplattengruppen erfolgt, wenn vSAN alle Daten im vSAN-Datenspeicher verschlüsselt.

# vSAN -Verschlüsselung und Core-Dumps

Wenn Ihr vSAN-Cluster die Verschlüsselung verwendet und auf dem ESXi-Host ein Fehler auftritt, ist der dadurch entstandene Core-Dump verschlüsselt, um Kundendaten zu schützen. Auch die Core-Dumps im `vm-support`-Paket sind verschlüsselt.

**Hinweis** Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie beim Umgang mit Core-Dumps die Datensicherheits- und Datenschutzrichtlinien Ihrer Organisation.

## Core-Dumps auf ESXi -Hosts

Wenn ein ESXi-Host ausfällt, wird ein verschlüsselter Core-Dump generiert und der Host neu gestartet. Der Core-Dump wird anhand des Hostschlüssels verschlüsselt, der sich im Schlüssel-Cache-Speicher von ESXi befindet. Ihr nächster Schritt hängt von mehreren Faktoren ab.

- In den meisten Fällen ruft vCenter Server den Schlüssel für den Host vom KMS ab und versucht, nach dem Neustart den Schlüssel an den ESXi-Host zu übermitteln. Wenn der Vorgang erfolgreich war, können Sie das `vm-support`-Paket generieren und den Core-Dump entschlüsseln bzw. neu verschlüsseln.
- Wenn vCenter Server keine Verbindung zum ESXi-Host herstellen kann, können Sie den Schlüssel möglicherweise vom KMS abrufen.
- Wenn der Host einen benutzerdefinierten Schlüssel verwendet hat und es sich bei diesem Schlüssel nicht um den Schlüssel handelt, den vCenter Server an den Host übermittelt, können Sie den Core-Dump nicht verändern. Vermeiden Sie die Verwendung von benutzerdefinierten Schlüsseln.

## Core-Dumps und vm-support-Pakete

Wenn Sie sich an den technischen Support von VMware wenden, um einen schwerwiegenden Fehler zu melden, werden Sie in der Regel von dem Support-Mitarbeiter gebeten, ein `vm-support`-Paket zu generieren. Das Paket enthält Protokolldateien und weitere Informationen, einschließlich Core-Dumps. Wenn die Support-Mitarbeiter mithilfe der Protokolldateien und weiteren Informationen die Probleme nicht beheben können, können Sie die Core-Dumps entschlüsseln, um relevante Informationen zur Verfügung zu stellen. Befolgen Sie die Sicherheits- und Datenschutzrichtlinien Ihrer Organisation, um vertrauliche Informationen wie beispielsweise die Host-Schlüssel zu schützen.

## Core-Dumps auf vCenter Server -Systemen

Ein Core-Dump auf einem vCenter Server-System ist nicht verschlüsselt. vCenter Server enthält bereits potenziell vertrauliche Informationen. Stellen Sie mindestens sicher, dass das Windows-System, auf dem vCenter Server ausgeführt wird, bzw. der vCenter Server Appliance geschützt ist. Alternativ können Sie Core-Dumps für das vCenter Server-System ausschalten. Weitere Informationen in den Protokolldateien können zum Ermitteln der Ursache des Problems dienlich sein.

## Abrufen eines vm-support-Pakets für einen ESXi -Host in einem verschlüsselten vSAN -Cluster

Falls auf einem vSAN-Cluster die Verschlüsselung aktiviert ist, sind die Core-Dumps im `vm-support`-Paket verschlüsselt. Sie können das Paket vom vSphere Web Client erfassen und ein Kennwort angeben, falls Sie davon ausgehen, dass der Core-Dump zu einem späteren Zeitpunkt entschlüsselt werden muss.

Das `vm-support` Paket enthält u. a. Protokolldateien und Core-Dump-Dateien.

### Voraussetzungen

Informieren Sie Ihren Supportmitarbeiter darüber, dass die Verschlüsselung für den vSAN-Cluster aktiviert ist. Der Supportmitarbeiter bittet Sie möglicherweise darum, Core-Dumps zu entschlüsseln, um relevante Informationen zu extrahieren.

---

**Hinweis** Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie die Sicherheits- und Datenschutzrichtlinien Ihrer Organisation, um vertrauliche Informationen wie beispielsweise den Host-Schlüssel zu schützen.

---

### Vorgehensweise

1. Melden Sie sich bei vCenter Server mit dem vSphere Web Client an.
2. Klicken Sie auf **Hosts und Cluster** und klicken Sie dann mit der rechten Maustaste auf den ESXi-Host.
3. Wählen Sie **Systemprotokolle exportieren** aus.
4. Wählen Sie im Dialogfeld **Kennwort für verschlüsselte Core-Dumps** aus, geben Sie ein Kennwort an und bestätigen Sie es.
5. Behalten Sie die Standardeinstellungen für die anderen Optionen bei oder nehmen Sie Änderungen vor, wenn dies vom technischen Support von VMware angefordert wird, und klicken Sie dann auf **Beenden**.
6. Geben Sie einen Speicherort für die Datei an.

7 Falls der Supportmitarbeiter Sie dazu aufgefordert hat, den Core-Dump im `vm-support`-Paket zu entschlüsseln, melden Sie sich bei einem ESXi-Host an und führen Sie die folgenden Schritte aus.

   a Melden Sie sich beim ESXi-Host an und stellen Sie eine Verbindung zu dem Verzeichnis her, in dem sich das `vm-support`-Paket befindet.

   Der Dateiname richtet sich nach folgendem Muster: **`esx.Datum_und_Uhrzeit.tgz`**.

   b Stellen Sie sicher, dass das Verzeichnis ausreichend Speicherplatz für das Paket, das dekomprimierte Paket und das erneut komprimierte Paket enthält, oder verschieben Sie das Paket.

   c Extrahieren Sie das Paket in das lokale Verzeichnis.

   ```
   vm-support -x *.tgz .
   ```

   Die daraus resultierende Dateihierarchie enthält möglicherweise Core-Dump-Dateien für den ESXi-Host (üblicherweise im Verzeichnis `/var/core`) und mehrere Core-Dump-Dateien für virtuelle Maschinen.

   d Entschlüsseln Sie jede verschlüsselte Core-Dump-Datei separat.

   ```
   crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
   --password encryptedZdump decryptedZdump
   ```

   *vm-support-incident-key-file* ist die Schlüsseldatei des Vorfalls. Sie befindet sich auf der obersten Ebene im Verzeichnis.

   *encryptedZdump* ist der Name der verschlüsselten Core-Dump-Datei.

   *decryptedZdump* ist der von dem Befehl generierte Name der Datei. Legen Sie einen Namen fest, der *encryptedZdump* ähnelt.

   e Geben Sie das Kennwort an, das Sie beim Erstellen des `vm-support`-Pakets angegeben haben.

   f Entfernen Sie die verschlüsselten Core-Dumps und komprimieren Sie das Paket erneut.

   ```
   vm-support --reconstruct
   ```

8 Entfernen Sie alle Dateien, die vertrauliche Informationen enthalten.

## Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump

Ein verschlüsselter Core-Dump auf einem ESXi-Host kann mithilfe der CLI `crypto-util` entschlüsselt oder erneut verschlüsselt werden.

Sie können die Core-Dumps im `vm-support`-Paket selbst entschlüsseln und untersuchen. Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie die Sicherheits- und Datenschutzrichtlinien Ihrer Organisation, um vertrauliche Informationen wie beispielsweise die Host-Schlüssel zu schützen.

Nähere Informationen zum erneuten Verschlüsseln eines Core-Dump und weiteren Funktionen von `crypto-util` finden Sie in der Befehlszeilenhilfe.

**Hinweis** `crypto-util` ist für fortgeschrittene Benutzer vorgesehen.

### Voraussetzungen

Der zum Verschlüsseln des Core-Dump verwendete ESXi-Hostschlüssel muss auf dem ESXi-Host verfügbar sein, der den Core-Dump generiert hat.

### Vorgehensweise

1 Melden Sie sich direkt beim ESXi-Host an, auf dem der Core-Dump generiert wurde.

   Falls sich der ESXi-Host im Sperrmodus befindet, oder wenn der SSH-Zugriff deaktiviert ist, müssen Sie möglicherweise zuerst den Zugriff aktivieren.

2 Ermitteln Sie, ob der Core-Dump verschlüsselt ist.

| Option | Beschreibung |
|---|---|
| **Core-Dump überwachen** | `crypto-util envelope describe vmmcores.ve` |
| **zdump-Datei** | `crypto-util envelope describe --offset 4096 zdumpFile` |

3 Entschlüsseln Sie den Core-Dump, je nach Typ.

| Option | Beschreibung |
|---|---|
| **Core-Dump überwachen** | `crypto-util envelope extract vmmcores.ve vmmcores` |
| **zdump-Datei** | `crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted` |

# Upgrade des vSAN -Clusters 9

Das Upgrade von vSAN ist ein Prozess mit verschiedenen Phasen, in dem die jeweiligen Vorgänge in der hier beschriebenen Reihenfolge ausgeführt werden müssen.

Stellen Sie vor dem Aktualisieren sicher, dass Sie den kompletten Upgradevorgang verstehen, um den Vorgang ohne Probleme und Unterbrechungen durchführen zu können. Wenn Sie mit dem allgemeinen Upgrade-Vorgang für vSphere nicht vertraut sind, sollten Sie zuerst die Dokumentation zum *vSphere Upgrade* lesen.

**Hinweis** Wenn die hier beschriebene Reihenfolge der Upgrade-Aufgaben nicht befolgt wird, führt dies zu Datenverlust und Ausfall des Clusters.

Das Upgrade des vSAN-Clusters wird in der folgenden Reihenfolge der Aufgaben ausgeführt.

1 Aktualisieren Sie den vCenter Server. Weitere Informationen finden Sie in der *vSphere-Upgrade*-Dokumentation.

2 Aktualisieren Sie die ESXi-Hosts. Siehe „Aktualisieren der ESXi-Hosts“, auf Seite 100. Informationen zum Migrieren und Vorbereiten der ESXi-Hosts für das Upgrade finden Sie in der *vSphere Upgrade*-Dokumentation.

3 Führen Sie ein Upgrade des vSAN-Festplattenformats durch. Das Upgrade des Festplattenformats ist optional. Um jedoch optimale Ergebnisse zu erzielen, sollten Sie ein Upgrade der zu verwendenden Objekte auf die aktuelle Version durchführen. Mit dem Festplattenformat wird Ihre Umgebung dem kompletten Funktionssatz von vSAN ausgesetzt. Siehe „Upgrade des vSAN-Festplattenformats mit RVC“, auf Seite 105.

Dieses Kapitel behandelt die folgenden Themen:

# Vor dem Upgrade von vSAN

Planen und entwerfen Sie ein ausfallsicheres Upgrade. Bevor Sie versuchen, vSAN zu aktualisieren, stellen Sie sicher, dass Ihre Umgebung die vSphere-Hardware- und -Softwareanforderungen erfüllt.

## Voraussetzungen für das Upgrade

Berücksichtigen Sie die Aspekte, die den allgemeinen Upgradevorgang verzögern können. Richtlinien und Best Practices finden Sie in der Dokumentation zum *vSphere-Upgrade*.

Prüfen Sie die wichtigsten Voraussetzungen, bevor Sie ein Upgrade des Clusters auf vSAN 6.6 durchführen.

**Tabelle 9-1.** Voraussetzungen für das Upgrade

| Voraussetzungen für das Upgrade | Beschreibung |
|---|---|
| Software, Hardware, Treiber, Firmware und Speicher-E/A-Controller | Stellen Sie sicher, dass Software- und Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller, die Sie zu verwenden beabsichtigen, von vSAN 6.6 und höher unterstützt werden und auf der Website des VMware-Kompatibilitätshandbuchs unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind. |
| vSAN-Version | Stellen Sie sicher, dass Sie die neueste Version von vSAN verwenden. Wenn Sie aktuell eine Beta-Version ausführen und planen, vSAN auf 6.6 zu aktualisieren, schlägt Ihr Upgrade fehl. Wenn Sie ein Upgrade von einer Beta-Version durchführen, müssen Sie eine neue Bereitstellung von vSAN ausführen. |
| Festplattenspeicher | Stellen Sie sicher, dass ausreichend Speicherplatz verfügbar ist, um das Upgrade der Softwareversion fertig zu stellen. Die Menge des benötigten Festplattenspeichers für die vCenter Server-Installation hängt von Ihrer vCenter Server-Konfiguration ab. Richtlinien zum erforderlichen Festplattenspeicher für ein vSphere-Upgrade finden Sie in der Dokumentation zum *vSphere-Upgrade*. |
| vSAN-Festplattenformat | Stellen Sie sicher, dass genügend Kapazität für das Upgrade des Festplattenformats verfügbar ist. Wenn der freie Speicherplatz auf den Festplattengruppen (ohne die zu konvertierende Festplattengruppe) geringer ist als die verbrauchte Kapazität der größten Festplattengruppe, müssen Sie **Verringerte Redundanz zulassen** als Datenmigrationsoption auswählen.<br>Angenommen, die größte Festplattengruppe in einem Cluster umfasst 10 TB physische Kapazität, aber nur 5 TB werden aktuell benötigt. Zusätzliche 5 TB Speicherplatz werden an anderer Stelle im Cluster, d. h. außerhalb der zu migrierenden Festplattengruppen, benötigt. Vergewissern Sie sich beim Upgrade des vSAN-Festplattenformats, dass die Hosts sich nicht im Wartungsmodus befinden. Wird ein Mitgliedshost eines vSAN-Clusters in den Wartungsmodus versetzt, wird die Clusterkapazität automatisch reduziert, weil der Speicher des Mitgliedshosts im Cluster nicht mehr bereitsteht und die Kapazität auf dem Host nicht für Daten zur Verfügung steht. Informationen zu verschiedenen Evakuierungsmodi finden Sie unter „Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus“, auf Seite 126. |

**Tabelle 9-1.** Voraussetzungen für das Upgrade (Fortsetzung)

| Voraussetzungen für das Upgrade | Beschreibung |
|---|---|
| vSAN-Hosts | Stellen Sie sicher, dass Sie die vSAN-Hosts in den Wartungsmodus versetzt und die Option **Datenzugriff sicherstellen** oder **Alle Daten evakuieren** ausgewählt haben.<br>**Sie können den vSphere Update Manager verwenden, um den Upgradevorgang zu automatisieren und zu testen.**Wenn Sie allerdings den vSphere Update Manager zum Aktualisieren von vSAN verwenden, lautet der Standardevakuierungsmodus **Datenzugriff sicherstellen**. Bei Verwendung des Modus **Datenzugriff sicherstellen** sind Ihre Daten nicht vollständig geschützt. Falls während des Upgrades von vSAN ein Fehler auftritt, kann dies einen unerwarteten Datenverlust zur Folge haben. Der Modus **Datenzugriff sicherstellen** ist jedoch schneller als der Modus **Alle Daten evakuieren**, weil nicht alle Daten auf einen anderen Host im Cluster verschoben werden müssen. Informationen zu verschiedenen Evakuierungsmodi finden Sie unter „Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus“, auf Seite 126. |
| Virtuelle Maschinen | Vergewissern Sie sich, dass Sie Ihre virtuellen Maschinen gesichert haben. |

## Empfehlungen

Berücksichtigen Sie die folgenden Empfehlungen beim Bereitstellen von ESXi-Hosts zur Verwendung mit vSAN:

- Wenn ESXi-Hosts mit einer Arbeitsspeicherkapazität von 512 GB oder weniger konfiguriert sind, verwenden Sie SATADOM-, SD-, USB- oder Festplattengeräte als Installationsmedium.
- Wenn ESXi-Hosts mit einer Arbeitsspeicherkapazität von mehr als 512 GB konfiguriert sind, verwenden Sie eine separate Magnetfestplatte oder ein eigenes Flash-Gerät als Installationsgerät. Wenn Sie ein separates Gerät verwenden, stellen Sie sicher, dass vSAN das Gerät nicht beansprucht.
- Wenn Sie einen vSAN-Host von einem SATADOM-Gerät aus starten, müssen Sie ein SLC-Gerät (Single-Level Cell) verwenden und die Größe des Startgeräts muss mindestens 16 GB betragen.

vSAN 6.5 und höher ermöglicht Ihnen, die Anforderungen der Boot-Größe für einen ESXi-Host in einem vSAN-Cluster anzupassen. Weitere Informationen finden Sie in dem VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2147881.

## Aktualisieren des Zeugenhosts in einem ausgeweiteten oder aus zwei Hosts bestehenden Cluster

Der Zeugenhost in einem ausgeweiteten oder aus zwei Hosts bestehenden Cluster befindet sich außerhalb des vSAN-Clusters, wird aber vom selben vCenter Server verwaltet. Sie können denselben Vorgang, den Sie für einen vSAN-Datenhost verwenden, auch zum Aktualisieren des Zeugenhosts verwenden.

Aktualisieren Sie den Zeugenhost erst, wenn alle Datenhosts aktualisiert wurden und den Wartungsmodus verlassen haben.

Die Verwendung von vSphere Update Manager zur gleichzeitigen Aktualisierung von Hosts kann unter Umständen dazu führen, dass der Zeugenhost gleichzeitig mit einem der Datenhosts aktualisiert wird. Um diese Probleme bei der Aktualisierung zu vermeiden, konfigurieren Sie vSphere Update Manager so, dass er den Zeugenhost nicht parallel mit den Datenhosts aktualisiert.

# Aktualisieren von vCenter Server

Bei dieser ersten Aufgabe im Rahmen des vSAN-Upgrades handelt es sich um ein allgemeines vSphere-Upgrade, das das Upgrade der vCenter Server- und ESXi-Hosts umfasst.

VMware unterstützt In-Place-Upgrades auf 64-Bit-Systemen von vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x und vCenter Server 5.5 auf vCenter Server 6.0 und höher. Das Upgrade von vCenter Server umfasst ein Upgrade des Datenbankschemas sowie ein Upgrade von vCenter Server. Statt ein In-Place-Upgrade auf vCenter Server durchzuführen, können Sie auch eine andere Maschine für das Upgrade verwenden. Detaillierte Anweisungen und verschiedene Upgrade-Optionen finden Sie in der Dokumentation zum *vSphere-Upgrade*.

# Aktualisieren der ESXi -Hosts

Nach dem Upgrade von vCenter Server müssen Sie beim Upgrade des vSAN-Clusters als nächstes ein Upgrade der ESXi-Hosts für die Verwendung der aktuellen Version durchführen.

Wenn der vSAN-Cluster mehrere Hosts enthält und Sie diese mit vSphere Update Manager aktualisieren, ist **Datenzugriff sicherstellen** der Standardevakuierungsmodus. Wenn Sie diesen Modus verwenden und beim Aktualisieren von vSAN ein Fehler auftritt, sind Ihre Daten gefährdet. Informationen zum Arbeiten mit Evakuierungsmodi finden Sie unter „Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus“, auf Seite 126.

Informationen zur Verwendung von vSphere Update Manager finden Sie auf der Dokumentations-Website unter https://www.vmware.com/support/pubs/vum_pubs.html.

Vor dem Aktualisieren der ESXi-Hosts sollten Sie die Informationen zu empfohlenen Vorgehensweisen im *vSphere Upgrade*-Handbuch lesen. VMware bietet verschiedene ESXi-Upgrade-Optionen. Wählen Sie die Upgrade-Option aus, die für den Hosttyp, den Sie aktualisieren, am besten geeignet ist. Weitere Informationen zu verschiedenen Upgrade-Optionen finden Sie in der *vSphere Upgrade*-Dokumentation.

### Voraussetzungen

- Prüfen Sie, ob Sie ausreichend Festplattenspeicherplatz zum Aktualisieren der ESXi-Hosts haben. Hinweise zu den Festplattenspeicherplatzanforderungen finden Sie in der *vSphere Upgrade*-Dokumentation.
- Stellen Sie sicher, dass Sie die neueste Version von ESXi verwenden. Sie können das neueste ESXi-Installationsprogramm von der VMware-Website für Produktdownloads unter https://my.vmware.com/web/vmware/downloads herunterladen.
- Stellen Sie sicher, dass Sie die neueste Version von vCenter Server verwenden.
- Prüfen Sie die Kompatibilität der Netzwerkkonfiguration, des E/A-Controllers des Speichers, des Speichergeräts und der Sicherungssoftware.
- Prüfen Sie, ob Sie die virtuellen Maschinen gesichert haben.
- Verwenden Sie den Distributed Resource Scheduler (DRS), um Ausfallzeiten virtueller Maschinen während der Aktualisierung zu verhindern. Stellen Sie sicher, dass die Automatisierungsebene für jede virtuelle Maschine auf **Vollautomatisiert** eingestellt ist, damit der DRS virtuelle Maschinen migrieren kann, wenn Hosts in den Wartungsmodus versetzt werden. Sie können aber auch alle virtuellen Maschinen ausschalten oder eine manuelle Migration durchführen.

### Vorgehensweise

1 Versetzen Sie den Host, den Sie aktualisieren möchten, in den Wartungsmodus.

Sie müssen Ihren Upgrade-Pfad mit ESXi 5.5-Hosts oder höher im vSAN-Cluster beginnen.

a Klicken Sie im vSphere Web Client-Navigator mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus > In den Wartungsmodus wechseln** aus.

b Wählen Sie je nach Ihren Anforderungen den Evakuierungsmodus **Datenzugriff sicherstellen** bzw. **Alle Daten evakuieren** aus und warten Sie, bis der Host in den Wartungsmodus gewechselt ist.

Wenn Sie den Host mit vSphere Update Manager aktualisieren oder mit einem 3-Host-Cluster arbeiten, ist **Datenzugriff sicherstellen** als Standardevakuierungsoption verfügbar. Dieser Modus ist schneller als der Modus **Alle Daten evakuieren**. Im Modus **Datenzugriff sicherstellen** sind Ihre Daten allerdings nicht vollständig geschützt. Bei einem Ausfall sind Ihre Daten eventuell gefährdet und es können Ausfallzeiten und unerwarteter Datenverlust auftreten.

2 Laden Sie die Software auf den Datenspeicher Ihres ESXi-Hosts hoch und stellen Sie sicher, dass die Datei im Verzeichnis innerhalb des Datenspeichers verfügbar ist. Sie können beispielsweise die Software auf `/vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip` hochladen.

3 Führen Sie den `esxcli`-Befehl `install -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check` aus. Verwenden Sie den `esxcli`-Software-VIB, um diesen Befehl auszuführen.

Wenn der ESXi-Host erfolgreich installiert wurde, wird sinngemäß die folgende Meldung eingeblendet:

```
Die Aktualisierung wurde erfolgreich abgeschlossen, aber das System muss neu gestartet werden, damit die Änderungen wirksam werden.
```

4 Sie müssen den ESXi-Host über den vSphere Web Client manuell neu starten.

a Navigieren Sie zum ESXi-Host in der vSphere Web Client-Bestandsliste.

b Klicken Sie mit der rechten Maustaste auf den Host, wählen Sie **Einschalten > Neustart** aus, klicken Sie auf **Ja**, um den Vorgang zu bestätigen, und warten Sie dann auf den Neustart des Hosts.

c Klicken Sie mit der rechten Maustaste auf den Host, wählen Sie **Verbindung > Trennen** und dann **Verbindung > Verbinden** aus, um den Host zu verbinden.

Zum Aktualisieren der restlichen Hosts im Cluster wiederholen Sie die Schritte für jeden Host.

Wenn der vSAN-Cluster mehrere Hosts enthält, können Sie mit vSphere Update Manager die restlichen Hosts aktualisieren.

5 Beenden Sie den Wartungsmodus.

### Weiter

1 (Optional) Führen Sie ein Upgrade des vSAN-Festplattenformats durch. Siehe „Upgrade des vSAN-Festplattenformats mit RVC“, auf Seite 105.

2 Prüfen Sie die Hostlizenz. In den meisten Fällen müssen Sie Ihre Hostlizenz neu anwenden. Sie können vSphere Web Client und vCenter Server zum Anwenden von Hostlizenzen verwenden. Weitere Informationen zum Anwenden von Hostlizenzen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

3 (Optional) Aktualisieren Sie die virtuellen Maschinen auf den Hosts mithilfe von vSphere Web Client oder vSphere Update Manager.

# Informationen zum vSAN -Festplattenformat

Das Upgrade des Festplattenformats ist optional. Ihr Cluster vSAN wird auch dann reibungslos ausgeführt, wenn Sie eine vorherige Festplattenformatversion verwenden.

Für optimale Ergebnisse sollten Sie jedoch ein Upgrade der Objekte auf das neue Festplattenformat durchführen. Das neue Festplattenformat stellt den kompletten Funktionssatz von vSAN für Ihre Umgebung bereit.

Je nach der Größe von Festplattengruppen kann das Upgrade des Festplattenformats zeitaufwändig sein, da jeweils nur eine Festplattengruppe aktualisiert. Für das Upgrade jeder Festplattengruppe werden alle Daten von jedem Gerät evakuiert und die Festplattengruppe wird aus dem vSAN-Cluster entfernt. Die Festplattengruppe wird dann wieder zu vSAN mit dem neuen Festplattenformat hinzugefügt.

**Hinweis** Sobald Sie das Festplattenformat aktualisiert haben, können Sie weder ein Rollback der Software auf den Hosts durchführen noch dem Cluster bestimmte ältere Hosts hinzufügen.

Wenn Sie ein Upgrade des Festplattenformats starten, führt vSAN mehrere Operationen durch, die Sie auf der Seite „Neusynchronisieren von Komponenten“ überwachen können. In der Tabelle wird jeder Vorgang zusammengefasst, der beim Upgrade des Festplattenformats durchgeführt wird.

**Tabelle 9-2.** Upgrade-Fortschritt

| Prozentsatz des Abschlusses | Beschreibung |
|---|---|
| 0 % - 5 % | Cluster-Prüfung. Die Cluster-Komponenten werden überprüft und für das Upgrade vorbereitet. Dieser Vorgang kann einige Minuten in Anspruch nehmen. vSAN überprüft, ob ausstehende Probleme vorhanden sind, die den Abschluss des Upgrades verhindern könnten.<br>■ Alle Hosts sind verbunden.<br>■ Alle Hosts weisen die richtige Softwareversion auf.<br>■ Alle Festplatten sind in einem ordnungsgemäßen Zustand.<br>■ Der Zugriff auf alle Objekte ist möglich. |
| 5 %-10 % | Upgrade der Festplattengruppe vSAN führt das anfängliches Datenträger-Upgrade ohne Datenmigration durch. Dieser Vorgang kann einige Minuten in Anspruch nehmen. |
| 10 %-15 % | Neuausrichtung der Objekte. vSAN ändert das Layout aller Objekte, um sicherzustellen, dass diese ordnungsgemäß ausgerichtet sind. Dieser Vorgang kann bei einem kleinen System mit wenigen Snapshots einige Minuten dauern. Bei einem großen System mit vielen Snapshots, vielen fragmentierten Schreibvorgängen und vielen nicht ausgerichteten Objekten kann der Vorgang mehrere Stunden oder sogar mehrere Tage dauern. |
| 15% - 95% | Entfernen und Neuformatieren von Festplattengruppen. Jede Festplattengruppe wird aus dem Cluster entfernt, neu formatiert und dem Cluster erneut hinzugefügt. Die Dauer für diesen Vorgang ist unterschiedlich und richtet sich nach der Anzahl an zugeteilten Megabyte und die Systemauslastung. Der Transfer eines Systems, das nahe an der E/A-Kapazität ist oder diese erreicht hat, erfolgt langsam. |
| 95% - 100% | Abschließendes Upgrade der Objektversion. Die Objektkonvertierung auf das neue Festplattenformat und die Neusynchronisierung sind abgeschlossen. Die Dauer für diesen Vorgang ist unterschiedlich und richtet sich nach der verwendeten Speichermenge und danach, ob die Option **Verringerte Redundanz zulassen** ausgewählt ist. |

Während des Upgrades können Sie den Vorgang auf dem vSphere Web Client durch Navigieren zur Seite „Neusynchronisieren von Komponenten“ überwachen. Siehe „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“, auf Seite 150. Sie können auch den RVC-Befehl `vsan.upgrade_status <cluster>` zur Überwachung des Upgrades verwenden. Verwenden Sie optional das Flag `–r <seconds>`, um den Upgrade-Status regelmäßig bis zum Drücken auf STRG+C zu aktualisieren. Zwischen jeder Aktualisierung sind mindestens 60 Sekunden zulässig.

Im vSphere Web Client können Sie im Fenster „Kürzlich bearbeitete Aufgaben“ der Statusleiste weitere Upgrade-Aufgaben, wie beispielsweise die Entfernung und das Upgrade von Geräten, überwachen.

Die folgenden Überlegungen gelten für das Upgrade des Festplattenformats:

- Wenn Sie einen Cluster mit drei Hosts aktualisieren und eine vollständige Evakuierung durchführen möchten, schlägt die Evakuierung für Objekte mit **Primäre Ebene von zu tolerierenden Fehlern** größer 0 fehl. Ein Cluster mit drei Hosts kann eine Festplattengruppe, die vollständig evakuiert wird, mit den Ressourcen von nur zwei Hosts nicht neu schützen. Wenn beispielsweise **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt ist, benötigt vSAN drei Schutzkomponenten (zwei Spiegel und einen Zeugen), wobei jede Schutzkomponente auf einem separaten Host platziert wird.

  Für einen Cluster mit drei Hosts müssen Sie den Evakuierungsmodus **Datenzugriff sicherstellen** auswählen. In diesem Modus kann jeder Hardwarefehler zum Datenverlust führen.

  Darüber hinaus müssen Sie sicherstellen, dass ausreichend freier Speicherplatz verfügbar ist. Der Speicherplatz muss der logischen verbrauchten Kapazität der größten Festplattengruppe entsprechen. Diese Kapazität muss auf einer Festplattengruppe separat von der zu migrierenden Festplattengruppe verfügbar sein.

- Sorgen Sie bei einem Upgrade eines Clusters mit drei Hosts oder beim Upgrade eines Clusters mit begrenzten Ressourcen dafür, dass die virtuellen Maschinen in einem reduzierten Redundanzmodus betrieben werden können. Führen Sie den RVC-Befehl mit der Option `vsan.ondisk_upgrade ––allow–reduced–redundancy` aus.

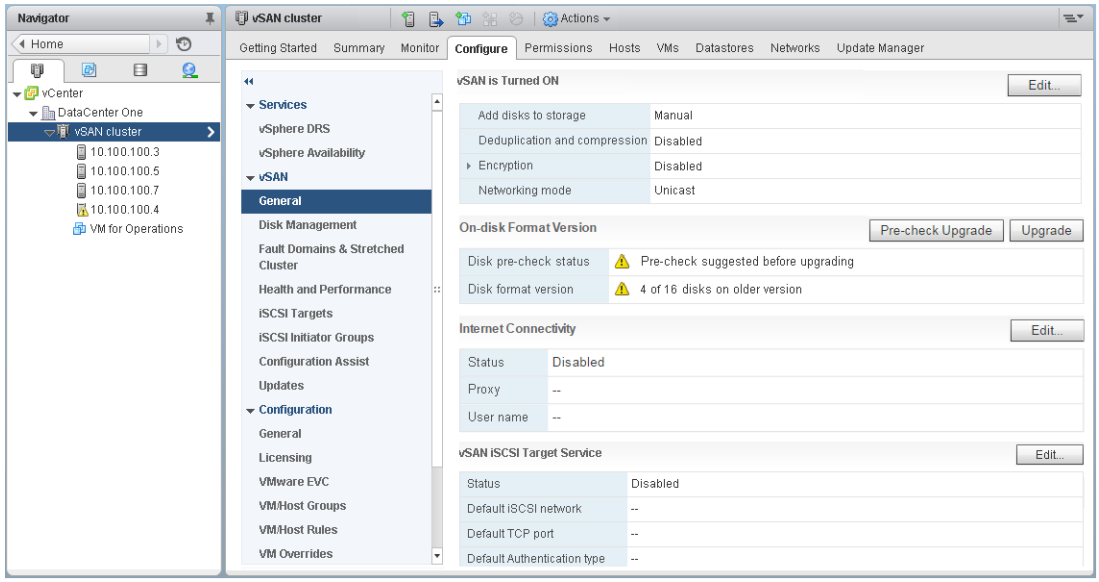
- Die Verwendung der Befehlsoption `––allow–reduced–redundancy` bedeutet, dass während der Migration bestimmte virtuelle Maschinen möglicherweise keine Fehler tolerieren können. Diese geringere Toleranz gegenüber Fehlern kann auch zum Datenverlust führen. vSAN stellt die vollständige Übereinstimmung und Redundanz nach Abschluss des Upgrades wieder her. Während des Upgrades lautet der Übereinstimmungsstatus von virtuellen Maschinen und deren Redundanzen vorübergehend „Nicht übereinstimmend“. Wenn Sie das Upgrade und alle Neuerstellungsaufgaben abgeschlossen haben, weisen die virtuellen Maschinen wieder den Status „Übereinstimmung“ auf.

- Entfernen oder Trennen Sie während des Upgrades keinen Host und platzieren Sie einen Host nicht in den Wartungsmodus. Diese Aktionen können dazu führen, dass das Upgrade fehlschlägt.

Informationen zu den RVC-Befehlen und Befehlsoptionen finden Sie im *Referenzhandbuch zu den RVC-Befehlen (RVC Command Reference Guide)*.

## Upgrade des vSAN -Festplattenformats mit dem vSphere Web Client

Nachdem Sie ein Upgrade der vSAN-Hosts durchgeführt haben, können Sie das Upgrade des Festplattenformats durchführen.




**Hinweis** Wenn Sie die Verschlüsselung oder die Deduplizierung und Komprimierung auf einem vorhandenen vSAN-Cluster aktivieren, wird das Festplattenformat automatisch auf die neueste Version aktualisiert. Dieser Vorgang ist nicht erforderlich. Sie können die zweimalige Neuformatierung der Festplattengruppen vermeiden. Siehe „Bearbeiten von vSAN-Einstellungen“, auf Seite 53.

### Voraussetzungen

- Stellen Sie sicher, dass Sie die aktualisierte Version von vCenter Server verwenden.
- Stellen Sie sicher, dass Sie die neueste Version von ESXi-Hosts verwenden.
- Stellen Sie sicher, dass die Festplatten einen ordnungsgemäßen Status aufweisen. Navigieren Sie in vSphere Web Client zur Seite „Festplattenverwaltung“, um den Objektstatus zu überprüfen.
- Stellen Sie sicher, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, zertifiziert und auf der VMware-Kompatibilitätshandbuch-Website unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind.
- Stellen Sie sicher, dass ausreichend freier Speicherplatz vorhanden ist, um das Upgrade des Festplattenformats durchzuführen. Führen Sie den RVC-Befehl `vsan.whatif_host_failures` aus, um festzustellen, ob ausreichend Kapazität zum Abschließen des Upgrades vorhanden ist, oder um eine Neuerstellung der Komponenten vorzunehmen, falls beim Upgrade ein Fehler auftritt.
- Stellen Sie sicher, dass sich Ihre Hosts nicht im Wartungsmodus befinden. Versetzen Sie Ihre Hosts beim Upgrade des Festplattenformats nicht in den Wartungsmodus. Die verfügbare Ressourcenkapazität im Cluster wird reduziert, wenn ein Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, weil die Kapazität des Mitgliedshosts im Cluster nicht mehr bereitsteht. Das Upgrade des Clusters schlägt dann möglicherweise fehl.
- Stellen Sie sicher, dass aktuell keine Komponentenneuerstellungsaufgaben im vSAN-Cluster ausgeführt werden. Siehe „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“, auf Seite 150.

### Vorgehensweise

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

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

3 Wählen Sie unter vSAN die Option **Allgemein**.

4 (Optional) Klicken Sie unter Datenträgerformat-Version auf **Upgrade der Vorabprüfung**.

Die Vorabprüfung zum Upgrade analysiert den Cluster, um Probleme aufzudecken, die ein erfolgreiches Upgrade möglicherweise verhindern. Einige der überprüften Punkte sind der Hoststatus, der Festplattenstatus, der Netzwerkstatus und der Objektstatus. Upgradeprobleme werden im Textfeld **Status der Festplattenvorabprüfung** angezeigt.

5 Klicken Sie unter Datenträgerformat-Version auf **Upgrade**.

6 Klicken Sie im Dialogfeld „Upgrade“ auf **Ja**, um das Upgrade des Festplattenformats durchzuführen.

vSAN führt einen rollenden Neustart für jede Festplattengruppe im Cluster durch. Die Spalte „Datenträgerformat-Version“ zeigt die Festplattenformat-Version der Speichergeräte im Cluster an. Die Spalte Datenträger mit veralteter Version zeigt die Anzahl der Geräte an, die das neue Format verwenden. Bei erfolgreichem Upgrade lautet die Anzahl der Datenträger mit veralteter Version 0.

Wenn beim Upgrade ein Fehler auftritt, können Sie die Seite „Neusynchronisieren von Komponenten“ im vSphere Web Client aufrufen. Warten Sie, bis die gesamte Neusynchronisierung abgeschlossen ist, und führen Sie das Upgrade erneut aus. Sie können die Cluster-Integrität auch mit dem Integritätsdienst überprüfen. Wenn Sie alle bei den Integritätsprüfungen aufgetretenen Fehler behoben haben, können Sie das Upgrade erneut ausführen.

## Upgrade des vSAN -Festplattenformats mit RVC

Nachdem Sie ein Upgrade der vSAN-Hosts durchgeführt haben, können Sie die RVC (Ruby vSphere Console) verwenden, um mit dem Upgrade des Festplattenformats fortzufahren.

### Voraussetzungen

- Stellen Sie sicher, dass Sie die aktualisierte Version von vCenter Server verwenden.
- Stellen Sie sicher, dass auf den ESXi-Hosts im vSAN-Cluster Version 6.5 oder höher ausgeführt wird.
- Stellen Sie sicher, dass die Festplatten auf der Seite „Festplattenverwaltung“ im vSphere Web Client einen ordnungsgemäßen Status aufweisen. Sie können auch den RVC-Befehl `vsan.disk_stats` ausführen, um den Festplattenstatus zu überprüfen.
- Stellen Sie sicher, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, zertifiziert und auf der VMware-Kompatibilitätshandbuch-Website unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind.
- Stellen Sie sicher, dass ausreichend freier Speicherplatz vorhanden ist, um das Upgrade des Festplattenformats durchzuführen. Führen Sie den RVC-Befehl `vsan.whatif_host_failures` aus, um festzustellen, ob ausreichend Kapazität zum Abschließen des Upgrades vorhanden ist, oder um eine Neuerstellung der Komponenten vorzunehmen, falls beim Upgrade ein Fehler auftritt.
- Stellen Sie sicher, dass PuTTY oder ein anderer SSH-Client für den Zugriff auf RVC installiert ist.

  Ausführliche Informationen zum Herunterladen des RVC-Tools und zum Verwenden der RVC-Befehle finden Sie im *Referenzhandbuch zu den RVC-Befehlen (RVC Command Reference Guide)*.
- Stellen Sie sicher, dass sich Ihre Hosts nicht im Wartungsmodus befinden. Versetzen Sie Ihre Hosts beim Upgrade des Festplattenformats nicht in den Wartungsmodus. Die verfügbare Ressourcenkapazität im Cluster wird reduziert, wenn ein Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, weil die Kapazität des Mitgliedshosts im Cluster nicht mehr bereitsteht. Das Upgrade des Clusters schlägt dann möglicherweise fehl.
- Stellen Sie sicher, dass aktuell keine Komponentenneuerstellungsaufgaben im vSAN-Cluster ausgeführt werden, indem Sie den RVC-Befehl `vsan.resync_dashboard` ausführen.

**Vorgehensweise**

1 Melden Sie sich mit RVC bei Ihrem vCenter Server an.

2 Führen Sie den Befehl `vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name>` aus, um den Festplattenstatus anzuzeigen.

Beispiel:`vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

Dieser Befehl listet die Namen aller Geräte und Hosts im vSAN-Cluster auf. Darüber hinaus zeigt dieser Befehl das aktuelle Festplattenformat und den Systemstatus an. In der Spalte **Systemstatus** der Seite Datenträgerverwaltung können Sie auch den aktuellen Systemstatus der Geräte prüfen. Beispielsweise wird der Gerätestatus „Nicht ordnungsgemäß“ in der Spalte **Systemstatus** für die Hosts oder Festplattengruppen mit fehlerhaften Geräten angezeigt.

3 Führen Sie den Befehl `vsan.ondisk_upgrade <path to vsan cluster>` aus.

Beispiel:`vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

4 Überwachen Sie den Fortschritt in RVC.

RVC führt das Upgrade für jeweils eine Festplattengruppe aus.

Nachdem das Upgrade des Festplattenformats erfolgreich abgeschlossen wurde, wird eine Meldung ähnlich der folgenden angezeigt.

```
Festplattenformat-Upgradephase abgeschlossen

Für n v1-Objekte ist ein Upgrade erforderlich Objekt-Upgrade-Fortschritt: n aktualisiert, 0 verblieben

Objekt-Upgrade abgeschlossen: n aktualisiert

VSAN-Upgrade abgeschlossen
```

5 Führen Sie den Befehl `vsan.obj_status_report` aus, um zu überprüfen, ob für die Objektversionen ein Upgrade auf das neue Festplattenformat durchgeführt wurde.

## Überprüfen des Upgrade des vSAN -Festplattenformats

Nachdem Sie das Upgrade des Festplattenformats abgeschlossen haben, müssen Sie überprüfen, ob der vSAN-Cluster das neue Festplattenformat verwendet.

**Vorgehensweise**

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

Das aktuelle Festplattenformat wird in der Spalte „Version des Festplattenformats“ angezeigt. Wenn Sie beispielsweise das Festplattenformat 2.0 verwenden, wird Version 2 in der Spalte „Version des Festplattenformats“ angezeigt. Für das Festplattenformat 3.0 wird Version 3 als Version des Festplattenformats angezeigt.

# Überprüfen des vSAN -Cluster-Upgrades

Das vSAN-Cluster-Upgrade ist erst abgeschlossen, wenn Sie sich vergewissert haben, dass Sie die neueste Version von vSphere verwenden und dass vSAN zur Nutzung zur Verfügung steht.

**Vorgehensweise**

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

2 Klicken Sie auf die Registerkarte **Konfigurieren** und stellen Sie sicher, dass vSAN aufgelistet ist.

- Sie können auch zu Ihrem ESXi-Host navigieren und **Übersicht** > **Konfiguration** auswählen, um sicherzustellen, dass Sie die neueste Version des ESXi-Hosts verwenden.

# Verwenden von RVC-Upgrade-Befehlsoptionen

Der Befehl `vsan.ondisk_upgrade` bietet verschiedene Befehlsoptionen zum Steuern und Verwalten der Upgrades eines vSAN-Clusters. Sie können z. B. verringerte Redundanz zulassen, um das Upgrade auszuführen, wenn Sie nur über wenig freien Speicherplatz verfügen.

Führen Sie den Befehl `vsan.ondisk_upgrade --help` aus, um die Liste der RVC-Befehlsoptionen anzuzeigen.

Verwenden Sie diese Befehlsoptionen mit dem Befehl `vsan.ondisk_upgrade`.

**Tabelle 9-3.** Optionen des Upgradebefehls

| Optionen | Beschreibung |
|---|---|
| `--hosts_and_clusters` | Hiermit geben Sie die Pfade zu allen Hostsystemen im Cluster oder den Computing-Ressourcen des Clusters an. |
| `--ignore-objects, -i` | Hiermit überspringen Sie das vSAN-Objektupgrade. Sie können mit dieser Befehlsoption auch die Versionsaktualisierung von Objekten eliminieren. Bei Verwendung dieser Befehlsoption verwenden Objekte weiterhin die aktuelle Version des Festplattenformats. |
| `--allow-reduced-redundancy, -a` | Mit dieser Option entfernen Sie die Anforderung, dass die Menge an freiem Speicherplatz während des Festplatten-Upgrades der Größe einer Festplattengruppe entsprechen muss. Mit dieser Option werden virtuelle Maschinen während des Upgrades in einem Modus mit reduzierter Redundanz betrieben. Das bedeutet, dass bestimmte virtuelle Maschinen möglicherweise vorübergehend keine Fehler tolerieren und dass ein Ausfall zu Datenverlust führen kann. vSAN stellt die vollständige Übereinstimmung und Redundanz nach Abschluss des Upgrades wieder her. |
| `--force, -f` | Verwenden Sie diese Option, um „force-proceed“ zu aktivieren und alle Bestätigungsanfragen automatisch zu beantworten. |
| `--help, -h` | Hiermit werden die Hilfeoptionen angezeigt. |

Informationen zum Verwenden der RVC-Befehle finden Sie im *Referenzhandbuch zu RVC-Befehlen*.

# vSAN -Build-Empfehlungen für vSphere Update Manager

vSAN generiert System-Baselines und Baseline-Gruppen, die mit vSphere Update Manager verwendet werden. Sie können diese empfohlenen Baselines verwenden, um Software, Patches und Erweiterungen für Hosts in Ihrem vSAN-Cluster zu aktualisieren.

vSAN 6.6.1 und höher generiert automatisierte Build-Empfehlungen für vSAN-Cluster. vSAN kombiniert Informationen im VMware-Kompatibilitätshandbuch und im vSAN-Versionskatalog mit Informationen zu den installierten ESXi-Versionen. Diese empfohlenen Updates stellen die beste verfügbare Version bereit, um die Hardware in einem unterstützten Status zu halten.

## vSAN -System-Baselines

vSAN-Build-Empfehlungen werden über vSAN-System-Baselines für Update Manager bereitgestellt. Diese System-Baselines werden von vSANverwaltet. Sie sind schreibgeschützt und können nicht angepasst werden.

vSAN generiert eine Baseline-Gruppe für jeden vSAN-Cluster. vSAN-System-Baselines werden im Bereich Baselines der Registerkarte „Baselines und Gruppen“ aufgelistet. Sie können weiterhin Ihre eigenen Baselines erstellen und standardisieren.

Update Manager prüft automatisch jeden vSAN-Cluster, um die Übereinstimmung anhand der Baseline-Gruppe zu überprüfen. Um ein Upgrade Ihres Clusters durchzuführen, müssen Sie die System-Baseline manuell über den Update Manager standardisieren. Sie können die vSAN-System-Baseline auf einem einzelnen Host oder auf dem gesamten Cluster standardisieren.

## vSAN -Versionskatalog

Der vSAN-Versionskatalog verwaltet Informationen zu verfügbaren Versionen, zur bevorzugten Reihenfolge der Versionen und zu kritischen Patches, die für die jeweilige Version erforderlich sind. Der vSAN-Versionskatalog wird in der VMware Cloud gehostet.

vSAN benötigt für den Zugriff auf den Versionskatalog eine Internetverbindung. Sie müssen nicht beim Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für vSAN registriert sein, um Zugriff auf den Versionskatalog zu erhalten.

## Arbeiten mit vSAN -Build-Empfehlungen

Update Manager überprüft die installierten ESXi-Versionen anhand der Informationen in der HCL im VMware-Kompatibilitätshandbuch. Er bestimmt den richtigen Upgrade-Pfad für jeden vSAN-Cluster basierend auf dem aktuellen vSAN-Versionskatalog. vSAN enthält auch die erforderlichen Treiber und Patch-Updates für die empfohlene Version in der System-Baseline.

vSAN-Build-Empfehlungen stellen sicher, dass für jeden vSAN-Cluster der aktuelle Hardwarekompatibilitätsstatus erhalten bleibt oder verbessert wird. Wenn Hardware im vSAN-Cluster nicht in der HCL enthalten ist, empfiehlt vSAN ein Upgrade auf die neueste Version, da sie nicht schlechter als der aktuelle Status ist.

Die folgenden Beispiele beschreiben die Logik der vSAN-Build-Empfehlungen.

**Beispiel 1** Ein vSAN-Cluster führt Version 6.0 Update 2 aus, und die Hardware ist in der HCL für 6.0 Update 2 enthalten. Die HCL gibt an, dass die Hardware bis zu Version 6.0 Update 3, aber nicht für 6.5 und höher unterstützt wird. vSAN empfiehlt ein Upgrade auf Version 6.0 Update 3, einschließlich der erforderlichen kritischen Patches für die Version.

**Beispiel 2** Ein vSAN-Cluster führt Version 6.0 Update 2 aus, und die Hardware ist in der HCL für 6.0 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 6.5 Update 1 unterstützt. vSAN empfiehlt ein Upgrade auf Version 6.5 Update 1.

**Beispiel 3** Ein vSAN-Cluster führt Version 6.0 Update 2 aus, und die Hardware ist nicht in der HCL für diese Version enthalten. vSAN empfiehlt ein Upgrade auf Version 6.5 Update 1, obwohl die Hardware nicht in der HCL für 6.5 Update 1 enthalten ist. vSAN empfiehlt das Upgrade, da der neue Status nicht schlechter als der aktuelle Status ist.

Die Engine für die Empfehlungen wird in regelmäßigen Abständen (einmal täglich) oder bei Eintreten der folgenden Ereignisse ausgeführt.

- Änderungen an Cluster-Mitgliedschaften. Beispiele hierfür sind das Hinzufügen oder Entfernen eines Hosts.
- Der vSAN Management Service wird neu gestartet.
- Ein Benutzer meldet sich über einen vSphere Client oder RVC bei My VMware (my.vmware.com) an.
- Das VMware-Kompatibilitätshandbuch oder der vSAN-Versionskatalog wird aktualisiert.

Die Systemdiagnose für die vSAN-Build-Empfehlung zeigt den aktuellen Build an, der für den vSAN-Cluster empfohlen wird. Sie kann Sie auch bezüglich etwaiger Probleme mit der Funktion warnen.

## Systemanforderungen

Update Manager muss auf Windows-vCenter Servermanuell installiert werden.

vSAN erfordert Internetzugriff für die Aktualisierung von Versionsmetadaten, die Überprüfung des VMware-Kompatibilitätshandbuchs und zum Herunterladen von ISO-Images aus My VMware.

vSAN erfordert gültige Anmeldedaten für My VMware (my.vmware.com) zum Herunterladen von ISO-Images für Upgrades. Für Hosts, auf denen Version 6.0 Update 1 und früher ausgeführt wird, müssen Sie für die Eingabe der My VMware-Anmeldedaten RVC verwenden. Für Hosts, auf denen eine höhere Version der Software ausgeführt wird, können Sie sich über die Systemdiagnose für die ESX-Build-Empfehlung anmelden.

Führen Sie zum Eingeben der My VMware-Anmeldedaten über RVC den folgenden Befehl aus:
**`vsan.login_iso_depot –u`** <*Benutzername*> **`–p`** <*Kennwort*>

# Geräteverwaltung in einem vSAN-Cluster 10

Sie können verschiedene Geräteverwaltungsaufgaben in einem vSAN-Cluster durchführen. Sie können Hybrid- oder All-Flash-Festplattengruppen erstellen, vSAN für die Beanspruchung von Geräten für Kapazität und Cache aktivieren, LED-Indikatoren auf Geräten aktivieren oder deaktivieren, Geräte als Flash-Geräte markieren, Remotegeräte als lokal markieren usw.

Dieses Kapitel behandelt die folgenden Themen:



## Verwalten von Festplattengruppen und Geräten

Wenn Sie vSAN in einem Cluster aktivieren, wählen Sie einen Modus für Festplattenbeanspruchung, um Geräte in Gruppen zu organisieren.

vSAN 6.6 und höhere Versionen bieten einen einheitlichen Workflow für das Beanspruchen von Festplatten über alle Szenarien hinweg. Er gruppiert alle verfügbaren Festplatten nach Modell und Größe bzw. nach Host. Sie müssen die Geräte auswählen, die für den Cache-Speicher bzw. für die Kapazität verwendet werden sollen.

### Erstellen einer Festplattengruppe auf einem Host

Bei der Erstellung von Festplattengruppen müssen Sie manuell alle Hosts und Geräte angeben, die für den vSAN-Datenspeicher verwendet werden sollen. Sie organisieren Cache- und Kapazitätsgeräte in Festplattengruppen.

Zum Erstellen einer Festplattengruppe definieren Sie die Festplattengruppe und wählen einzeln die Geräte aus, die in die Gruppe aufgenommen werden sollen. Jede Festplattengruppe enthält ein Flash-Cache- und mindestens ein Kapazitätsgerät.

Beachten Sie bei der Erstellung einer Festplattengruppe das Verhältnis zwischen Flash-Cache und belegter Kapazität. Obwohl das Verhältnis von den Anforderungen und der Arbeitslast des Clusters abhängt, sollten Sie in Betracht ziehen, mindestens 10 Prozent der belegten Kapazität zu verwenden (Replikate wie z. B. Spiegel sind dabei nicht einzubeziehen).

Der vSAN-Cluster enthält zunächst einen einzelnen vSAN-Datenspeicher mit 0 Byte Belegung.

Wenn Sie Festplattengruppen auf allen Hosts erstellen und Cache- und Kapazitätsgeräte hinzufügen, nimmt die Größe des Datenspeichers entsprechend der Menge der physischen Kapazität zu, die durch diese Geräte hinzugefügt wird. vSAN erstellt einen einzelnen verteilten Datenspeicher für vSAN und verwendet dabei die lokale leere Kapazität, die durch die dem Cluster hinzugefügten Hosts verfügbar ist.

Wenn mehrere Flash-Geräte für den Cluster erforderlich sind, müssen Sie mehrere Festplattengruppen manuell erstellen, da maximal ein Flash-Cache-Gerät pro Festplattengruppe erlaubt ist.

**Hinweis** Wenn einem vSAN-Cluster ein neuer ESXi-Host hinzugefügt wird, wird der lokale Speicher dieses Hosts nicht automatisch dem Datenspeicher für vSAN hinzugefügt. Sie müssen eine Festplattengruppe erstellen und dieser die Geräte hinzufügen, um den neuen Speicher des neuen ESXi-Hosts verwenden zu können.

**Beanspruchen von Festplatten für den vSAN-Cluster**

Sie können mehrere Geräte aus den Hosts auswählen und vSAN erstellt Standardfestplattengruppen.

Wenn Sie die Kapazität von Hosts erhöhen oder neue Hosts mit Kapazität zum vSAN-Cluster hinzufügen, können Sie zum Erhöhen der Kapazität des vSAN-Datenspeichers die neuen Geräte auswählen. In einem reinen Flash-Cluster können Sie die Flash-Geräte zur Nutzung als Kapazität markieren.

Nachdem vSAN Geräte beansprucht hat, wird der gemeinsam genutzte vSAN-Datenspeicher erstellt. Die Gesamtgröße des Datenspeichers spiegelt die Kapazität aller Kapazitätsgeräte in Festplattengruppen auf allen Hosts im Cluster wider. Ein geringer Kapazitäts-Overhead wird für Metadaten verwendet.

## Erstellen einer Festplattengruppe auf einem vSAN -Host

Sie können bestimmte Cache-Geräte manuell mit bestimmten Kapazitätsgeräten kombinieren, um Festplattengruppen auf einem bestimmten Host zu definieren.

Bei dieser Methode wählen Sie manuell Geräte zum Erstellen einer Festplattengruppe für einen Host aus. Sie können der Festplattengruppe ein Cache- und mindestens ein Kapazitätsgerät hinzufügen.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie den Host aus und klicken Sie auf das Symbol **Neue Festplattengruppe erstellen** ( ).

- Wählen Sie das für den Cache zu verwendende Flash-Gerät aus.
- Wählen Sie im Dropdown-Menü **Kapazitätstyp** den Typ der zu verwendenden Kapazitätsfestplatte aus. Ihre Auswahl richtet sich nach dem Typ der Festplattengruppe, die Sie erstellen möchten (HDD für Hybrid oder Flash für All-Flash).
- Wählen Sie die Geräte aus, die Sie für die Kapazität verwenden möchten.

5 Klicken Sie auf **OK**.

Die neue Festplattengruppe wird in der Liste angezeigt.

## Beanspruchen von Speichergeräten für einen vSAN -Cluster

Sie können eine Gruppe von Cache- und Kapazitätsgeräten auswählen. Diese werden dann von vSAN in Standardfestplattengruppen eingeteilt.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Klicken Sie auf das Symbol **Festplatten beanspruchen** (  ).

5 Wählen Sie Geräte zum Hinzufügen zur Festplattengruppe aus.

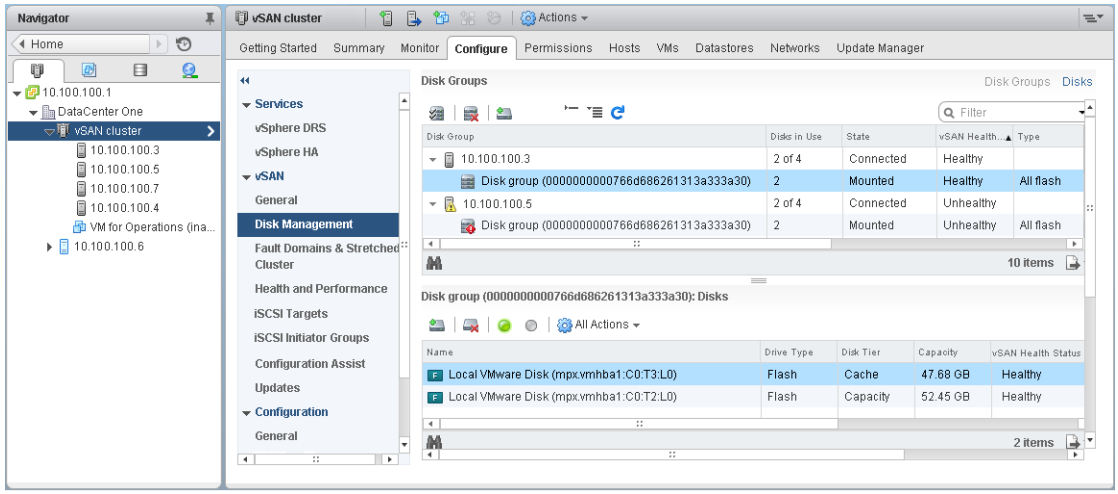
- Jeder Host, der Speicher für eine Hybridfestplattengruppe bereitstellt, muss ein Flash-Cache-Gerät und mindestens ein Kapazitätsgerät bereitstellen. Pro Festplattengruppe kann nur ein Flash-Cache-Gerät hinzugefügt werden.
  - Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf das Symbol **Für Cache-Schicht beanspruchen** (  ).
  - Wählen Sie ein HDD-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf das Symbol **Für Kapazitätsschicht beanspruchen** (  ).
  - Klicken Sie auf **OK**.
- Wählen Sie für All-Flash-Festplattengruppen Flash-Geräte für Kapazität und Cache aus.
  - Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf das Symbol **Für Cache-Schicht beanspruchen** (  ).
  - Wählen Sie ein Flash-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf das Symbol **Für Kapazitätsschicht beanspruchen** (  ).
  - Klicken Sie auf **OK**.

Um die Rolle aller zur All-Flash-Festplattengruppe hinzugefügten Geräte zu überprüfen, navigieren Sie unten auf der Seite „Festplattenverwaltung“ zur Spalte „Festplattenrolle“. Die Spalte zeigt eine Liste der Geräte und ihrem jeweiligen Zweck in einer Datenträgergruppe an.

vSAN beansprucht die von Ihnen ausgewählten Geräte und ordnet sie in standardmäßigen Festplattengruppen zur Unterstützung des vSAN-Datenspeichers an.

# Arbeiten mit einzelnen Geräten

Sie können verschiedene Geräteverwaltungsaufgaben im vSAN-Cluster durchführen, wie zum Beispiel Hinzufügen von Geräten zu einer Festplattengruppe, Entfernen von Geräten aus einer Festplattengruppe, Aktivieren oder Deaktivieren von Locator-LEDs und Markieren von Geräten.




## Hinzufügen von Geräten zu einer Festplattengruppe

Wenn Sie vSAN für die Beanspruchung von Festplatten im manuellen Modus konfigurieren, können Sie zusätzliche lokale Geräte zu vorhandenen Festplattengruppen hinzufügen.

Die Geräte müssen denselben Typ wie die vorhandenen Geräte in den Festplattengruppen aufweisen, also beispielsweise SSD oder Magnetfestplatten.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie die Festplattengruppe aus und klicken Sie auf das Symbol **Fügt eine Festplatte zur ausgewählten Festplattengruppe hinzu** ( ).

5 Wählen Sie das Gerät aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

Wenn Sie ein verwendetes Gerät hinzufügen, das verbleibende Daten oder Partitionsinformationen enthält, müssen Sie das Gerät zuerst bereinigen. Informationen zum Entfernen von Partitionsinformationen von Geräten finden Sie unter „Entfernen der Partition von Geräten“, auf Seite 119. Sie können auch den RVC-Befehl `host_wipe_vsan_disks` ausführen, um das Gerät zu formatieren. Informationen zu den RVC-Befehlen finden Sie im *Referenzhandbuch zu den RVC-Befehlen (RVC Command Reference Guide)*.

## Entfernen von Festplattengruppen oder Geräten aus vSAN

Sie können die ausgewählten Geräte aus der Festplattengruppe oder eine komplette Festplattengruppe entfernen.

Durch das Entfernen von nicht geschützten Geräten können der vSAN-Datenspeicher und virtuelle Maschinen im Datenspeicher gestört werden, weshalb Sie das Entfernen von Geräten oder Festplattengruppen vermeiden sollten.

In der Regel löschen Sie Geräte oder Festplattengruppen aus vSAN, wenn Sie ein Upgrade für ein Geräte durchführen, ein Gerät aufgrund eines Gerätefehlers ersetzt wird oder ein Cache-Geräte entfernt werden muss. Andere vSphere Storage-Funktionen können jedes Flash-basierte Gerät verwenden, das Sie aus dem vSAN-Cluster entfernen.

Durch das Löschen einer Festplattengruppe werden die Festplattenmitgliedschaft sowie die auf den Geräten gespeicherten Daten endgültig gelöscht.

**Hinweis** Durch das Entfernen eines einzelnen Flash-Cache-Geräts oder aller Kapazitätsgeräte aus einer Festplattengruppe wird die gesamte Festplattengruppe entfernt.

Das Evakuieren der Daten aus Geräten oder Festplattengruppen kann zur vorübergehenden Nichtübereinstimmung mit VM-Speicherrichtlinien führen.

### Voraussetzungen

- Sie können den vSAN-Host durch Auswählen der Option **Alle Daten evakuieren** oder, wenn Sie ein Gerät oder eine Festplattengruppe löschen möchten, durch Auswählen der Option **Datenzugriff sicherstellen** in den Wartungsmodus versetzen. Wenn Sie die Option **Keine Datenverlagerung** aus dem Dropdown-Menü auswählen, sind Ihre Daten möglicherweise einem Risiko ausgesetzt, falls während der Evakuierung ein Fehler auftritt.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Entfernen Sie eine Festplattengruppe oder ausgewählte Geräte.

| Option | Beschreibung |
|---|---|
| **Festplattengruppe entfernen** | a Wählen Sie unter „Festplattengruppen“ die zu entfernende Festplattengruppe aus und klicken Sie auf das Symbol **Festplattengruppe entfernen** (  ).<br>b Wählen Sie einen Datenevakuierungsmodus aus. |
| **Ausgewählte Festplatte entfernen** | a Wählen Sie unter „Festplattengruppen“ die Festplattengruppe aus, die das zu entfernende Gerät enthält.<br>b Wählen Sie unter „Festplatten“ das zu entfernende Gerät aus und klicken Sie auf das Symbol **Ausgewählte Festplatte(n) aus der Festplattengruppe entfernen** (  ).<br>c Wählen Sie einen Datenevakuierungsmodus aus. |

Sie können die evakuierten Daten auf eine andere Festplatte oder Festplattengruppe auf demselben Host verschieben.

5 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Die Daten werden aus den ausgewählten Geräten oder einer Festplattengruppe evakuiert und sind nicht mehr für vSAN verfügbar.

## Verwenden von Locator-LEDs

Sie können Locator-LEDs verwenden, um bestimmte Speichergeräte ausfindig zu machen.

vSAN ist in der Lage, Ihnen anhand einer leuchtenden LED am ausgefallenen Gerät dessen Identifizierung zu erleichtern. Dies ist besonders nützlich, wenn Sie mit mehreren Hot-Plug- und Hostauslagerungsszenarien arbeiten.

Sie sollten die Verwendung von E/A-Speicher-Controllern im Passthrough-Modus in Betracht ziehen, weil Controller im RAID 0-Modus zusätzliche Schritte erfordern, um die Erkennung von Locator-LEDs durch die Controller zu ermöglichen.

Informationen zum Konfigurieren von Speicher-Controllern im RAID 0-Modus finden Sie in der Dokumentation Ihres Anbieters.

### Aktivieren und Deaktivieren von Locator-LEDs

Sie können Locator-LEDs auf vSAN-Speichergeräten ein- oder ausschalten. Wenn Sie die Locator-LED einschalten, können Sie den Standort eines bestimmten Speichergeräts ermitteln.

Wenn Sie keine visuelle Warnung zu Ihren vSAN-Geräten mehr benötigen, können Sie die Locator-LEDs auf den ausgewählten Geräten ausschalten.

#### Voraussetzungen

- Vergewissern Sie sich, dass Sie die unterstützten Treiber für Speicher-E/A-Controller installiert haben, die diese Funktion ermöglichen. Informationen zu den von VMware zertifizierten Treibern finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php.
- In einigen Fällen müssen Sie möglicherweise Dienstprogramme von Drittanbietern zum Konfigurieren der Locator-LED-Funktion auf Ihren Speicher-E/A-Controllern verwenden. Wenn Sie z. B. HP verwenden, sollten Sie überprüfen, ob die HP SSA-Befehlszeilenschnittstelle installiert ist.

Informationen zum Installieren von Drittanbieter-VIBs finden Sie in der Dokumentation zum *vSphere-Upgrade*.

#### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie einen Host aus, um die Liste der Geräte anzuzeigen.

5 Wählen Sie unten auf der Seite ein oder mehrere Speichergeräte aus der Liste aus und aktivieren bzw. deaktivieren Sie die Locator-LEDs für die ausgewählten Speichergeräte.

| Option | Aktion |
|---|---|
| **Symbol Locator-LED der ausgewählten Festplatte(n) einschalten** | Aktiviert die Locator-LED des ausgewählten Speichergeräts. Sie können Locator-LEDs über die Registerkarte **Verwalten** aktivieren, indem Sie auf **Speicher > Speichergeräte** klicken. |
| **Symbol Locator-LED der ausgewählten Festplatte(n) ausschalten** | Deaktiviert die Locator-LED des ausgewählten Speichergeräts. Sie können Locator-LEDs über die Registerkarte **Verwalten** deaktivieren, indem Sie auf **Speicher > Speichergeräte** klicken. |

## Markieren von Geräten als Flash-Gerät

Wenn Flash-Geräte von ESXi-Hosts nicht automatisch als Flash-Geräte erkannt werden, können Sie sie manuell als lokale Flash-Geräte markieren.

Dies kann auch geschehen, wenn sie für den RAID 0-Modus anstelle des Passthrough-Modus aktiviert werden. Werden Geräte nicht als lokale Flash-Geräte erkannt, werden sie aus der Liste der für vSAN angebotenen Geräte ausgeschlossen und können nicht im vSAN-Cluster verwendet werden. Wenn diese Geräte als lokale Flash-Geräte markiert werden, stehen sie für vSAN zur Verfügung.

#### Voraussetzungen

- Vergewissern Sie sich, dass das Gerät für Ihren Host lokal ist.

- Stellen Sie sicher, dass das Gerät nicht verwendet wird.
- Stellen Sie sicher, dass die virtuellen Maschinen, die auf das Gerät zugreifen, ausgeschaltet sind und dass der Datenspeicher nicht gemountet ist.

**Vorgehensweise**

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie den Host aus, um die Liste der verfügbaren Geräte anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie mindestens ein Flash-Gerät aus der Liste aus und klicken Sie auf das Symbol **Ausgewählte Festplatte(n) als Flash-Festplatten markieren** (  ).

7 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

Als Festplattentyp der ausgewählten Geräte wird „Flash“ angezeigt.

## Markieren von Geräten als HDD-Geräte

Wenn lokale Magnetfestplatten von ESXi-Hosts nicht automatisch als HDD-Geräte erkannt werden, können Sie sie manuell als lokale HDD-Geräte markieren.

Wenn Sie eine Magnetfestplatte als Flash-Gerät markiert haben, können Sie den Festplattentyp des Geräts ändern, indem Sie es als eine Magnetfestplatte markieren.

**Voraussetzungen**

- Vergewissern Sie sich, dass die Magnetfestplatte für Ihren Host lokal ist.
- Vergewissern Sie sich, dass die Magnetfestplatte leer und nicht in Gebrauch ist.
- Vergewissern Sie sich, dass die virtuellen Maschinen, die auf das Gerät zugreifen, ausgeschaltet sind.

**Vorgehensweise**

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie den Host aus, um die Liste der verfügbaren Magnetfestplatten anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie eine oder mehrere Magnetfestplatten aus der Liste aus und klicken Sie auf das Symbol **Ausgewählte Festplatte(n) als HDD-Festplatten markieren** (  ).

7 Klicken Sie zum Speichern auf **Ja**.

Als Festplattentyp der ausgewählten Magnetfestplatte wird „HDD“ angezeigt.

## Markieren von Geräten als lokal

Wenn Hosts externe SAS-Gehäuse verwenden, ist es möglich, dass vSAN bestimmte Geräte als Remotegeräte betrachtet und diese nicht automatisch als lokale Geräte beansprucht.

In solchen Fällen können Sie die Geräte als lokale Geräte markieren.

#### Voraussetzungen

Stellen Sie sicher, dass das Speichergerät nicht gemeinsam genutzt wird.

#### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum Cluster für vSAN.

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie einen Host aus, um die Liste der Geräte anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie aus der Liste der Geräte ein oder mehrere Remotegeräte aus, die Sie als lokale Geräte markieren möchten, und klicken Sie auf das Symbol **Ausgewählte Festplatte(n) als lokal relativ zum Host markieren** aus.

7 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

## Markieren von Geräten als Remotegeräte

Hosts, die externe SAS-Controller verwenden, können Geräte gemeinsam nutzen. Sie können diese freigegebenen Geräte manuell als Remotegeräte markieren, damit vSAN sie beim Erstellen von Festplattengruppen nicht beansprucht.

In vSAN können Sie keine freigegebenen Geräte zu einer Festplattengruppe hinzufügen.

#### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum Cluster für vSAN.

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie einen Host aus, um die Liste der Geräte anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie die Geräte aus, die Sie als Remotegeräte markieren möchten, und klicken Sie auf das Symbol **Ausgewählte(n) Festplatte(n) als Remote-Festplatten relativ zum Host markieren**.

7 Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

## Hinzufügen eines Kapazitätsgeräts

Sie können einer vorhandenen vSAN-Festplattengruppe ein Kapazitätsgerät hinzufügen.

Sie können ein gemeinsam genutztes Gerät nicht einer Festplattengruppe hinzufügen.

#### Voraussetzungen

Stellen Sie sicher, dass das Gerät formatiert ist und nicht verwendet wird.

#### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie eine Festplattengruppe aus.

5 Klicken Sie unten auf der Seite auf das Symbol **Fügt eine Festplatte zur ausgewählten Festplattengruppe hinzu** (  ).

6 Wählen Sie das Kapazitätsgerät aus, das Sie zur Festplattengruppe hinzufügen möchten.

7 Klicken Sie auf **OK**.

Das Gerät wird zur Festplattengruppe hinzugefügt.

## Entfernen der Partition von Geräten

Sie können Partitionsinformationen von einem Gerät entfernen, sodass vSAN das Gerät zur Verwendung beanspruchen kann.

Wenn Sie ein Gerät hinzugefügt haben, das verbleibende Daten oder Partitionsinformationen enthält, müssen Sie alle bereits vorhandenen Partitionsinformationen vom Gerät entfernen, bevor Sie es zur Verwendung durch vSAN beanspruchen können. VMware empfiehlt das Hinzufügen von bereinigten Geräten zu Festplattengruppen.

Wenn Sie Partitionsinformationen von einem Gerät entfernen, löscht vSAN die primäre Partition, die Informationen zum Festplattenformat und logische Partitionen vom Gerät enthält.

### Voraussetzungen

Vergewissern Sie sich, dass das Gerät nicht von ESXi als Startfestplatte, VMFS-Datenspeicher oder vSAN verwendet wird.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie einen Host aus, um die Liste der verfügbaren Geräte anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht geeignet** aus.

6 Wählen Sie ein Gerät aus der Liste aus und klicken Sie auf das Symbol **Partitionen auf den ausgewählten Festplatten löschen** (  ) aus.

7 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Das Gerät ist bereinigt und enthält keine Partitionsinformationen mehr.

# Erweitern und Verwalten eines vSAN -Clusters

11

Nachdem Sie den vSAN-Cluster eingerichtet haben, können Sie mit dem vSphere Web Client Hosts und Kapazitätsgeräte hinzufügen, Hosts und Geräte entfernen sowie Fehlerszenarien verwalten.

Dieses Kapitel behandelt die folgenden Themen:



## Erweitern eines vSAN -Clusters

Sie können einen vorhandenen vSAN-Cluster erweitern, indem Sie Hosts hinzufügen oder den Hosts Geräte hinzufügen, ohne laufende Vorgänge unterbrechen zu müssen.

Erweitern Sie Ihren Cluster für vSAN mit einer der folgenden Methoden.

- Fügen Sie dem Cluster mithilfe der unterstützten Cache- und Kapazitätsgeräte konfigurierte neue ESXi-Hosts hinzu. Siehe „Hinzufügen eines Hosts zu einem vSAN-Cluster“, auf Seite 122. Wenn Sie ein Gerät oder einen Host mit Kapazität hinzufügen, verteilt vSAN nicht automatisch Daten an das neu hinzugefügte Gerät. Um vSAN für Verteilung von Daten auf kürzlich hinzugefügte Geräte zu aktivieren, müssen Sie den Cluster unter Verwendung von Ruby vSphere Console (RVC) manuell neu verteilen. Siehe „Manuelle Neuverteilung“, auf Seite 160.
- Verschieben Sie vorhandene ESXi-Hosts mithilfe eines Hostprofils in den vSAN-Cluster. Siehe „Konfigurieren von Hosts mit dem Hostprofil“, auf Seite 123. Neue Clustermitglieder fügen Speicher- und Rechenkapazität hinzu. Sie müssen manuell eine Teilmenge von Festplattengruppen erstellen, die die lokalen Kapazitätsgeräte des neu hinzugefügten Hosts enthalten. Siehe „Erstellen einer Festplattengruppe auf einem vSAN-Host“, auf Seite 112.

  Stellen Sie sicher, dass die Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller, die Sie verwenden möchten, zertifiziert und im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind. Stellen Sie beim Hinzufügen von Kapazitätsgeräten sicher, dass die Geräte nicht formatiert und nicht partitioniert sind, damit vSAN die Geräte erkennen und beanspruchen kann.
- Fügen Sie den ESXi-Hosts, die Clustermitglieder sind, neue Kapazitätsgeräte hinzu. Sie müssen das Gerät manuell zur Datenträgergruppe auf dem Host hinzufügen. Siehe „Hinzufügen von Geräten zu einer Festplattengruppe“, auf Seite 114.

## Erweitern der vSAN -Clusterkapazität und -leistung

Wenn in Ihrem vSAN-Cluster nicht genügend Speicherkapazität vorhanden ist oder wenn Sie eine Leistungsbeeinträchtigung des Clusters feststellen, können Sie die Kapazität und die Leistung des Clusters erweitern.

- Erweitern Sie die Speicherkapazität Ihres Clusters durch Hinzufügen von Speichergeräten zu vorhandenen Festplattengruppen oder durch Erstellen einer neuen Festplattengruppe. Für neue Festplattengruppen sind Flash-Geräte für den Cache erforderlich. Informationen zum Hinzufügen von Geräten zu Festplattengruppen finden Sie unter „Hinzufügen von Geräten zu einer Festplattengruppe“, auf Seite 114. Durch das Hinzufügen von Kapazitätsgeräten ohne Erhöhung des Caches wird möglicherweise das Verhältnis von Cache und Kapazität auf ein nicht unterstütztes Maß reduziert. Siehe „Design-Überlegungen für Flash-Caching-Geräte in vSAN“, auf Seite 24.
- Verbessern Sie die Clusterleistung, indem Sie mindestens ein Flash-Cache-Gerät und ein Kapazitätsgerät (Flash- oder Magnetfestplatte) zu einem vorhandenen Speicher-E/A-Controller oder zu einem neuen Server-Host hinzufügen. Sie können einen oder mehrere Server mit zusätzlichen Festplattengruppen hinzufügen, was dieselbe Auswirkung auf die Leistung hat, nachdem vSAN eine proaktive Neuverteilung im vSAN-Cluster durchgeführt hat.

Reine Computing-Hosts können zwar in einer vSAN-Umgebung vorhanden sein und Kapazität von anderen Hosts im Cluster belegen, für einen reibungslosen Ablauf sollten Sie aber einheitlich konfigurierte Hosts hinzufügen.

Für optimale Ergebnisse sollten Sie mit Cache- und Kapazitätsgeräten konfigurierte Hosts hinzufügen. Informationen zum Hinzufügen von Geräten zu Festplattengruppen finden Sie unter „Hinzufügen von Geräten zu einer Festplattengruppe“, auf Seite 114.

## Hinzufügen eines Hosts zu einem vSAN -Cluster

Sie können einen ESXi-Host zu einem ausgeführten vSAN-Cluster ohne Unterbrechungen laufender Vorgänge hinzufügen. Die Ressourcen des Hosts werden dem Cluster zugeordnet.

### Voraussetzungen

- Stellen Sie sicher, dass die Ressourcen, einschließlich Treiber, Firmware und Speicher-E/A-Controller, im VMware-Kompatibilitätshandbuchs unter http://www.vmware.com/resources/compatibility/search.php aufgeführt sind.
- VMware empfiehlt die Erstellung einheitlich konfigurierter Hosts im vSAN-Cluster, um eine gleichmäßige Verteilung von Komponenten und Objekten über die Geräte im Cluster zu erreichen. Es kann jedoch Situationen geben, in denen es in einem Cluster zu einer ungleichmäßigen Verteilung kommt, insbesondere während der Wartung oder bei einem Overcommit der Kapazität des vSAN-Datenspeichers mit übermäßig vielen VM-Bereitstellungen.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Host hinzufügen**.
3. Geben Sie den Hostnamen oder die IP-Adresse ein und klicken Sie auf **Weiter**.
4. Geben Sie den Benutzernamen und das Kennwort für den Host ein und klicken Sie auf **Weiter**.
5. Zeigen Sie die Informationsübersicht an, und klicken Sie auf **Weiter**.
6. Weisen Sie einen Lizenzschlüssel zu und klicken Sie auf **Weiter**.

7 (Optional) Aktivieren Sie einen Sperrmodus, um zu verhindern, dass sich Remotebenutzer direkt beim Host anmelden.

Sie können diese Option später konfigurieren, indem Sie das Sicherheitsprofil in den Hosteinstellungen bearbeiten.

8 Geben Sie die weitere Verfahrensweise mit den virtuellen Maschinen und Ressourcenpools des Hosts an.

- **Alle virtuellen Maschinen dieses Hosts im Root-Ressourcenpool des Clusters platzieren**

  vCenter Server entfernt alle vorhandenen Ressourcenpools des Hosts. Die virtuellen Maschinen in der Hierarchie des Hosts werden alle Root zugeordnet. Anteilige Zuordnungen sind relativ zu einem Ressourcenpool. Sie müssen daher die Freigaben einer virtuellen Maschine möglicherweise ändern. Diese Änderung zerstört die Hierarchie des Ressourcenpools.

- **Einen Ressourcenpool für die virtuellen Maschinen und Ressourcenpools dieses Hosts erstellen**

  vCenter Server erstellt einen Ressourcenpool auf oberster Ebene, der zu einem dem Cluster direkt untergeordneten Element wird, und fügt alle untergeordneten Elemente des Hosts zu diesem neuen Ressourcenpool hinzu. Sie können einen Namen für den neuen Ressourcenpool auf oberster Ebene eingeben. Der Standard ist **Übertragen von <host_name>**.

9 Überprüfen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.

Der Host wurde zum Cluster hinzugefügt.

## Konfigurieren von Hosts mit dem Hostprofil

Wenn mehrere Hosts im vSAN-Cluster vorhanden sind, können Sie das Profil eines vorhandenen vSAN-Hosts wiederverwenden und dessen Profileinstellungen auf die restlichen Hosts im vSAN-Cluster anwenden.

Das Hostprofil enthält Informationen über die Speicherkonfiguration, die Netzwerkkonfiguration oder andere Hostmerkmale. Wenn Sie einen Cluster mit einer großen Anzahl von Hosts (z. B. 8, 16, 32 oder 64 Hosts) erstellen möchten, verwenden Sie die Hostprofilfunktion, um jeweils mehr als einen Host zum vSAN-Cluster hinzuzufügen.

### Voraussetzungen

- Stellen Sie sicher, dass sich der Host im Wartungsmodus befindet.
- Stellen Sie sicher, dass die Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind.

### Vorgehensweise

1 Erstellen Sie ein Hostprofil.

a Navigieren Sie zur Ansicht „Hostprofile“.

b Klicken Sie auf das Symbol **Profil vom Host extrahieren** ( ✚ ).

c Wählen Sie den Host aus, den Sie als Referenzhost verwenden möchten, und klicken Sie auf **Weiter**.

Der ausgewählte Host muss ein aktiver Host sein.

d Geben Sie einen Namen und eine Beschreibung für das neue Profil ein und klicken Sie auf **Weiter**.

e Überprüfen Sie die Zusammenfassung für das neue Hostprofil und klicken Sie auf **Beenden**.

Das neue Profil wird in der Liste „Hostprofile“ angezeigt.

2 Hängen Sie den Host an das gewünschte Hostprofil an.

   a Wählen Sie in der Profilliste in der Ansicht „Hostprofile“ das Hostprofil aus, das Sie für den vSAN-Host übernehmen möchten.

   b Klicken Sie auf das Symbol **Hosts und Cluster an ein Hostprofil anhängen bzw. davon trennen** ( ).

   c Wählen Sie den Host aus der erweiterten Liste aus und klicken Sie auf **Anhängen**, um den Host an das Profil anzuhängen.

      Der Host wird zur Liste der verbundenen Elemente hinzugefügt.

   d Klicken Sie auf **Weiter**.

   e Klicken Sie auf **Beenden**, um das Trennen des Hosts vom Profil abzuschließen.

3 Trennen Sie den referenzierten vSAN-Host vom Hostprofil.

   Wenn ein Hostprofil an einen Cluster angehängt wird, wird den Hosts in diesem Cluster ebenfalls das Hostprofil zugewiesen. Wenn das Hostprofil allerdings vom Cluster getrennt wird, bleibt die Verknüpfung zwischen dem Host bzw. den Hosts im Cluster und dem des Hostprofils bestehen.

   a Wählen Sie in der Profilliste in der Ansicht „Hostprofile“ das Hostprofil aus, das Sie von einem Host oder Cluster trennen möchten.

   b Klicken Sie auf das Symbol **Hosts und Cluster an ein Hostprofil anhängen bzw. davon trennen** ( ).

   c Wählen Sie den Host oder Cluster in der erweiterten Liste aus und klicken Sie auf **Trennen**.

   d Klicken Sie auf **Alle trennen**, um alle aufgelisteten Hosts und Cluster vom Profil zu trennen.

   e Klicken Sie auf **Weiter**.

   f Klicken Sie auf **Beenden**, um das Trennen des Hosts vom Hostprofil abzuschließen.

4 Überprüfen Sie die Übereinstimmung des vSAN-Hosts mit dem angehängten Hostprofil und bestimmen Sie, ob es Konfigurationsparameter auf dem Host gibt, die sich von den im Hostprofil angegebenen Konfigurationsparametern unterscheiden.

   a Navigieren Sie zu einem Hostprofil.

      Auf der Registerkarte **Objekte** werden alle Hostprofile, die Anzahl der an dieses Hostprofil angehängten Hosts sowie eine Zusammenfassung der Ergebnisse der letzten Übereinstimmungsüberprüfung angezeigt.

   b Klicken Sie auf das Symbol **Hostprofil-Übereinstimmung überprüfen** ( ).

      Wenn Sie bestimmte Details zu den Parametern anzeigen möchten, die zwischen dem Host, bei dem eine Nichtübereinstimmung gefunden wurde, und dem Hostprofil voneinander abweichen, klicken Sie auf die Registerkarte **Überwachen** und wählen Sie die Übereinstimmungsansicht aus. Erweitern Sie die Objekthierarchie und wählen Sie den nicht übereinstimmenden Host aus. Die abweichenden Parameter werden in der Übereinstimmungsansicht unterhalb der Hierarchie angezeigt.

      Verwenden Sie bei einem Übereinstimmungsfehler die Standardisierungsaktion, um die Hostprofileinstellungen auf den Host anzuwenden. Dabei werden alle vom Hostprofil verwalteten Parameter in die in dem Hostprofil vorhandenen Werte geändert, das dem Host zugeordnet ist.

c Wenn Sie bestimmte Details zu den Parametern anzeigen möchten, die zwischen dem Host, bei dem eine Nichtübereinstimmung gefunden wurde, und dem Hostprofil voneinander abweichen, klicken Sie auf die Registerkarte **Überwachen** und wählen Sie die Übereinstimmungsansicht aus.

d Erweitern Sie die Objekthierarchie und wählen Sie den fehlerhaften Host aus.

Die abweichenden Parameter werden in der Übereinstimmungsansicht unterhalb der Hierarchie angezeigt.

5 Standardisieren Sie den Host, um Übereinstimmungsfehler auf dem Host zu beheben.

a Wählen Sie die Registerkarte **Überwachen** aus und klicken Sie auf **Übereinstimmung**.

b Klicken Sie mit der rechten Maustaste auf den Host bzw. die Hosts, den bzw. die Sie standardisieren möchten, und wählen Sie **Alle vCenter-Aktionen > Hostprofile > Standardisieren** aus.

Sie können die Benutzereingabeparameter für die Hostprofil-Richtlinien aktualisieren oder ändern, indem Sie den Host anpassen.

c Klicken Sie auf **Weiter**.

d Überprüfen Sie die erforderlichen Aufgaben, um das Hostprofil zu standardisieren, und klicken Sie auf **Beenden**.

Der Host ist Teil des vSAN-Clusters, und seine Ressourcen sind für den vSAN-Cluster zugänglich. Der Host kann auch auf alle vorhandenen Speicher-E/A-Richtlinien von vSAN im vSAN-Cluster zugreifen.

## Arbeiten mit dem Wartungsmodus

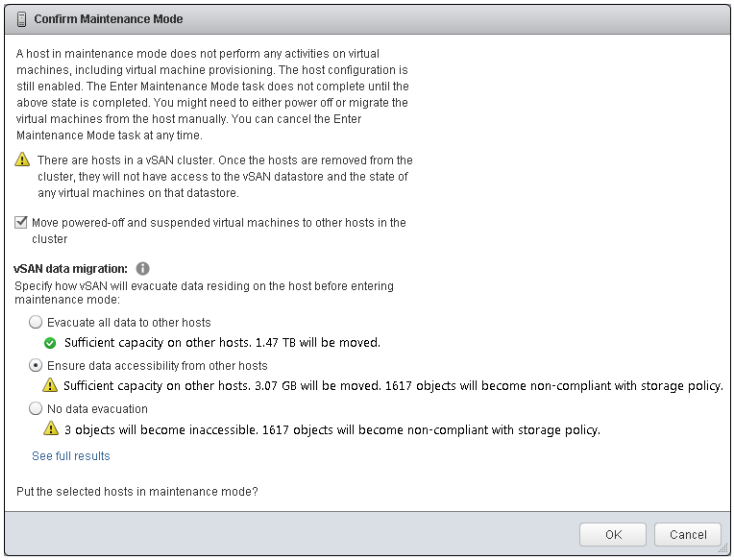
Bevor Sie einen Host, der zu einem Cluster für vSAN gehört, herunterfahren, neu starten oder trennen, müssen Sie den Host in den Wartungsmodus versetzen.

Wenn Sie mit dem Wartungsmodus arbeiten, beachten Sie folgende Einschränkungen:

- Wenn Sie einen ESXi-Host in den Wartungsmodus versetzen, müssen Sie einen Datenevakuierungsmodus auswählen, z. B. **Möglichkeit des Datenzugriffs auf anderen Hosts sicherstellen** oder **Alle Daten auf andere Hosts evakuieren**.
- Wenn ein beliebiger Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, wird die Clusterkapazität automatisch reduziert, weil der Speicher des Mitgliedshosts im Cluster nicht mehr bereitsteht.
- Die Rechenressourcen einer virtuellen Maschine befinden sich möglicherweise nicht auf dem Host, der in den Wartungsmodus versetzt wird, und der Speicher für virtuelle Maschinen kann sich an beliebiger Stelle im Cluster befinden.
- Der Modus **Datenzugriff sicherstellen** ist schneller als der Modus **Alle Daten evakuieren**, weil der Modus **Datenzugriff sicherstellen** nur die Komponenten von den Hosts migriert, die entscheidend für die Ausführung der virtuellen Maschinen sind. Wenn in diesem Modus ein Fehler auftritt, ist die Verfügbarkeit Ihrer virtuellen Maschine davon betroffen. Durch Auswählen des Modus **Datenzugriff sicherstellen** werden Ihre Daten bei einem Ausfall nicht neu geschützt und eventuell tritt ein unerwarteter Datenverlust auf.
- Wenn Sie den Modus **Alle Daten evakuieren** auswählen, werden Ihre Daten automatisch neu vor einem Ausfall geschützt, wenn Ressourcen verfügbar sind und für **Primäre Ebene von zu tolerierenden Fehlern** der Wert 1 oder höher festgelegt wurde. In diesem Modus werden alle Komponenten vom Host migriert und je nach der Menge der Daten auf dem Host kann die Migration länger dauern. Im Modus **Alle Daten evakuieren** können Ihre virtuellen Maschinen Ausfälle tolerieren, selbst während einer geplanten Wartung.
- Wenn Sie einen Cluster mit drei Hosts verwenden, können Sie einen Server nicht mit **Alle Daten evakuieren** in den Wartungsmodus versetzen. Sie sollten einen Cluster mit vier oder mehr Hosts für maximale Verfügbarkeit erstellen.

Vor dem Versetzen eines Hosts in den Wartungsmodus müssen Sie Folgendes prüfen:

- Wenn Sie den Modus **Alle Daten evakuieren** verwenden, stellen Sie sicher, dass Sie über genügend Hosts und verfügbare Kapazität im Cluster verfügen, um die Anforderungen der Richtlinie **Primäre Ebene von zu tolerierenden Fehlern** zu erfüllen.
- Stellen Sie sicher, dass die restlichen Hosts genug Flash-Kapazität zur Verarbeitung von Flash Read Cache-Reservierungen haben. Sie können den RVC-Befehl `vsan.whatif_host_failures` ausführen, um die aktuelle Kapazitätsnutzung pro Host zu analysieren. Diese Informationen können dabei helfen, zu ermitteln, ob der Ausfall eines einzelnen Hosts dazu führen kann, dass der Cluster keinen freien Speicherplatz mehr hat, und ob sich der Ausfall auf die Clusterkapazität, die Cache-Reservierung und die Clusterkomponenten auswirken kann. Informationen zu den RVC-Befehlen finden Sie im *Referenzhandbuch zu RVC-Befehlen*.
- Stellen Sie sicher, dass Sie genug Kapazitätsgeräte in den verbleibenden Hosts haben, um Richtlinienanforderungen in Bezug auf Stripe-Breite erfüllen zu können, falls ausgewählt.
- Stellen Sie sicher, dass auf den restlichen Hosts genug freie Kapazität verfügbar ist, um die Menge der Daten verarbeiten zu können, die von dem in den Wartungsmodus wechselnden Host migriert werden müssen.




Das Dialogfeld „Wartungsmodus bestätigen“ bietet Informationen hinsichtlich Ihrer Wartungsaktivitäten. Sie können die Auswirkungen einer jeden Datenevakuierungsoption anzeigen.

- Ob es ausreichend Kapazität gibt, um den Vorgang durchzuführen.
- Der Umfang der Daten, der verschoben wird.
- Die Anzahl der Objekte, die dann nicht mehr übereinstimmen.
- Die Anzahl der Objekte, auf die kein Zugriff mehr möglich wird.

## Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus

Bevor Sie einen Host, der zu einem vSAN-Cluster gehört, herunterfahren, neu starten oder trennen, müssen Sie den Host in den Wartungsmodus versetzen. Wenn Sie einen Host in den Wartungsmodus versetzen, müssen Sie einen Datenevakuierungsmodus auswählen, z. B. **Möglichkeit des Datenzugriffs auf anderen Hosts sicherstellen** oder **Alle Daten auf andere Hosts evakuieren**.

Die Clusterkapazität wird automatisch reduziert, wenn ein Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, weil die Kapazität des Mitgliedshosts im Cluster nicht mehr bereitsteht.

### Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung die für die gewählte Option erforderlichen Funktionen aufweist.

### Vorgehensweise

1 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus > In den Wartungsmodus wechseln** aus.

2 Wählen Sie einen Datenevakuierungsmodus aus und klicken Sie auf **OK**.

| Option | Beschreibung |
|---|---|
| **Möglichkeit des Datenzugriffs auf anderen Hosts sicherstellen** | Dies ist die Standardoption. Wenn Sie den Host ausschalten oder ihn aus dem Cluster entfernen, stellt vSAN sicher, dass auch weiterhin der Zugriff auf alle virtuellen Maschinen auf diesem Host möglich ist. Wählen Sie diese Option aus, wenn Sie den Host vorübergehend aus dem Cluster entfernen möchten, beispielsweise um Upgrades zu installieren, und den Host wieder zum Cluster hinzufügen möchten. Diese Option ist nicht geeignet, wenn Sie den Host dauerhaft aus dem Cluster entfernen möchten.<br>In der Regel muss nur ein Teil der Daten verlagert werden. Die virtuelle Maschine ist jedoch möglicherweise während der Verlagerung nicht mehr vollständig mit einer VM-Speicherrichtlinie kompatibel. Dies bedeutet, dass sie möglicherweise keinen Zugriff auf alle Replikate hat. Wenn ein Fehler auftritt, während sich der Host im Wartungsmodus befindet und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt ist, können im Cluster Datenverluste auftreten.<br>**Hinweis** Dies ist der einzig verfügbare Evakuierungsmodus, wenn Sie einen Cluster mit drei Hosts oder einen vSAN-Cluster mit drei konfigurierten Fault Domains verwenden. |
| **Alle Daten auf andere Hosts evakuieren** | vSAN verlagert alle Daten an andere Hosts im Cluster, bewahrt die Verfügbarkeitsübereinstimmung für alle betroffenen Komponenten im Cluster auf bzw. behebt diese und schützt die Daten, wenn ausreichend Ressourcen im Cluster vorhanden sind. Wählen Sie diese Option aus, wenn Sie den Host dauerhaft migrieren möchten. Wenn Sie Daten vom letzten Host im Cluster verlagern, stellen Sie sicher, dass Sie die virtuellen Maschinen an einen anderen Datenspeicher migrieren und dann den Host in den Wartungsmodus versetzen.<br>Dieser Evakuierungsmodus führt zur größten Menge an Datenübertragungen und verbraucht die meiste Zeit und die meisten Ressourcen. Alle Komponenten im lokalen Speicher des ausgewählten Hosts werden anderswo im Cluster migriert. Wenn der Host dann in den Wartungsmodus wechselt, haben alle virtuellen Maschinen Zugriff auf die Speicherkomponenten und sind weiterhin mit den zugewiesenen Speicherrichtlinien kompatibel.<br>**Hinweis** Der Host kann nicht in den Wartungsmodus wechseln, falls kein Zugriff auf ein VM-Objekt, das Daten auf dem Host aufweist, möglich ist, und die vollständige Evakuierung wird nicht durchgeführt. |
| **Keine Evakuierung der Daten** | vSAN verlagert keine Daten von diesem Host. Wenn Sie den Host ausschalten oder ihn aus dem Cluster entfernen, kann möglicherweise auf manche virtuelle Maschinen nicht mehr zugegriffen werden. |

Für einen Cluster mit drei Fault Domains gelten dieselben Beschränkungen wie für einen Cluster mit drei Hosts, z. B. dass der Modus **Alle Daten evakuieren** nicht verwendet werden kann oder dass Daten nach einem Fehler erneut geschützt werden müssen.

### Weiter

Den Fortschritt der Datenmigration im Cluster können Sie nachverfolgen. Siehe „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“, auf Seite 150.

# Verwalten von Fault Domains in vSAN -Clustern

Wenn sich Ihr Cluster für vSAN über mehrere Racks oder Blade-Server-Gestelle in einem Datencenter erstreckt und Sie sicherstellen möchten, dass Ihre Hosts vor Rack- oder Gestellversagen geschützt sind, können Sie Fault Domains erstellen und jeder Fault Domain einen oder mehrere Hosts hinzufügen.

Eine Fault Domain besteht aus einem oder mehreren vSAN-Hosts, die entsprechend ihrem physischen Speicherort im Datencenter zusammengefasst sind. Nach dem Konfigurieren versetzen Fault Domains vSAN in die Lage, Ausfälle eines ganzen physischen Racks sowie Ausfälle eines Einzelhosts, Kapazitätsgeräts, Netzwerklinks oder eines Netzwerk-Switches, der speziell für eine Fault Domain vorgesehen ist, zu tolerieren.

Die Richtlinie **Primäre Ebene von zu tolerierenden Fehlern** für den Cluster hängt von der Anzahl der Ausfälle ab, die eine virtuelle Maschine tolerieren kann. Beispiel: Wenn **Primäre Ebene von zu tolerierenden Fehlern** für eine virtuelle Maschine auf 1 `(PFTT = 1)` festgelegt und diese zur Verwendung mehrerer Fault Domains konfiguriert ist, kann vSAN einen einzelnen Ausfall beliebiger Art einer beliebigen Komponente in einer Fault Domain tolerieren, einschließlich des Ausfalls eines ganzen Racks.

Wenn Sie Fault Domains auf einem Rack konfigurieren und eine neue virtuelle Maschine bereitstellen, stellt vSAN sicher, dass Schutzobjekte wie Replikate und Zeugen in verschiedenen Fault Domains platziert werden. Beispiel: Wenn in der Speicherrichtlinie einer virtuellen Maschine **Primäre Ebene von zu tolerierenden Fehlern** auf N `(PFTT = n)` festgelegt ist, benötigt vSAN mindestens `2*n+1` Fault Domains im Cluster. Wenn virtuelle Maschinen in einem Cluster mit Fault Domains und dieser Richtlinie bereitgestellt sind, werden die Kopien der damit verknüpften VM-Objekte auf verschiedenen Racks gespeichert.

Es werden mindestens drei Fault Domains benötigt. Konfigurieren Sie vier oder mehr Fault Domains im Cluster, um optimale Ergebnisse zu erhalten. Für einen Cluster mit drei Fault Domains gelten dieselben Einschränkungen wie für einen Cluster mit drei Hosts, wie z. B. die Unmöglichkeit, Daten nach einem Ausfall neu zu schützen oder den Modus **Vollständige Datenmigration** zu verwenden. Informationen zum Entwerfen und Dimensionieren von Fault Domains finden Sie unter „Entwerfen und Dimensionieren von vSAN-Fault Domains“, auf Seite 33.

Betrachten Sie ein Szenario mit einem vSAN-Cluster mit 16 Hosts. Die Hosts verteilen sich auf 4 Racks, das heißt 4 Hosts pro Rack. Zum Tolerieren eines Ausfalls eines ganzen Racks sollten Sie eine Fault Domain für jedes Rack erstellen. Ein Cluster einer solchen Kapazität kann durch Festlegen der Option **Primäre Ebene von zu tolerierenden Fehlern** auf 1 konfiguriert werden. Wenn Sie den Cluster so konfigurieren möchten, dass virtuelle Maschinen ermöglicht werden, für die **Primäre Ebene von zu tolerierenden Fehlern** auf 2 festgelegt ist, sollten Sie fünf Fehlerdomänen in einem Cluster konfigurieren.

Wenn ein Rack ausfällt, ist keine Ressource (CPU, Speicher usw.) mehr im Rack für den Cluster verfügbar. Um die Auswirkungen eines möglichen Rackausfalls zu verringern, sollten Sie kleinere Fault Domains konfigurieren. Damit erhöht sich die Gesamtmenge der Ressourcenverfügbarkeit im Cluster nach einem Rackausfall.

Befolgen Sie diese empfohlenen Vorgehensweisen beim Arbeiten mit Fault Domains.

- Konfigurieren Sie mindestens drei Fault Domains im vSAN-Cluster. Konfigurieren Sie vier oder mehr Fault Domains, um optimale Ergebnisse zu erhalten.
- Bei einem Host, der zu keiner Fault Domain gehört, wird davon ausgegangen, dass dieser sich in seiner eigenen Fault Domain mit einem Host befindet.
- Sie brauchen nicht jeden vSAN-Host einer Fault Domain zuzuweisen. Wenn Sie Fault Domains zum Schützen der vSAN-Umgebung verwenden möchten, sollten Sie gleich große Fault Domains erstellen.
- Die Zuweisungen zu Fault Domains bleiben für vSAN-Hosts, die in einen anderen Cluster verschoben werden, erhalten.
- Es wird empfohlen, beim Entwerfen von Fault Domains diese mit derselben Anzahl von Hosts zu konfigurieren.

Anweisungen zum Entwerfen von Fault Domains finden Sie unter „Entwerfen und Dimensionieren von vSAN-Fault Domains“, auf Seite 33.

- Sie können einer Fault Domain beliebig viele Hosts hinzufügen. Jede Fault Domain muss mindestens einen Host beinhalten.

## Erstellen einer neuen Fault Domain im vSAN -Cluster

Um bei einem Rackausfall die Funktionsfähigkeit der VM-Objekte sicherzustellen, können Sie Hosts in verschiedenen Fault Domains gruppieren.

Wenn Sie eine virtuelle Maschine auf dem Cluster mit Fault Domains bereitstellen, verteilt vSAN Schutzkomponenten wie Zeugen und Repliken der VM-Objekte auf verschiedene Fault Domains. Folglich kann die vSAN-Umgebung komplette Rackausfälle neben dem Ausfall eines einzelnen Hosts, einer Speicherfestplatte oder des Netzwerks tolerieren.

### Voraussetzungen

- Wählen Sie einen eindeutigen Namen für die Fault Domain aus. In vSAN können Fault Domain-Namen in einem Cluster nicht mehrmals verwendet werden.
- Prüfen Sie die Version Ihrer ESXi-Hosts. Sie können in Fault Domains nur Hosts der Version 6.0 oder höher einbeziehen.
- Stellen Sie sicher, dass Ihre vSAN-Hosts online sind. Sie können Hosts keiner Fault Domain zuweisen, die offline oder aufgrund eines Hardwarekonfigurationsproblems nicht verfügbar ist.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.
4. Klicken Sie auf das Symbol **Neue Fault Domain erstellen** (  ).
5. Geben Sie den Namen der Fault Domain ein.
6. Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Hosts nicht in Fault Domain** zum Anzeigen der Liste der Hosts aus, die keiner Fault Domain zugewiesen sind, oder wählen Sie **Alle Hosts anzeigen** zum Anzeigen aller Hosts im Cluster aus.
7. Wählen Sie mindestens einen Host zum Hinzufügen zur Fault Domain aus.

   Eine Fault Domain darf nicht leer sein. Sie müssen mindestens einen Host für die Fault Domain auswählen.
8. Klicken Sie auf **OK.**

   Die ausgewählten Hosts werden in der Fault Domain angezeigt.

## Verschieben von Hosts in eine ausgewählte Fault Domain

Sie können einen Host in eine ausgewählte Fault Domain im vSAN-Cluster verschieben.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Wählen Sie die Fault Domain aus und klicken Sie auf das Symbol **Hosts in ausgewählte Fault Domain verschieben** (  ).

5 Wählen Sie aus dem Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Hosts nicht in Fault Domain** aus, um die verfügbaren Hosts anzuzeigen, die zu Fault Domains hinzugefügt werden können, oder wählen Sie **Alle Hosts anzeigen** aus, um alle Hosts im Cluster anzuzeigen.

6 Wählen Sie den Host aus, den Sie zur Fault Domain hinzufügen möchten.

7 Klicken Sie auf **OK**.

Der ausgewählte Host wird in der Fault Domain angezeigt.

## Verschieben von Hosts in eine vorhandene Fault Domain

Sie können einen Host in eine vorhandene Fault Domain im vSAN-Cluster verschieben.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Wählen Sie mindestens einen Host aus und klicken Sie auf das Symbol **Hosts in Fault Domain verschieben** (  ).

5 Wählen Sie eine Fault Domain aus und klicken Sie auf **OK**.

Jede Fault Domain muss mindestens einen Host beinhalten. Falls der Host, den Sie verschieben, der einzige Host in der Fault Domain-Quellinstanz ist, löscht vSAN die leere Fault Domain im Cluster.

## Verschieben von Hosts aus einer Fault Domain

Je nach Ihren Anforderungen können Sie Hosts aus einer Fault Domain verschieben.

### Voraussetzungen

Stellen Sie sicher, dass der Host online ist. Sie können keine Hosts verschieben, die offline sind oder auf die von einer Fault Domain aus nicht zugegriffen werden kann.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Wählen Sie den zu verschiebenden Host aus und klicken Sie auf das Symbol **Hosts aus Fault Domain verschieben** (  ).

5 Klicken Sie auf **Ja**.

Der ausgewählte Host ist nicht mehr Teil einer Fault Domain. Jeder Host, der nicht Teil einer Fault Domain ist, wird als in einer eigenen Einzelhost-Fault Domain vorhanden betrachtet.

### Weiter

Sie können Hosts zu Fault Domains hinzufügen. Siehe „Verschieben von Hosts in eine vorhandene Fault Domain“, auf Seite 130.

## Umbenennen einer Fault Domain

Sie können den Name einer vorhandenen Fault Domain in Ihrem vSAN-Cluster ändern.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Wählen Sie die Fault Domain aus, die Sie umbenennen möchten, und klicken Sie auf das Symbol **Ausgewählte Fault Domain umbenennen** (  ).

5 Geben Sie einen neuen Fault Domain-Namen ein.

6 Klicken Sie auf **OK.**

Der neue Name wird in der Liste der Fault Domains angezeigt.

## Entfernen ausgewählter Fault Domains

Wenn Sie keine Fault Domain mehr brauchen, können Sie sie aus dem vSAN-Cluster entfernen.

### Vorgehensweise

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

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen und ausgeweiteter Cluster**.

4 Wählen Sie die zu löschende Fault Domain aus und klicken Sie auf das Symbol **Ausgewählte Fault Domains entfernen** (  ).

5 Klicken Sie auf **Ja**.

Alle Hosts in der Fault Domain werden entfernt und die ausgewählte Fault Domain wird im vSAN-Cluster gelöscht. Jeder Host, der nicht Teil einer Fault Domain ist, wird als in einer eigenen Einzelhost-Fault Domain vorhanden betrachtet.

# Verwenden des vSAN -iSCSI-Zieldiensts

Mit dem iSCSI-Zieldienst können Sie Hosts und physische Arbeitslasten aktivieren, die außerhalb des vSAN-Clusters liegen, um auf den vSAN-Datenspeicher zuzugreifen.

Diese Funktion aktiviert einen iSCSI-Initiator auf einem Remotehost, um Blockebenendaten an ein iSCSI-Ziel auf einem Speichergerät im vSAN-Cluster zu übertragen.

Nachdem Sie den vSAN-iSCSI-Zieldienst konfiguriert haben, können Sie die vSAN-iSCSI-Ziele über einen ortsfernen Host ermitteln. Um vSAN-iSCSI-Ziele zu ermitteln, verwenden Sie die IP-Adresse eines beliebigen Hosts im vSAN-Cluster und den TCP-Port des iSCSI-Ziels. Um Hochverfügbarkeit des vSAN-iSCSI-Ziels sicherzustellen, konfigurieren Sie die MultiPath-Unterstützung für Ihre iSCSI-Anwendung. Sie können die IP-Adressen von zwei oder mehreren Hosts verwenden, um den MultiPath zu konfigurieren.

**Hinweis** Der vSAN iSCSI-Zieldienst unterstützt keine anderen vSphere- oder ESXi-Clients oder -Initiatoren, Hypervisoren von Drittanbietern oder Migrationen mit RDMs (Raw Device Mapping).

Der vSAN-iSCSI-Zieldienst unterstützt die folgenden CHAP-Authentifizierungsmethoden:

| | |
|---|---|
| **CHAP** | Bei der CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel. |
| **Beiderseitiges CHAP** | Bei der beidseitigen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels. |

## iSCSI-Ziele

Sie können ein oder mehrere iSCSI-Ziele hinzufügen, um Speicherblöcke als logische Einheitsnummern (LUNs) bereitzustellen. vSAN identifiziert jedes iSCSI-Ziel durch einen eindeutigen qualifizierten iSCSI-Namen (IQN). Sie können den IQN verwenden, um das iSCSI-Ziel bei einem ortsfernen iSCSI-Initiator vorzulegen, sodass der Initiator auf die LUN des Ziels zugreifen kann.

Jedes iSCSI-Ziel enthält eine oder mehrere LUNs. Sie legen die Größe jeder LUN fest, weisen jeder LUN eine vSAN-Speicherrichtlinie zu und aktivieren den iSCSI-Zieldienst auf einem vSAN-Cluster. Sie können eine Speicherrichtlinie konfigurieren, um diese als Standardrichtlinie für das Startobjekt des vSAN-iSCSI-Zieldienstes zu verwenden.

## iSCSI-Initiatorgruppen

Sie können eine Gruppe von iSCSI-Initiatoren definieren, die Zugriff auf ein bestimmtes iSCSI-Ziel haben. Die iSCSI-Initiatorgruppe beschränkt den Zugriff nur auf solche Initiatoren, die auch Mitglieder der Gruppe sind. Falls Sie keinen iSCSI-Initiator oder keine Initiatorgruppe definieren, haben alle iSCSI-Initiatoren Zugriff auf jedes Ziel.

Ein eindeutiger Name identifiziert jede iSCSI-Initiatorgruppe. Sie können einen oder mehrere iSCSI-Initiatoren als Mitglieder der Gruppe hinzufügen. Verwenden Sie den IQN des Initiators als Initiatornamen des Mitglieds.

## Aktivieren des iSCSI-Zieldiensts

Bevor Sie iSCSI-Ziele und -LUNs erstellen und iSCSI-Initiatorgruppen definieren können, müssen Sie den iSCSI-Zieldienst auf dem vSAN-Cluster aktivieren.

### Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**. Klicken Sie unter vSAN auf **Allgemein**.

3 Klicken Sie auf die Schaltfläche **Bearbeiten** für „vSAN-iSCSI-Zieldienst“.

4 Aktivieren Sie das Kontrollkästchen **vSAN-iSCSI-Zieldienst aktivieren**. Sie können gegenwärtig das Standardnetzwerk, den TCP-Port und die Authentifizierungsmethode auswählen. Sie können auch eine vSAN-Speicherrichtlinie auswählen.

5 Klicken Sie auf **OK**.

### Weiter

Nach dem Aktivieren des iSCSI-Zieldiensts können Sie iSCSI-Ziele und -LUNs erstellen und iSCSI-Initiatorgruppen definieren.

## Erstellen eines iSCSI-Ziels

Sie können ein iSCSI-Ziel und die zugehörige LUN erstellen oder bearbeiten.

### Voraussetzungen

Vergewissern Sie sich, dass der iSCSI-Zieldienst aktiviert ist.

### Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**. Klicken Sie unter vSAN auf **iSCSI-Ziele**.

3 Klicken Sie im Abschnitt „vSAN-iSCSI-Ziele“ auf das Symbol **Neues iSCSI-Ziel hinzufügen** (✚).

Das Dialogfeld Neues iSCSI-Ziel wird angezeigt. Der Ziel-IQN wird automatisch generiert.

4 Geben Sie einen Ziel-Alias ein. Sie können auch das Netzwerk, den TCP-Port und die Authentifizierungsmethode für dieses Ziel bearbeiten.

5 (Optional) Klicken Sie zum Definieren der LUN für das Ziel auf das Kontrollkästchen **Erste LUN zum iSCSI-Ziel hinzufügen** und geben Sie die Größe der LUN ein.

6 Klicken Sie auf **OK**.

### Weiter

Definieren Sie eine Liste von iSCSI-Initiatoren, die auf dieses Ziel zugreifen können.

## Hinzufügen einer LUN zu einem iSCSI-Ziel

Sie können einem iSCSI-Ziel eine oder mehrere LUNs hinzufügen oder eine vorhandene LUN bearbeiten.

### Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**. Klicken Sie unter vSAN auf **iSCSI-Ziele**.

3 Wählen Sie im Abschnitt „Zieldetails“ der Seite die Registerkarte **LUNs** aus.

4 Klicken Sie auf das Symbol **Neue iSCSI-LUN zum Ziel hinzufügen** (✚).

Das Dialogfeld LUN zu Ziel hinzufügen wird angezeigt.

5 Geben Sie die Größe der LUN ein.

Die für den iSCSI-Zieldienst konfigurierte vSAN-Speicherrichtlinie wird automatisch zugewiesen. Sie können jeder LUN eine andere Richtlinie zuweisen.

6 Klicken Sie auf **OK**.

## Erstellen einer iSCSI-Initiatorgruppe

Sie können eine iSCSI-Initiatorgruppe erstellen, um Zugriffssteuerung für iSCSI-Ziele bereitzustellen. Nur iSCSI-Initiatoren, die Mitglieder der Initiatorgruppe sind, können auf die iSCSI-Ziele zugreifen.

### Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**. Klicken Sie unter vSAN auf **iSCSI-Initiatorgruppen**.

3 Klicken Sie im Abschnitt „vSAN-iSCSI-Initiatorgruppen“ auf das Symbol **Neue iSCSI-Initiatorgruppe hinzufügen** (✚).

Das Dialogfeld Neue vSAN-iSCSI-Initiatorgruppe wird angezeigt.

4 Geben Sie einen Namen für die iSCSI-Initiatorgruppe ein.

5 (Optional) Geben Sie zum Hinzufügen von Mitgliedern zu der Initiatorgruppe den IQN jedes Mitglieds ein.

Verwenden Sie für die Eingabe des IQN der Mitglieder folgendes Format:

*iqn.YYYY-MM.domain:name*

Dabei gilt:

- YYYY = Jahr, z. B. 2016
- MM = Monat, z. B. 09
- domain = Domäne, in der sich der Initiator befindet
- name = Name des Mitglieds (optional)

6 Klicken Sie auf **OK**.

### Weiter

Fügen Sie der iSCSI-Initiatorgruppe die Mitglieder hinzu.

## Zuweisen eines Ziels zu einer iSCSI-Initiatorgruppe

Sie können einer iSCSI-Initiatorgruppe ein iSCSI-Ziel zuweisen. Nur Initiatoren, die Mitglieder der Initiatorgruppe sind, können auf die zugewiesenen Ziele zugreifen.

### Voraussetzungen

Vergewissern Sie sich, dass eine iSCSI-Initiatorgruppe vorhanden ist.

### Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Konfigurieren**. Klicken Sie unter vSAN auf **iSCSI-Initiatorgruppen**.

3 Wählen Sie im Abschnitt „Gruppendetails“ die Registerkarte **Zugängliche Ziele** aus.

4 Klicken Sie auf das Symbol **Neues zugängliches Ziel für iSCSI-Initiatorgruppe hinzufügen** (✚).

Das Dialogfeld Zugriff auf Ziel für Initiatorgruppe zulassen wird angezeigt.

5 Wählen Sie auf der Registerkarte **Filter** aus der Liste der verfügbaren Ziele ein Ziel aus.

Die Registerkarte „Ausgewählte Objekte“ zeigt die derzeit ausgewählten Ziele an.

6 Klicken Sie auf **OK**.

## Überwachen des vSAN -iSCSI-Zieldiensts

Sie können den iSCSI-Zieldienst überwachen, um die physische Platzierung von iSCSI-Zielkomponenten anzuzeigen und nach fehlgeschlagenen Komponenten zu suchen. Sie können auch den Integritätsstatus des iSCSI-Zieldienstes überwachen.

### Voraussetzungen

Stellen Sie sicher, dass Sie den vSAN-iSCSI-Zieldienst aktiviert und Ziele sowie LUNs erstellt haben.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster.

2 Klicken Sie auf **Überwachen** und wählen Sie **vSAN** aus.

3 Klicken Sie auf **iSCSI-Ziele**.

iSCSI-Ziele und -LUNs werden oben auf der Seite aufgelistet.

4 Klicken Sie auf einen Ziel-Alias und zeigen Sie dessen Status an.

Die Registerkarte „Platzierung physischer Festplatten“ unten auf der Seite zeigt an, wo sich die Datenkomponenten des Ziels befinden. Die Registerkarte „Übereinstimmungsfehler“ zeigt fehlgeschlagene Komponenten an.

5 Klicken Sie auf eine LUN und zeigen Sie deren Status an.

Die Registerkarte „Platzierung physischer Festplatten“ unten auf der Seite zeigt an, wo sich die Datenkomponenten des Ziels befinden. Die Registerkarte „Übereinstimmungsfehler“ zeigt fehlgeschlagene Komponenten an.

## Migrieren eines hybriden vSAN -Clusters auf einen All-Flash-Cluster

Sie können die Festplattengruppen in einem hybriden vSAN-Cluster auf All-Flash-Festplattengruppen migrieren.

Der hybride vSAN-Cluster verwendet Magnetplattenspeicher für die Kapazitätsschicht und Flash-Geräte für die Cache-Ebene. Sie können die Konfiguration der Festplattengruppen im Cluster so ändern, dass Flash-Geräte auf der Cache-Ebene und der Kapazitätsebene verwendet werden.

### Vorgehensweise

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

2 Entfernen Sie die hybriden Festplattengruppen für jeden Host im Cluster.

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

b Klicken Sie unter vSAN auf **Festplattenverwaltung**.

c Wählen Sie unter „Festplattengruppen“ die zu entfernende Festplattengruppe aus und klicken Sie auf das Symbol **Festplattengruppe entfernen** (  ).

d Wählen Sie **Vollständige Datenmigration** als Migrationsmodus aus und klicken Sie auf **Ja**.

3 Entfernen Sie die physischen Festplatten vom Host.

4 Fügen Sie die Flash-Geräte zum Host hinzu.

Stellen Sie sicher, dass keine Partitionen auf den Flash-Geräten vorhanden sind.

5 Erstellen Sie die All-Flash-Festplattengruppen auf jedem Host.

## Ausschalten eines vSAN -Clusters

Sie können einen vSAN-Cluster ausschalten.

### Voraussetzungen

Falls die vCenter Server-VM auf dem vSAN-Cluster ausgeführt wird, migrieren Sie die VM auf den ersten Host oder erfassen Sie den Host, auf dem sie gerade ausgeführt wird.

### Vorgehensweise

1 Schalten Sie alle virtuellen Maschinen aus, die auf dem vSAN-Cluster ausgeführt werden.

Die vCenter Server-VM muss zuletzt ausgeschaltet werden.

2 Versetzen Sie alle ESXi-Hosts, aus denen sich der Cluster zusammensetzt, in den Wartungsmodus.

Führen Sie den `esxcli`-Befehl aus, um den vSAN-Modus für die Aktivierung des Wartungszustands festzulegen.

```
esxcli system maintenanceMode set –e true –m noAction
```

3 Schalten Sie die ESXi-Hosts aus.

# Verwenden von vSAN - Speicherrichtlinien 12

Wenn Sie vSAN verwenden, können Sie Speicheranforderungen für virtuelle Maschinen wie Leistung und Verfügbarkeit in einer Richtlinie definieren. vSAN sorgt dafür, dass jeder in vSAN-Datenspeichern bereitgestellten virtuellen Maschine mindestens eine Speicherrichtlinie zugewiesen wird.

Die Speicherrichtlinienanforderungen werden nach der Zuweisung der Speicherrichtlinien an die vSAN-Ebene übertragen, wenn eine virtuelle Maschine erstellt wird. Das virtuelle Gerät wird über den Datenspeicher für vSAN verteilt, um die Anforderungen in Bezug auf Leistung und Verfügbarkeit zu erfüllen.

vSAN verwendet Speicheranbieter, um dem vCenter Server Informationen zu zugrunde liegendem Speicher bereitzustellen. Mit diesen Informationen können Sie leichter die richtige Entscheidung in Bezug auf die Platzierung der virtuellen Maschine treffen und Ihre Speicherumgebung überwachen.

Dieses Kapitel behandelt die folgenden Themen:



## Informationen zu vSAN -Richtlinien

vSAN-Speicherrichtlinien definieren Speicheranforderungen für virtuelle Maschinen. Diese Richtlinien legen fest, wie die VM-Speicherobjekte bereitgestellt und innerhalb des Datenspeichers zugeteilt werden, um den erforderlichen Service-Level zu garantieren.

Wenn Sie vSAN auf einem Host-Cluster aktivieren, wird ein einzelner vSAN-Datenspeicher erstellt und dem Datenspeicher wird eine standardmäßige Speicherrichtlinie zugeteilt.

Wenn Sie die Speicheranforderungen Ihrer virtuellen Maschinen kennen, können Sie eine Speicherrichtlinie erstellen, die die vom Datenspeicher angekündigten Funktionen referenziert. Sie können mehrere Richtlinien erstellen, um verschiedene Anforderungstypen bzw. -klassen zu erfassen.

Jeder in vSAN-Datenspeichern bereitgestellten virtuellen Maschinen wird mindestens eine VM-Speicherrichtlinie zugewiesen. Speicherrichtlinien können Sie beim Erstellen oder Bearbeiten von virtuellen Maschinen zuweisen.

**Hinweis** Falls Sie einer virtuellen Maschine keine Speicherrichtlinie zuweisen, weist vSAN eine Standardrichtlinie zu. Bei der Standardrichtlinie ist die Option **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt, und sie hat einen einzelnen Disk-Stripe pro Objekt sowie eine schnell („thin“) bereitgestellte virtuelle Festplatte.

Das VM-Auslagerungsobjekt und das VM-Snapshot-Arbeitsspeicherobjekt sind nicht an die einer VM zugeordneten Speicherrichtlinien gebunden. Diese Objekte werden mit der auf 1 festgelegten Option **Primäre Ebene von zu tolerierenden Fehlern** konfiguriert. Diese Objekte haben nicht dieselbe Verfügbarkeit wie andere Objekte, denen eine Richtlinie mit einem anderen Wert für **Primäre Ebene von zu tolerierenden Fehlern** zugewiesen wurde.

**Tabelle 12-1.** Speicherrichtlinienattribute

| Funktionalität | Beschreibung |
|---|---|
| Anzahl der Festplatten-Stripes pro Objekt | Die Mindestanzahl der Kapazitätsgeräte, über die das Striping der einzelnen Replikate eines Objekts der virtuellen Maschine erfolgt. Ein höherer Wert als 1 kann zu besserer Leistung führen, bedeutet aber auch eine höhere Beanspruchung der Systemressourcen.<br>Der Standardwert ist 1. Der Höchstwert ist 12.<br>Ändern Sie diesen Standard-Striping-Wert nicht.<br>In einer Hybridumgebung erstrecken sich die Festplatten-Stripes über die magnetischen Datenträger. In einer All-Flash-Konfiguration erstrecken sich die Stripes über die Flash-Geräte, die die Kapazitätsschicht bilden. Stellen Sie sicher, dass Ihre vSAN-Umgebung ausreichend Kapazitätsgeräte enthält, um die entsprechenden Anforderungen zu erfüllen. |
| Flash Read Cache-Reservierung | Die als Lesecache reservierte Flash-Kapazität für das virtuelle Maschinenobjekt. Wird als Prozentsatz der logischen Größe des Festplattenobjekts der virtuellen Maschine (VMDK) angegeben. Reservierte Flash-Kapazität kann nicht von anderen Objekten verwendet werden. Unreservierter Flash wird gleichmäßig unter allen Objekten verteilt. Verwenden Sie diese Option nur zur Behebung bestimmter Leistungsfehler.<br>Sie brauchen keine Reservierung für Zwischenspeicher festzulegen. Wenn Sie Reservierungen für den Lesezwischenspeicher festlegen, kann dies beim Verschieben des VM-Objekts Probleme verursachen, weil die Einstellungen für die Zwischenspeicherreservierung immer beim Objekt enthalten sind.<br>Das Speicherrichtlinienattribut der Flash Read Cache-Reservierung wird nur für Hybrid-Konfigurationen unterstützt. Sie dürfen dieses Attribut beim Definieren einer VM-Speicherrichtlinie für einen reinen Flash-Cluster nicht verwenden.<br>Der Standardwert ist 0%. Der Höchstwert ist 100%.<br>**Hinweis** Standardmäßig weist das vSAN den Speicherobjekten den Lesecache dynamisch nach Bedarf zu. Diese Funktion stellt die flexibelste und optimalste Ressourcennutzung dar. Daher braucht der Standardwert 0 für diesen Parameter in der Regel nicht geändert zu werden.<br>Gehen Sie beim Erhöhen des Werts zum Lösen eines Leistungsproblems vorsichtig vor. Wenn auf mehreren virtuellen Maschinen zu viel Cache reserviert wird, kann Flash-Festplattenspeicherplatz für zu viele Reservierungen verschwendet werden. Diese Cache-Reservierungen stehen dann nicht zur Verfügung, um die Arbeitslasten zu unterstützen, die zu gegebener Zeit den erforderlichen Speicherplatz benötigen. Diese Speicherverschwendung und Nichtverfügbarkeit können zu einem Leistungsabfall führen. |

**Tabelle 12-1.** Speicherrichtlinienattribute (Fortsetzung)

| Funktionalität | Beschreibung |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Definiert die Anzahl von Host- und Gerätefehlern, die ein Objekt einer virtuellen Maschine tolerieren kann. Für n tolerierte Fehler werden alle geschriebenen Daten an n+1 Stellen gespeichert. Dazu zählen auch Paritätskopien bei Verwendung von RAID 5 oder RAID 6.<br>Wenn Sie beim Bereitstellen einer virtuellen Maschine keine Speicherrichtlinie auswählen, weist vSAN diese Richtlinie als Standard-VM-Speicherrichtlinie zu.<br>Wenn Fault Domains konfiguriert sind, sind 2n+1 Fault Domains mit Kapazität bereitstellenden Hosts erforderlich. Ein Host, der nicht Teil einer Fault Domain ist, wird als eigene Einzelhost-Fault Domain gezählt.<br>Der Standardwert ist 1. Der Höchstwert ist 3.<br>**Hinweis** Wenn vSAN eine einzelne Spiegelkopie von VM-Objekten nicht schützen soll, können Sie **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festlegen. Beim Host können allerdings ungewöhnliche Verzögerungen beim Wechseln in den Wartungsmodus auftreten. Die Verzögerungen treten auf, weil vSAN das Objekt vom Host evakuieren muss, um den Wartungsvorgang erfolgreich abschließen zu können. Wenn Sie **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festlegen, sind Ihre Daten nicht geschützt und Sie verlieren eventuell Daten, wenn beim vSAN-Cluster ein Gerätefehler auftritt.<br>**Hinweis** Wenn Sie eine Speicherrichtlinie erstellen und keinen Wert für **Primäre Ebene von zu tolerierenden Fehlern** angeben, erstellt vSAN eine einzelne Spiegelkopie der VM-Objekte. IT kann einen einzelnen Ausfall tolerieren. Wenn allerdings mehrere Komponenten ausfallen, sind Ihre Daten möglicherweise gefährdet.<br>Definiert in einem ausgeweiteten Cluster die Anzahl von Host- und Gerätefehlern, die ein Objekt einer virtuellen Maschine tolerieren kann. Sie können die Option **Primäre Ebene von zu tolerierenden Fehlern** zusammen mit **Sekundäre Ebene von zu tolerierenden Fehlern** verwenden, um für Objekte innerhalb einer einzelnen Site einen lokalen Fehlerschutz anzubieten. |
| Sekundäre Ebene von zu tolerierenden Fehlern | In einem ausgeweiteten Cluster definiert diese Regel die Anzahl von Host- und Objektfehlern, die ein Objekt einer virtuellen Maschine innerhalb einer einzelnen Site tolerieren kann.<br>Der Standardwert ist 1. Der Höchstwert ist 3. |
| Affinität | In einem ausgeweiteten Cluster steht diese Regel nur dann zur Verfügung, wenn die Option **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist. Sie können die Affinitätsregel auf **Keine**, **Bevorzugt** oder **Sekundär** festlegen. Diese Regel ermöglicht es Ihnen, die VM-Objekte auf eine ausgewählte Site im ausgeweiteten Cluster zu begrenzen.<br>Der Standardwert ist „Keine“. |
| Bereitstellung erzwingen | Wenn die Option auf **Ja** festgelegt ist, wird das Objekt bereitgestellt, auch wenn die in der Speicherrichtlinie angegebenen Richtlinien **Primäre Ebene von zu tolerierenden Fehlern**, **Anzahl der Festplatten-Stripes pro Objekt** und **Flash Read Cache-Reservierung** vom Datenspeicher nicht erfüllt werden können. Verwenden Sie diesen Parameter in Bootstrapping-Szenarien und bei Ausfällen, wenn keine Standardbereitstellung mehr möglich ist.<br>Der Standardwert **Nein** ist für die meisten Produktionsumgebungen akzeptabel. vSAN kann keine virtuelle Maschine bereitstellen, wenn die Richtlinienanforderungen nicht erfüllt werden, erstellt allerdings erfolgreich eine benutzerdefinierte Speicherrichtlinie. |
| Reservierter Objektspeicherplatz | Prozentsatz der logischen Größe des Festplattenobjekts der virtuellen Maschine (VMDK), der reserviert oder beim Bereitstellen von virtuellen Maschinen „thick“ bereitgestellt werden sollte.<br>Der Standardwert ist 0%. Der Höchstwert ist 100%. |

**Tabelle 12-1.** Speicherrichtlinienattribute (Fortsetzung)

| Funktionalität | Beschreibung |
|---|---|
| Objektprüfsumme deaktivieren | Wenn die Option auf **Nein** festgelegt ist, berechnet das Objekt die Prüfsummeninformationen, um die Integrität der Daten sicherzustellen. Wenn diese Option auf **Ja** festgelegt ist, berechnet das System keine Prüfsummeninformationen.<br>vSAN verwendet End-to-End-Prüfsummen, um die Datenintegrität sicherzustellen. Bei diesem Vorgang wird bestätigt, dass es sich bei jeder Kopie einer Datei um die genaue Entsprechung der Quelldatei handelt. Das System prüft die Gültigkeit der Daten während Lese-/Schreibvorgängen und wenn ein Fehler auftritt, repariert vSAN die Daten oder erstellt einen Fehlerbericht.<br>Wenn ein Prüfsummenkonflikt auftritt, repariert vSAN automatisch die Daten durch Überschreiben der falschen Daten mit den richtigen Daten. Prüfsummenberechnung und Fehlerkorrektur werden im Hintergrund ausgeführt.<br>Die Standardeinstellung für alle Objekte im Cluster ist **Nein**. Dies bedeutet, dass Prüfsumme aktiviert ist. |
| Fehlertoleranzmethode | Gibt an, ob die Datenreplizierungsmethode für Leistung und Kapazität optimiert wird. Bei Auswahl von **RAID-1 (Spiegelung) - Leistung** verwendet vSAN mehr Festplattenspeicher, um die Objektkomponenten zu platzieren. Die Verwendung dieser Option führt jedoch zu verbesserten Leistung beim Zugreifen auf die Objekte. Bei Auswahl von **RAID-5/6 (Erasure Coding) - Kapazität** verwendet vSAN weniger Festplattenspeicher, die Leistung nimmt jedoch ab. Sie können RAID 5 verwenden, indem Sie das Attribut **RAID-5/6 (Erasure Coding) - Kapazität** für Cluster mit vier oder mehr Fehlerdomänen anwenden und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festlegen. Sie können RAID 6 verwenden, indem Sie das Attribut **RAID-5/6 (Erasure Coding) - Kapazität** für Cluster mit sechs oder mehr Fehlerdomänen anwenden und **Primäre Ebene von zu tolerierenden Fehlern** auf 2 festlegen.<br>In ausgeweiteten Clustern mit konfigurierter Option **Sekundäre Ebene von zu tolerierenden Fehlern** gilt diese Regel nur für die **Sekundäre Ebene von zu tolerierenden Fehlern**.<br>Weitere Informationen zu RAID 5 oder RAID 6 finden Sie unter „Verwenden von RAID 5- oder RAID 6-Erasure Coding“, auf Seite 80. |
| IOPS-Grenzwert für Objekt | Definiert den IOPS-Grenzwert für ein Objekt, zum Beispiel eine VMDK. IOPS wird als Anzahl der E/A-Vorgänge unter Verwendung einer gewichteten Größe berechnet. Wenn das System die Standardbasisgröße von 32 KB verwendet, stellt ein 64-KB-E/A-Vorgang zwei E/A-Vorgänge dar.<br>Bei der IOPS-Berechnung werden Lese- und Schreibvorgänge als Äquivalente betrachtet, die Cache-Zugriffsrate und die Aufeinanderfolge bleiben hingegen unberücksichtigt. Wenn der IOPS-Grenzwert einer Festplatte überschritten wird, werden E/A-Vorgänge gedrosselt. Wenn der **IOPS-Grenzwert für Objekt** auf 0 festgelegt ist, werden keine IOPS-Grenzwerte erzwungen.<br>vSAN lässt zu, dass das Objekt die Rate für den IOPS-Grenzwert während der ersten Sekunde des Vorgangs oder nach einem gewissen Inaktivitätszeitraum verdoppeln kann. |

Beim Arbeiten mit VM-Speicherrichtlinien müssen Sie verstehen, wie sich die Speicherfunktionen auf die Nutzung von Speicherkapazität im vSAN-Cluster auswirken. Weitere Informationen zu Entwurfs- und Dimensionierungsüberlegungen zu Speicherrichtlinien finden Sie unter Kapitel 3, „Entwerfen und Dimensionieren eines vSAN-Clusters“, auf Seite 21.

# Anzeigen von vSAN -Speicheranbietern

Durch die Aktivierung von vSAN wird ein Speicheranbieter für jeden Host im vSAN-Cluster automatisch konfiguriert und registriert.

vSAN-Speicheranbieter sind integrierte Softwarekomponenten, die Datenspeicherfunktionen an vCenter Server übermitteln. Eine Speicherfunktion wird in der Regel durch ein Schlüssel-Wert-Paar dargestellt, wobei der Schlüssel eine spezielle Eigenschaft ist, die vom Datenspeicher angeboten wird. Der Wert ist eine Zahl oder ein Bereich, den der Datenspeicher für ein bereitgestelltes Objekt, z. B. ein VM-Home-Namespace-Objekt oder eine virtuelle Festplatte, zur Verfügung stellen kann. Außerdem können Sie Tags verwenden, um benutzerdefinierte Speicherfunktionen zu erstellen, und bei der Definition einer Speicherrichtlinie für eine virtuelle Maschine auf diese verweisen. Informationen zur Verwendung und Anwendung von Tags für Datenspeicher finden Sie in der Dokumentation *vSphere-Speicher*.

Die Speicheranbieter des vSAN berichten eine Reihe von zugrunde liegenden Speicherfunktionen an vCenter Server. Sie kommunizieren auch mit der Ebene des vSAN, um über die Speicheranforderungen der virtuellen Maschinen zu berichten. Weitere Informationen zu Speicheranbietern finden Sie in der Dokumentation *vSphere-Speicher*.

Das vSAN registriert einen getrennten Speicheranbieter für jeden Host im Cluster für vSAN über die folgende URL:

http://*host_ip*:8080/version.xml

wobei *host_ip* die tatsächliche IP des Hosts ist.

Überprüfen Sie, dass die Speicheranbieter registriert sind.

### Vorgehensweise

1 Navigieren Sie im Navigator von vSphere Web Client zu vCenter Server.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.

Die Speicheranbieter für vSAN werden in der Liste aufgeführt. Alle Hosts verfügen über einen Speicheranbieter, aber nur einer ist aktiv. Speicheranbieter anderer Hosts befinden sich im Standby-Modus. Wenn der Host, der zurzeit über den aktiven Speicheranbieter verfügt, ausfällt, wird der Speicheranbieter eines anderen Hosts aktiv.

**Hinweis** Die Registrierung von Speicheranbietern, die von vSAN verwendet werden, kann nicht manuell aufgehoben werden. Wenn Sie die Speicheranbieter für vSAN entfernen oder deren Registrierung aufheben müssen, entfernen Sie die entsprechenden Hosts im vSAN-Cluster und fügen Sie die Hosts dann wieder hinzu. Stellen Sie sicher, dass mindestens ein Speicheranbieter aktiv ist.

# Informationen zur vSAN -Standardspeicherrichtlinie

Bei vSAN muss den auf den vSAN-Datenspeichern bereitgestellten virtuellen Maschinen mindestens eine Speicherrichtlinie zugewiesen werden. Wenn Sie beim Bereitstellen einer virtuellen Maschine dieser nicht explizit eine Speicherrichtlinie zuweisen, wird ihr die Standardspeicherrichtlinie für vSAN zugewiesen.

Die Standardrichtlinie enthält vSAN-Regelsätze und einen Satz elementarer Speicherfunktionen, die gewöhnlich zur Platzierung von auf Datenspeichern für vSAN bereitgestellten virtuellen Maschinen verwendet werden.

**Tabelle 12-2.** Spezifikationen für die vSAN -Standardspeicherrichtlinie

| Spezifikation | Einstellung |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | 1 |
| Anzahl der Festplatten-Stripes pro Objekt | 1 |

**Tabelle 12-2.** Spezifikationen für die vSAN -Standardspeicherrichtlinie (Fortsetzung)

| Spezifikation | Einstellung |
|---|---|
| Die Flash Read Cache-Reservierung oder die Flash-Kapazität für den Lesecache | 0 |
| Reservierter Objektspeicherplatz | 0<br>**Hinweis** Durch das Festlegen des reservierten Objektspeicherplatzes auf 0 wird die virtuelle Festplatte standardmäßig schnell (thin) bereitgestellt. |
| Bereitstellung erzwingen | Nein |

Sie können die Konfigurationseinstellungen für die VM-Standardspeicherrichtlinie über den vSphere Web Client prüfen, wenn Sie zu **VM-Speicherrichtlinien** > **Standardspeicherrichtlinie für vSAN** > **Verwalten** > **Regelsatz 1: VSAN** navigieren.

Um optimale Ergebnisse zu erzielen, sollten Sie Ihre eigenen VM-Speicherrichtlinien erstellen und verwenden, selbst wenn die Anforderungen der Richtlinie mit den in der Standardspeicherrichtlinie definierten identisch sind. Informationen zum Erstellen einer benutzerdefinierten VM-Speicherrichtlinie finden Sie unter „Definieren einer VM-Speicherrichtlinie für vSAN“, auf Seite 144.

Wenn Sie einem Datenspeicher eine benutzerdefinierte Speicherrichtlinie als Standardrichtlinie zuweisen, entfernt vSAN automatisch die Verknüpfung mit der Standardspeicherrichtlinie und wendet die Einstellungen für die benutzerdefinierte Richtlinie auf den festgelegten Datenspeicher an. Sie können dem Datenspeicher für vSAN jeweils nur eine VM-Speicherrichtlinie als Standardrichtlinie zuweisen.

## Merkmale

Die folgenden Merkmale gelten für die Standardspeicherrichtlinie für vSAN.

- Die vSAN-Standardspeicherrichtlinie wird allen VM-Objekten zugewiesen, wenn Sie beim Bereitstellen einer virtuellen Maschine keine andere vSAN-Richtlinie auswählen, das heißt, wenn auf der Seite „Speicher auswählen“ das Feld **VM-Speicherrichtlinie** auf **Datenspeicherstandardwert** eingestellt ist. Informationen zum Verwenden von Speicherrichtlinien finden Sie in der *vSphere-Speicher*-Dokumentation.

  **Hinweis** VM-Auslagerungsobjekte und VM-Arbeitsspeicherobjekte erhalten die Standardspeicherrichtlinie für vSAN, wobei **Bereitstellung erzwingen** auf **Ja** festgelegt ist.

- Die vSAN-Standardrichtlinie gilt nur für vSAN-Datenspeicher. Sie können die Standardspeicherrichtlinie nicht auf Nicht-vSAN-Datenspeicher wie NFS- oder VMFS-Datenspeicher anwenden.
- Weil die VM-Standardspeicherrichtlinie kompatibel zu jedem Datenspeicher für vSAN im vCenter Server ist, können Sie die mit der Standardrichtlinie bereitgestellten VM-Objekte in einen beliebigen Datenspeicher für vSAN im vCenter Server verschieben.
- Sie können die Standardrichtlinie klonen und als Vorlage zum Erstellen einer benutzerdefinierten Speicherrichtlinie verwenden.
- Sie können die Standardrichtlinie bearbeiten, wenn Sie über die Berechtigung „StorageProfile.View“ verfügen. Sie müssen mindestens über einen für vSAN aktivierten Cluster verfügen, der mindestens einen Host enthält. VMware empfiehlt dringend, die Einstellungen der Standardspeicherrichtlinie nicht zu bearbeiten.
- Sie können den Namen und die Beschreibung der Standardrichtlinie oder die Spezifikation des Speicheranbieters für vSAN nicht bearbeiten. Alle anderen Parameter einschließlich der Richtlinienregeln sind bearbeitbar.
- Sie können die Standardrichtlinie nicht löschen.

- Die Standardspeicherrichtlinie wird zugewiesen, wenn die beim Bereitstellen einer virtuellen Maschine zugewiesene Richtlinie keine spezifischen Regeln für vSAN enthält.

# Zuweisen einer Standardspeicherrichtlinie zu vSAN -Datenspeichern

Sie können einem Datenspeicher eine benutzerdefinierte Speicherrichtlinie als Standardrichtlinie zuweisen, um eine Speicherrichtlinie erneut zu verwenden, die Ihre Anforderungen erfüllt.

### Voraussetzungen

Vergewissern Sie sich, dass die VM-Speicherrichtlinie, die Sie dem vSAN-Datenspeicher als Standardrichtlinie zuweisen möchten, die Anforderungen Ihrer virtuellen Maschinen im vSAN-Cluster erfüllt.

### Vorgehensweise

1 Navigieren Sie zum vSAN-Datenspeicher im vSphere Web Client.

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

3 Klicken Sie unter „Allgemein“ auf die Schaltfläche **Bearbeiten** der Standardspeicherrichtlinie und wählen Sie die Speicherrichtlinie aus, die Sie dem vSAN-Datenspeicher als Standardrichtlinie zuweisen möchten.

   Der vSphere Web Client zeigt eine Liste der mit dem vSAN-Datenspeicher kompatiblen Speicherrichtlinien an, z. B. die vSAN-Standardspeicherrichtlinie und benutzerdefinierte Speicherrichtlinien, für die die vSAN-Regelsätze definiert sind.

4 Wählen Sie eine Richtlinie aus und klicken Sie auf **OK**.

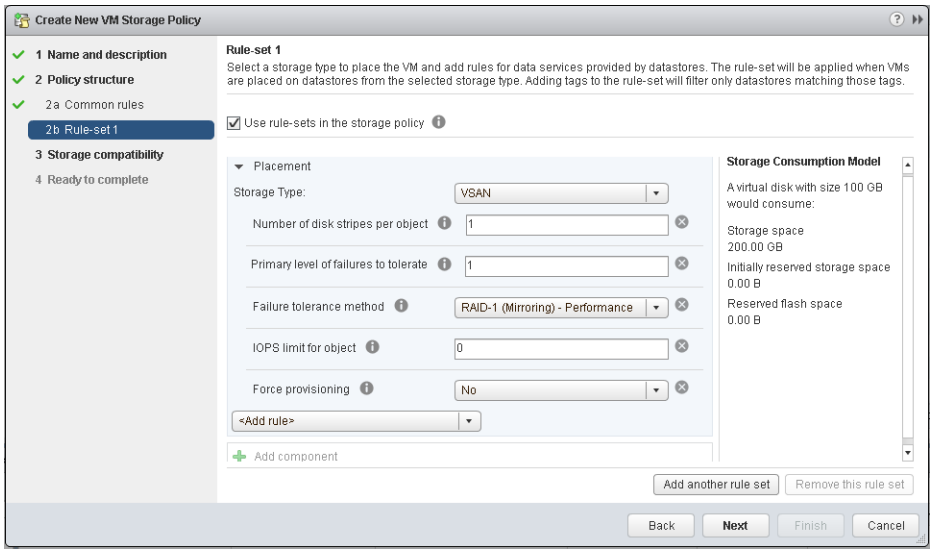
   Die Speicherrichtlinie wird als Standardrichtlinie angewendet, wenn Sie neue virtuelle Maschinen bereitstellen, ohne für einen Datenspeicher explizit eine Speicherrichtlinie festzulegen.

### Weiter

Sie können eine neue Speicherrichtlinie für virtuelle Maschinen definieren. Siehe „Definieren einer VM-Speicherrichtlinie für vSAN“, auf Seite 144.

# Definieren einer VM-Speicherrichtlinie für vSAN

Sie können eine Speicherrichtlinie erstellen, die Speicheranforderungen für eine VM und ihre virtuellen Festplatten definiert. In dieser Richtlinie geben Sie Speicherfunktionen an, die vom vSAN-Datenspeicher unterstützt werden.




### Voraussetzungen

- Vergewissern Sie sich, dass der Speicheranbieter für vSAN verfügbar ist. Siehe „Anzeigen von vSAN-Speicheranbietern“, auf Seite 141.
- Stellen Sie sicher, dass die VM-Speicherrichtlinien aktiviert sind. Informationen zu Speicherrichtlinien finden Sie in der Dokumentation zu *vSphere-Speicher*.
- Erforderliche Berechtigungen: **Profilgesteuerter Speicher.Ansicht des profilgesteuerten Speichers** und **Profilgesteuerter Speicher.Update des profilgesteuerten Speichers**

### Vorgehensweise

1. Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile** und dann auf **VM-Speicherrichtlinien**.
2. Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen** ( ).
3. Wählen Sie auf der Seite „Name und Beschreibung“ einen vCenter Server aus.
4. Geben Sie einen Namen und eine Beschreibung für die Speicherrichtlinie ein und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite „Richtlinienstruktur“ auf **Weiter**.
6. Klicken Sie auf der Seite **Gemeinsame Regeln für von Hosts bereitgestellte Datendienste** auf **Weiter**.
7. Definieren Sie auf der Seite „Regelsatz 1“ den ersten Regelsatz.
   a. Aktivieren Sie das Kontrollkästchen **Regelsätze in der Speicherrichtlinie verwenden**.
   b. Wählen Sie **VSAN** aus dem Dropdown-Menü **Speichertyp** aus.

      Die Seite wird beim Hinzufügen von Regeln für den vSAN-Datenspeicher erweitert.

c Wählen Sie im Dropdown-Menü **Regel hinzufügen** eine Regel aus.

Stellen Sie sicher, dass die eingegebenen Werte innerhalb des von Speicherfunktionen des vSAN-Datenspeichers angegebenen Wertebereichs liegen.

Über das Speicherbelegungsmodell können Sie die verfügbare Größe der virtuellen Festplatte und den entsprechenden Flash-Cache und die Kapazitätsanforderungen einschließlich des reservierten Speicherplatzes überprüfen, die von Ihren virtuellen Maschinen potenziell genutzt würden, wenn Sie die angegebene Speicherrichtlinie anwenden.

d (Optional) Fügen Sie Tag-basierte Funktionen hinzu.

8 (Optional) Klicken Sie auf die Schaltfläche **Weiteren Regelsatz hinzufügen**, um einen weiteren Regelsatz hinzuzufügen.

9 Klicken Sie auf **Weiter**.

10 Überprüfen Sie auf der Seite „Speicherkompatibilität“ die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen, und klicken Sie auf **Weiter**.

Ein geeigneter Datenspeicher muss nicht alle Regelsätze der Richtlinie erfüllen. Der Datenspeicher muss mindestens einen Regelsatz und alle Regeln innerhalb dieses Regelsatzes erfüllen. Stellen Sie sicher, dass der Datenspeicher für vSAN die in der Speicherrichtlinie festgelegten Anforderungen erfüllt und in der Liste kompatibler Datenspeicher angezeigt wird.

11 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Richtlinieneinstellungen und klicken Sie auf **Beenden**.

Die neue Richtlinie wird zur Liste hinzugefügt.

#### Weiter

Weisen Sie diese Richtlinie einer virtuellen Maschine und deren virtuellen Festplatten zu. vSAN platziert das VM-Objekt entsprechend den in der Richtlinie angegebenen Anforderungen. Informationen zum Anwenden der Speicherrichtlinien auf VM-Objekte finden Sie in der Dokumentation zu *vSphere-Speicher*.

# 13 Überwachen von vSAN

Sie können Ihre vSAN-Umgebung über den vSphere Web Client überwachen.

Sie können alle Objekte in einer vSAN-Umgebung überwachen. Dazu zählen Hosts in einem vSAN-Cluster sowie der vSAN-Datenspeicher. Weitere Informationen zur Überwachung von Objekten und Speicherressourcen in einem vSAN-Cluster finden Sie in der Dokumentation zu *vSphere-Überwachung und -Leistung*.

Dieses Kapitel behandelt die folgenden Themen:



## Überwachen des vSAN -Clusters

Sie können den vSAN-Cluster und alle mit dem Cluster verwandten Objekte überwachen.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.
3. Wählen Sie **Physische Festplatten** aus, um Hosts, Cache-Geräte und Kapazitätsgeräte im Cluster zu überprüfen.

   vSAN zeigt Informationen zu Kapazitätsgeräten an, z. B. Gesamtkapazität, verwendete Kapazität, reservierte Kapazität, Funktionszustand, physischer Speicherort usw. Der physische Speicherort basiert auf dem Hardwarespeicherort der Cache- und Kapazitätsgeräte auf vSAN-Hosts.
4. Wählen Sie ein Kapazitätsgerät aus und klicken Sie auf **Virtuelle Festplatten**, um die virtuellen Maschinen zu überprüfen, die das Gerät verwenden.

   Sie können viele Aspekte der VM-Objekte überwachen, einschließlich des aktuellen Status und der Übereinstimmung mit den zugewiesenen Speicherrichtlinien.

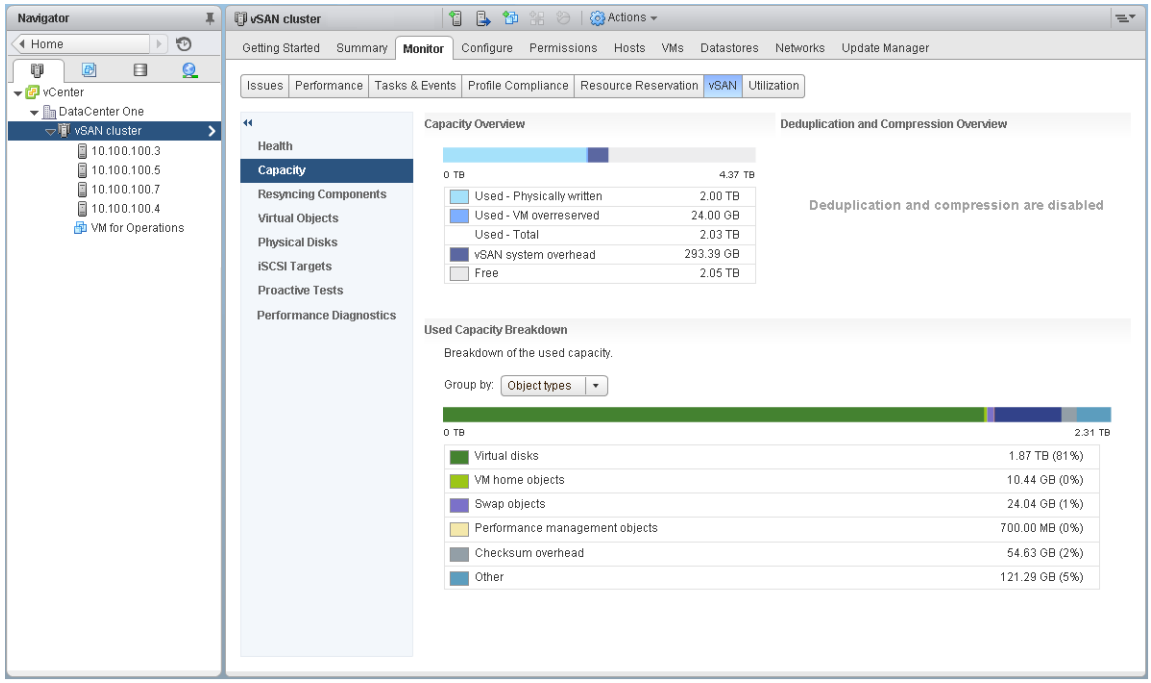
5 Wählen Sie **Kapazität** aus, um Informationen zu der im Cluster bereitgestellten und genutzten Speichermenge sowie eine Aufschlüsselung der nach Objekttyp oder Datentyp genutzten Kapazität zu überprüfen.

6 Wählen Sie die Registerkarte **Konfigurieren** aus und wählen Sie **Allgemein** aus, um den Status des vSAN-Clusters zu ermitteln, die Internetverbindung zu testen und das im Cluster verwendete Festplattenformat zu überprüfen.

# Überwachen der vSAN -Kapazität

Sie können die Kapazität des vSAN-Datenspeichers, die Effizienz von Deduplizierung und Komprimierung sowie die Kapazitätsnutzung überwachen.

Auf der Registerkarte „Übersicht“ des vSphere Web Client-Clusters finden Sie eine Übersicht der vSAN-Kapazität. Sie können auch detailliertere Informationen in der Kapazitätsüberwachung anzeigen.




### Vorgehensweise

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

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.

3 Wählen Sie **Kapazität** aus, um die vSAN-Kapazitätsinformationen anzuzeigen.

In der Kapazitätsübersicht wird die Speicherkapazität des vSAN-Datenspeichers, einschließlich Speicherplatz und freier Speicherplatz, angezeigt. Unter „Verwendete Kapazitätsaufschlüsselung“ wird der Prozentsatz der von verschiedenen Objekt- und Datentypen verwendeten Kapazität angezeigt. Bei Auswahl von „Datentypen“ zeigt vSAN den Prozentsatz der Kapazität an, die von Daten der primären VM, vSAN-Overhead und temporärem Overhead belegt wird. Bei Auswahl von „Objekttypen“ zeigt vSAN den Prozentsatz der Kapazität an, die von folgenden Objekttypen belegt wird:

- Virtuelle Festplatten
- VM-Home-Objekte
- Auslagerungsobjekte
- Leistungsverwaltungsobjekte

- .vmem-Dateien
- Prüfsummen-Overhead
- Snapshot-Arbeitsspeicher
- Overhead durch Deduplizierung und Komprimierung
- Speicherplatz bei der Berücksichtigung der Deduplizierungs-Engine
- iSCSI-Start- und -Zielobjekte und iSCSI-LUNs
- Weitere Typen, wie zum Beispiel von Benutzern erstellte Dateien, VM-Vorlagen usw.

Wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren, werden in der Übersicht zur Deduplizierung und Komprimierung Kapazitätsinformationen zu dieser Funktion angezeigt. Bei Aktivierung von Deduplizierung und Komprimierung kann es einige Minuten dauern, bis Aktualisierungen der Kapazität in der Kapazitätsüberwachung angezeigt werden, da Festplattenspeicher in Anspruch genommen und neu zugeteilt wird. Weitere Informationen zu Deduplizierung und Komprimierung finden Sie unter „Verwenden von Deduplizierung und Komprimierung“, auf Seite 75.

# Überwachen virtueller Geräte im vSAN -Cluster

Sie können den Status virtueller Festplatten im vSAN-Cluster anzeigen.

Wenn mindestens ein Host nicht mit dem vSAN-Datenspeicher kommunizieren kann, werden keine Informationen zu virtuellen Geräten angezeigt.

### Vorgehensweise

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

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.

3 Wählen Sie **Virtuelle Festplatten** aus, um alle Hosts und die entsprechenden virtuellen Festplatten, die zum vSAN-Cluster gehören, anzuzeigen, darunter auch, welche Hosts, Cache- und Kapazitätsgeräte ihre Komponenten derzeit nutzen.

4 Wählen Sie den Ordner **VM-Home** aus einer der virtuellen Maschinen aus und klicken Sie auf die Registerkarte **Platzierung physischer Festplatten**, um Geräteinformationen wie Name, Bezeichner oder UUID anzuzeigen.

   Klicken Sie auf die Registerkarte **Übereinstimmungsfehler**, um den Übereinstimmungsstatus Ihrer virtuellen Maschinen zu überprüfen.

5 Wählen Sie eine **Festplatte** aus einer der virtuellen Maschinen aus und klicken Sie auf die Registerkarte **Platzierung physischer Festplatten**, um Geräteinformationen wie Name, Bezeichner oder UUID, Anzahl der für jede virtuelle Maschine verwendeten Geräte und die Art ihrer Spiegelung auf den Hosts anzuzeigen.

   Klicken Sie auf die Registerkarte **Übereinstimmungsfehler**, um den Übereinstimmungsstatus Ihres virtuellen Geräts zu überprüfen.

6 Klicken Sie auf die Registerkarte **Übereinstimmungsfehler** zum Prüfen des Übereinstimmungsstatus Ihrer virtuellen Maschinen.

# Informationen zur Neusynchronisierung eines vSAN -Clusters

Sie können den Status von VM-Objekten, die im vSAN-Cluster neu synchronisiert werden, überwachen.

Wenn ein Hardwaregerät, Host oder Netzwerk ausfällt oder wenn ein Host in den Wartungsmodus versetzt wird, initiiert vSAN eine Neusynchronisierung im vSAN-Cluster. Vor der Initiierung der Neusynchronisierungsaufgabe wartet vSAN jedoch möglicherweise kurz ab, ob die ausgefallenen Komponenten wieder online geschaltet werden.

Die folgenden Ereignisse lösen eine Neusynchronisierung im Cluster aus:

- Bearbeiten einer VM-Speicherrichtlinie. Wenn Sie die VM-Speicherrichtlinieneinstellungen ändern, kann vSAN die Objektneuerstellung und die nachfolgende Neusynchronisierung der Objekte initiieren.

  Bestimmte Richtlinienänderungen können bewirken, dass vSAN eine andere Version eines Objekts erstellt und dieses mit der vorherigen Version synchronisiert. Nach Abschluss der Synchronisierung wird das ursprüngliche Objekt verworfen.

  vSAN stellt sicher, dass VMs ihren Betrieb fortsetzen und durch diesen Prozess nicht unterbrochen werden. Der Prozess kann zusätzliche temporäre Kapazität erfordern.

- Neustarten eines Hosts nach einem Ausfall.
- Wiederherstellen von Hosts nach einem dauerhaften oder langfristigen Ausfall. Wenn ein Host länger als 60 Minuten (Standardeinstellung) nicht verfügbar ist, erstellt vSAN Datenkopien, um die vollständige Richtlinieneinhaltung wiederherzustellen.
- Evakuieren von Daten unter Verwendung des Modus „Vollständige Datenmigration“, bevor Sie einen Host in den Wartungsmodus versetzen.
- Überschreiten des Nutzungsschwellenwerts eines Kapazitätsgeräts. Eine Kapazitätsgerätenutzung im vSAN-Cluster, die sich dem Schwellenwert von 80 Prozent nähert oder diesen bereits überschreitet, löst eine Neusynchronisierung aus.

Falls eine VM aufgrund der Latenz, die von einer Neusynchronisierung verursacht wurde, nicht antwortet, können Sie die für die Neusynchronisierung verwendeten IOPS drosseln.

## Überwachen der Neusynchronisierungsaufgaben im vSAN -Cluster

Zur Auswertung des Status der Objekte, die neu synchronisiert werden, können Sie die Neusynchronisierungsaufgaben überwachen, die aktuell ausgeführt werden.

### Voraussetzungen

Vergewissern Sie sich, dass Hosts in Ihrem vSAN-Cluster ESXi 6.5 oder höher ausführen.

### Vorgehensweise

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

2 Wählen Sie die Registerkarte **Überwachen** und klicken Sie dann auf **vSAN**.

3 Wählen Sie **Neusynchronisieren von Komponenten** aus, um den Fortschritt der Neusynchronisierung von VM-Objekten und die Anzahl der verbleibenden Bytes bis zum Abschluss der Neusynchronisierung nachzuverfolgen.

  Sie können auch folgende Informationen anzeigen: Anzahl der Objekte, die aktuell im Cluster synchronisiert werden, die geschätzte Zeit bis zum Abschluss der Neusynchronisierung, die verbleibende Zeit, bis die Speicherobjekte die zugewiesene Speicherrichtlinie vollständig erfüllen usw.

  Wenn Ihr Cluster Verbindungsprobleme aufweist, werden die Daten auf der Seite „Neusynchronisieren von Komponenten“ möglicherweise nicht wie erwartet aktualisiert und in den Feldern werden unter Umständen falsche Informationen angezeigt.

### Drosseln der Neusynchronisierungsaktivitäten im vSAN -Cluster

Sie können die Anzahl der IOPS, die zum Durchführen der Neusynchronisierung von Festplattengruppen im vSAN-Cluster verwendet werden, verringern. Die Drosselung der Neusynchronisierung ist eine clusterweite Einstellung und wird pro Festplattengruppe angewendet.

Falls VMs aufgrund der Latenz, die von einer Neusynchronisierung verursacht wurde, nicht antwortet, können Sie die für die Neusynchronisierung verwendete Anzahl der IOPS drosseln. Ziehen Sie die Drosselung der Neusynchronisierung nur dann in Betracht, wenn Latenzen im Cluster aufgrund der Neusynchronisierung zunehmen oder wenn der auf die Neusynchronisierung bezogene Datenverkehr auf einem Host zu hoch ist.

Die Drosselung der Neusynchronisierung kann dazu führen, dass die Neusynchronisierung länger dauert. Der erneute Schutz von nicht übereinstimmenden virtuellen Maschinen kann sich verzögern.

#### Vorgehensweise

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

2 Wählen Sie die Registerkarte **Überwachen** und klicken Sie dann auf **vSAN**.

3 Wählen Sie **Neusynchronisieren von Komponenten** und klicken Sie auf **Drosselung neu synchronisieren**.

4 (Optional) Klicken Sie auf **Aktuellen Neusynchronisierungsdatenverkehr pro Host anzeigen**, um die Neusynchronisierungsaktivitäten anzuzeigen.

5 Aktivieren Sie das Kontrollkästchen **Drosselung zur Neusynchronisierung des Komponentendatenverkehrs aktivieren**.

6 Bewegen Sie den Schieberegler zum Festlegen der Drosselung wie folgt:

- Bewegen Sie den Schieberegler nach rechts, um die Anzahl der für die Neusynchronisierung zulässigen IOPS zu erhöhen.
- Bewegen Sie den Schieberegler nach links, um die Anzahl der für die Neusynchronisierung zulässigen IOPS zu verringern.

Eine allgemeine Regel besteht darin, die IOPS um die Hälfte zu drosseln und einige Zeit einzuräumen, damit sich der Cluster anpassen kann. Wenn weitere Aktionen erforderlich sind, drosseln Sie die IOPS erneut um die Hälfte, bis sich der Cluster stabilisiert hat.

7 Klicken Sie auf **OK**.

## Überwachen von Geräten in vSAN -Datenspeichern

Überprüfen Sie den Status der Geräte, die den Datenspeicher für vSAN sichern. Sie können prüfen, ob bei den Geräten Probleme auftreten.

#### Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum Speicher.

2 Wählen Sie den vSAN-Datenspeicher aus.

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

Sie können allgemeine Informationen zum vSAN-Datenspeicher anzeigen, unter anderem Kapazität, Funktionen und die Standardspeicherrichtlinie.

4 Klicken Sie auf **Geräte-Backing** und wählen Sie unten auf der Seite die Festplattengruppe zum Anzeigen von lokalen Geräten in der Tabelle Festplatten aus.

5 Um nicht sichtbare Spalten anzuzeigen, klicken Sie mit der rechten Maustaste auf die Spaltenüberschrift und wählen Sie **Spalten anzeigen/ausblenden** aus.

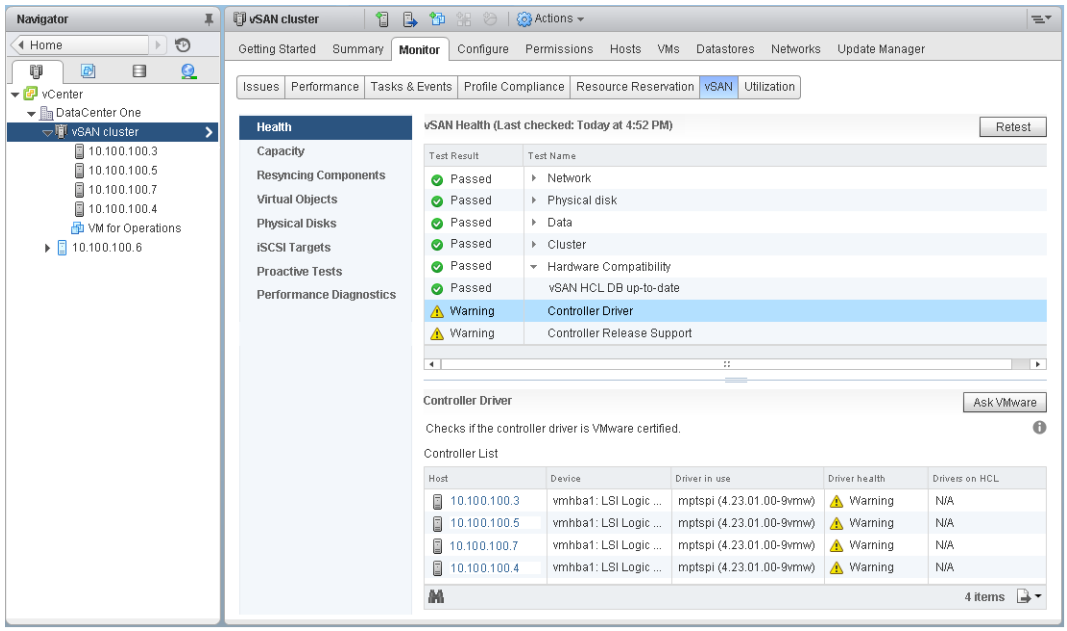
6 Wählen Sie die Spalten aus, die Sie anzeigen möchten, und klicken Sie auf **OK**.

Die ausgewählten Spalten werden in der Tabelle Festplatten angezeigt.

# Überwachen der vSAN -Integrität

Sie können die Integrität des vSAN-Clusters überprüfen.

Sie können die vSAN-Integritätsprüfungen verwenden, um den Status von Clusterkomponenten zu überwachen, Probleme zu diagnostizieren und Fehlerbehebungsmaßnahmen durchzuführen. Die Integritätsprüfungen umfassen Hardwarekompatibilität, Konfiguration und Betrieb des Netzwerks, erweiterte vSAN-Konfigurationsoptionen, Integrität der Speichergeräte sowie VM-Objekte.




Die vSAN-Integritätsprüfungen sind in Kategorien unterteilt. Jede Kategorie enthält individuelle Integritätsprüfungen.

**Tabelle 13-1.** vSAN -Integritätsprüfungskategorien

| Integritätsprüfungskategorie | Beschreibung |
|---|---|
| Hardwarekompatibilität | Überwachen der Clusterkomponenten, um sicherzustellen, dass diese unterstützte Hardware, Software und Treiber verwenden. |
| Leistungsdienst | Überwachen der Integrität eines vSAN-Leistungsdiensts. |
| Netzwerk | Überwachen der vSAN-Netzwerkintegrität. |
| Physische Festplatte | Überwachen der Integrität von physischen Geräten im vSAN-Cluster. |
| Daten | Überwachen der vSAN-Datenintegrität. |
| Cluster | Überwachen der vSAN-Clusterintegrität. |
| Grenzwerte | Überwachen der vSAN-Clustergrenzwerte. |
| Onlineintegrität | Integrität von vSAN-Clustern überwachen und zur eingehenden Analyse an das Analyse-Back-End-System von VMware senden. Sie müssen am Programm zur Verbesserung der Kundenzufriedenheit (CEIP) teilnehmen, um Online-Integritätsprüfungen durchführen zu können. |

**Tabelle 13-1.** vSAN -Integritätsprüfungskategorien (Fortsetzung)

| Integritätsprüfungskategorie | Beschreibung |
|---|---|
| vSAN-iSCSI-Zieldienst | Überwachen des iSCSI-Zieldiensts, einschließlich der Netzwerkkonfiguration und des Laufzeitstatus. |
| Verschlüsselung | Überwachen der vSAN-Verschlüsselungsintegrität. |
| Ausgeweiteter Cluster | Überwachen der Integrität eines ausgeweiteten Clusters (falls zutreffend). |

vSAN testet jede Integritätsprüfung erneut und aktualisiert die Ergebnisse. Klicken Sie auf **Erneut testen**, um die Integritätsprüfungen durchzuführen und die Ergebnisse umgehend zu aktualisieren.

Wenn Sie am Programm zur Verbesserung der Kundenzufriedenheit (CEIP) teilnehmen, können Sie Integritätsprüfungen durchführen und die Daten zur eingehenden Analyse an VMware senden. Klicken Sie auf **Erneut testen mit Online-Integrität**.

Weitere Informationen zu vSAN-Integritätsprüfungen finden Sie im *VMware Virtual SAN Health Check Plugin Guide* (Handbuch zum VMware Virtual SAN-Integritätsprüfungs-Plug-In).

## Überwachen der vSAN -Integrität auf einem Host

Der ESXi-Host-Client ist eine browserbasierte Schnittstelle zum Verwalten eines einzelnen ESXi-Hosts. Sie können mit seiner Hilfe den Host verwalten, wenn vCenter Server nicht zur Verfügung steht. Der Host-Client stellt Registerkarten für das Verwalten und Überwachen von vSAN auf Hostebene bereit.

- Auf der Registerkarte **vSAN** wird die vSAN-Basiskonfiguration angezeigt.
- Auf der Registerkarte **Hosts** werden die Hosts angezeigt, die am vSAN-Cluster beteiligt sind.
- Auf der Registerkarte **Integrität** werden Integritätsprüfungen auf Hostebene angezeigt.

## Konfigurieren des vSAN -Integritätsdiensts

Sie können das Integritätsprüfungsintervall für den vSAN-Integritätsdienst konfigurieren.

Der vSAN-Integritätsdienst ist standardmäßig aktiviert. Sie können regelmäßige Integritätsprüfungen aktivieren bzw. deaktivieren und das Integritätsprüfungsintervall festlegen.

### Vorgehensweise

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

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

3 Wählen Sie unter „vSAN“ die Option **Integrität und Leistung** aus.

4 Klicken Sie auf die Schaltfläche **Einstellungen bearbeiten** für die Integritätsdienste.

   a Um regelmäßige Integritätsprüfungen zu deaktivieren, deaktivieren Sie die Option **Regelmäßige Systemprüfung aktivieren**.

   Sie können auch das Zeitintervall zwischen den Integritätsprüfungen festlegen.

   b Um regelmäßige Integritätsprüfungen zu aktivieren, aktivieren Sie die Option **Regelmäßige Systemprüfung aktivieren**.

## Überprüfen der vSAN -Integrität

Sie können den Status von vSAN-Integritätsprüfungen anzeigen, um die Konfiguration und den Betrieb Ihres vSAN-Clusters zu überprüfen.

### Voraussetzungen

Der vSAN-Integritätsdienst muss aktiviert werden, bevor Sie Integritätsprüfungen anzeigen können.

#### Vorgehensweise

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

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.

3 Wählen Sie **Integrität** aus, um die Kategorien für die vSAN-Integritätsprüfung zu überprüfen.

Wenn in der Spalte „Testergebnis“ das Ergebnis „Warnung“ oder „Fehlgeschlagen“ angezeigt wird, erweitern Sie die Kategorie, um die Ergebnisse der einzelnen Integritätsprüfungen zu überprüfen.

4 Wählen Sie eine einzelne Integritätsprüfung aus und prüfen Sie die detaillierten Informationen unten auf der Seite.

Sie können auf die Schaltfläche **VMware fragen** klicken, um einen Knowledgebase-Artikel zu öffnen, in dem die Integritätsprüfung beschrieben wird und Informationen zur Fehlerbehebung bereitgestellt werden.

## Überwachen von vSAN über den ESXi-Host-Client

Sie können die Integrität und die grundlegende Konfiguration von vSAN über den ESXi-Host Client überwachen.

#### Voraussetzungen

Der vSAN-Integritätsdienst muss aktiviert werden, bevor Sie Integritätsprüfungen anzeigen können.

#### Vorgehensweise

1 Starten Sie einen Browser und geben Sie die IP-Adresse des Hosts ein.

Der Browser leitet Sie auf die Anmeldeseite für den Host Client um.

2 Geben Sie den Benutzernamen und das Kennwort für den Host ein und klicken Sie auf **Anmelden**.

3 Klicken Sie im Navigator des Host Clients auf **Speicher**.

4 Klicken Sie auf der Hauptseite auf den vSAN-Datenspeicher, um den Link „Überwachen“ im Navigator anzuzeigen.

5 Klicken Sie auf die Registerkarten, um die vSAN-Informationen für den Host anzuzeigen.

a Klicken Sie auf die Registerkarte **vSAN**, um die vSAN-Basiskonfiguration anzuzeigen.

b Klicken Sie auf die Registerkarte **Hosts**, um die Hosts anzuzeigen, die am vSAN-Cluster beteiligt sind.

c Klicken Sie auf die Registerkarte **Integrität**, um Integritätsprüfungen auf Hostebene anzuzeigen.

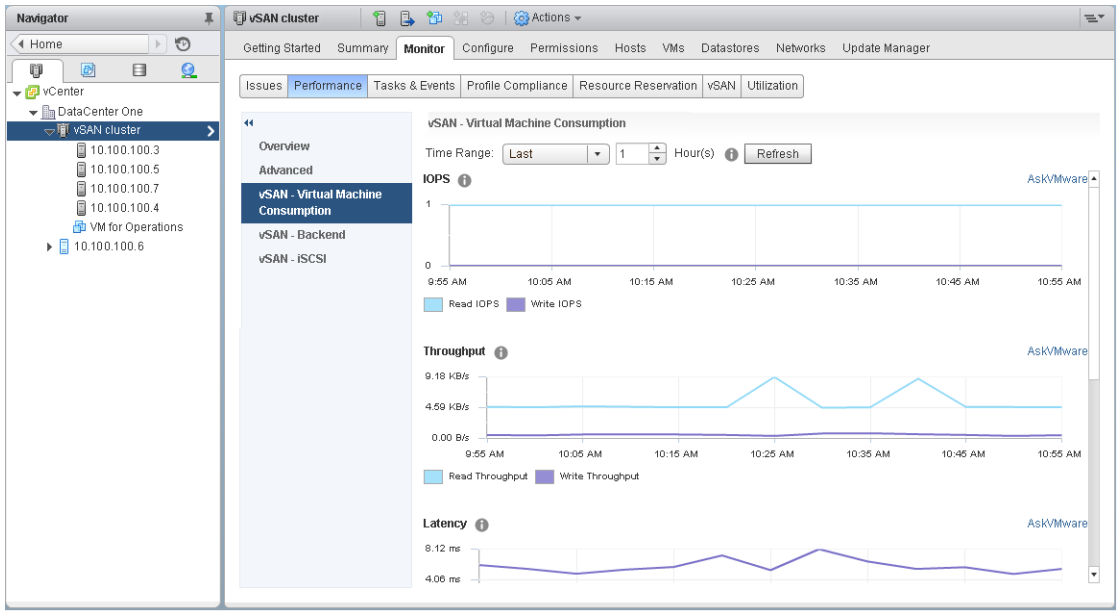
6 (Optional) Klicken Sie auf der Registerkarte **vSAN** auf **Einstellungen bearbeiten**, um Konfigurationsprobleme auf Hostebene zu beheben. Wählen Sie die Werte aus, die der Konfiguration des vSAN-Clusters entsprechen.

Wählen Sie die Werte aus, die der Konfiguration des vSAN-Clusters entsprechen und klicken Sie auf **Speichern**.

# Überwachen der vSAN -Leistung

Sie können den vSAN-Leistungsdienst verwenden, um die Leistung Ihrer vSAN-Umgebung zu überwachen und potenzielle Probleme zu untersuchen.

Der Leistungsdienst erfasst und analysiert Leistungsstatistiken und zeigt die Daten in einem grafischen Format an. Sie können die Leistungsdiagramme verwenden, um Ihre Arbeitslast zu verwalten und Problemursachen zu ermitteln.




Wenn der vSAN-Leistungsdienst eingeschaltet ist, finden Sie in der Cluster-Übersicht eine Zusammenfassung der vSAN-Leistungsstatistiken, einschließlich IOPS, Durchsatz und Latenz. Sie können detaillierte Leistungsstatistiken für den Cluster und für alle Hosts, Festplattengruppen und Festplatten im vSAN-Cluster anzeigen. Sie können auch Leistungsdiagramme für virtuelle Maschinen und virtuelle Festplatten anzeigen.

## Einschalten des vSAN -Leistungsdiensts

Wenn Sie einen vSAN-Cluster erstellen, ist der Leistungsdienst deaktiviert. Schalten Sie den vSAN-Leistungsdienst ein, um die Leistung von vSAN-Clustern, Hosts, Festplatten und VMs zu überwachen.

Wenn Sie den Leistungsdienst einschalten, platziert vSAN ein Statistikdatenbankobjekt in der Datenbank, um Statistikdaten zu erfassen. Die Statistikdatenbank ist ein Namespace-Objekt im vSAN-Datenspeicher des Clusters.

### Voraussetzungen

- Auf allen Hosts im vSAN-Cluster muss ESXi 6.5 oder höher ausgeführt werden.
- Bevor Sie den vSAN-Leistungsdienst aktivieren, stellen Sie sicher, dass der Cluster ordnungsgemäß konfiguriert ist und keine ungelösten Integritätsprobleme aufweist.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Integrität und Leistung** aus.
4. Klicken Sie auf **Bearbeiten**, um die Einstellungen für den Leistungsdienst zu bearbeiten.
5. Aktivieren Sie das Kontrollkästchen **vSAN-Leistungsdienst einschalten**.

   Sie können den vSAN-Leistungsdienst ausschalten, indem Sie dieses Kontrollkästchen deaktivieren.
6. Wählen Sie eine Speicherrichtlinie für das Statistikdatenbankobjekt aus und klicken Sie auf **OK**.

## Verwenden eines gespeicherten Zeitbereichs

Sie können über die Zeitbereichsauswahl in den Leistungsansichten gespeicherte Zeitbereiche auswählen.

Sie können einen Zeitbereich mit benutzerdefiniertem Namen manuell speichern. Wenn Sie einen Speicherleistungstest durchführen, wird der ausgewählte Zeitbereich automatisch gespeichert. Sie können einen Zeitbereich für jede der Leistungsansichten speichern.

### Voraussetzungen

- Der vSAN-Leistungsdienst muss aktiviert sein.
- Auf allen Hosts im vSAN-Cluster muss ESXi 6.6 oder höher ausgeführt werden.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster.

2 Klicken Sie auf der Registerkarte **Überwachen** auf **Leistung**.

3 Wählen Sie eine beliebige Registerkarte aus, z. B. **vSAN - Back-End**. Wählen Sie in der Dropdown-Liste für Zeitbereiche **Zeitbereich speichern...** aus.

4 Geben Sie einen Namen für den ausgewählten Zeitbereich ein.

5 Klicken Sie auf **OK**.

## Anzeigen der Leistung von vSAN -Clustern

Sie können die Leistungsdiagramme für vSAN-Cluster verwenden, um die Arbeitslast in Ihrem Cluster zu verwalten und Problemursachen zu ermitteln.

Wenn der Leistungsdienst eingeschaltet ist, finden Sie in der Cluster-Übersicht eine Zusammenfassung der vSAN-Leistungsstatistiken. Dazu zählen vSAN-IOPS, Durchsatz und Latenz. Auf der Ebene der Cluster können Sie detaillierte Statistikdiagramme für die Nutzung der virtuellen Maschine sowie für das vSAN-Back-End anzeigen.

### Voraussetzungen

Der vSAN-Leistungsdienst muss aktiviert werden, bevor Sie Leistungsdiagramme anzeigen können.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster.

2 Klicken Sie auf der Registerkarte **Überwachen** auf **Leistung**.

3 Wählen Sie **vSAN - Nutzung der virtuellen Maschine** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

   vSAN zeigt Leistungsdiagramme für Clients an, die auf dem Cluster ausgeführt werden. Dazu zählen IOPS, Durchsatz, Latenz, Überlastung und ausstehende E/A-Vorgänge. Die Statistiken auf diesen Diagrammen werden aus den Hosts innerhalb des Clusters kumuliert.

4 Wählen Sie **vSAN - Back-End** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

   vSAN zeigt Leistungsdiagramme für Cluster-Back-End-Vorgänge an. Dazu zählen IOPS, Durchsatz, Latenz, Überlastung und ausstehende E/A-Vorgänge. Die Statistiken auf diesen Diagrammen werden aus den Hosts innerhalb des Clusters kumuliert.

5 Wählen Sie **vSAN - iSCSI** und wählen Sie ein iSCSI-Ziel oder eine iSCSI-LUN aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

**Hinweis** Um die iSCSI-Leistungsdiagramme anzeigen zu können, muss auf allen Hosts im vSAN-Cluster ESXi 6.6 oder höher ausgeführt werden.

vSAN zeigt Leistungsdiagramme für iSCSI-Ziele bzw. -LUNs an. Dazu zählen IOPS, Bandbreite, Latenz und ausstehende E/A-Vorgänge.

## Anzeigen der Leistung von vSAN -Hosts

Sie können die Leistungsdiagramme für vSAN-Hosts verwenden, um Ihre Arbeitslast zu verwalten und Problemursachen zu ermitteln. Sie können vSAN-Leistungsdiagramme für Hosts, Festplattengruppen und einzelne Speichergeräte verwenden.

Wenn der Leistungsdienst eingeschaltet ist, werden in der Host-Übersicht Leistungsstatistiken für jeden Host und für die jeweils verknüpften Festplatten angezeigt. Auf der Ebene der Hosts können Sie detaillierte Statistikdiagramme für die Nutzung der virtuellen Maschine sowie für das vSAN-Back-End anzeigen. Dazu zählen IOPS, Durchsatz, Latenz und Überlastung. Es sind zusätzliche Diagramme verfügbar, um die Lesecache-IOPS- und Zugriffsrate des lokalen Clients anzuzeigen. Auf der Ebene der Festplattengruppen können Sie Statistiken für die Festplattengruppe anzeigen. Auf der Ebene der Festplatten können Sie Statistiken für ein einzelnes Speichergerät anzeigen.

### Voraussetzungen

Der vSAN-Leistungsdienst muss aktiviert werden, bevor Sie Leistungsdiagramme anzeigen können.

Um die folgenden Leistungsdiagramme anzuzeigen, muss auf Hosts im vSAN-Cluster ESXi 6.6 oder höher ausgeführt werden: physische Adapter, VMkernel-Adapter, Zusammenfassen von VMkernel-Adaptern, iSCSI, vSAN - Back-End-Neusynchronisierungs-E/A, Neusynchronisierungs-IOPS, Neusynchronisierungsdurchsatz, Festplattengruppen-Neusynchronisierungslatenz.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster und wählen Sie einen Host aus.

2 Klicken Sie auf der Registerkarte **Überwachen** auf **Leistung**.

3 Wählen Sie **vSAN - Nutzung der virtuellen Maschine** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für Clients an, die auf dem Host ausgeführt werden. Dazu zählen IOPS, Durchsatz, Latenz, Überlastung und ausstehende E/A-Vorgänge.

4 Wählen Sie **vSAN - Back-End** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für Host-Back-End-Vorgänge an. Dazu zählen IOPS, Durchsatz, Latenz, Überlastung, ausstehende E/A-Vorgänge und Neusynchronisierungs-E/A-Vorgänge.

5 Wählen Sie **vSAN - Festplattengruppe** und dann eine Festplattengruppe aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für die Festplattengruppe an. Dazu zählen Front-End (Gast)-IOPS, Durchsatz, Latenz sowie Overhead-IOPS und Latenz. Angezeigt wird ebenfalls: Lesecache-Zugriffsrate, Bereinigungen, Prozentsatz des freien Schreibpuffers, Kapazität und Nutzung, Destaging-Rate der Festplatte, Überlastungen, ausstehende E/A-Vorgänge, ausstehende E/A-Größe, Prozentsatz der E/A-Verzögerungen, durchschnittliche Latenz der E/A-Verzögerungen, IOPS der internen Warteschlangen, Durchsatz der internen Warteschlange, Neusynchronisierungs-IOPS, Neusynchronisierungsdurchsatz und Neusynchronisierungslatenz.

6 Wählen Sie **vSAN - Festplatte** und dann eine Festplatte aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für die VM an. Dazu zählen IOPS der physischen/Firmware-Ebene, Durchsatz und Latenz.

7 Wählen Sie **vSAN - Physische Adapter** und dann eine Netzwerkkarte aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für die physische Netzwerkkarte (pNIC) an, z. B. Datendurchsatz, Paket pro Sekunde und die Paketverlustrate.

8 Wählen Sie **vSAN - VMkernel-Adapter** und wählen Sie einen VMkernel-Adapter aus, z. B. vmk1. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für den VMkernel-Adapter an, z. B. Datendurchsatz, Paket pro Sekunde und die Paketverlustrate.

9 Wählen Sie **vSAN - Zusammenfassen von VMkernel-Adaptern** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt für alle Netzwerk-E/A-Vorgänge, z. B. Datendurchsatz, Paket pro Sekunde und die Paketverlustrate, die in den von vSAN verwendeten Netzwerkadaptern verarbeitet werden, Leistungsdiagramme an.

10 Wählen Sie **vSAN - iSCSI** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für alle iSCSI-Dienste auf dem Host an. Dazu zählen IOPS, Bandbreite, Latenz und ausstehende E/A-Vorgänge.

## Anzeigen der vSAN -VM-Leistung

Sie können die VM-Leistungsdiagramme für vSAN verwenden, um die Arbeitslast auf Ihren virtuellen Maschinen und virtuellen Festplatten zu überwachen.

Wenn der Leistungsdienst eingeschaltet ist, können Sie detaillierte statistische Diagramme über die VM-Leistung und die Leistung virtueller Festplatten anzeigen. VM-Leistungsstatistiken können nicht während der Migration zwischen Hosts erfasst werden. Daher kann im VM-Leistungsdiagramm eine Lücke von mehreren Minuten entstehen.

**Hinweis** Der Leistungsdienst unterstützt nur virtuelle SCSI-Controller für virtuelle Festplatten. Virtuelle Festplatten, die andere Controller wie zum Beispiel IDE verwenden, werden nicht unterstützt.

### Voraussetzungen

Der vSAN-Leistungsdienst muss aktiviert werden, bevor Sie Leistungsdiagramme anzeigen können.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster und wählen Sie eine VM aus.

2 Klicken Sie auf der Registerkarte **Überwachen** auf **Leistung**.

3 Wählen Sie **vSAN - Nutzung der virtuellen Maschine** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für die VM an. Dazu zählen IOPS, Durchsatz und Latenz.

4 Wählen Sie **vSAN - Virtuelle Festplatte** aus. Wählen Sie einen Zeitraum für Ihre Abfrage aus.

vSAN zeigt Leistungsdiagramme für die virtuellen Festplatten an. Dazu zählen IOPS, verzögerte normalisierte IOPS, virtuelle SCSI-IOPS, virtueller SCSI-Durchsatz und SCSI-Latenz.

## Verwenden der vSAN -Leistungsdiagnose

Mit der vSAN-Leistungsdiagnose können Sie die Leistung Ihres vSAN-Clusters verbessern und Leistungsprobleme beheben.

Das vSAN-Leistungsdiagnosetool analysiert zuvor ausgeführte und vom vSAN-Leistungsdienst erfasste Benchmarks. Dieses Tool erkennt Probleme, schlägt Schritte zur Fehlerbehebung vor und stellt unterstützende Leistungsdiagramme für weitergehende Analysen bereit.

Der vSAN-Leistungsdienst stellt die Daten bereit, die zur Analyse der vSAN-Leistungsdiagnose verwendet werden. vSAN verwendet CEIP, um Daten zur Analyse an VMware zu senden.

**Hinweis** Verwenden Sie die vSAN-Leistungsdiagnose nicht für die allgemeine Auswertung der Leistung für ein vSAN-Produktionscluster.

### Voraussetzungen

- Der vSAN-Leistungsdienst muss aktiviert sein.
- vCenter Server benötigt Internetzugriff, um die ISO-Images und -Patches herunterzuladen.
- Sie müssen am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teilnehmen.

### Vorgehensweise

1 Navigieren Sie im vSphere Web Client-Navigator zum vSAN-Cluster.

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.

3 Wählen Sie **Leistungsdiagnose** aus.

4 Wählen Sie im Dropdown-Menü ein Benchmark-Ziel aus.

Sie können ein Ziel basierend auf der Leistungsverbesserung auswählen, die Sie erreichen möchten, z. B. maximale IOPS-Kapazität, maximaler Durchsatz oder minimale Latenz.

5 Wählen Sie einen Zeitraum für Ihre Abfrage aus.

Der Standardzeitraum ist die aktuelle Stunde. Sie können den Bereich erhöhen, um den letzten 24 Stunden aufzunehmen, oder einen benutzerdefinierten Zeitraum innerhalb der letzten 90 Tage definieren. Wenn Sie das HCIbench-Tool zum Ausführen des Benchmark-Leistungstests auf dem vSAN-Cluster verwenden, wird der Zeitraum dieser Tests im Dropdown-Menü angezeigt.

6 Klicken Sie auf **Senden**.

Wenn Sie auf **Senden** klicken, überträgt vSAN die Leistungsdaten an den vSphere-Back-End-Analyseserver. Nach der Analyse der Daten zeigt das vSAN-Leistungsdiagnosetool eine Liste der Problem an, die sich möglicherweise auf die Benchmark-Leistung für das ausgewählte Ziel ausgewirkt haben.

Durch Klicken können Sie weitere Details zu jedem Problem anzeigen, wie zum Beispiel eine Liste der jeweils betroffenen Elemente. Sie können auch auf den Link **VMware fragen** klicken, um einen Knowledgebase-Artikel mit Empfehlungen zum Beheben des Problems und zum Erreichen Ihres Leistungsziels anzuzeigen.

# Informationen zur Neuverteilung im vSAN -Cluster

Wenn ein Kapazitätsgerät in Ihrem Cluster 80 % Auslastung erreicht, nimmt vSAN automatisch eine Neuverteilung im Cluster vor, bis die Nutzung aller Kapazitätsgeräte unter dem Schwellenwert liegt.

Bei der Neuverteilung im Cluster werden die Ressourcen gleichmäßig im Cluster verteilt, um eine konsistente Leistung und Verfügbarkeit des Clusters zu gewährleisten.

Andere Vorgänge können ebenfalls eine Neuverteilung im Cluster auslösen:

- Wenn vSAN Hardwarefehler im Cluster feststellt
- Wenn vSAN-Hosts mit der Option **Alle Daten evakuieren** in den Wartungsmodus versetzt werden
- Wenn vSAN-Hosts mit der Option **Datenzugriff sicherstellen** in den Wartungsmodus versetzt werden und den Objekten auf dem Host PFTT=0 zugewiesen wurde.

---

**Hinweis** Um ausreichend Speicherplatz für Wartung und erneuten Schutz bereitzustellen und die automatischen Neuverteilungsereignisse im vSAN-Cluster zu minimieren, sollten Sie ständig 30 Prozent freie Kapazität sicherstellen.

---

Sie können die Neuverteilung in Ihrem vSAN-Cluster auch manuell mit dem RVC-Tool (Ruby vSphere Console) durchführen. Siehe „Manuelle Neuverteilung“, auf Seite 160.

## Automatische Neuverteilung

Standardmäßig verteilt vSAN den vSAN Cluster automatisch neu, wenn ein Kapazitätsgerät 80 % Auslastung erreicht. Die Neuverteilung wird auch aktiviert, wenn Sie einen vSAN-Host in den Wartungsmodus versetzen.

Führen Sie die folgenden RVC-Befehle aus, um die Neuverteilung im Cluster zu überwachen:

- `vsan.check_limits`. Überprüft, ob die Festplattenspeichernutzung im Cluster ausgeglichen ist.
- `vsan.whatif_host_failures`. Analysiert die aktuelle Kapazitätsauslastung pro Host, stellt fest, ob ein einzelner Hostfehler den Cluster zwingen kann, dass für den erneuten Schutz nicht ausreichend Speicherplatz verfügbar ist, und analysiert, wie sich ein Hostfehler auf Clusterkapazität, Cache-Reservierung und Clusterkomponenten auswirkt.

  Die als Befehlsausgabe angezeigte physische Kapazitätsnutzung entspricht der durchschnittlichen Nutzung aller Geräte im vSAN-Cluster.
- `vsan.resync_dashboard`. Überwacht alle Neuerstellungsaufgaben im Cluster.

Informationen zu den RVC-Befehlsoptionen finden Sie im *Referenzhandbuch zu den RVC-Befehlen*.

## Manuelle Neuverteilung

Mit Hilfe der Cluster-Integritätsprüfung oder mit RVC-Befehlen können Sie eine manuelle Neuverteilung durchführen.

Wenn die Integritätsprüfung für die vSAN-Festplattenverteilung fehlschlägt, können Sie im vSphere Web Client eine manuelle Neuverteilung initiieren. Greifen Sie unter „Clusterintegrität“ auf die Integritätsprüfung für die vSAN-Festplattenverteilung zu und klicken Sie auf die Schaltfläche **Datenträger neu verteilen**.

Führen Sie die folgenden RVC-Befehle aus, um die Neuverteilung im Cluster durchzuführen:

- `vsan.check_limits`. Überprüft, ob sich die Auslastung irgendeines Kapazitätsgeräts im vSAN-Cluster dem Schwellenwert von 80 Prozent nähert.

- `vsan.proactive_rebalance [opts]<Path to ClusterComputeResource> --start`. Startet den Neuverteilungsvorgang manuell. Wenn Sie diesen Befehl ausführen, überprüft vSAN für den Cluster die aktuelle Verteilung von Komponenten und beginnt mit der Neuverteilung von Komponenten im Cluster. Mithilfe der Befehlsoptionen geben Sie an, wie lange der Neuverteilungsvorgang im Cluster ausgeführt werden soll und wie viele Daten pro Stunde für jeden vSAN-Host verschoben werden sollen. Weitere Informationen zu den Befehlsoptionen für die Verwaltung des Neuverteilungsvorgangs im vSAN-Cluster finden Sie im *Referenzhandbuch zu den RVC-Befehlen*.

  Die Neuverteilung im Cluster generiert viele E/A-Vorgänge. Sie ist deshalb zeitaufwändig und kann die Leistung von virtuellen Maschinen beeinträchtigen.

**Hinweis** Wenn Sie die Festplatten manuell neu verteilen, wird der Vorgang über den ausgewählten Zeitraum hinweg ausgeführt, bis keine weiteren Daten verschoben werden müssen. Der Standardzeitraum beträgt 24 Stunden. Wenn keine Daten verschoben werden, beendet vSAN die Neuverteilungsaufgabe.

Sie können einen Alarm konfigurieren, damit Sie benachrichtigt werden, wenn der bereitgestellte Speicherplatz einen bestimmten Schwellenwert erreicht. Siehe „Erstellen eines vCenter Server-Alarms für ein vSAN-Ereignis“, auf Seite 164.

## Herstellen einer ausgewogenen Festplattennutzung im vSAN -Cluster

Wenn die Festplattennutzung in Ihrem vSAN-Cluster nicht mehr ausgewogen ist, können Sie eine Neuverteilung vornehmen.

Wenn Sie Kapazitätsgeräte aus dem vSAN-Cluster entfernen und neue Kapazitätsgeräte hinzufügen, kann die Kapazitätsauslastung im vSAN-Cluster unausgewogen werden. Wenn der Integritätsüberwachungsdienst von vSAN Sie wegen möglicher Unausgewogenheiten warnt, können Sie eine Neuverteilung in Ihrem Cluster vornehmen.

### Voraussetzungen

Führen Sie den Neuverteilungsvorgang während einer produktionsfreien Zeit aus, um übermäßige Auswirkungen auf den Cluster zu vermeiden.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN**.
3. Klicken Sie auf **Integrität**.
4. Wählen Sie in der Tabelle „vSAN-Integritätsdienst“ die Option **Warnung: vSAN-Datenträgerverteilung** aus.

   Sie können die Datenträgerverteilung der Hosts anzeigen.
5. Klicken Sie auf die Schaltfläche **Datenträger neu verteilen**, um die Neuverteilung in Ihrem Cluster vorzunehmen.

Bei diesem Vorgang werden Komponenten von den überausgelasteten Festplatten zu den unterausgelasteten Festplatten verschoben.

# Verwenden der vSAN -Standardalarme

Sie können die vSAN-Standardalarme zum Überwachen des Clusters, der Hosts und der vorhandenen vSAN-Lizenzen verwenden.

Die Standardalarm werden automatisch ausgelöst, wenn die mit den Ereignissen verbundenen Alarme aktiviert werden oder wenn eine oder alle Bedingungen erfüllt sind, die in den Alarmen angegeben sind. Die Standardalarme können nicht bearbeitet oder gelöscht werden. Um die in Ihren Anforderungen angegebenen Alarme zu konfigurieren, erstellen Sie benutzerdefinierte Alarme für vSAN. Siehe „Erstellen eines vCenter Server-Alarms für ein vSAN-Ereignis“, auf Seite 164.

In der Tabelle sind die vSAN-Standardalarme aufgeführt.

**Tabelle 13-2.** vSAN -Standardalarme

| vSAN-Alarme | Beschreibung |
|---|---|
| Abgelaufene zeitlich begrenzte Lizenz für vSAN | Überwachen der vSAN-Testlizenzen. |
| Registrierung/Aufheben der Registrierung eines VASA-Anbieter-Anbieters auf vSAN-Hosts schlägt fehl | Registrieren oder Aufheben der Registrierung eines VASA-Anbieters ist auf den vSAN-Hosts fehlgeschlagen. |
| Abgelaufene Lizenz für vSAN | Überwachen der abgelaufenen vSAN-Lizenzen. |
| Fehler bei Festplatte(n) eines vSAN-Hosts | Überwachen von Fehlern auf vSAN-Geräten. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Clusterintegrität' | Überwachen der vSAN-Clusterintegrität. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Datenintegrität' | Überwachen der Datenintegrität für vSAN-Cluster. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Grenzwertintegrität' | Überwachen der vSAN-Clustergrenzwerte. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Netzwerkintegrität' | Überwachen der vSAN-Netzwerkintegrität. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Integrität der physischen Festplatte' | Überwachen der Integrität von physischen Geräten im Cluster. |
| vSAN-Integritätsdienstalarm für Gruppentest 'vSAN-HCL-Integrität' | Überwachen der Clusterkomponenten, um sicherzustellen, dass diese unterstützte Hardware, Software und Treiber verwenden. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Softwarezustand-Integrität' | Überwachen der Integrität der aktuell im Cluster verwendeten Software. |
| vSAN-Integritätsdienstalarm für Gruppentest 'Unerwartete vSAN-Integrität' | Überwachen aller unerwarteter Integritätsprobleme im Cluster. |
| vSAN-Integritätsdienstalarm für Gruppentest 'vSAN CLOMD-Aktivität' | Überwachen, dass der CLOMD (Cluster Level Object Manager Daemon), der auf ESXi-Hosts ausgeführt wird und für Datenverschiebungen und -evakuierungen verantwortlich ist, aktiv oder inaktiv ist. |
| vSAN-Integritätsdienstalarm für Gruppentest 'vSAN-Clusterpartition' | Überwachen der vSAN-Clusterpartition. |

Informationen zur Überwachung von Alarmen und Ereignissen sowie zum Bearbeiten vorhandener Alarmeinstellungen finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*.

## Anzeigen von vSAN -Standardalarmen

Verwenden Sie die vSAN-Standardalarme, um Ihre Cluster und Hosts zu überwachen, alle neuen Ereignisse zu analysieren und die Integrität des gesamten Clusters zu bewerten.

**Vorgehensweise**

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

2 Klicken Sie auf **Konfigurieren** und dann auf **Alarmdefinitionen**.

3 Geben Sie im Suchfeld **vSAN** als Suchbegriff für die Anzeige der Alarme ein, die spezifisch für vSAN sind.

Geben Sie die vSAN-Integritätsdienstalarm ein, um nach Integritätsdienstalarmen für vSAN zu suchen.

Die vSAN-Standardalarme werden angezeigt.

4 Klicken Sie in der Liste der Alarme auf jeden einzelnen Alarm, um dessen Alarmdefinition anzuzeigen.

# Verwenden der VMkernel-Beobachtungen zum Erstellen von Alarmen

VMkernel-Beobachtungen (VOBs) sind Systemereignisse, die Sie verwenden können, um vSAN-Alarme zur Überwachung und Fehlerbehebung bei Leistungs- und Netzwerkfehlern im vSAN-Cluster einzurichten. In vSAN werden diese Ereignisse als Beobachtungen bezeichnet.

## VMware ESXi-Beobachtungs-IDs für vSAN

Jedem VOB-Ereignis ist eine ID zugeordnet. Bevor Sie einen vSAN-Alarm in vCenter Server erstellen, müssen Sie eine geeignete VOB-ID für das vSAN-Ereignis ermitteln, für das Sie eine Warnung erstellen möchten. Sie können Warnungen in der VMware ESXi-Beobachtungsprotokolldatei (`vobd.log`) erstellen. Sie sollten z. B. die folgenden VOB-IDs zum Erstellen von Warnungen für einen beliebigen Geräteausfall im Cluster verwenden.

- `esx.problem.vob.vsan.lsom.diskerror`
- `esx.problem.vob.vsan.pdl.offline`

Um die Liste der VOB-IDs für vSAN anzuzeigen, öffnen Sie die Datei `vobd.log`, die sich auf Ihrem ESXi-Host im Verzeichnis `/var/log` befindet. Die Protokolldatei enthält die folgenden VOB-IDs, die Sie zum Erstellen von vSAN-Alarmen verwenden können.

**Tabelle 13-3.** VOB-IDs für vSAN

| VOB-ID | Beschreibung |
|---|---|
| esx.audit.vsan.clustering.enabled | Der vSAN-Clusterdienst ist aktiviert. |
| esx.clear.vob.vsan.pdl.online | Das vSAN-Gerät ist in den Onlinemodus gewechselt. |
| esx.clear.vsan.clustering.enabled | Die vSAN-Clusterdienste sind aktiviert. |
| esx.clear.vsan.vsan.network.available | vSAN verfügt über eine aktive Netzwerkkonfiguration. |
| esx.clear.vsan.vsan.vmknic.ready | Eine zuvor gemeldete Vmknic hat eine gültige IP erhalten. |
| esx.problem.vob.vsan.lsom.componentthreshold | vSAN hat die maximale Anzahl von Knotenkomponenten fast erreicht. |
| esx.problem.vob.vsan.lsom.diskerror | Ein vSAN-Gerät befindet sich in einem permanenten Fehlerzustand. |
| esx.problem.vob.vsan.lsom.diskgrouplimit | Das Erstellen einer neuen Festplattengruppe in vSAN schlägt fehl. |
| esx.problem.vob.vsan.lsom.disklimit | Das Hinzufügen von Geräten zu einer Festplattengruppe in vSAN schlägt fehl. |
| esx.problem.vob.vsan.lsom.diskunhealthy | vSAN-Festplatte ist fehlerhaft. |

**Tabelle 13-3.** VOB-IDs für vSAN (Fortsetzung)

| VOB-ID | Beschreibung |
|---|---|
| esx.problem.vob.vsan.pdl.offline | Ein vSAN-Gerät ist offline. |
| esx.problem.vsan.clustering.disabled | Die vSAN-Clusterdienste sind deaktiviert. |
| esx.problem.vsan.lsom.congestionthreshold | Die Arbeitsspeicher- bzw. SSD-Überlastung des vSAN-Geräts wurde aktualisiert. |
| esx.problem.vsan.net.not.ready | Eine vmknic ohne eine gültige IP-Adresse wurde zur vSAN-Netzwerkkonfiguration hinzugefügt. Dies geschieht, wenn das vSAN-Netzwerk nicht bereit ist. |
| esx.problem.vsan.net.redundancy.lost | Die vSAN-Netzwerkkonfiguration verfügt nicht über die erforderliche Redundanz. |
| esx.problem.vsan.no.network.connectivity | vSAN verfügt nicht über eine Netzwerkkonfiguration. |
| esx.problem.vsan.vmknic.not.ready | Eine vmknic ohne eine gültige IP-Adresse wurde zur vSAN-Netzwerkkonfiguration hinzugefügt. |

## Erstellen eines vCenter Server-Alarms für ein vSAN -Ereignis

Sie können Alarme zum Überwachen von Ereignissen für das ausgewählte vSAN-Objekt erstellen, einschließlich des Clusters, der Hosts, Datenspeicher, Netzwerke und virtuellen Maschinen.

### Voraussetzungen

Sie müssen über die erforderliche Berechtigungsstufe `Alarms.Create Alarm` oder `Alarm.Modify Alarm` verfügen.

### Vorgehensweise

1 Wählen Sie das vCenter Server-Objekt in der Bestandsliste aus, das Sie überwachen möchten.

2 Klicken Sie auf die Registerkarte **Konfigurieren** > **Alarmdefinitionen** > und klicken Sie dann auf das ✚-Symbol.

3 Geben Sie einen Namen und eine Beschreibung für den neuen Alarm ein.

4 Wählen Sie im Dropdown-Menü **Überwachen** das Objekt aus, für das Sie einen Alarm konfigurieren möchten.

5 Klicken Sie auf **bestimmte Ereignisse, die auf dieses Objekt wirken, z. B. VM-Einschaltvorgänge** und klicken Sie dann auf **Weiter**.

6 Klicken Sie auf **Auslöser**, um ein vSAN-Ereignis hinzuzufügen, das den Alarm auslöst. Die verfügbaren Optionen auf der Seite „Auslöser“ hängen vom Aktivitätstyp ab, den Sie überwachen möchten.

7 Klicken Sie auf das Symbol **Hinzufügen** ( ✚ ).

8 Klicken Sie auf die Spalte **Ereignis** und wählen Sie eine Option aus dem Dropdown-Menü aus.

9 Klicken Sie auf die Spalte **Status** und wählen Sie eine Option aus dem Dropdown-Menü aus.

10 (Optional) Konfigurieren Sie zusätzliche Bedingungen, die eintreten müssen, bevor der Alarm auslöst.

   a Klicken Sie auf das Symbol **Hinzufügen**, um ein Argument hinzuzufügen.

   b Klicken Sie in die Spalte **Argument** und wählen Sie eine Option aus dem Dropdown-Menü aus.

   c Klicken Sie auf die Spalte **Operator** und wählen Sie eine Option aus dem Dropdown-Menü aus.

   d Klicken Sie auf die Spalte **Wert** und geben Sie einen Wert in das Textfeld ein.

   Sie können mehrere Argumente hinzufügen.

11 Klicken Sie auf **Weiter**.

Sie haben Alarmauslöser ausgewählt und konfiguriert.

# Behandeln von Fehlern und Fehlerbehebung in vSAN 14

Falls bei der Verwendung vom vSAN Probleme auftreten, können Sie Fehlerbehebungsthemen heranziehen. Diese Themen helfen Ihnen beim Verständnis des Problems und bieten soweit verfügbar eine Problemumgehung an.

Dieses Kapitel behandelt die folgenden Themen:



## Verwenden von Esxcli-Befehlen mit vSAN

Verwenden Sie Esxcli-Befehle zum Abrufen von Informationen zu vSAN und für die Problembehandlung Ihrer vSAN-Umgebung.

Die folgenden Befehle sind verfügbar:

| Befehl | Beschreibung |
|---|---|
| `esxcli vsan network list` | Überprüft, welche VMkernel-Adapter für die Kommunikation des vSAN verwendet werden. |
| `esxcli vsan storage list` | Listet die von vSAN beanspruchten Speicherfestplatten auf. |
| `esxcli vsan cluster get` | Ruft vSAN-Clusterinformationen ab. |
| `esxcli vsan health` | Ruft den vSAN-Clusterintegritätsstatus ab. |
| `esxcli vsan debug` | Rufen vSAN-Cluster-Debuginformationen ab. |

Die `esxcli vsan debug`Befehle helfen Ihnen beim Debuggen und bei der Fehlerbehebung in Bezug auf den vSAN-Cluster, insbesondere wenn vCenter Server nicht verfügbar ist.

Verwendung: `esxcli vsan debug {cmd} [cmd options]`

Debugbefehle:

| Befehl | Beschreibung |
|---|---|
| `esxcli vsan debug disk` | Debuggen von physischen vSAN-Festplatten. |
| `esxcli vsan debug object` | Debuggen von vSAN-Objekten. |

| Befehl | Beschreibung |
|---|---|
| `esxcli vsan debug resync` | Debuggen von vSAN-Objekten zur Neusynchronisierung. |
| `esxcli vsan debug controller` | Debuggen von vSAN-Festplatten-Controllern. |
| `esxcli vsan debug limit` | Debuggen von vSAN-Grenzwerten. |
| `esxcli vsan debug vmdk` | Debuggen von vSAN-VMDKs. |

Beispiel für `esxcli vsan debug`-Befehle:

```
esxcli vsan debug disk summary get
   Overall Health: green
   Component Metadata Health: green
   Memory Pools (heaps): green
   Memory Pools (slabs): green

esxcli vsan debug disk list
UUID: 52e1d1fa-af0e-0c6c-f219-e5e1d224b469
   Name: mpx.vmhba1:C0:T1:L0
   SSD: False
   Overall Health: green
   Congestion Health:
         State: green
         Congestion Value: 0
         Congestion Area: none
   In Cmmds: true
   In Vsi: true
   Metadata Health: green
   Operational Health: green
   Space Health:
         State: green
         Capacity: 107365793792 bytes
         Used: 1434451968 bytes
         Reserved: 150994944 bytes

esxcli vsan debug object health summary get
    Health Status                                 Number Of Objects
    --------------------------------------------  -----------------
    reduced-availability-with-no-rebuild-delay-timer                0
    reduced-availability-with-active-rebuild                        0
    inaccessible                                                    0
    data-move                                                       0
    healthy                                                         1
    nonavailability-related-incompliance                            0
    nonavailability-related-reconfig                                0
    reduced-availability-with-no-rebuild                            0

esxcli vsan debug object list
    Object UUID: 47cbdc58-e01c-9e33-dada-020010d5dfa3
       Version: 5
       Health: healthy
       Owner:
       Policy:
          stripeWidth: 1
          CSN: 1
          spbmProfileName: vSAN Default Storage Policy
          spbmProfileId: aa6d5a82-1c88-45da-85d3-3d74b91a5bad
          forceProvisioning: 0
```

```
            cacheReservation: 0
            proportionalCapacity: [0, 100]
            spbmProfileGenerationNumber: 0
            hostFailuresToTolerate: 1

         Configuration:
            RAID_1
               Component: 47cbdc58-6928-333f-0c51-020010d5dfa3
                 Component State: ACTIVE,  Address Space(B): 273804165120 (255.00GB),
                 Disk UUID: 52e95956-42cf-4d30-9cbe-763c616614d5, Disk Name: mpx.vmhba1..
                 Votes: 1,  Capacity Used(B): 373293056 (0.35GB),
                 Physical Capacity Used(B): 369098752 (0.34GB),  Host Name: sc-rdops...
               Component: 47cbdc58-eebf-363f-cf2b-020010d5dfa3
                 Component State: ACTIVE,  Address Space(B): 273804165120 (255.00GB),
                 Disk UUID: 52d11301-1720-9901-eb0a-157d68b3e4fc,  Disk Name: mpx.vmh...
                 Votes: 1,  Capacity Used(B): 373293056 (0.35GB),
                 Physical Capacity Used(B): 369098752 (0.34GB),  Host Name: sc-rdops-vm..
            Witness: 47cbdc58-21d2-383f-e45a-020010d5dfa3
              Component State: ACTIVE,  Address Space(B): 0 (0.00GB),
              Disk UUID: 52bfd405-160b-96ba-cf42-09da8c2d7023,  Disk Name: mpx.vmh...
              Votes: 1,  Capacity Used(B): 12582912 (0.01GB),
              Physical Capacity Used(B): 4194304 (0.00GB),  Host Name: sc-rdops-vm...

         Type: vmnamespace
         Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/New Virtual Machine
         Group UUID: 00000000-0000-0000-0000-000000000000
         Directory Name: New Virtual Machine

esxcli vsan debug controller list
    Device Name: vmhba1
         Device Display Name: LSI Logic/Symbios Logic 53c1030 PCI-X Fusion-MPT Dual Ult..
         Used By VSAN: true
         PCI ID: 1000/0030/15ad/1976
         Driver Name: mptspi
         Driver Version: 4.23.01.00-10vmw
         Max Supported Queue Depth: 127

esxcli vsan debug limit get
         Component Limit Health: green
         Max Components: 750
         Free Components: 748
         Disk Free Space Health: green
         Lowest Free Disk Space: 99 %
         Used Disk Space: 1807745024 bytes
         Used Disk Space (GB): 1.68 GB
         Total Disk Space: 107365793792 bytes
         Total Disk Space (GB): 99.99 GB
         Read Cache Free Reservation Health: green
```

```
       Reserved Read Cache Size: 0 bytes
       Reserved Read Cache Size (GB): 0.00 GB
       Total Read Cache Size: 0 bytes
       Total Read Cache Size (GB): 0.00 GB

esxcli vsan debug vmdk list
    Object: 50cbdc58-506f-c4c2-0bde-020010d5dfa3
       Health: healthy
       Type: vdisk
       Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/47cbdc58-e01c-9e33-
             dada-020010d5dfa3/New Virtual Machine.vmdk
       Directory Name: N/A

esxcli vsan debug resync list
   Object            Component              Bytes Left To Resync  GB Left To Resync
   ----------------  ---------------------  --------------------  -----------------
   31cfdc58-e68d...  Component:23d1dc58...             536870912  0.50
   31cfdc58-e68d...  Component:23d1dc58...            1073741824  1.00
   31cfdc58-e68d...  Component:23d1dc58...            1073741824  1.00
```

# Die Konfiguration von vSAN auf einem ESXi -Host schlägt möglicherweise fehl

Unter bestimmten Umständen kann die Konfiguration für vSAN auf einem bestimmten Host fehlschlagen.

### Problem

Ein ESXi-Host, der einem vSAN-Cluster beitritt, kann vSAN möglicherweise nicht konfigurieren.

### Ursache

Falls ein Host die Hardwareanforderungen nicht erfüllt oder sonstige Probleme auftreten, kann vSAN möglicherweise den Host nicht konfigurieren. Beispielsweise kann die Konfiguration für vSAN durch nicht genügend Arbeitsspeicher auf dem Host verhindert werden.

### Lösung

1 Versetzen Sie den Host, der den Fehler verursacht, in den Wartungsmodus.

2 Verschieben Sie den Host aus dem Cluster für vSAN.

3 Beheben Sie das Problem, das die Konfiguration des vSAN für den Host verhindert.

4 Beenden Sie den Wartungsmodus.

5 Verschieben Sie den Host wieder in den Cluster für vSAN.

# Nicht übereinstimmende VM-Objekte stimmen nicht sofort überein

Wenn Sie die Schaltfläche **Übereinstimmung prüfen** verwenden, ändert ein VM-Objekt seinen Status von „Keine Übereinstimmung“ auf „Übereinstimmung“ auch dann nicht, wenn die Ressourcen für vSAN verfügbar sind und das Profil der virtuellen Maschine erfüllen.

### Problem

Wenn Sie die Option zum Erzwingen der Bereitstellung verwenden, können Sie ein VM-Objekt auch dann verwenden, wenn die im Profil der virtuellen Maschine angegebene Richtlinie nicht durch die derzeit im Cluster für vSAN verfügbaren Ressourcen erfüllt werden können. Das Objekt wurde erstellt, bleibt aber im Status „Keine Übereinstimmung“.

vSAN sollte die Anforderungen für das Objekt erfüllen, wenn die Speicherressourcen im Cluster verfügbar werden, wenn Sie zum Beispiel einen Host hinzufügen. Der Status des Objekts ändert sich nicht sofort auf „Übereinstimmung“, nachdem Sie die Ressourcen hinzugefügt haben.

### Ursache

Dies tritt auf, weil vSAN die Geschwindigkeit der Neukonfiguration reguliert, um eine Systemüberlastung zu verhindern. Die Zeitdauer bis zur zu erreichenden Übereinstimmung hängt von der Anzahl der Objekte im Cluster, der E/A-Last auf dem Cluster und der Größe des betroffenen Objekts ab. In den meisten Fällen wird die Übereinstimmung innerhalb einer angemessenen Zeit erreicht.

## vSAN -Cluster-Konfigurationsprobleme

Nachdem Sie die vSAN-Konfiguration geändert haben, führt vCenter Server Validierungsprüfungen für die vSAN-Konfiguration durch. Validierungsprüfungen werden auch als Teil eines Hostsynchronisierungsvorgangs durchgeführt. Falls vCenter Server Probleme bei der Konfiguration feststellt, werden Fehlermeldungen angezeigt.

### Problem

Fehlermeldungen deuten darauf hin, dass vCenter Server ein Problem mit der vSAN-Konfiguration erkannt hat.

### Lösung

Verwenden Sie die folgenden Methoden, um Probleme bei der Konfiguration des vSAN zu beheben.

**Tabelle 14-1.** vSAN -Konfigurationsfehler und entsprechende Lösungen

| vSAN-Konfigurationsfehler | Lösung |
|---|---|
| Host mit aktiviertem VSAN-Dienst gehört nicht zum vCenter-Cluster. | Fügen Sie den Host zum vSAN-Cluster hinzu.<br>1 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wechseln zu**.<br>2 Wählen Sie den vSAN-Cluster aus und klicken Sie auf **OK**. |
| Host gehört zu einem Cluster mit aktiviertem VSAN, hat jedoch selbst den VSAN-Dienst nicht aktiviert. | Prüfen Sie, ob das vSAN-Netzwerk ordnungsgemäß konfiguriert und auf dem Host aktiviert ist. Siehe „Konfigurieren eines vSAN-Netzwerks“, auf Seite 44. |
| VSAN-Netzwerk ist nicht konfiguriert | Konfigurieren Sie das vSAN-Netzwerk. Siehe „Konfigurieren eines vSAN-Netzwerks“, auf Seite 44. |
| Host kann nicht mit den anderen Knoten in dem Cluster mit aktiviertem VSAN kommunizieren | Könnte durch die Netzwerkisolation verursacht worden sein. Weitere Informationen finden Sie in der Dokumentation „Netzwerkanforderungen für vSAN“, auf Seite 19. |
| Es wurde ein weiterer Host gefunden, der am VSAN-Dienst teilnimmt und kein Mitglied des vCenter-Clusters dieses Hosts ist. | Stellen Sie sicher, dass die vSAN-Clusterkonfiguration korrekt ist und sich alle vSAN-Hosts im selben Subnetz befinden. Siehe „Entwerfen des vSAN-Netzwerks“, auf Seite 30. |

# Behandeln von Fehlern in vSAN

vSAN reagiert auf Fehler der Speichergeräte, Hosts und des Netzwerks im Cluster entsprechend der Schwere des Fehlers. Sie können Probleme in vSAN durch Überwachen der Leistung des Datenspeichers und Netzwerks für vSAN diagnostizieren.

## Fehlerbehandlung in vSAN

vSAN implementiert Mechanismen, um auf Fehler hinzuweisen und nicht verfügbare Daten für den Datenschutz neu zu erstellen.

### Fehlerzustände von vSAN -Komponenten

In vSAN können fehlerhafte Komponenten im Zustand „Abwesend“ oder „Herabgestuft“ sein. Entsprechend dem Komponentenzustand verwendet vSAN verschiedene Ansätze zum Wiederherstellen von Daten der virtuellen Maschine.

vSAN bietet auch Informationen zu der Art des Komponentenfehlers. Siehe „Verwenden der VMkernel-Beobachtungen zum Erstellen von Alarmen“, auf Seite 163 und „Verwenden der vSAN-Standardalarme“, auf Seite 162.

vSAN unterstützt zwei Arten von Fehlerzuständen für Komponenten:

**Tabelle 14-2.** Fehlerzustände von Komponenten in vSAN

| Komponenten-fehlerzustand | Beschreibung | Wiederherstellen | Ursache |
|---|---|---|---|
| Herabgestuft | Eine Komponente befindet sich im herabgestuften Zustand, wenn vSAN einen permanenten Komponentenfehler erkennt und annimmt, dass eine Wiederherstellung der Komponente in einen funktionsfähigen Zustand nicht erfolgt. | vSAN beginnt sofort mit dem Neuaufbau der betroffenen Komponenten. | ■ Fehler eines Flash-Zwischenspeichergeräts<br>■ Fehler bei einem magnetischen Gerät oder einem Flash-Kapazitätsgerät<br>■ Speicher-Controller-Ausfall |
| Abwesend | Eine Komponente befindet sich im Zustand „Abwesend“, wenn vSAN einen temporären Komponentenfehler erkennt und eine Wiederherstellung der Komponente in einen funktionsfähigen Zustand möglich scheint. | vSAN beginnt mit dem Neuaufbau abwesender Komponenten, wenn sie innerhalb eines bestimmten Zeitraums nicht verfügbar sind. Standardmäßig beginnt vSAN nach 60 Minuten mit dem Neuaufbau abwesender Komponenten. | ■ Netzwerkkonnektivität unterbrochen<br>■ Fehler eines physischen Netzwerkadapters<br>■ ESXi-Hostfehler<br>■ Nicht angeschlossenes Flash-Zwischenspeichergerät<br>■ Magnetische Festplatte oder Flash-Kapazitätsgerät nicht angeschlossen |

#### Analysieren des Fehlerstatus einer Komponente

Mit dem vSphere Web Client können Sie analysieren, ob eine Komponente den Fehlerstatus „Abwesend“ oder „Herabgestuft“ aufweist.

Wenn ein Fehler im Cluster auftritt, markiert vSAN die Komponenten für ein Objekt in Abhängigkeit vom Schweregrad des Fehlers als „Abwesend“ oder „Herabgestuft“.

#### Vorgehensweise

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

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN** und wählen Sie **Virtuelle Festplatten** aus.

Die Stammverzeichnisse und virtuellen Festplatten der virtuellen Maschinen im Cluster werden angezeigt.

3 Wählen Sie ein VM-Objekt aus.

4 Analysieren Sie auf der Registerkarte **Platzierung physischer Festplatten** für das ausgewählte Objekt die Eigenschaft „Komponentenzustand" der Komponenten.

Die Eigenschaft „Komponentenzustand" entspricht „Abwesend" oder „Herabgestuft", wenn ein Fehler im vSAN-Cluster aufgetreten ist.

## Objektzustände, die auf Probleme in vSAN hinweisen

Prüfen Sie den Übereinstimmungsstatus und den Betriebszustand eines VM-Objekts, um zu ermitteln, wie ein Fehler im Cluster sich auf die virtuelle Maschine auswirkt.

**Tabelle 14-3.** Objektstatus

| Objektstatustyp | Beschreibung |
|---|---|
| Übereinstimmungsstatus | Der Übereinstimmungsstatus eines VM-Objekts zeigt an, ob es die Anforderungen der zugewiesen VM-Speicherrichtlinie erfüllt. |
| Betriebszustand | Der Betriebszustand eines Objekts kann „Ordnungsgemäß" oder „Nicht ordnungsgemäß" sein. Er zeigt die Art und die Anzahl der Fehler im Cluster an.<br>Ein Objekt ist ordnungsgemäß, wenn eine unbeschädigte Replik verfügbar ist und mehr als 50 Prozent der Stimmen des Objekts noch verfügbar sind.<br>Ein Objekt ist nicht ordnungsgemäß, wenn keine vollständige Replik verfügbar ist oder weniger als 50 Prozent der Stimmen des Objekts nicht verfügbar sind. Ein Objekt kann beispielsweise nicht ordnungsgemäß werden, wenn ein Netzwerkfehler im Cluster auftritt und ein Host isoliert wird. |

Um zu ermitteln, welchen Einfluss ein Fehler auf einer virtuellen Maschine insgesamt hat, untersuchen Sie den Übereinstimmungsstatus und den Betriebszustand. Wenn der Betriebszustand ordnungsgemäß bleibt, obwohl das Objekt nicht übereinstimmend ist, kann die virtuelle Maschine den Datenspeicher für vSAN weiter verwenden. Wenn der Betriebszustand nicht ordnungsgemäß ist, kann die virtuelle Maschine den Datenspeicher nicht verwenden.

### Untersuchen des Systemzustands eines Objekts in vSAN

Verwenden Sie vSphere Web Client, um den Systemzustand einer virtuellen Maschine zu untersuchen. Der Systemzustand einer virtuellen Maschine wird als ordnungsgemäß betrachtet, wenn ein Replikat des VM-Objekts und mehr als 50 Prozent der Stimmen für ein Objekt verfügbar sind.

#### Vorgehensweise

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

2 Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN** und wählen Sie **Virtuelle Festplatten** aus.

Die Stammverzeichnisse und virtuellen Festplatten der virtuellen Maschinen im Cluster werden angezeigt.

3 Untersuchen Sie für ein VM-Objekt den Wert der Eigenschaft „Betriebszustand".

Ist der Betriebszustand nicht ordnungsgemäß, wird der Grund für den nicht ordnungsgemäßen Zustand von vSphere Web Client in Klammern angezeigt.

### Untersuchen der Übereinstimmung einer virtuellen Maschine in vSAN

Verwenden Sie vSphere Web Client, um zu untersuchen, ob ein VM-Objekt die zugewiesene VM-Speicherrichtlinie einhält.

#### Vorgehensweise

1 Überprüfen Sie den Status der Richtlinieneinhaltung einer virtuellen Maschine.

   a Navigieren Sie zur virtuellen Maschine im Navigator von vSphere Web Client.

   b Untersuchen Sie auf der Registerkarte **Übersicht** den Wert der Eigenschaft „VM-Speicherrichtlinieneinhaltung“ unter „VM-Speicherrichtlinien“.

2 Überprüfen Sie den Status der Richtlinieneinhaltung der Objekte der virtuellen Maschine.

   a Navigieren Sie im vSphere Web Client zum vSAN-Cluster.

   b Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN** und wählen Sie **Virtuelle Festplatten** aus.

   c Wählen Sie ein VM-Objekt aus.

   d Untersuchen Sie den Wert der Eigenschaft „Übereinstimmungsstatus“ für das Objekt. Wenn der Übereinstimmungsstatus nicht „Übereinstimmung“ lautet, ermitteln Sie die Ursache für die Nichtübereinstimmung.

      - Untersuchen Sie den Betriebszustand des Objekts und überprüfen Sie, ob es einen ordnungsgemäßen Systemzustand aufweist.
      - Untersuchen Sie auf der Registerkarte **Übereinstimmungsfehler**, welche Anforderungen der VM-Speicherrichtlinie das Objekt nicht einhalten kann.
      - Untersuchen Sie auf der Registerkarte **Platzierung physischer Festplatten** den Zustand der Objektkomponenten.

## Zugriffsfähigkeit von virtuellen Maschinen bei einem Fehler in vSAN

Wenn eine virtuelle Maschine vSAN-Speicher verwendet, ändert sich möglicherweise ihre Zugriffsfähigkeit auf den Speicher in Abhängigkeit von der Art des Fehlers im vSAN-Cluster.

Änderungen bei der Zugriffsfähigkeit ergeben sich, wenn im Cluster mehr Fehler auftreten, als von der Richtlinie für ein VM-Objekt toleriert werden.

Aufgrund eines Fehlers im vSAN-Cluster ist möglicherweise kein Zugriff mehr auf ein VM-Objekt möglich. Auf ein Objekt ist kein Zugriff möglich, wenn kein vollständiges Replikat des Objekts verfügbar ist, da der Fehler alle Replikate betrifft, oder wenn weniger als 50 Prozent der Stimmen des Objekts verfügbar sind.

In Abhängigkeit vom Objekttyp, auf den kein Zugriff möglich ist, verhalten sich virtuelle Maschinen wie folgt:

**Tabelle 14-4.** Keine Zugriffsmöglichkeit auf VM-Objekte

| Objekttyp | Zustand der virtuellen Maschine | VM-Symptome |
|---|---|---|
| VM-Home-Namespace | ■ Kein Zugriff<br>■ Verwaist, wenn vCenter Server oder der ESXi-Host nicht auf die `.vmx`-Datei der virtuellen Maschine zugreifen kann. | Der Prozess der virtuellen Maschine stürzt möglicherweise ab und die virtuelle Maschine wird ausgeschaltet. |
| VMDK | Kein Zugriff | Die virtuelle Maschine bleibt eingeschaltet, aber die E/A-Vorgänge auf der VMDK werden nicht ausgeführt. Nach Ablauf einer festgelegten Zeitüberschreitung beendet das Gastbetriebssystem die Vorgänge. |

Der Zustand, dass nicht auf eine virtuelle Maschine zugegriffen werden kann, ist nicht permanent. Nachdem das zugrunde liegende Problem behoben wurde und ein vollständiges Replikat und mehr als 50 Prozent der Stimmen des Objekts wiederhergestellt wurden, ist der Zugriff auf die virtuelle Maschine automatisch wieder möglich.

## Speichergerät schlägt in einem vSAN -Cluster fehl

vSAN überwacht die Leistung aller Speichergeräte und isoliert proaktiv fehlerhafte Geräte. Graduelle Fehler eines Speichergeräts werden erkannt und das Gerät wird isoliert, bevor der Überlastungsschwellenwert innerhalb des betroffenen Hosts und des gesamten vSAN-Clusters erreicht wird.

Falls ein Festplatte anhaltend hohe Latenzen hat oder anhaltend überlastet ist, betrachtet vSAN das Gerät als Festplatte, die auszufallen droht, und evakuiert die Daten von der Festplatte. vSAN reagiert auf eine Festplatte, die auszufallen droht, indem es Daten evakuiert oder neu erstellt. Es ist keine Benutzeraktion erforderlich, es sei denn, dem Cluster mangelt es an Ressourcen oder er enthält Objekte, auf die nicht zugegriffen werden kann.

### Komponentenfehlerzustand und Zugriffsfähigkeit

Die vSAN-Komponenten, die sich auf der Magnetfestplatte oder dem Flash-Kapazitätsgerät befinden, sind als abwesend gekennzeichnet.

### Verhalten von vSAN

vSAN reagiert wie folgt auf den Speichergerätefehler.

| Parameter | Verhalten |
|---|---|
| Alarme | Wenn auf einem Host ein fehlerhaftes Gerät erkannt wird, wird ein Alarm generiert. Es wird eine Warnung ausgegeben, wenn eine Festplatte als fehlerhaft erachtet wird. |
| Systemstatusprüfung | Die Prüfung **Gesamtintegrität der Festplatte** gibt für die Festplatte, die auszufallen droht, eine Warnung aus. |
| Systemstatus | Auf der Seite „Festplattenverwaltung“ wird der Systemstatus der Festplatte, die auszufallen droht, als **Unhealthy** angegeben. Wenn vSAN die Evakuierung der Daten abgeschlossen hat, wird der Systemstatus **DyingDiskEmpty** angezeigt. |
| Neuerstellen von Daten | vSAN prüft, ob die Hosts und die Kapazitätsgeräte die Anforderungen in Bezug auf Speicherplatz und Platzierungsregeln für die Objekte auf dem fehlerhaften Gerät oder der fehlerhaften Festplattengruppe erfüllen können. Wenn ein solcher Host mit Kapazität verfügbar ist, startet vSAN sofort die Wiederherstellung, weil die Komponenten als herabgestuft gekennzeichnet sind.<br>Falls Ressourcen zur Verfügung stehen, schützt vSAN die Daten automatisch neu. |

Wenn vSAN eine Festplatte mit einem permanenten Fehlerzustand erkennt, unternimmt es eine begrenzte Anzahl an Versuchen, um sie durch Unmounten und erneutes Mounten wiederzubeleben.

## Kein Zugriff auf ein Kapazitätsgerät in einem vSAN -Cluster

Wenn eine Magnetfestplatte oder ein Flash-Kapazitätsgerät fehlschlägt, wertet vSAN die Zugriffsfähigkeit der Objekte auf dem Gerät aus und erstellt sie auf einem anderen Host neu, falls Speicherplatz verfügbar ist und **Primäre Ebene von zu tolerierenden Fehlern** auf mindestens 1 festgelegt ist.

### Komponentenfehlerzustand und Zugriffsfähigkeit

Die vSAN-Komponenten, die sich auf der Magnetfestplatte oder dem Flash-Kapazitätsgerät befinden, sind als herabgestuft gekennzeichnet.

### Verhalten von vSAN

vSAN reagiert wie folgt auf den Kapazitätsgerätefehler.

| Parameter | Verhalten |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Wenn **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie gleich oder größer als 1 ist, sind die VM-Objekte weiterhin von einem anderen ESXi-Host im Cluster aus zugänglich. Wenn Ressourcen verfügbar sind, startet vSAN einen automatischen erneuten Schutz.<br>Wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist, kann auf ein VM-Objekt nicht zugegriffen werden, falls sich eine der Komponenten des Objekts auf dem fehlgeschlagenen Kapazitätsgerät befindet.<br>Stellen Sie die virtuelle Maschine aus einer Sicherung wieder her. |
| E/A-Vorgänge auf dem Kapazitätsgerät | vSAN unterbricht 5 - 7 Sekunden lang alle laufenden E/A-Vorgänge, bis es neu bestimmt hat, ob ein Objekt ohne die fehlerhafte Komponente weiterhin verfügbar ist.<br>Wenn vSAN ermittelt hat, dass das Objekt verfügbar ist, werden alle laufenden E/A-Vorgänge wieder aufgenommen. |
| Neuerstellen von Daten | vSAN prüft, ob die Hosts und die Kapazitätsgeräte die Anforderungen in Bezug auf Speicherplatz und Platzierungsregeln für die Objekte auf dem fehlerhaften Gerät oder der fehlerhaften Festplattengruppe erfüllen können. Wenn ein solcher Host mit Kapazität verfügbar ist, startet vSAN sofort die Wiederherstellung, weil die Komponenten als herabgestuft gekennzeichnet sind.<br>Wenn Ressourcen verfügbar sind, erfolgt der automatische erneute Schutz. |

## Kein Zugriff auf ein Flash-Cache-Gerät in einem vSAN -Cluster

Wenn ein Flash-Cache-Gerät fehlschlägt, wertet vSAN die Zugriffsfähigkeit der Objekte in der Festplattengruppe aus, die das Cache-Gerät enthält, und erstellt sie auf einem anderen Host neu, falls dies möglich ist und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 oder mehr festgelegt ist.

### Komponentenfehlerzustand und Zugriffsfähigkeit

Sowohl das Cache-Gerät als auch die Kapazitätsgeräte, die sich in der Festplattengruppe befinden (z. B. Magnetfestplatten), sind als herabgestuft gekennzeichnet. vSAN interpretiert einen Fehler bei einem einzelnen Flash-Cache-Gerät als Fehler der gesamten Festplattengruppe.

### Verhalten von vSAN

vSAN reagiert wie folgt auf den Fehler eines Flash-Cache-Geräts:

| Parameter | Verhalten |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Wenn **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie gleich oder größer als 1 ist, sind die VM-Objekte weiterhin von einem anderen ESXi-Host im Cluster aus zugänglich. Wenn Ressourcen verfügbar sind, startet vSAN einen automatischen erneuten Schutz.<br>Wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist, kann auf ein VM-Objekt nicht zugegriffen werden, falls sich eine der Komponenten des Objekts in der fehlgeschlagenen Festplattengruppe befindet. |
| E/A-Vorgänge in der Festplattengruppe | vSAN unterbricht 5 - 7 Sekunden lang alle laufenden E/A-Vorgänge, bis es neu bestimmt hat, ob ein Objekt ohne die fehlerhafte Komponente weiterhin verfügbar ist.<br>Wenn vSAN ermittelt hat, dass das Objekt verfügbar ist, werden alle laufenden E/A-Vorgänge wieder aufgenommen. |
| Neuerstellen von Daten | vSAN prüft, ob die Hosts und die Kapazitätsgeräte die Anforderungen in Bezug auf Speicherplatz und Platzierungsregeln für die Objekte auf dem fehlerhaften Gerät oder der fehlerhaften Festplattengruppe erfüllen können. Wenn ein solcher Host mit Kapazität verfügbar ist, startet vSAN sofort die Wiederherstellung, weil die Komponenten als herabgestuft gekennzeichnet sind. |

## Ein Host in einem vSAN -Cluster reagiert nicht

Wenn ein Host wegen eines Fehlers oder Neustarts des Hosts nicht mehr antwortet, wartet vSAN, bis der Host wieder reagiert, bevor vSAN die Komponenten auf dem Host an anderer Stelle im Cluster neu aufbaut.

### Komponentenfehlerzustand und Zugriffsfähigkeit

Die vSAN-Komponenten, die sich auf dem Host befinden, sind als abwesend gekennzeichnet.

### Verhalten von vSAN

vSAN antwortet in der folgenden Weise auf den Hostfehler:

| Parameter | Verhalten |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Wenn **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie gleich oder größer als 1 ist, sind die VM-Objekte weiterhin von einem anderen ESXi-Host im Cluster aus zugänglich. Wenn Ressourcen verfügbar sind, startet vSAN einen automatischen erneuten Schutz.<br>Wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist, kann auf ein VM-Objekt nicht zugegriffen werden, falls sich die Objektkomponenten auf dem fehlerhaften Host befinden. |
| E/A-Vorgänge auf dem Host | vSAN unterbricht 5 - 7 Sekunden lang alle laufenden E/A-Vorgänge, bis es neu bestimmt hat, ob ein Objekt ohne die fehlerhafte Komponente weiterhin verfügbar ist.<br>Wenn vSAN ermittelt hat, dass das Objekt verfügbar ist, werden alle laufenden E/A-Vorgänge wieder aufgenommen. |
| Neuerstellen von Daten | Wenn der Host nicht innerhalb von 60 Minuten wieder dem Cluster beitritt, prüft vSAN, ob andere Hosts im Cluster die Anforderungen in Bezug auf Zwischenspeicher, Speicherplatz und Platzierungsregeln für die Objekte auf dem unzugänglichen Host erfüllen können. Wenn ein solcher Host verfügbar ist, startet vSAN sofort die Wiederherstellung.<br>Wenn der Host nach 60 Minuten wieder dem Cluster beitritt und die Wiederherstellung gestartet wurde, evaluiert vSAN, ob die Wiederherstellung fortgesetzt oder beendet werden soll und die Ausgangskomponenten neu synchronisiert werden sollen. |

## Netzwerkkonnektivität im vSAN -Cluster unterbrochen

Wenn die Konnektivität zwischen den Hosts im Cluster unterbrochen wird und nicht wiederhergestellt werden kann, bestimmt vSAN die aktive Partition und erstellt die Komponenten aus der isolierten Partition auf der aktiven Partition neu.

### Komponentenfehlerzustand und Zugriffsfähigkeit

vSAN bestimmt die Partition, in der mehr als 50 Prozent der Stimmen eines Objekts verfügbar sind. Die Komponenten auf den isolierten Hosts werden als abwesend markiert.

### Verhalten von vSAN

vSAN reagiert auf einen Netzwerkausfall folgendermaßen:

| Parameter | Verhalten |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Wenn **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie gleich oder größer als 1 ist, sind die VM-Objekte weiterhin von einem anderen ESXi-Host im Cluster aus zugänglich. Wenn Ressourcen verfügbar sind, startet vSAN einen automatischen erneuten Schutz.<br>Wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist, kann auf ein VM-Objekt nicht zugegriffen werden, falls sich die Objektkomponenten auf isolierten Hosts befinden. |
| E/A-Vorgänge auf den isolierten Hosts | vSAN unterbricht 5 - 7 Sekunden lang alle laufenden E/A-Vorgänge, bis es neu bestimmt hat, ob ein Objekt ohne die fehlerhafte Komponente weiterhin verfügbar ist.<br>Wenn vSAN ermittelt hat, dass das Objekt verfügbar ist, werden alle laufenden E/A-Vorgänge wieder aufgenommen. |
| Neuerstellen von Daten | Wenn der Host innerhalb von 60 Minuten dem Cluster wieder beitritt, synchronisiert vSAN die Komponenten auf dem Host.<br>Wenn der Host nicht innerhalb von 60 Minuten wieder dem Cluster beitritt, prüft vSAN, ob andere Hosts im Cluster die Anforderungen in Bezug auf Zwischenspeicher, Speicherplatz und Platzierungsregeln für die Objekte auf dem unzugänglichen Host erfüllen können. Wenn ein solcher Host verfügbar ist, startet vSAN sofort die Wiederherstellung.<br>Wenn der Host nach 60 Minuten wieder dem Cluster beitritt und die Wiederherstellung gestartet wurde, evaluiert vSAN, ob die Wiederherstellung fortgesetzt oder beendet werden soll und die Ausgangskomponenten neu synchronisiert werden sollen. |

## Ein Speicher-Controller in einem vSAN -Cluster schlägt fehl

Wenn ein Speicher-Controller fehlschlägt, evaluiert vSAN die Zugriffsfähigkeit der Objekte in den an den Controller angeschlossenen Festplattengruppen und erstellt sie auf einem anderen Host neu.

### Symptome

Wenn ein Host einen einzelnen Speicher-Controller und mehrere Festplattengruppen enthält und alle Geräte in allen Festplattengruppen ausgefallen sind, können Sie davon ausgehen, dass ein Fehler im gemeinsamen Speicher-Controller die Hauptursache ist. Untersuchen Sie die VMkernel-Protokollmeldungen, um die Art des Fehlers zu ermitteln.

### Komponentenfehlerzustand und Zugriffsfähigkeit

Wenn ein Speicher-Controller fehlschlägt, werden die Komponenten auf den Flash-Caching- und Kapazitätsgeräten in allen mit dem Controller verbundenen Festplattengruppen als herabgestuft markiert.

Wenn ein Host mehrere Controller enthält und nur auf die Geräte, die mit einem bestimmten Controller verbunden sind, nicht zugegriffen werden kann, können Sie davon ausgehen, dass dieser eine Controller ausgefallen ist.

### Verhalten von vSAN

vSAN reagiert auf einen Speicher-Controller-Ausfall folgendermaßen:

| Parameter | Verhalten |
|---|---|
| Primäre Ebene von zu tolerierenden Fehlern | Wenn **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie gleich oder größer als 1 ist, sind die VM-Objekte weiterhin von einem anderen ESXi-Host im Cluster aus zugänglich. Wenn Ressourcen verfügbar sind, startet vSAN einen automatischen erneuten Schutz.<br>Wenn **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist und die Komponenten eines VM-Objekts sich in den Festplattengruppen befinden, die mit dem Speicher-Controller verbunden sind, kann auf das Objekt nicht zugegriffen werden. |
| Neuerstellen von Daten | vSAN prüft, ob die Hosts und die Kapazitätsgeräte die Anforderungen in Bezug auf Speicherplatz und Platzierungsregeln für die Objekte auf dem fehlerhaften Gerät oder der fehlerhaften Festplattengruppe erfüllen können. Wenn ein solcher Host mit Kapazität verfügbar ist, startet vSAN sofort die Wiederherstellung, weil die Komponenten als herabgestuft gekennzeichnet sind. |

### Die Site eines ausgeweiteten Clusters schlägt fehl oder die Netzwerkverbindung wird unterbrochen

Ein ausgeweiteter vSAN-Cluster verwaltet Fehler, die aufgrund des Verlusts einer Netzwerkverbindung zwischen den Sites oder aufgrund eines vorübergehenden Verlusts einer Site auftreten.

#### Fehlerbehandlung für ausgeweiteten Cluster

In den meisten Fällen wird der ausgeweitete Cluster während eines Fehlers weiterhin ausgeführt und automatisch wiederhergestellt, nachdem der Fehler behoben ist.

**Tabelle 14-5.** Fehlerbehandlung durch ausgeweiteten Cluster

| Fehlertyp | Verhalten |
|---|---|
| Die Netzwerkverbindung zwischen aktiven Sites ist unterbrochen | Wenn die Netzwerkverbindung zwischen den beiden aktiven Sites fehlschlägt, führen der Zeugenhost und die bevorzugte Site nach wie vor Speichervorgänge durch und sorgen dafür, dass die Daten verfügbar bleiben. Wenn die Netzwerkverbindung erneut hergestellt ist, werden die beiden aktiven Sites neu synchronisiert. |
| Die sekundäre Site schlägt fehl oder die Netzwerkverbindung wird unterbrochen | Wenn die sekundäre Site offline geschaltet oder von der bevorzugten Site und dem Zeugenhost isoliert wird, führen der Zeugenhost und die bevorzugte Site nach wie vor Speichervorgänge durch und sorgen dafür, dass die Daten verfügbar bleiben. Wenn die sekundäre Site erneut eine Verbindung zum Cluster herstellt, werden die beiden aktiven Sites neu synchronisiert. |
| Die bevorzugte Site schlägt fehl oder die Netzwerkverbindung wird unterbrochen | Wenn die bevorzugte Site offline geschaltet oder von der sekundären Site und dem Zeugenhost isoliert wird, führt die sekundäre Site weiterhin Speichervorgänge durch, solange sie mit dem Zeugenhost verbunden ist. Wenn die bevorzugte Site erneut eine Verbindung zum Cluster herstellt, werden die beiden aktiven Sites neu synchronisiert. |
| Der Zeugenhost schlägt fehl oder die Netzwerkverbindung wird unterbrochen | Wenn der Zeugenhost offline geschaltet oder von der bevorzugten Site oder der sekundären Site isoliert wird, stimmen die Objekte zwar nicht mehr überein, aber die Daten bleiben verfügbar. Aktuell ausgeführte VMs sind davon nicht betroffen. |

## Fehlerbehebung für vSAN

Analysieren Sie die Leistung und Zugriffsfähigkeit von virtuellen Maschinen, um Probleme im vSAN-Cluster zu diagnostizieren.

### Überprüfen von Treibern, Firmware und Speicher-E/A-Controllern anhand des *VMware-Kompatibilitätshandbuch* s

Verwenden Sie den vSAN-Integritätsdienst, um zu überprüfen, ob Ihre Hardwarekomponenten, Treiber und Firmware mit vSAN kompatibel sind.

Die Verwendung von Hardwarekomponenten, Treibern und Firmware, die nicht mit vSAN kompatibel sind, kann Probleme beim Betrieb des vSAN-Clusters und der darin ausgeführten virtuellen Maschinen verursachen.

Mit den Integritätsprüfungen für die Hardwarekompatibilität wird Ihre Hardware basierend auf dem *VMware-Kompatibilitätshandbuch* überprüft. Weitere Informationen zur Verwendung des vSAN-Integritätsdiensts finden Sie unter „Überwachen der vSAN-Integrität“, auf Seite 152.

## Untersuchen der Leistung in einem vSAN -Cluster

Überwachen Sie die Leistung von virtuellen Maschinen, Hosts und des Datenspeichers für vSAN, um mögliche Speicherprobleme zu erkennen.

Überwachen Sie regelmäßig die folgenden Leistungsindikatoren, um Fehler im vSAN-Speicher zu erkennen. Sie können dazu zum Beispiel die Leistungsdiagramme im vSphere Web Client verwenden:

- Datenspeicher. Rate der E/A-Vorgänge auf dem zusammengefassten Datenspeicher.
- Virtuelle Maschine. E/A-Vorgänge, Speicher- und CPU-Auslastung, Netzwerkdurchsatz und Bandbreite.

Sie können den vSAN-Leistungsdienst verwenden, um auf detaillierte Leistungsdiagramme zuzugreifen. Informationen zur Verwendung des Leistungsdiensts finden Sie unter „Überwachen der vSAN-Leistung“, auf Seite 154. Ausführliche Informationen zur Verwendung von Leistungsdaten in einem vSAN-Cluster finden Sie im *Referenzhandbuch zur vSAN-Fehlerbehebung*.

## Netzwerkfehlkonfigurationsstatus in einem vSAN -Cluster

Nach der Aktivierung von vSAN in einem Cluster wird der Datenspeicher aufgrund einer erkannten Netzwerkfehlkonfiguration nicht ordnungsgemäß zusammengesetzt.

### Problem

Nachdem Sie vSAN in einem Cluster aktiviert haben, wird auf der Registerkarte **Übersicht** für den Cluster `Fehlkonfiguration erkannt` als Netzwerkstatus für vSAN angezeigt.

### Ursache

Mindestens ein Clustermitglied kann aus einem der folgenden Gründe nicht kommunizieren:

- Ein Host im Cluster weist keinen VMkernel-Adapter für vSAN auf.
- Die Hosts können keine Verbindung miteinander im Netzwerk herstellen.

### Lösung

Fügen Sie die Clustermitglieder zu demselben Netzwerk hinzu. Siehe „Konfigurieren eines vSAN-Netzwerks“, auf Seite 44.

## Virtuelle Maschine wird in vSAN als nicht übereinstimmend, nicht erreichbar oder verwaist angezeigt

Der Zustand einer virtuellen Maschine, die Daten in einem vSAN-Datenspeicher speichert, wird aufgrund von Fehlern im vSAN-Cluster als nicht übereinstimmend, nicht zugreifbar oder verwaist angezeigt.

### Problem

Eine virtuelle Maschine in einem vSAN-Datenspeicher weist einen der folgenden Zustände auf, die auf einen Fehler im vSAN-Cluster hindeuten.

- Die virtuelle Maschine wird als nicht übereinstimmend angezeigt und der Übereinstimmungsstatus einiger ihrer Objekte ist „Nicht übereinstimmend“. Siehe „Untersuchen der Übereinstimmung einer virtuellen Maschine in vSAN“, auf Seite 174.
- Auf das VM-Objekt kann nicht zugegriffen werden oder es ist verwaist. Siehe „Analysieren des Fehlerstatus einer Komponente“, auf Seite 172.

Wenn ein Replikat des Objekts auf einem anderen Host verfügbar ist, leitet vSAN die E/A-Vorgänge der virtuellen Maschine an das Replikat weiter.

### Ursache

Wenn das Objekt der virtuellen Maschine die Anforderungen der zugewiesenen VM-Speicherrichtlinie nicht mehr erfüllen kann, wird es von vSAN als nicht übereinstimmend betrachtet. Die Verbindung eines Hosts kann z. B. vorübergehend getrennt werden. Siehe „Objektzustände, die auf Probleme in vSAN hinweisen“, auf Seite 173.

Wenn vSAN kein vollständiges Replikat bzw. nicht mehr als 50 Prozent der Stimmen für das Objekt finden kann, ist kein Zugriff auf die virtuelle Maschine mehr möglich. Wenn vSAN feststellt, dass auf die `.vmx`-Datei nicht zugegriffen werden kann, weil der VM-Start-Namespace beschädigt ist, wird die virtuelle Maschine verwaist. Siehe „Zugriffsfähigkeit von virtuellen Maschinen bei einem Fehler in vSAN“, auf Seite 174.

### Lösung

Sofern es sich um einen dauerhaften Fehler handelt und der Cluster über genügend Ressourcen verfügt, stellt vSAN die beschädigten Objekte automatisch wieder her.

Wenn der Cluster nicht über genügend Ressourcen für die Neuerstellung der beschädigten Objekte verfügt, erweitern Sie den Speicherplatz im Cluster. Siehe „Erweitern der vSAN-Clusterkapazität und -leistung“, auf Seite 122 und „Hinzufügen eines Hosts zu einem vSAN-Cluster“, auf Seite 122.

## Fehler beim Erstellen einer virtuellen Maschine in vSAN

Der Versuch, eine virtuelle Maschine in einem vSAN-Cluster bereitzustellen, schlägt mit einer Fehlermeldung fehl, dass die VM-Dateien nicht erstellt werden können.

### Problem

Der Vorgang zum Erstellen einer virtuellen Maschine schlägt mit folgender Fehlermeldung fehl: `Das Erstellen der Datei kann nicht abgeschlossen werden.`

### Ursache

Die Bereitstellung einer virtuellen Maschine in vSAN kann aus mehreren Gründen fehlschlagen.

- vSAN kann für die VM-Speicherrichtlinien und die VM-Objekte keinen Speicherplatz zuteilen. Dieser Fehler kann auftreten, wenn der Datenspeicher nicht ausreichend nutzbare Kapazität aufweist, beispielsweise wenn eine physische Festplatte vorübergehend vom Host getrennt ist.
- Die virtuelle Maschine weist sehr große virtuelle Festplatten auf und die Hosts im Cluster können hierfür keinen Speicher basierend auf den Platzierungsregeln in der VM-Speicherrichtlinie bereitstellen.

  Wenn beispielsweise **Primäre Ebene von zu tolerierenden Fehlern** in der VM-Speicherrichtlinie den Wert 1 aufweist, muss vSAN zwei Replikate einer virtuellen Festplatte im Cluster speichern, und zwar jedes Replikat auf einem anderen Host. Der Datenspeicher weist möglicherweise nach der Zusammenführung des freien Speicherplatzes auf allen Hosts im Cluster den erforderlichen Speicherplatz auf. Es dürfen jedoch keine zwei Hosts im Cluster verfügbar sein, von denen jeder ausreichend Speicherplatz zum Speichern eines separaten Replikats der virtuellen Festplatte bereitstellt.

  vSAN verschiebt keine Komponenten zwischen Hosts oder Festplattengruppen, um Speicherplatz für ein neues Replikat freizugeben, obwohl der Cluster möglicherweise ausreichend Speicherplatz für die Bereitstellung der neuen virtuellen Maschine enthält.

### Lösung

- Überprüfen Sie den Status der Kapazitätsgeräte im Cluster.
  a. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
  b. Klicken Sie auf der Registerkarte **Überwachen** auf **vSAN** und wählen Sie **Physische Festplatten** aus.
  c. Prüfen Sie die Kapazität und den Systemstatus der Gerät auf den Hosts im Cluster.

## Stretched-Cluster-Konfigurationsfehler beim Hinzufügen eines Hosts

Bevor Sie einem Stretched Cluster neue Hosts hinzufügen können, müssen alle aktuellen Hosts verbunden werden. Wenn ein aktueller Host nicht verbunden ist, ist die Konfiguration des neuen Hosts unvollständig.

### Problem

Nachdem Sie einen neuen Host zu einem ausgeweiteten, in dem einige Hosts getrennt sind, hinzugefügt haben, wird auf der Registerkarte „Übersicht“ für den Cluster der Konfigurationsstatus für das vSAN als `Der Unicast-Agent des Hosts ist nicht festgelegt` angezeigt.

### Ursache

Wenn ein neuer Host einem ausgeweiteten Cluster beitritt, muss vSAN die Konfiguration auf allen Hosts im Cluster aktualisieren. Das Updade schlägt fehl, wenn ein oder mehrere Hosts vom vCenter Server getrennt sind. Der neue Host tritt dem Cluster erfolgreich bei, aber die Konfiguration ist unvollständig.

### Lösung

Stellen Sie sicher, dass alle Hosts mit dem vCenter Server verbunden sind, und klicken Sie auf den Link in der Konfigurationsstatusmeldung, um die Konfiguration des neuen Hosts zu aktualisieren.

Wenn der Beitritt des getrennten Hosts nicht möglich ist, entfernen Sie den getrennten Host aus dem Cluster und klicken Sie auf den Link in der Konfigurationsstatusmeldung, um die Konfiguration des neuen Hosts zu aktualisieren.

## Fehler bei der Konfiguration des ausgeweiteten Clusters bei Verwendung von RVC zum Hinzufügen eines Hosts

Wenn Sie das RVC-Tool zum Hinzufügen eines neuen Hosts zu einem ausgeweiteten Cluster verwenden, ist die Konfiguration des neuen Hosts unvollständig.

### Problem

Nachdem Sie das RVC-Tool zum Hinzufügen eines neuen Hosts zu einem ausgeweiteten Cluster verwendet haben, wird auf der Registerkarte „Übersicht“ der Konfigurationsstatus für vSAN als `Der Unicast-Agent des Hosts ist nicht festgelegt` für den Cluster angezeigt.

### Ursache

Wenn ein neuer Host einem ausgeweiteten Cluster beitritt, muss vSAN die Konfiguration auf allen Hosts im Cluster aktualisieren. Wenn Sie das RVC-Tool zum Hinzufügen des Hosts verwenden, wird kein Update durchgeführt. Der neue Host tritt dem Cluster erfolgreich bei, aber die Konfiguration ist unvollständig.

### Lösung

Stellen Sie sicher, dass alle Hosts mit dem vCenter Server verbunden sind, und klicken Sie auf den Link in der Konfigurationsstatusmeldung, um die Konfiguration des neuen Hosts zu aktualisieren.

### Hinzufügen oder Entfernen des Zeugenhosts in einem ausgeweiteten Cluster nicht möglich

Vor dem Hinzufügen oder Entfernen des Zeugenhosts zu bzw. aus einem ausgeweiteten Cluster müssen alle aktuellen Hosts verbunden werden. Wenn ein aktueller Host getrennt ist, können Sie den Zeugenhost nicht hinzufügen oder entfernen.

#### Problem

Wenn Sie einen Zeugenhost zu einem ausgeweiteten Cluster hinzufügen oder daraus entfernen, in dem einige Hosts sind nicht verbunden sind, schlägt der Vorgang mit folgender Fehlermeldung fehl: `Der Vorgang ist im aktuellen Zustand nicht zulässig. Nicht alle Hosts im Cluster sind mit Virtual Center verbunden.`

#### Ursache

Wenn der Zeugenhost einem ausgeweiteten Cluster beitritt oder diesen verlässt, muss vSAN die Konfiguration auf alle Hosts im Cluster aktualisieren. Wenn ein oder mehrere Hosts vom vCenter Server getrennt werden, kann der Zeugenhost nicht hinzugefügt oder entfernt werden.

#### Lösung

Vergewissern Sie sich, dass alle Hosts mit vCenter Server verbunden sind, und wiederholen Sie den Vorgang. Wenn Sie den getrennten Host nicht erneut verbinden können, entfernen Sie den getrennten Host aus dem Cluster. Im Anschluss daran können Sie den Zeugenhost hinzufügen oder entfernen.

### Festplattengruppe wird gesperrt

Wenn in einem verschlüsselten vSAN-Cluster die Kommunikation zwischen einem Host und dem KMS verloren geht, kann die Festplattengruppe gesperrt werden, falls der Host neu startet.

#### Problem

vSAN sperrt die Festplattengruppen eines Hosts, wenn der Host neu startet, und der KEK vom KMS nicht abgerufen werden kann. Die Festplatten verhalten sich, als seien sie nicht gemountet. Auf die Objekte auf den Festplatten ist kein Zugriff möglich.

Sie können im vSphere Web Client auf der Seite „Festplattenverwaltung“ die Integrität einer Festplattengruppe anzeigen. Über eine Verschlüsselungsintegritätsprüfungs-Warnung werden Sie benachrichtigt, dass eine Festplatte gesperrt ist.

#### Ursache

Hosts in einem verschlüsselten vSAN-Cluster speichern den KEK nicht auf Festplatte. Wenn der Host neu startet und der KEK vom KMS nicht abgerufen werden kann, sperrt vSAN die Festplattengruppen des Hosts.

#### Lösung

Um die Sperrung aufzuheben, müssen Sie die Kommunikation mit dem KMS und die Vertrauensbeziehung wiederherzustellen.

## Ersetzen vorhandener Hardwarekomponenten

Unter bestimmten Bedingungen müssen Sie Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller im vSAN-Cluster ersetzen.

In vSAN sollten Sie Hardwaregeräte ersetzen, wenn Sie Fehler feststellen oder wenn Sie ein Upgrade Ihres Clusters durchführen müssen.

## Austauschen eines Flash-Cache-Geräts auf einem Host

Sie sollten ein Flash-Cache-Gerät austauschen, wenn Sie einen Fehler feststellen oder wenn Sie ein Upgrade für das Gerät ausführen müssen. Bevor Sie ein Flash-Gerät physisch vom Host trennen, müssen Sie das Gerät manuell aus vSAN entfernen.

**Vorsicht** Wenn Sie das Flash-Cache-Gerät außer Betrieb nehmen, ohne es zuvor aus vSAN zu entfernen, verwendet vSAN weniger Cache als erwartet. Die Leistung des Clusters ist deshalb beeinträchtigt.

Beim Austausch eines Flash-Cache-Geräts ist kein Zugriff mehr auf die virtuellen Maschinen in der Festplattengruppe möglich und die Komponenten in der Gruppe werden als herabgestuft gekennzeichnet. Siehe „Kein Zugriff auf ein Flash-Cache-Gerät in einem vSAN-Cluster“, auf Seite 176.

### Voraussetzungen

- Stellen Sie sicher, dass die Speicher-Controller auf den Hosts im Passthrough-Modus konfiguriert sind und die Hotplug-Funktion unterstützen.

  Wenn die Speicher-Controller im RAID 0-Modus konfiguriert sind, lesen Sie in der Dokumentation des Anbieters die Informationen zum Hinzufügen und Entfernen von Geräten.

- Überprüfen Sie die folgenden Anforderungen, wenn Sie ein Upgrade des Flash-Cache-Geräts durchführen:
  - Überprüfen Sie beim Upgrade des Flash-Cache-Geräts, ob der Cluster ausreichend Speicherplatz enthält, um die Daten aus der Festplattengruppe, die dem Flash-Gerät zugeordnet ist, zu migrieren.
  - Versetzen Sie den Host in den Wartungsmodus. Siehe „Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus“, auf Seite 126.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf der Registerkarte **Konfigurieren** unter vSAN auf **Festplattenverwaltung**.
3. Wählen Sie die Festplattengruppe mit dem Gerät aus, das Sie ersetzen möchten.
4. Wählen Sie das Flash-Cache-Gerät aus und klicken Sie auf **Entfernt die ausgewählte(n) Festplatte(n) aus der Festplattengruppe**.

Nachdem das Flash-Cache-Gerät aus dem vSAN-Cluster gelöscht wurde, werden in den Clusterdetails die aktuelle Clusterkapazität und die aktuellen Konfigurationseinstellungen angezeigt. vSAN verwirft die Festplattengruppenmitgliedschaften, löscht Partitionen und entfernt veraltete Daten auf allen Geräten.

### Weiter

1. Fügen Sie dem Host ein neues Gerät hinzu.

   Der Host erkennt das Gerät automatisch.
2. Wenn der Host das Gerät nicht erkennen kann, prüfen Sie das Gerät erneut.

## Ersetzen eines Kapazitätsgeräts

Sie sollten ein Flash-Kapazitätsgerät oder eine Magnetfestplatte ersetzen, wenn Sie einen Fehler feststellen oder wenn Sie das Gerät bzw. die Festplatte aktualisieren. Bevor Sie das Gerät physisch aus dem Host entfernen, müssen Sie es manuell aus vSAN löschen.

Wenn Sie ein Kapazitätsgerät trennen, ohne es zuvor aus dem vSAN-Cluster entfernt zu haben, kann auf die virtuellen Maschinen in der Festplattengruppe nicht mehr zugegriffen werden und die Komponenten in der Gruppe werden als abwesend markiert.

Wenn das Kapazitätsgerät ausfällt, kann auf die virtuellen Maschinen nicht mehr zugegriffen werden und die Komponenten in der Gruppe werden als herabgestuft markiert. Siehe „Kein Zugriff auf ein Kapazitätsgerät in einem vSAN-Cluster“, auf Seite 175.

### Voraussetzungen

- Stellen Sie sicher, dass die Speicher-Controller auf den Hosts im Passthrough-Modus konfiguriert sind und die Hotplug-Funktion unterstützen.

  Wenn die Speicher-Controller im RAID 0-Modus konfiguriert sind, lesen Sie in der Dokumentation des Anbieters die Informationen zum Hinzufügen und Entfernen von Geräten.
- Wenn Sie ein Upgrade des Kapazitätsgeräts ausführen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:
  - Stellen Sie sicher, dass der Cluster über genügend Speicherplatz für die Migration der Daten des Kapazitätsgeräts verfügt.
  - Versetzen Sie den Host in den Wartungsmodus. Siehe „Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus“, auf Seite 126.

### Vorgehensweise

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf der Registerkarte **Konfigurieren** unter vSAN auf **Festplattenverwaltung**.
3. Wählen Sie die Festplattengruppe mit dem Gerät aus, das Sie ersetzen möchten.
4. Wählen Sie das Flash-Kapazitätsgerät oder die Magnetfestplatte aus und klicken Sie auf **Ausgewählte Festplatte(n) aus der Festplattengruppe entfernen**.

### Weiter

1. Fügen Sie dem Host ein neues Gerät hinzu.

   Der Host erkennt das Gerät automatisch.
2. Wenn der Host das Gerät nicht erkennen kann, prüfen Sie das Gerät erneut.

## Entfernen eines Geräts von einem Host mithilfe eines ESXCLI-Befehls

Wenn Sie ein fehlerhaftes Speichergerät erkennen oder ein Upgrade für ein Gerät durchführen, können Sie es mithilfe eines ESXCLI-Befehls manuell von einem Host entfernen.

Wenn Sie ein Flash-Zwischenspeichergerät entfernen, löscht vSAN die mit dem Flash-Gerät verknüpfte Festplattengruppe und alle zugehörigen Mitgliedsgeräte.

### Voraussetzungen

Stellen Sie sicher, dass die Speicher-Controller auf den Hosts im Passthrough-Modus konfiguriert sind und die Hotplug-Funktion unterstützen.

Wenn die Speicher-Controller im RAID 0-Modus konfiguriert sind, lesen Sie in der Dokumentation des Anbieters die Informationen zum Hinzufügen und Entfernen von Geräten.

### Vorgehensweise

1. Stellen Sie eine SSH-Verbindung mit dem ESXi-Host her.
2. Um die Gerätekennung des fehlerhaften Geräts zu bestimmen, führen Sie diesen Befehl aus. Die Gerätekennung entnehmen Sie dann der Ausgabe.

   ```
   esxcli vsan storage list
   ```

3 Um das Gerät aus vSAN zu entfernen, führen Sie diesen Befehl aus.

```
esxcli vsan storage remove –d Geräte–ID
```

#### Weiter

1 Fügen Sie dem Host ein neues Gerät hinzu.

Der Host erkennt das Gerät automatisch.

2 Wenn der Host das Gerät nicht erkennen kann, prüfen Sie das Gerät erneut.

## Herunterfahren des vSAN -Clusters

Bei Bedarf können Sie den gesamten vSAN-Cluster herunterfahren.

Wenn Sie den vSAN-Cluster herunterfahren möchten, müssen Sie vSAN manuell auf dem Cluster deaktivieren.

#### Vorgehensweise

1 Schalten Sie alle virtuellen Maschinen (VMs) aus, die im vSAN-Cluster ausgeführt werden.

2 Versetzen Sie die ESXi-Hosts in den Wartungsmodus.

a Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **In den Wartungsmodus wechseln**.

b Wählen Sie den Evakuierungsmodus **Keine Datenmigration** aus und klicken Sie auf **OK**.

3 Deaktivieren Sie im Assistenten „Wartungsmodus bestätigen“ das Kontrollkästchen **Ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster verschieben**.

Wenn Sie dieses Kontrollkästchen deaktivieren, migriert vSAN die VMs nicht auf andere Hosts. Wenn Sie den gesamten Cluster herunterfahren und alle Hosts in den Wartungsmodus versetzen möchten, müssen Sie die VM-Speicherobjekte nicht auf andere Hosts oder Geräte im Cluster verschieben oder migrieren.

4 Schalten Sie die Hosts aus, nachdem sie erfolgreich in den Wartungsmodus versetzt wurden.

5 Schalten Sie die ESXi-Hosts ein.

a Drücken Sie am Gehäuse des Computers, auf dem ESXi installiert ist, den Netzschalter, bis der Einschaltvorgang eingeleitet wird.

Der ESXi-Host wird gestartet, sucht nach den VMs und arbeitet wie gewohnt.

Nachdem Sie die Hosts eingeschaltet haben, wird der vSAN-Cluster automatisch neu erstellt.

Wenn Sie zum ESXi-Host navigieren und auf **Übersicht** klicken, wird als Netzwerkstatus des Clusters möglicherweise `Fehlkonfiguration erkannt` angezeigt.

Sie können die Statusmeldung ignorieren, falls Sie keine Netzwerkkonfigurationsänderungen vorgenommen haben und der vSAN-Cluster wie erwartet funktionierte, bevor Sie den Cluster heruntergefahren haben. Diese Meldung wird angezeigt, wenn mindestens drei Hosts dem Cluster beigetreten sind.

6 Deaktivieren Sie den Wartungsmodus für die Hosts.

7 Starten Sie die VMs neu.

# Index

## V

## W



## Z