# Verwalten von VMware vSAN

Update 3

VMware vSphere 7.0
VMware vSAN 7.0

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

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

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

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

# Inhalt

# Informationen zum Verwalten von VMware vSAN

In *Verwalten von VMware vSAN* wird beschrieben, wie Sie einen vSAN-Cluster in einer VMware vSphere®-Umgebung konfigurieren und verwalten. Darüber hinaus wird in *Verwalten von VMwarevSAN* erläutert, wie die lokalen physischen Speicherressourcen, die als Speicherkapazitätsgeräte in einem vSAN-Cluster dienen, verwaltet werden und wie Speicherrichtlinien für virtuelle Maschinen, die für vSAN-Datenspeicher bereitgestellt werden, definiert werden.

Wir bei VMware legen Wert auf Inklusion. Um dieses Prinzip innerhalb unserer Kunden-, Partner- und internen Community zu fördern, erstellen wir Inhalte mit inklusiver Sprache.

## Zielgruppe

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

Weitere Informationen zu vSAN und zum Erstellen eines vSAN-Clusters finden Sie im Handbuch *vSAN-Planung und -Bereitstellung*.

Weitere Informationen zum Überwachen eines vSAN-Clusters und Beheben von Problemen finden Sie im Handbuch *vSAN-Überwachung und -Fehlerbehebung*.

# Aktualisierte Informationen

1

Dieses Dokument wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf von *Verwalten von VMware vSAN*.

| Revision | Beschreibung |
|---|---|
| 12. Juni 2023 | ■ Die Anleitung für das Upgrade von Stretched Clustern und Clustern mit zwei Hosts wurde aktualisiert, um darauf hinzuweisen, dass der Zeugenhost vor den Datenhosts aktualisiert wird: Vor dem Upgrade von vSAN.<br>■ Weitere kleinere Updates. |
| 08. Nov. 2021 | ■ Die Voraussetzungen für die Konfiguration der vSAN-Dateidienste in Konfigurieren von Dateidiensten wurden aktualisiert.<br>■ Informationen zu Datenträger-Upgrades wurden unter Informationen zum vSAN-Festplattenformat hinzugefügt.<br>■ Bei Verwendung einer vSphere with Tanzu-Umgebung finden Sie weitere Informationen zum Herunterfahren oder Starten der Komponenten im *VMware Cloud Foundation-Betriebshandbuch*. Manuelles Herunterfahren und Neustarten des vSAN-Clusters aktualisiert. |
| 16. April 2021 | ■ Aktualisierte Einschränkungen und Überlegungen für vSAN-Dateidienste in Einschränkungen und Überlegungen.<br>■ Aktualisierte Einschränkungen der AD-Unterstützung in Konfigurieren von Dateidiensten.<br>■ VMware hat das **My VMware**-Portal in **VMware Customer Connect** umbenannt. Das Thema vSAN-Build-Empfehlungen für vSphere Lifecycle Manager wurde aktualisiert, um diese Namensänderung zu berücksichtigen. |
| 12. Nov. 2020 | ■ Aktualisierte Überlegungen zum HCI-Netzwerkdesign in Freigeben von Remote-Datenspeichern mit HCI-Netz .<br>■ Aktualisierte ESXi-Aktualisierungsinformationen in Aktualisieren der ESXi-Hosts. |
| 06. OKT 2020 | Erstversion. |

# Einführung in vSAN

2

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.

# Konfigurieren und Verwalten eines vSAN-Clusters

3

Sie können einen vSAN-Cluster mithilfe des vSAN-Clusters, mithilfe von Esxcli-Befehlen oder mit anderen Tools konfigurieren und verwalten.

Dieses Kapitel enthält die folgenden Themen:

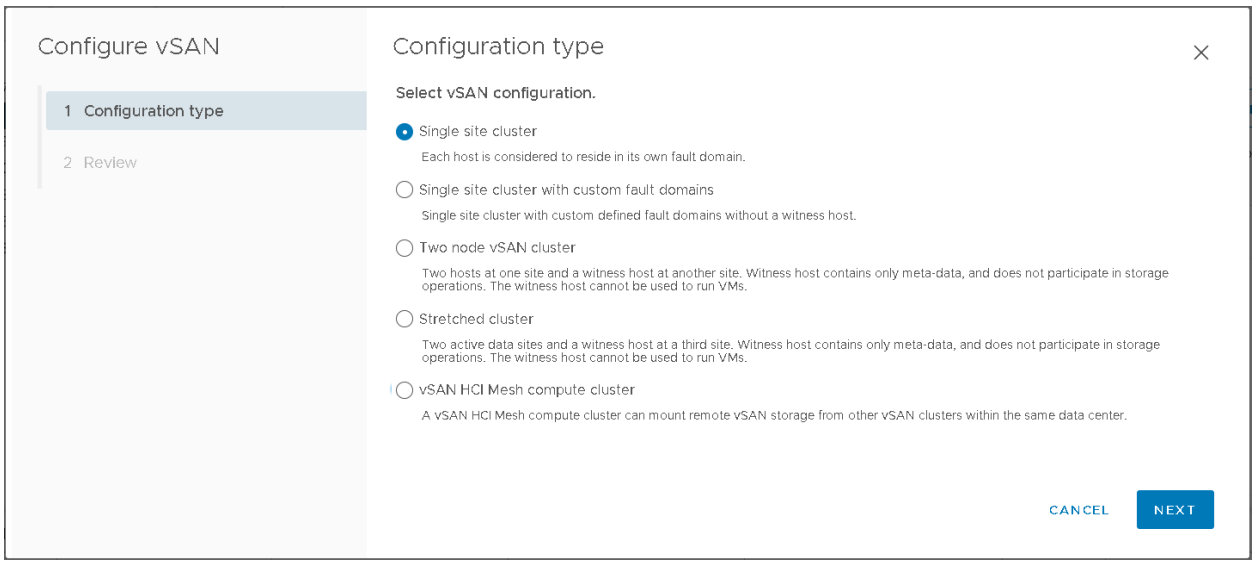


## Konfigurieren eines Clusters für vSAN mit dem vSphere Client

Sie können den HTML5-basierten vSphere Client verwenden, um Ihren vSAN-Cluster zu konfigurieren.

**Hinweis** Sie können Schnellstart verwenden, um einen vSAN-Cluster schnell zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter „Verwenden von Schnellstart zum Konfigurieren und Erweitern eines vSAN-Clusters“ in *vSAN-Planung und -Bereitstellung*.

**Hinweis** vSAN HCI Mesh-Computing-Cluster haben begrenzte Konfigurationsoptionen.




### Voraussetzungen

Vergewissern Sie sich, dass Ihre Umgebung alle Anforderungen erfüllt. Weitere Informationen finden Sie unter „Anforderungen für die Aktivierung von vSAN“ in *vSAN-Planung und -Bereitstellung*.

Erstellen Sie einen Cluster und fügen Sie dem Cluster Hosts hinzu, bevor Sie vSAN aktivieren und konfigurieren.

### Verfahren

1. Navigieren Sie zu einem vorhandenen Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
4. Klicken Sie auf **vSAN konfigurieren**, um den Assistenten „vSAN konfigurieren“ zu öffnen.
5. Wählen Sie den Typ des vSAN-Clusters aus, den Sie konfigurieren möchten, und klicken Sie auf **Weiter**.
   - Einzelner Standortcluster. Weitere Informationen finden Sie unter „vSAN-Bereitstellungsoptionen“ in *vSAN-Planung und -Bereitstellung*.
   - Einzelner Standortcluster mit benutzerdefinierten Fehlerdomänen.
   - vSAN-Cluster mit zwei Knoten.
   - Stretched Cluster.
   - vSAN HCI Mesh-Computing-Cluster. Weitere Informationen finden Sie unter „Freigeben von Remote-Datenspeichern mit HCI Mesh“ in *Verwalten von VMware vSAN*.

6 Konfigurieren Sie die zu verwendenden vSAN-Dienste, und klicken Sie auf **Weiter**.

   Konfigurieren Sie Datenverwaltungsfunktionen, einschließlich Deduplizierung und Komprimierung, Verschlüsselung von ruhenden Daten und Verschlüsselung in Übertragung begriffener Daten. Weitere Informationen finden Sie unter Bearbeiten von vSAN-Einstellungen.

7 Beanspruchen Sie Festplatten für den vSAN-Cluster, und klicken Sie auf **Weiter**.

   Jeder Host benötigt mindestens ein Flash-Gerät in der Cache-Schicht und ein oder mehrere Geräte in der Kapazitätsschicht. Weitere Informationen finden Sie unter „Verwalten von Festplattengruppen und Geräten“ in *Verwalten von VMware vSAN*.

8 Überprüfen Sie die Konfiguration und klicken Sie auf **Beenden**.

### Ergebnisse

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

### Nächste Schritte

Beanspruchen Sie Festplatten oder erstellen Sie Festplattengruppen. Weitere Informationen finden Sie unter „Verwalten von Festplattengruppen und Geräten“ in *Verwalten von VMware vSAN*.

Vergewissern Sie sich, dass der Datenspeicher für vSAN erstellt wurde.

Vergewissern Sie sich, dass der Speicheranbieter für vSAN registriert ist.

## Aktivieren von vSAN für einen vorhandenen Cluster

Sie können Clustereigenschaften bearbeiten, um vSAN in einem vorhandenen Cluster zu aktivieren.

### Voraussetzungen

Vergewissern Sie sich, dass Ihre Umgebung alle Anforderungen erfüllt. Weitere Informationen finden Sie unter „Anforderungen für die Aktivierung von vSAN“ in *vSAN-Planung und -Bereitstellung*.

**Hinweis** vSAN HCI Mesh-Computing-Cluster haben begrenzte Konfigurationsoptionen.

### Verfahren

1 Navigieren Sie zu einem vorhandenen Host-Cluster.

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

3 Wählen Sie unter „vSAN“ die Option **Dienste** aus.

4 Klicken Sie auf **vSAN konfigurieren**.

5 Wählen Sie den Typ des vSAN-Clusters aus, den Sie konfigurieren möchten, und klicken Sie auf **Weiter**.

- Einzelner Standortcluster.
- Einzelner Standortcluster mit benutzerdefinierten Fehlerdomänen.
- vSAN-Cluster mit zwei Knoten.
- Stretched Cluster.
- vSAN HCI Mesh-Computing-Cluster. Weitere Informationen finden Sie unter „Freigeben von Remote-Datenspeichern mit HCI Mesh“ in *Verwalten von VMware vSAN*.

6 Konfigurieren Sie die zu verwendenden vSAN-Dienste, und klicken Sie auf **Weiter**.

- Konfigurieren Sie den vSAN-Leistungsdienst. Weitere Informationen finden Sie unter „Überwachen der vSAN-Leistung“ in *vSAN-Überwachung und -Fehlerbehebung*.
- Aktivieren Sie den Dateidienst. Weitere Informationen finden Sie unter „vSAN-Dateidienst“ in *Verwalten von VMware vSAN*.
- Konfigurieren Sie vSAN-Netzwerkoptionen. Weitere Informationen finden Sie unter „Entwerfen des vSAN-Netzwerks“ in *vSAN-Planung und -Bereitstellung*.
- Aktivieren Sie den vSAN-Verlaufsintegritätsdienst.
- Konfigurieren Sie den iSCSI-Zieldienst. Weitere Informationen finden Sie unter „Verwenden des vSAN-iSCSI-Zieldiensts“ in *Verwalten von VMware vSAN*.
- Konfigurieren Sie Datenverwaltungsoptionen, einschließlich Deduplizierung und Komprimierung, Verschlüsselung ruhender Daten und Verschlüsselung in Übertragung begriffener Daten.
- Konfigurieren Sie Kapazitätsreservierungen und -warnungen. Weitere Informationen finden Sie unter „Übersicht über reservierte Kapazität“ in *vSAN-Überwachung und -Fehlerbehebung*.
- Konfigurieren Sie erweiterte Optionen:
  - Objektreparatur-Timer
  - Site-Lesebelegung für Stretched Cluster
  - Bereitstellung von Thin-Auslagerung
  - Unterstützung großer Cluster für maximal 64 Hosts
  - Automatische Neuverteilung

7 Beanspruchen Sie Festplatten für den vSAN-Cluster, und klicken Sie auf **Weiter**.

Jeder Host benötigt mindestens ein Flash-Gerät in der Cache-Schicht und ein oder mehrere Geräte in der Kapazitätsschicht. Weitere Informationen finden Sie unter „Verwalten von Festplattengruppen und Geräten“ in *Verwalten von VMware vSAN*.

8 Überprüfen Sie die Konfiguration und klicken Sie auf **Beenden**.

# vSAN Ausschalten

Sie können vSAN für einen Host-Cluster deaktivieren.

Wenn Sie vSAN für einen Cluster ausschalten, kann auf alle virtuellen Maschinen und Datendienste, die sich auf dem vSAN-Datenspeicher befinden, nicht mehr zugegriffen werden. Wenn Sie Speicher auf dem vSAN-Cluster mit vSAN Direct verbraucht haben, dann sind auch die vSAN Direct-Überwachungsdienste, wie z. B. Integritätsprüfungen, Speicherplatzberichte und Leistungsüberwachung, nicht verfügbar. Wenn Sie beabsichtigen, virtuelle Maschinen zu verwenden, während vSAN deaktiviert ist, stellen Sie sicher, dass Sie virtuelle Maschinen vor dem Ausschalten des vSAN-Clusters aus dem vSAN-Datenspeicher zu einem anderen Datenspeicher migrieren.

### Voraussetzungen

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

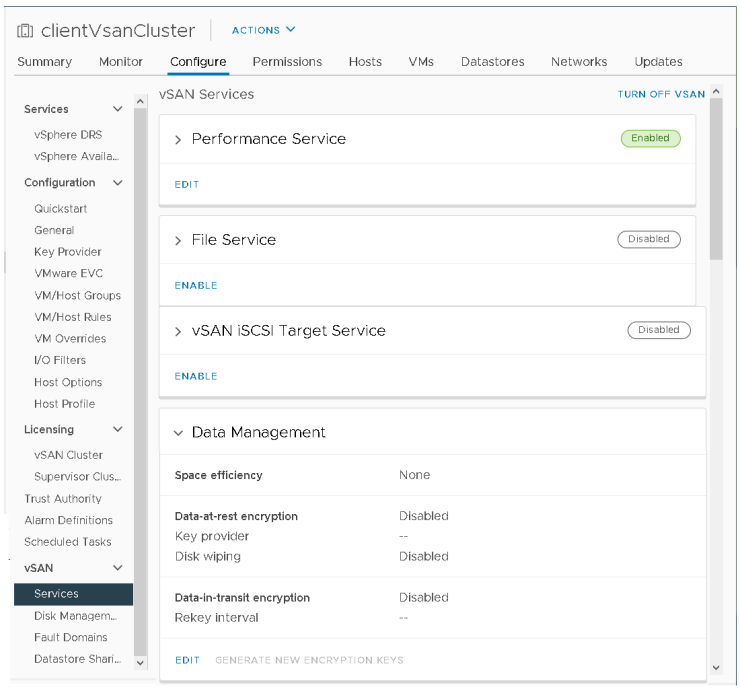
### Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
4. Klicken Sie auf **vSAN ausschalten**.
5. Bestätigen Sie Ihre Auswahl im Dialogfeld „vSAN ausschalten“.

# Bearbeiten von vSAN-Einstellungen

Sie können die Einstellungen Ihres vSAN-Clusters bearbeiten, um die Datenverwaltungsfunktionen zu konfigurieren und die vom Cluster bereitgestellten Dienste 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.




## Verfahren

1 Navigieren Sie zum vSAN-Host-Cluster.

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

   a Wählen Sie unter „vSAN“ die Option **Dienste** aus.

   b Klicken Sie für den Dienst, den Sie konfigurieren möchten, auf die Schaltfläche **Bearbeiten** oder **Aktivieren**.

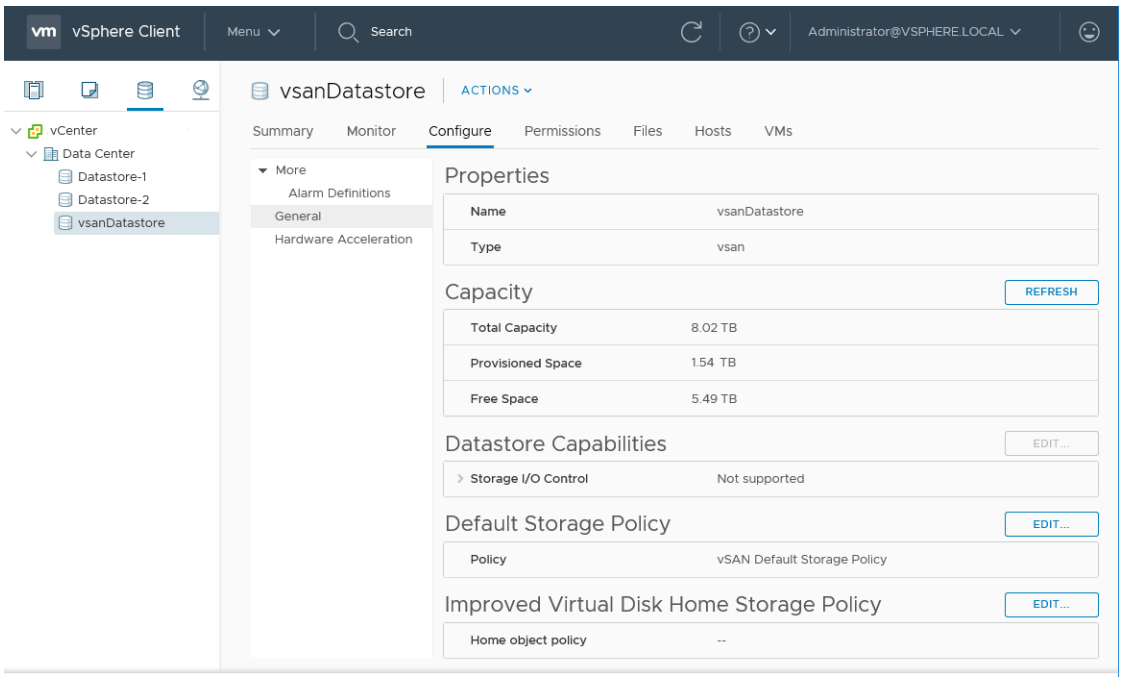
      - Konfigurieren Sie den vSAN-Leistungsdienst. Weitere Informationen finden Sie unter „Überwachen der vSAN-Leistung“ in *vSAN-Überwachung und -Fehlerbehebung*.
      - Aktivieren Sie den Dateidienst. Weitere Informationen finden Sie unter „vSAN-Dateidienst“ unter *Verwalten von VMware vSAN*.
      - Konfigurieren Sie vSAN-Netzwerkoptionen. Weitere Informationen finden Sie unter „Konfigurieren des vSAN-Netzwerks“ in *vSAN-Planung und -Bereitstellung*.
      - Aktivieren Sie den vSAN-Verlaufsintegritätsdienst.
      - Konfigurieren Sie den iSCSI-Zieldienst. Weitere Informationen finden Sie unter „Verwenden des vSAN-iSCSI-Zieldiensts“ in *Verwalten von VMware vSAN*.
      - Konfigurieren Sie Datenverwaltungsoptionen, einschließlich Deduplizierung und Komprimierung, Verschlüsselung ruhender Daten und Verschlüsselung in Übertragung begriffener Daten.
      - Konfigurieren Sie Kapazitätsreservierungen und -warnungen. Weitere Informationen finden Sie unter „Übersicht über reservierte Kapazität“ in *vSAN-Überwachung und -Fehlerbehebung*.
      - Konfigurieren Sie erweiterte Optionen:
         - Objektreparatur-Timer
         - Site-Lesebelegung für Stretched Cluster
         - Bereitstellung von Thin-Auslagerung
         - Unterstützung großer Cluster für maximal 64 Hosts
         - Automatische Neuverteilung

   c Ändern Sie die Einstellungen Ihren Anforderungen entsprechend.

3 Klicken Sie auf **Übernehmen**, um Ihre Auswahl zu bestätigen.

# 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.

### Verfahren

1. Navigieren Sie 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 Kapazitätsgeräte 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. Bei Verwendung der All-Flash-Konfiguration werden Flash-Geräte für die Kapazität verwendet. 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.

### Nächste Schritte

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

# Hochladen von Dateien oder Ordnern in vSAN-Datenspeicher

Sie können VMDK-Dateien in einen vSAN-Datenspeicher hochladen. Sie können auch Ordner in einen vSAN-Datenspeicher hochladen. Weitere Informationen zu Datenspeichern finden Sie unter *vSphere Storage*.

Wenn Sie eine VMDK-Datei in einen vSAN-Datenspeicher hochladen, gelten die folgenden Überlegungen:

- Sie können nur Stream-optimierte VMDK-Dateien in einen vSAN-Datenspeicher hochladen. Das Stream-optimierte VMware-Dateiformat ist ein monolithisches, für Streaming komprimiertes Sparse-Format. Wenn Sie eine VMDK-Datei hochladen möchten, die nicht im Stream-optimierten Format vorliegt, konvertieren Sie sie vor dem Hochladen mit dem Befehlszeilendienstprogramm vmware-vdiskmanager in das gewünschte Format. Weitere Informationen finden Sie im *Benutzerhandbuch zu Virtual Disk Manager*.
- Wenn Sie eine VMDK-Datei in einen vSAN-Datenspeicher hochladen, erbt die VMDK-Datei die Standardrichtlinie dieses Datenspeichers. Die VMDK erbt nicht die Richtlinie der VM, aus der sie heruntergeladen wurde. vSAN erstellt die Objekte durch Anwenden der vsanDatastore-Standardrichtlinie vom Typ „RAID-1“. Sie können die Standardrichtlinie des Datenspeichers ändern. Siehe Ändern der Standardspeicherrichtlinie für vSAN-Datenspeicher .
- Sie müssen eine VMDK-Datei in den VM-Stammordner hochladen.

### Verfahren

1 Navigieren Sie zum vSAN-Datenspeicher.

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

| Option | Beschreibung |
|---|---|
| **Dateien hochladen** | a Wählen Sie den Zielordner aus und klicken Sie auf **Dateien hochladen**. Es wird eine Meldung mit dem Hinweis angezeigt, dass Sie VMDK-Dateien nur im Stream-optimierten VMware-Format hochladen können. Wenn Sie eine VMDK-Datei in einem anderen Format hochladen, wird ein interne Serverfehler angezeigt.<br>b Klicken Sie auf **Hochladen**.<br>c Suchen Sie auf dem lokalen Computer nach dem hochzuladenden Element und klicken Sie auf **Öffnen**. |
| **Ordner hochladen** | a Wählen Sie den Zielordner aus und klicken Sie auf **Ordner hochladen**. Es wird eine Meldung mit dem Hinweis angezeigt, dass Sie VMDK-Dateien nur im Stream-optimierten VMware-Format hochladen können.<br>b Klicken Sie auf **Hochladen**.<br>c Suchen Sie auf dem lokalen Computer nach dem hochzuladenden Element und klicken Sie auf **Öffnen**. |

# Herunterladen von Dateien oder Ordnern aus vSAN-Datenspeichern

Sie können Dateien und Ordner aus einem vSAN-Datenspeicher herunterladen. Weitere Informationen zu Datenspeichern finden Sie unter *vSphere Storage*.

Die VMDK-Dateien werden als Stream-optimierte Dateien mit dem Dateinamen `<vmdkName>_stream.vmdk` heruntergeladen. Das Stream-optimierte VMware-Dateiformat ist ein monolithisches, für Streaming komprimiertes Sparse-Format.

Sie können eine Stream-optimierte VMware-VMDK-Datei mit dem Befehlszeilendienstprogramm vmware-vdiskmanager in andere VMDK-Dateiformate konvertieren. Weitere Informationen finden Sie im *Benutzerhandbuch zu Virtual Disk Manager*.

### Verfahren

1 Navigieren Sie zum vSAN-Datenspeicher.

2 Klicken Sie auf die Registerkarte **Dateien** und dann auf **Herunterladen**.

Sie erhalten eine Meldung mit dem Hinweis, dass VMDK-Dateien aus den vSAN-Datenspeichern im Stream-optimierten VMware-Format mit der Dateinamenerweiterung `.stream.vmdk` heruntergeladen werden.

3 Klicken Sie auf **Herunterladen**.

4 Suchen Sie nach dem herunterzuladenden Element und klicken Sie dann auf **Herunterladen**.

# Verwenden von vSAN-Speicherrichtlinien

4

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 enthält 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 der Wert für **Zu tolerierende Fehler** auf 1 festgelegt und sie hat einen einzelnen Datenträger-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 **Zu tolerierende Fehler** konfiguriert. Diese Objekte haben nicht dieselbe Verfügbarkeit wie andere Objekte, denen eine Richtlinie mit einem anderen Wert für **Zu tolerierende Fehler** zugewiesen wurde.

### Tabelle 4-1. Speicherrichtlinienregeln

| Funktionalität | Beschreibung |
| --- | --- |
| Zu tolerierende Fehler (Failures to Tolerate, FTT) | 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 Fault Domains konfiguriert sind, sind `2n+1` Fault Domains mit Kapazität bereitstellenden Hosts erforderlich. Ein Host, der nicht zu einer Fehlerdomäne gehört, wird als eigene Einzelhost-Fehlerdomäne gezählt.<br>Sie können eine Datenreplikationsmethode auswählen, die für Leistung oder Kapazität optimiert ist. RAID-1 (Spiegelung) verwendet mehr Festplattenspeicher, um die Objektkomponenten zu platzieren. Die Verwendung dieser Option führt jedoch zu verbesserter Leistung beim Zugriff auf die Objekte. RAID-5/6 (Erasure Coding) verwendet weniger Festplattenspeicher, die Leistung nimmt jedoch ab.<br>**Hinweis** Wenn vSAN eine einzelne Spiegelkopie von VM-Objekten nicht schützen soll, können Sie **Keine Datenredundanz** angeben. 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. Bei der Einstellung **Keine Datenredundanz**, 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 **FTT** angeben, erstellt vSAN eine einzelne Spiegelkopie der VM-Objekte. Sie kann einen einzelnen Ausfall tolerieren. Wenn allerdings mehrere Komponenten ausfallen, sind Ihre Daten möglicherweise gefährdet. |
| Ausfalltoleranz von Site | In einem Stretched Cluster definiert diese Regel die Anzahl von zusätzlichen Hostfehlern, die ein Objekt einer virtuellen Maschine innerhalb einer einzelnen Site tolerieren kann, nachdem die Anzahl der mit **FTT** definierten tolerierbaren Fehler erreicht ist.<br>Keine – Standardcluster ist der Standardwert. Bei einem Stretched Cluster können Sie die Daten auf der bevorzugten oder sekundären Site für die Hostaffinität aufbewahren.<br>Hostspiegelung – Cluster mit zwei Knoten definiert die Anzahl zusätzlicher Fehler, die ein Objekt tolerieren kann, nachdem die mit FTT definierte Anzahl von Fehlern erreicht ist. vSAN führt eine Objektspiegelung auf Festplattengruppenebene durch. Jeder Datenhost muss über mindestens drei Festplattengruppen verfügen, um diese Regel zu verwenden.<br>Site-Spiegelung – Stretched Cluster definiert die Anzahl der zusätzlichen Hostfehler, die ein Objekt tolerieren kann, nachdem die mit FTT definierte Anzahl von Fehlern erreicht ist. |

Tabelle 4-1. Speicherrichtlinienregeln (Fortsetzung)

| 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. Bei 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 4-1. Speicherrichtlinienregeln (Fortsetzung)

| Funktionalität | Beschreibung |
| --- | --- |
| Bereitstellung erzwingen | Wenn die Option auf **Ja** festgelegt ist, wird das Objekt bereitgestellt, auch wenn die in der Speicherrichtlinie angegebenen Richtlinien für **Zu tolerierende Fehler**, **Anzahl der Datenträger-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. Die folgenden Optionen sind verfügbar:<br>■ Thin Provisioning (Standard)<br>■ 25 % Reservierung<br>■ 50 % Reservierung<br>■ 75 % Reservierung<br>■ Thick Provisioning |

Tabelle 4-1. Speicherrichtlinienregeln (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. |
| 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 Überlegungen bezüglich des Entwerfens und Dimensionierens von Speicherrichtlinien finden Sie unter „Entwerfen und Dimensionieren eines vSAN-Clusters“ in *Verwalten von VMware vSAN*.

## Vorgehensweise zur Verwaltung von Richtlinienänderungen in vSAN

vSAN 6.7 Update 3 und höher verwaltet Richtlinienänderungen, um die Menge des vorübergehenden Speichers zu reduzieren, der von den Clustern verbraucht wird. Vorübergehende Kapazität wird erzeugt, wenn vSAN Objekte für eine Richtlinienänderung neu konfiguriert.

Wenn Sie eine Richtlinie ändern, wird die Änderung akzeptiert, aber nicht sofort angewendet. vSAN stapelt die Änderungsanforderungen für Richtlinien und führt sie asynchron aus, um eine bestimmte Menge an vorübergehendem Speicher beizubehalten.

Richtlinienänderungen werden aus nicht kapazitätsbezogenen Gründen sofort abgelehnt, wie z. B. beim Ändern einer RAID5-Richtlinie in RAID6 auf einem Cluster mit fünf Knoten.

Sie können die vorübergehende Kapazitätsnutzung in der vSAN-Kapazitätsüberwachung anzeigen. Verwenden Sie zum Überprüfen des Status einer Richtlinienänderung in einem Objekt den vSAN-Integritätsdienst, um den Zustand des vSAN-Objekts zu überprüfen.

# 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*.

vSAN 6.7 und höhere Versionen registrieren nur einen vSAN-Speicheranbieter für alle vSAN-Cluster, die von vCenter Server unter folgender URL verwaltet werden:

```
https://<VC fqdn>:<VC https port>/vsanHealth/vsanvp/version.xml
```

Überprüfen Sie, dass die Speicheranbieter registriert sind.

### Verfahren

1. Navigieren Sie zu vCenter Server.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.

### Ergebnisse

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. Um die Speicheranbieter für vSAN zu entfernen oder deren Registrierung aufzuheben, 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 in der Regel zur Platzierung von auf Datenspeichern für vSAN bereitgestellten virtuellen Maschinen verwendet werden.

**Tabelle 4-2. Spezifikationen für die vSAN-Standardspeicherrichtlinie**

| Spezifikation | Einstellung |
|---|---|
| Zu tolerierende Fehler | 1 |
| Anzahl der Festplatten-Stripes pro Objekt | 1 |
| 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 prüfen, wenn Sie zu **VM-Speicherrichtlinien** > **vSAN-Standardspeicherrichtlinie** > **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. In einigen Fällen müssen Sie bei dem Vergrößern eines Clusters die Standardspeicherrichtlinie ändern, um die Anforderungen des Service Level Agreements für VMware Cloud on AWS einzuhalten.

Wenn Sie einem Datenspeicher eine benutzerdefinierte Speicherrichtlinie zuweisen, wendet vSAN die Einstellungen für die benutzerdefinierte Richtlinie auf den angegebenen 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, sofern Sie beim Bereitstellen einer virtuellen Maschine keine andere vSAN-Richtlinie zuweisen. Das Textfeld **VM-Speicherrichtlinie** ist auf der Seite „Speicher auswählen“ auf **Datenspeicherstandardwert** festgelegt. 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. In der Regel bearbeiten Sie die Einstellungen der Standardspeicherrichtlinie nicht.
- 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.

# Ändern der Standardspeicherrichtlinie für vSAN-Datenspeicher

Sie können die Standardspeicherrichtlinie für einen ausgewählten vSAN-Datenspeicher ändern.

### 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.

### Verfahren

1. Navigieren Sie zum vSAN-Datenspeicher.
2. Klicken Sie auf **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.

   Treffen Sie eine Auswahl aus einer Liste von mit dem vSAN-Datenspeicher kompatiblen Speicherrichtlinien, wie z. B. die vSAN-Standardspeicherrichtlinie oder benutzerdefinierte Speicherrichtlinien, für die vSAN-Regelsätze definiert sind.
4. Wählen Sie eine Richtlinie aus und klicken Sie auf **OK**.

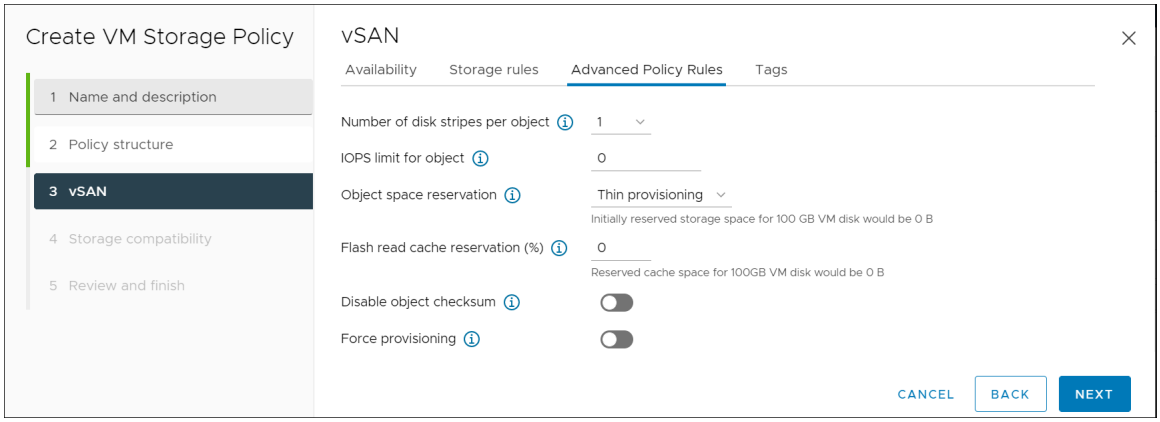
   Die Speicherrichtlinie wird als Standardrichtlinie angewendet, wenn Sie neue virtuelle Maschinen bereitstellen, ohne für einen Datenspeicher explizit eine Speicherrichtlinie festzulegen.

### Nächste Schritte

Sie können eine neue Speicherrichtlinie für virtuelle Maschinen definieren. Siehe Definieren einer Speicherrichtlinie für vSAN mit dem vSphere Client.

# Definieren einer Speicherrichtlinie für vSAN mit dem vSphere Client

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.
- Erforderliche Berechtigungen: **Profilgesteuerter Speicher.Ansicht des profilgesteuerten Speichers** und **Profilgesteuerter Speicher.Update des profilgesteuerten Speichers**

### Verfahren

1. Navigieren Sie zu **Richtlinien und Profile** und klicken Sie anschließend 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. Wählen Sie auf der Seite „Richtlinienstruktur“ die Option „Regeln für vSAN-Speicher aktivieren“ aus und klicken Sie auf **Weiter**.

6 Definieren Sie auf der vSAN-Seite den Satz an Richtlinienregeln und klicken Sie auf **Weiter**.

a Definieren Sie auf der Registerkarte „Verfügbarkeit“ die **Site-Ausfalltoleranz** und die **Anzahl der zu tolerierenden Fehler**.

Die Verfügbarkeitsoptionen definieren die Regeln für die zu tolerierenden Fehler, Datenbelegung und Fehlertoleranzmethode.

- **Ausfalltoleranz von Site** definiert den Typ der für VM-Objekte verwendeten Site-Ausfalltoleranz.
- **Zu tolerierende Ausfälle** legt die Anzahl der Host- und Gerätefehler, die ein VM-Objekt tolerieren kann, sowie die Datenreplizierungsmethode fest.

Beispiel: Wenn Sie **Spiegelung mit zwei Sites** und **2 Fehler – RAID-6 (Erasure Coding)** auswählen, konfiguriert vSAN die folgenden Richtlinienregeln:

- Zu tolerierende Fehler: 1
- Sekundäre Ebene der zu tolerierenden Ausfälle: 2
- Datenbelegung: Keine
- Fehlertoleranzmethode: RAID-5/6 (Erasure Coding) – Kapazität

b Definieren Sie auf der Registerkarte „Speicherregeln“ die Regeln für die Verschlüsselung, die Speicherplatzeffizienz und die Speicherschicht, die zusammen mit dem HCI-Netz zur Unterscheidung der entfernten Datenspeicher verwendet werden können.

- **Verschlüsselungsdienste**: Definiert die Verschlüsselungsregeln für virtuelle Maschinen, die Sie mit dieser Richtlinie bereitstellen. Wählen Sie eine der folgenden Optionen aus:
  - **Verschlüsselung ruhender Daten**: Die Verschlüsselung ist auf den virtuellen Maschinen aktiviert.
  - **Keine Verschlüsselung**: Die Verschlüsselung ist auf den virtuellen Maschinen nicht aktiviert.
  - **Keine Voreinstellung**: Macht die virtuellen Maschinen kompatibel mit den beiden Optionen „Verschlüsselung ruhender Daten“ und „Keine Verschlüsselung“.
- **Speicherplatzeffizienz**: Definiert die Regeln zum Platzsparen für die virtuellen Maschinen, die Sie mit dieser Richtlinie bereitstellen. Wählen Sie eine der folgenden Optionen aus:
  - **Deduplizierung und Komprimierung**: Aktiviert sowohl Deduplizierung als auch Komprimierung auf den virtuellen Maschinen. Deduplizierung und Komprimierung sind nur auf All-Flash-Festplattengruppen verfügbar. Weitere Informationen finden Sie unter Design-Überlegungen für Deduplizierung und Komprimierung.

- **Nur Komprimierung**: Aktiviert nur die Komprimierung auf den virtuellen Maschinen. Die Komprimierung ist nur für All-Flash-Festplattengruppen verfügbar. Weitere Informationen finden Sie unter Design-Überlegungen für Deduplizierung und Komprimierung.
- **Keine Speicherplatzeffizienz**: Die Speicherplatzeffizienzfunktionen sind auf den virtuellen Maschinen nicht aktiviert. Wenn Sie diese Option wählen, müssen Datenspeicher ohne Optionen für Speicherplatzeffizienz aktiviert sein.
- **Keine Voreinstellung**: Macht die virtuellen Maschinen mit allen Optionen kompatibel.

- **Speicherebene**: Gibt die Speicherebene für die virtuellen Maschinen an, die Sie mit dieser Richtlinie bereitstellen. Wählen Sie eine der folgenden Optionen aus: Durch die Auswahl der Option **Keine Voreinstellung** sind die virtuellen Maschinen sowohl mit Hybrid- als auch mit All-Flash-Umgebungen kompatibel.
  - **All-Flash**
  - **Hybrid**
  - **Keine Voreinstellung**

c Legen Sie auf der Registerkarte „Erweiterte Richtlinien“ die erweiterten Richtlinien fest, wie z. B. die Anzahl der Festplatten-Stripes pro Objekt und IOPS-Grenzwerte.

d Klicken Sie auf der Registerkarte „Tags“ auf **Tag-Regel hinzufügen** und definieren Sie die Optionen für Ihre Tag-Regel.

Stellen Sie sicher, dass die eingegebenen Werte innerhalb des von Speicherfunktionen des vSAN-Datenspeichers angegebenen Wertebereichs liegen.

7 Überprüfen Sie auf der Seite „Speicherkompatibilität“ die Liste der Datenspeicher unter den Registerkarten **KOMPATIBEL** und **INKOMPATIBEL** 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.

8 Überprüfen Sie auf der Seite „Überprüfen und beenden“ die Richtlinieneinstellungen und klicken Sie auf **Beenden**.

### Ergebnisse

Die neue Richtlinie wird zur Liste hinzugefügt.

### Nächste Schritte

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*.

# Erweitern und Verwalten eines vSAN-Clusters

5

Nachdem Sie den vSAN-Cluster eingerichtet haben, können Sie Hosts und Kapazitätsgeräte hinzufügen, Hosts und Geräte entfernen sowie Fehlerszenarien verwalten.

Dieses Kapitel enthält 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. Wenn Sie ein Gerät oder einen Host mit Kapazität hinzufügen, verteilt vSAN automatisch Daten an das neu hinzugefügte Gerät. Siehe „Automatische Neuverteilung konfigurieren“ in *vSAN-Überwachung und -Fehlerbehebung*.
- Verschieben Sie vorhandene ESXi-Hosts mithilfe eines Hostprofils in den vSAN-Cluster. Siehe Konfigurieren von Hosts mit dem Hostprofil. 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.

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.

## 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 Hinzufügen von Festplattengruppen. 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. Durch das Hinzufügen von Kapazitätsgeräten ohne Erhöhung des Caches wird möglicherweise das Verhältnis von Cache und Kapazität auf ein nicht unterstütztes Maß reduziert. Weitere Informationen finden Sie unter *vSAN-Planung und -Bereitstellung*.
- Verbessern Sie die Clusterleistung, indem Sie einem vorhandenen Speicher-E/A-Controller oder einem neuen Host mindestens ein Flash-Cache-Gerät und ein Kapazitätsgerät (Flash- oder Magnetfestplatte) hinzufügen. Um dieselbe Auswirkung auf die Leistung zu erzielen, können Sie einen oder mehrere Hosts mit Festplattengruppen hinzufügen, nachdem vSAN eine proaktive Neuverteilung im vSAN-Cluster durchgeführt hat.

Reine Computing-Hosts können zwar in einem vSAN-Cluster vorhanden sein und Kapazität von anderen Hosts im Cluster belegen, für einen effizienten Ablauf sollten Sie aber einheitlich konfigurierte Hosts hinzufügen. Fügen Sie für optimale Ergebnisse Hosts mit Zwischenspeicher- und Kapazitätsgeräten hinzu, um die Clusterkapazität zu erhöhen. Auch wenn es am besten ist, in Ihren Festplattengruppen dieselben oder ähnliche Geräte zu verwenden, wird jedes in der Hardwarekompatibilitätsliste (HCL) für vSAN aufgeführte Gerät unterstützt. Versuchen Sie, die Kapazität gleichmäßig auf Hosts und Festplattengruppen zu verteilen. Informationen zum Hinzufügen von Geräten zu Festplattengruppen finden Sie unter Hinzufügen von Geräten zu einer Festplattengruppe.

Führen Sie nach dem Erweitern der Clusterkapazität eine manuelle Neuverteilung durch, um die Ressourcen im Cluster gleichmäßig zu verteilen. Weitere Informationen finden Sie unter *vSAN-Überwachung und -Fehlerbehebung*.

# Verwenden von Schnellstart zum Hinzufügen von Hosts zu einem vSAN-Cluster

Wenn Sie Ihren vSAN-Cluster über Schnellstart konfiguriert haben, können Sie mithilfe des Schnellstart-Workflows Hosts und Speichergeräte zum Cluster hinzufügen.

Wenn Sie neue Hosts zum vSAN-Cluster hinzufügen, können Sie auch den Konfigurationsassistenten für den Cluster verwenden, um die Hostkonfiguration abzuschließen. Weitere Informationen zu Schnellstart finden Sie unter „Verwenden von Schnellstart zum Konfigurieren und Erweitern eines vSAN-Clusters“ in *vSAN-Planung und -Bereitstellung*.

**Hinweis** Wenn Sie vCenter Server auf einem Host ausführen, kann der Host nicht in den Wartungsmodus versetzt werden, wenn Sie ihn unter Verwendung des Schnellstart-Workflows einem Cluster hinzufügen. Auf demselben Host kann auch ein Platform Services Controller ausgeführt werden. Alle anderen VMs auf dem Host müssen ausgeschaltet sein.

### Voraussetzungen

- Der Schnellstart-Workflow muss für Ihren vSAN-Cluster verfügbar sein.
- Die im Schnellstart-Workflow durchgeführte Netzwerkkonfiguration wurde außerhalb des Schnellstart-Workflows geändert.

### Verfahren

1. Navigieren Sie im zum Cluster in vSphere Client zum Cluster .
2. Klicken Sie auf die Registerkarte „Konfigurieren“ und wählen Sie **Konfiguration > Schnellstart** aus.
3. Klicken Sie auf der Karte „Hosts hinzufügen“ auf **Starten**, um den Assistenten zum Hinzufügen von Hosts zu öffnen.
   a. Geben Sie auf der Seite „Hosts hinzufügen“ Informationen für neue Hosts ein oder klicken Sie auf „Bestehende Hosts“ und treffen Sie unter den in der Bestandsliste aufgeführten Hosts eine Auswahl.
   b. Überprüfen Sie auf der Seite „Hostübersicht“ die Hosteinstellungen.
   c. Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.
4. Klicken Sie auf der Karte „Clusterkonfiguration“ auf **Starten**, um den Assistenten für die Clusterkonfiguration zu öffnen.
   a. Geben Sie auf der Seite „Distributed Switches konfigurieren“ die Netzwerkeinstellungen für die neuen Hosts ein.
   b. (Optional) Wählen Sie auf der Seite „Festplatten beanspruchen“ die Festplatten auf jedem neuen Host.

c (Optional) Verschieben Sie auf der Seite Fehlerdomänen erstellen die neuen Hosts in ihren entsprechenden Fehlerdomänen.

Weitere Informationen zu Fehlerdomänen finden Sie unter Verwalten von Fault Domains in vSAN-Clustern.

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

## Hinzufügen eines Hosts zu einem vSAN-Cluster

Sie können ESXi-Hosts zu einem ausgeführten vSAN-Cluster ohne Unterbrechung laufender Vorgänge hinzufügen. Die Ressourcen des neuen 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.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

2 Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie **Hosts hinzufügen** aus. Der Assistent zum Hinzufügen von Hosts wird angezeigt.

| Option | Beschreibung |
|---|---|
| **Neue Hosts** | a Geben Sie den Hostnamen oder die IP-Adresse ein.<br>b Geben Sie den Benutzernamen und das Kennwort für den Host ein. |
| **Vorhandene Hosts** | a Wählen Sie die Hosts aus, die Sie vCenter Server zuvor hinzugefügt haben. |

3 Klicken Sie auf **Weiter**.

4 Zeigen Sie die Informationsübersicht an, und klicken Sie auf **Weiter**.

5 Überprüfen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.

Der Host wurde zum Cluster hinzugefügt.

### Nächste Schritte

Stellen Sie sicher, dass die Integritätsprüfung für die vSAN-Datenträgerverteilung grün ist.

Weitere Informationen zur Konfiguration von vSAN-Clustern und zur Fehlerbehebung finden Sie unter „Konfigurationsprobleme bei vSAN-Clustern“ in *vSAN-Überwachung und -Fehlerbehebung* .

## Konfigurieren von Hosts mit dem Hostprofil

Wenn mehrere Hosts im vSAN-Cluster vorhanden sind, können Sie das Profil eines vorhandenen vSAN-Hosts zum Konfigurieren der restlichen Hosts im vSAN-Cluster verwenden.

Das Hostprofil enthält Informationen über die Speicherkonfiguration, die Netzwerkkonfiguration oder andere Hostmerkmale. Wenn Sie vorhaben, einen Cluster mit vielen Hosts (z. B. 8, 16, 32 oder 64 Hosts) zu erstellen, verwenden Sie die Hostprofilfunktion. Mit Hostprofilen können Sie dem vSAN-Cluster mehrere Hosts gleichzeitig hinzufügen.

### 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.

### Verfahren

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-Konformität 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 Konformitätsfehler zu korrigieren.

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.

# Freigeben von Remote-Datenspeichern mit HCI-Netz

vSAN-Cluster können ihre Datenspeicher gemeinsam mit anderen vSAN-Clustern nutzen. Sie können VMs bereitstellen, die auf dem lokalen Cluster ausgeführt werden und Speicherplatz auf dem Remote-Datenspeicher verwenden.

Verwenden Sie die Ansicht „Datenspeicherfreigabe“, um Remote-Datenspeicher zu überwachen und zu verwalten, die auf dem vSAN-Cluster bereitgestellt sind. Jeder vSAN-Clientcluster des Clients kann Remote-Datenspeicher aus vSAN-Serverclustern bereitstellen, die sich innerhalb des von vCenter Server verwalteten Datencenters befinden. Jeder kompatible vSAN-Cluster kann auch als Server agieren und anderen vSAN-Clustern erlauben, seine lokalen Datenspeicher bereitzustellen.

Das Bereitstellen eines Remote-Datenspeichers per HCI-Netz ist eine clusterweite Konfiguration. Sie können einen Remote-Datenspeicher für einen vSAN-Cluster bereitstellen, der dann auf allen Hosts im Cluster bereitgestellt wird.

Wenn Sie eine neue virtuelle Maschine bereitstellen, können Sie einen im Clientcluster bereitgestellten Remote-Datenspeicher auswählen. Weisen Sie alle für den Datenspeicher konfigurierten kompatiblen Speicherrichtlinien zu.

Überwachungsansichten für Kapazität, Leistung, Integrität und Platzierung von virtuellen Objekte zeigen den Status von Remote-Objekten und Datenspeichern an.

Für HCI-Netz vSAN gibt es folgende Design-Überlegungen:

- Cluster müssen über denselben vCenter Server verwaltet werden und sich innerhalb desselben Datencenters befinden.
- Auf den Clustern muss das 7.0 Update 1 oder höher ausgeführt werden.
- Ein vSAN-Cluster kann seinen lokalen Datenspeicher für bis zu zehn vSAN-Clientcluster zur Verfügung stellen.
- Ein Clientcluster kann bis zu fünf Remote-Datenspeicher aus einem oder mehreren vSAN-Serverclustern bereitstellen.
- Ein einzelner Remote-Datenspeicher kann auf bis zu 128 vSAN-Hosts bereitgestellt werden, einschließlich der Hosts im vSAN-Servercluster.
- Alle Objekte, die eine VM erstellen, müssen sich auf demselben Datenspeicher befinden.
- Damit vSphere HA mit HCI Mesh funktioniert, konfigurieren Sie die folgende Ausfallreaktion für Datastore mit APD: VMs ausschalten und sie neu starten.
- Clienthosts, die nicht Teil eines Clusters sind, werden nicht unterstützt. Sie können einen einzelnen hostbasierten rechnergestützten Cluster konfigurieren, aber vSphere HA funktioniert nicht, es sei denn, Sie fügen dem Cluster einen zweiten Host hinzu.

Die folgenden Funktionen werden mit HCI Mesh nicht unterstützt:

- vSAN-Verschlüsselung in Übertragung begriffener Daten
- vSAN Stretched Clusters
- vSAN-2-Knoten-Cluster

Die folgenden Konfigurationen werden mit HCI Mesh nicht unterstützt:

- Remotebreitstellung der vSAN-Dateifreigabe, iSCSI-Volumes oder CNS-persistente Volumes. Sie können sie auf dem lokalen vSAN-Datenspeicher, aber nicht auf einem beliebigen vSAN-Remotedatenspeicher verwenden.
- vSAN-Netzwerke oder -Cluster mit Air Gap, die mehrere vSAN-VMkernel-Ports verwenden
- vSAN-Kommunikation über RDMA

## Reiner HCI Mesh-Computing-Client

Mit vSAN 7.0 Update 2 und höher können Sie einen Nicht-vSAN-Cluster als HCI Mesh-Client konfigurieren. Die Hosts in einem reinen HCI Mesh-Computing-Client-Cluster benötigen keinen lokalen Speicher. Sie können Remote-Datenspeicher aus einem vSAN-Cluster mounten, der sich innerhalb desselben Datencenters befindet.

Für HCI Mesh-Computing-Cluster gelten die folgenden Designüberlegungen:

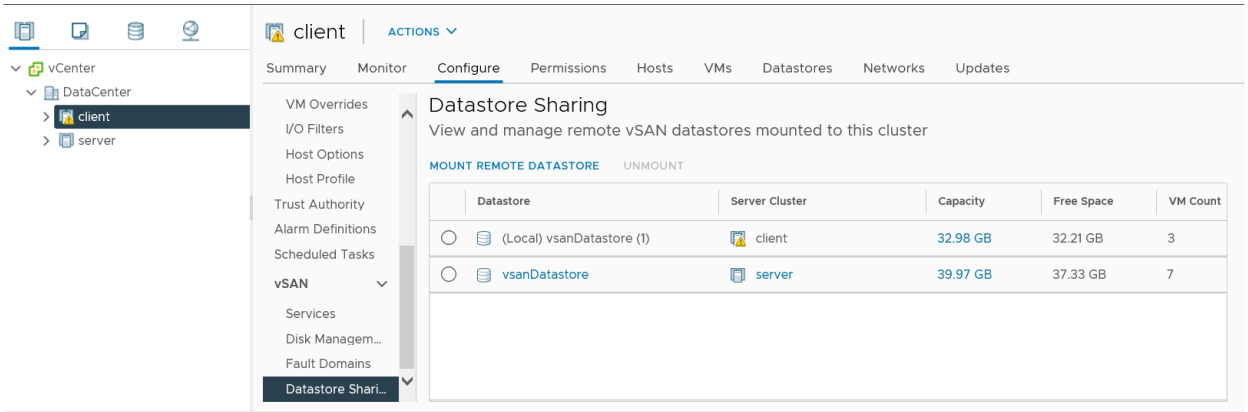
- Auf den Client-Hosts muss das vSAN-Netzwerk konfiguriert sein.

- Auf reinen vSAN-Computing-Hosts können keine Festplattengruppen vorhanden sein.
- Auf dem reinen Computing-Cluster können keine vSAN-Datenverwaltungsfunktionen konfiguriert werden.

Wenn Sie einen vSphere-Cluster für vSAN konfigurieren, können Sie ihn als HCI Mesh-Computing-Cluster angeben. Sie können einen Remote-Datenspeicher mounten und die Kapazität, den Zustand und die Leistung des Remote-vSAN-Datenspeichers überwachen.

## Anzeigen von Remote-Datenspeichern

Auf der Seite „Datenspeicherfreigabe“ können Sie die für den lokalen vSAN-Cluster bereitgestellten Remote-Datenspeicher sowie Clientcluster anzeigen, die den lokalen Datenspeicher gemeinsam nutzen.




### Verfahren

1. Gehen Sie zum lokalen vSAN-Cluster.
2. Klicken Sie auf die Registerkarte „Konfigurieren“.
3. Klicken Sie unter vSAN auf **Datenspeicherfreigabe**.

### Ergebnisse

In dieser Ansicht werden Informationen zu jedem Datenspeicher aufgelistet, der auf dem lokalen Cluster gemountet ist.

- Server-Cluster, der den Datenspeicher hostet
- Kapazität des Datenspeichers
- Verfügbarer freier Speicherplatz
- Die Anzahl VMs, die den Datenspeicher verwenden (Anzahl VMs, die die Rechenressourcen des lokalen Clusters, aber die Speicherressourcen des Serverclusters nutzen)
- Client-Cluster, für die der Datenspeicher bereitgestellt wurde

### Nächste Schritte

Auf dieser Seite können Sie Remotedatenspeicher mounten oder unmounten.

## Remotedatenspeicher mounten

Sie können einen oder mehr Datenspeicher aus anderen vSAN-Clustern mounten, die von demselben vCenter Server verwaltet werden.

### Verfahren

1. Gehen Sie zum lokalen vSAN-Cluster.
2. Klicken Sie auf die Registerkarte „Konfigurieren“.
3. Klicken Sie unter vSAN auf **Datenspeicherfreigabe**.
4. Klicken Sie auf **Remotedatenspeicher mounten**.
5. Wählen Sie einen Datenspeicher aus und klicken Sie auf **Weiter**.
6. Überprüfen Sie die Datenspeicherkompatibilität und klicken Sie auf **Beenden**.

### Ergebnisse

Der Remote-Datenspeicher wird auf dem lokalen vSAN-Cluster gemountet.

### Nächste Schritte

Bei der Bereitstellung einer VM können Sie den Remote-Datenspeicher als Speicherressource auswählen. Weisen Sie eine Speicherrichtlinie zu, die vom Remote-Datenspeicher unterstützt wird.

## Remote-Datenspeicher unmounten

Sie können einen Remote-Datenspeicher von einem vSAN unmounten.

Wenn keine virtuellen Maschinen auf dem lokalen Cluster den vSAN-Remote-Datenspeicher verwenden, können Sie die Bereitstellung des Datenspeichers für Ihren lokalen vSAN-Cluster aufheben.

### Verfahren

1. Gehen Sie zum lokalen vSAN-Cluster.
2. Klicken Sie auf die Registerkarte „Konfigurieren“.
3. Klicken Sie unter vSAN auf **Datenspeicherfreigabe**.
4. Wählen Sie einen Remote-Datenspeicher aus und klicken Sie auf **Unmounten**.
5. Klicken Sie auf **Unmounten**, um den Vorgang zu bestätigen.

### Ergebnisse

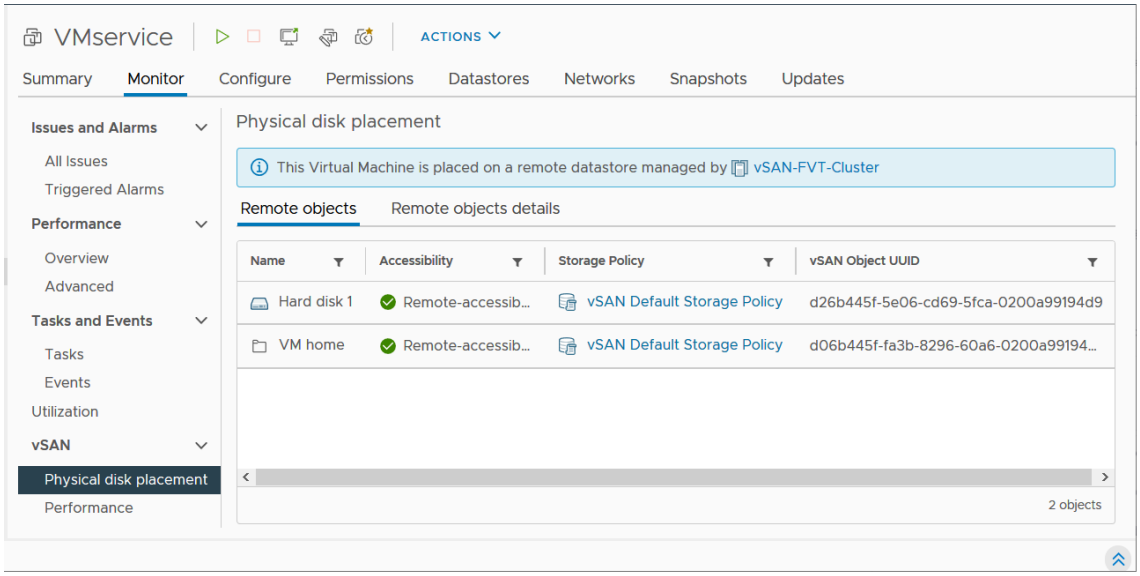
Der ausgewählte Datenspeicher wird von dem lokalen Cluster unmountet.

# Überwachen des HCI-Netzes

Sie können den vSphere Client verwenden, um den Status von HCI-Netz-Vorgängen zu überwachen.

Die vSAN-Kapazitätsüberwachung benachrichtigt Sie, wenn Remote-Datenspeicher für den Cluster bereitgestellt werden. Sie können den Remote-Datenspeicher auswählen, um die zugehörigen Kapazitätsinformationen anzuzeigen.

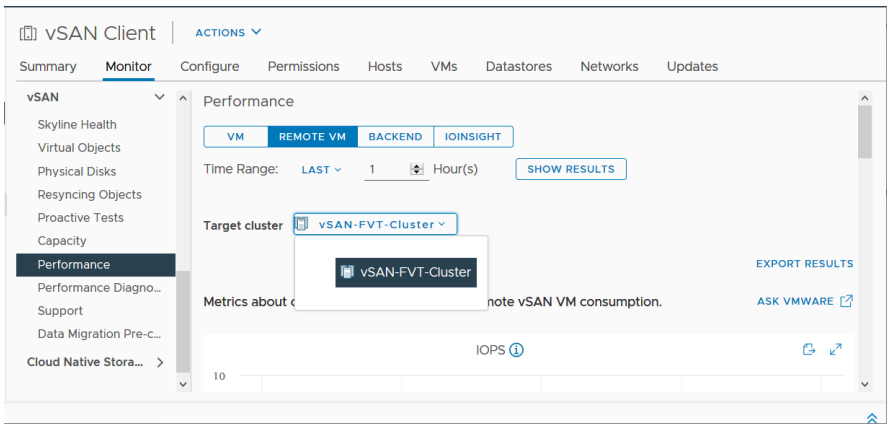
In der Ansicht „Virtuelle Eigenschaften“ wird der Datenspeicher angezeigt, in dem sich virtuelle Objekte befinden. In der Ansicht „Platzierung physischer Festplatten“ für eine VM, die sich auf einem Remote-Datenspeicher befindet, werden Informationen über den zugehörigen Remote-Standort angezeigt.




Die vSAN-Integritätsprüfungen melden den Status der HCI-Funktion.

- Unter „Daten > vSAN Objektintegritätsprüfung“ werden Informationen zur Barrierefreiheit von Remote-Objekten angezeigt.
- Die Partitionsüberprüfung unter „Netzwerk > Server-Clusterpartition“ liefert Berichte über Netzwerkpartitionen zwischen Hosts im Clientcluster und Servercluster.
- Unter „Netzwerk > Latenz“ wird die Latenz zwischen Hosts im Clientcluster und Servercluster überprüft.

Die Leistungsansichten für den vSAN-Cluster umfassen VM-Leistungsdiagramme, in den die Leistung des Clientclusters auf VM-Ebene aus der Perspektive des Remote-Clusters angezeigt wird. Sie können einen Remote-Datenspeicher auswählen, um die Leistung anzuzeigen.




Sie können proaktive Tests für Remote-Datenspeicher durchführen, um die Erstellung und Netzwerkleistung der VM zu überprüfen. Beim VM-Erstellungstest wird eine VM auf dem Remote-Datenspeicher erstellt. Mit dem Netzwerkleistungstest wird die Netzwerkleistung zwischen allen Hosts im Clientcluster und allen Hosts der Servercluster überprüft.

# 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.

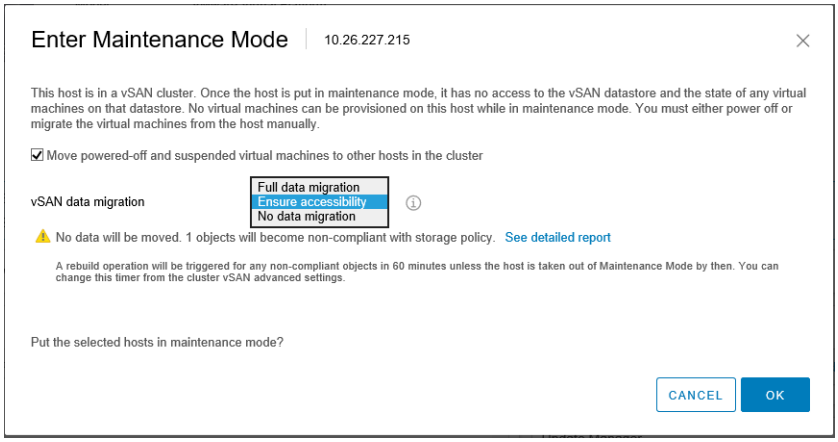
Wenn Sie mit dem Wartungsmodus arbeiten, beachten Sie folgende Einschränkungen:

- Wenn Sie einen ESXi-Host in den Wartungsmodus versetzen, müssen Sie einen Datenevakuierungsmodus wie zum Beispiel **Zugriff sicherstellen** oder **Vollständige Datenmigration** auswählen.
- 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 **Zugriff sicherstellen** ist schneller als der Modus **Vollständige Datenmigration**, weil der Modus **Zugriff 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 **Zugriff sicherstellen** werden Ihre Daten bei einem Ausfall nicht neu geschützt und eventuell tritt ein unerwarteter Datenverlust auf.

- Wenn Sie den Modus **Vollständige Datenmigration** auswählen, werden Ihre Daten automatisch neu vor einem Ausfall geschützt, wenn Ressourcen verfügbar sind und der Wert für **Zu tolerierende Fehler** auf 1 oder mehr 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 **Vollständige Datenmigration** 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 **Vollständige Datenmigration** 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 **Vollständige Datenmigration** verwenden, stellen Sie sicher, dass der Cluster über genügend Hosts und verfügbare Kapazität verfügt, um die Anforderungen der Richtlinie **Zu tolerierende Fehler** zu erfüllen.
- Stellen Sie sicher, dass auf den restlichen Hosts genügend Flash-Kapazität vorhanden ist, um Flash Read Cache-Reservierungen verarbeiten zu können. Führen Sie den folgenden RVC-Befehl aus, um die aktuell genutzte Kapazität pro Host zu analysieren und um zu ermitteln, ob der Ausfall eines einzelnen Hosts zu einem Speicherplatzmangel auf dem Cluster führen kann und sich auf die Clusterkapazität, die Cachereservierung und die Clusterkomponenten auswirkt: `vsan.whatif_host_failures`. 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.

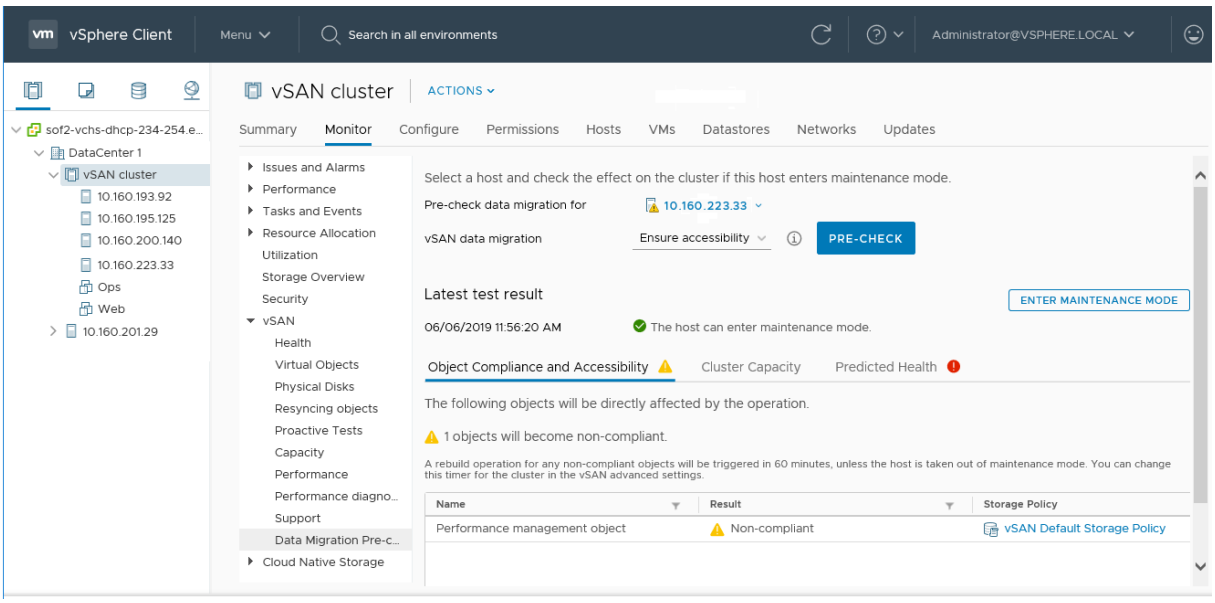
- Ob es ausreichend Kapazität gibt, um den Vorgang durchzuführen.

- 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.

## Überprüfen der Datenmigrationsfunktionen eines Hosts

Verwenden Sie die Vorabprüfung der Datenmigration, um die Auswirkungen von Datenmigrationsoptionen zu ermitteln, wenn Sie einen Host in den Wartungsmodus versetzen oder aus dem Cluster entfernen.

Bevor Sie einen vSAN-Host in den Wartungsmodus versetzen, führen Sie die Vorabprüfung der Datenmigration aus. Die Testergebnisse enthalten Informationen, mit denen Sie die Auswirkungen auf die Clusterkapazität, die vorhergesagten Integritätsprüfungen und alle abweichenden Objekte ermitteln können. Bei einem Fehlschlagen des Vorgangs stellt die Vorabprüfung Informationen zu den Ressourcen bereit, die benötigt werden.




### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

2 Klicken Sie auf die Registerkarte „Überwachen“.

3 Klicken Sie unter vSAN auf **Vorabprüfung der Datenmigration**.

4 Wählen Sie einen Host und eine Datenmigrationsoption aus und klicken Sie auf **Vorabprüfung**.

   vSAN führt die Tests für die Vorabprüfung der Datenmigration aus.

5 Zeigen Sie die Testergebnisse an.

Die Ergebnisse der Vorabprüfung zeigen, ob der Host sicher in den Wartungsmodus versetzt werden kann.

- Auf der Registerkarte „Objektübereinstimmung und Zugriffsfähigkeit“ werden Objekte angezeigt, die nach der Datenmigration Probleme aufweisen können.
- Auf der Registerkarte „Clusterkapazität“ werden die Auswirkungen der Datenmigration auf den vSAN-Cluster vor und nach der Durchführung des Vorgangs angezeigt.
- Auf der Registerkarte „Systemzustand“ werden die Integritätsprüfungen angezeigt, die unter Umständen von der Datenmigration betroffen sind.

### Nächste Schritte

Wenn der Host gemäß Vorabprüfung in den Wartungsmodus versetzt werden kann, können Sie auf **In den Wartungsmodus wechseln** klicken, um die Daten zu migrieren und den Host in den Wartungsmodus zu versetzen.

## 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 wie zum Beispiel **Zugriff sicherstellen** oder **Vollständige Datenmigration** auswählen.

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.

Von diesem Host bediente vSAN-iSCSI-Ziele werden auf andere Hosts im Cluster übertragen, und der iSCSI-Initiator wird somit zum neuen Besitzer des Ziels umgeleitet.

### Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung die für die gewählte Option erforderlichen Funktionen aufweist.

### Verfahren

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 |
|---|---|
| **Zugriff 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 der Wert für **Zu tolerierende Fehler** 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. |
| **Vollständige Datenmigration** | vSAN verlagert alle Daten in andere Hosts im Cluster und behält den Übereinstimmungsstatus des aktuellen Objekts bei. 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.<br>Alle Komponenten im lokalen Speicher des ausgewählten Hosts werden anderswo im Cluster migriert. Wenn der Host in den Wartungsmodus wechselt, haben alle virtuellen Maschinen Zugriff auf ihre Speicherkomponenten und halten weiterhin die ihnen zugewiesenen Speicherrichtlinien ein.<br>**Hinweis** Bei Objekten mit reduziertem Verfügbarkeitszustand behält dieser Modus diesen Übereinstimmungsstatus bei und gibt keine Garantie, dass die Objekte kompatibel werden.<br>Der Host kann nicht in den Wartungsmodus wechseln, wenn auf ein VM-Objekt mit Daten auf dem Host nicht zugegriffen werden kann und das Objekt nicht vollständig verlagert wird. |
| **Keine Datenmigration** | 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 **Vollständige Datenmigration** nicht verwendet werden kann oder dass Daten nach einem Fehler erneut geschützt werden müssen.

Alternativ können Sie einen Host mithilfe von ESXCLI in den Wartungsmodus versetzen. Bevor Sie einen Host in diesen Modus versetzen, stellen Sie sicher, dass Sie die auf dem Host ausgeführten VMs ausgeschaltet haben.

Führen Sie folgenden Befehl auf dem Host aus, um in den Wartungsmodus zu wechseln:

```
esxcli system maintenanceMode set --enable 1
```

Zum Überprüfen des Status des lokalen Benutzers führen Sie folgenden Befehl aus:

```
esxcli system maintenanceMode get
```

Zum Beenden des Wartungsmodus führen Sie folgenden Befehl aus:

```
esxcli system maintenanceMode set --enable 0
```

### Nächste Schritte

Den Fortschritt der Datenmigration im Cluster können Sie nachverfolgen. Weitere Informationen finden Sie unter *vSAN-Überwachung und -Fehlerbehebung*.

# Verwalten von Fault Domains in vSAN-Clustern

Fehlerdomänen ermöglichen es Ihnen, sich vor Rack- oder Gehäuseausfällen zu schützen, wenn Ihr vSAN-Cluster über mehrere Racks oder Blade-Server-Gehäuse verteilt ist. Sie können Fehlerdomänen erstellen und jeder von ihnen einen oder mehrere Hosts hinzufügen.

Eine Fehlerdomäne besteht aus einem oder mehreren vSAN-Hosts, die entsprechend ihrem physischen Speicherort im Datencenter zusammengefasst sind. Konfigurierte Fehlerdomänen ermöglichen es vSAN, Ausfälle ganzer physikalischer Racks sowie Ausfälle eines einzelnen Hosts, eines Kapazitätsgeräts, einer Netzwerkverbindung oder eines Netzwerk-Switches, der einer Fehlerdomäne zugeordnet ist, zu tolerieren.

Die Richtlinie **Zu tolerierende Fehler** für den Cluster hängt von der Anzahl der Ausfälle ab, die eine virtuelle Maschine tolerieren kann. Wenn das Attribut **Zu tolerierende Fehler** (FTT) für eine virtuelle Maschine auf 1 `(FTT=1)` festgelegt ist, kann vSAN einen einzelnen Ausfall beliebiger Art einer beliebigen Komponente in einer Fehlerdomäne 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 der Wert für **Zu tolerierende Fehler** auf „N“ `(FTT=n)` festgelegt ist, benötigt vSAN mindestens `2*n+1` Fehlerdomänen 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.

Für die Unterstützung der Festlegung von FTT auf 1 sind mindestens drei Fehlerdomänen erforderlich. 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 Fehlerdomänen finden Sie unter „Entwerfen und Dimensionieren von vSAN-Fehlerdomänen“ in *vSAN-Planung und -Bereitstellung*.

Betrachten Sie ein Szenario mit einem vSAN-Cluster mit 16 Hosts. Die Hosts verteilen sich auf vier Racks, das heißt vier Hosts pro Rack. Erstellen Sie für jedes Rack eine Fehlerdomäne, damit der Ausfall eines ganzen Racks toleriert wird. Sie können einen Cluster mit einer solchen Kapazität mit dem Wert „1“ für **Zu tolerierende Fehler** konfigurieren. Wenn Sie das Attribut **Zu tolerierende Fehler** auf 2 festlegen möchten, konfigurieren Sie 5 Fehlerdomänen im Cluster.

Wenn ein Rack ausfällt, ist keine Ressource (CPU, Speicher usw.) mehr im Rack für den Cluster verfügbar. Konfigurieren Sie daher kleinere Fehlerdomänen, um die Auswirkungen eines möglichen Rackausfalls zu verringern. Je mehr Fehlerdomänen Sie erstellen, desto höher ist die Gesamtverfügbarkeit der Ressourcen 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.
- Platzieren Sie beim Entwerfen von Fehlerdomänen eine einheitliche Anzahl an Hosts in jeder Fehlerdomäne.

  Richtlinien zum Entwerfen von Fehlerdomänen finden Sie unter „Entwerfen und Dimensionieren von vSAN-Fehlerdomänen“ in *vSAN-Planung und -Bereitstellung*.
- 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.
- Überprüfen 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.

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen**.
4. Klicken Sie auf das Plussymbol. Der Assistent „Neue Fehlerdomäne“ wird geöffnet.
5. Geben Sie den Namen der Fehlerdomäne ein.
6. 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.
7. Klicken Sie auf **Erstellen**.

   Die ausgewählten Hosts werden in der Fehlerdomäne angezeigt. In jeder Fehlerdomäne werden die Informationen zur verwendeten und reservierten Kapazität angezeigt. Auf diese Weise können Sie die Kapazitätsverteilung in der Fehlerdomäne anzeigen.

## Verschieben von Hosts in eine ausgewählte Fault Domain

Sie können einen Host in eine ausgewählte Fault Domain im vSAN-Cluster verschieben.

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen**.
4. Klicken Sie auf den hinzuzufügenden Host und ziehen Sie ihn in die vorhandene Fehlerdomäne.

   Der ausgewählte Host wird in der Fault Domain angezeigt.

## 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.

### Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen**.
   a. Klicken Sie auf den Host und ziehen Sie ihn aus der Fehlerdomäne in den Bereich „Eigenständige Hosts“.
   b. Klicken Sie auf **Verschieben**, um den Vorgang zu bestätigen.

### Ergebnisse

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.

### Nächste Schritte

Sie können Hosts zu Fault Domains hinzufügen. Siehe Verschieben von Hosts in eine ausgewählte Fault Domain.

## Umbenennen einer Fault Domain

Sie können den Name einer vorhandenen Fault Domain in Ihrem vSAN-Cluster ändern.

### Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Fehlerdomänen**.
   a. Klicken Sie auf das Symbol „Aktionen“ auf der rechten Seite der Fehlerdomäne und wählen Sie **Bearbeiten** aus.
   b. Geben Sie einen neuen Fault Domain-Namen ein.
4. Klicken Sie auf **Übernehmen** oder **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.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

3 Klicken Sie unter vSAN auf **Fehlerdomänen**.

4 Klicken Sie auf das Symbol „Aktionen“ auf der rechten Seite der Fehlerdomäne und wählen Sie **Löschen** aus.

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

Ergebnisse

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.

## Tolerieren zusätzlicher Ausfälle mit Fehlerdomänen

Fehlerdomänen in einem vSAN-Cluster bieten Ausfallsicherheit und stellen sicher, dass die Daten auch bei richtlinienbedingten Ausfällen verfügbar sind. Wenn „Anzahl der zu tolerierenden Fehler“ (FTT) auf 1 gesetzt ist, kann das Objekt einen Ausfall tolerieren. Ein temporärer Ausfall gefolgt von einem permanenten Ausfall in einem Cluster kann jedoch zu Datenverlusten führen.

Eine zusätzliche Fehlerdomäne bietet vSAN die Möglichkeit, eine Haltbarkeitskomponente zu erstellen, ohne zusätzliche FTTs für das Objekt zu haben. vSAN löst diese zusätzliche Komponente bei geplanten und ungeplanten Ausfällen aus. Zu den ungeplanten Ausfällen gehören Netzwerkunterbrechungen, Festplattenausfälle und Hostausfälle. Zu den geplanten Ausfällen gehört der Eintritt in den Wartungsmodus (EMM). Beispielsweise kann ein 6-Host-Cluster mit RAID 6-Objekt bei einem Hostausfall keine Haltbarkeitskomponente erstellen.

vSAN stellt die Datenverfügbarkeit der Objekte sicher, wenn die Komponenten offline gehen und unerwartet wieder online kommen, basierend auf den in der Speicherrichtlinie festgelegten FTTs. Bei einem Ausfall werden die Schreibvorgänge der ausgefallenen Komponente auf die Haltbarkeitskomponente umgeleitet. Wenn sich die Komponente von dem vorübergehenden Fehler erholt und wieder online geht, verschwindet die Haltbarkeitskomponente und führt zur Resynchronisierung der Komponente.

Ohne die Haltbarkeitskomponente gehen bei einem zweiten dauerhaften Ausfall im Cluster, von dem das Spiegelobjekt betroffen ist, die Objektdaten dauerhaft verloren, auch wenn der Ausfall behoben wurde.

# 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. vSAN 6.7 und neuere Versionen unterstützen Windows Server Failover Clustering (WSFC), damit WSFC-Knoten auf vSAN-iSCSI-Ziele zugreifen können.

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.

Weitere Informationen zur Verwendung des vSAN-iSCSI-Zieldiensts finden Sie im Handbuch zur Verwendung von iSCSI-Targets.

## 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-Zieldiensts 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.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dienste**.

2 Klicken Sie in der Zeile des vSAN-iSCSI-Zieldiensts auf **AKTIVIEREN**.

Der Assistent „vSAN-iSCSI-Zieldienst bearbeiten“ wird geöffnet.

3 Die Konfiguration des vSAN iSCSI-Zieldienstes bearbeiten.

Sie können gegenwärtig das Standardnetzwerk, den TCP-Port und die Authentifizierungsmethode auswählen. Sie können auch eine vSAN-Speicherrichtlinie auswählen.

4 Klicken Sie auf den Schieberegler **vSAN-iSCSI-Zieldienst aktivieren** um ihn einzuschalten, und klicken Sie dann auf **ÜBERNEHMEN**.

### Ergebnisse

Der vSAN iSCSI-Zieldienst ist aktiviert.

### Nächste Schritte

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.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.

b Klicken Sie auf die Registerkarte „iSCSI-Ziele“.

c Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neues iSCSI-Ziel** wird angezeigt. Wenn Sie das Feld „Ziel-IQN“ leer lassen, wird der IQN automatisch generiert.

d Geben Sie einen Ziel-**Alias** ein.

e Wählen Sie eine **Speicherrichtlinie**, ein **Netzwerk**, einen **TCP-Port** und eine Methode für die **Authentifizierung** aus.

f Wählen Sie den **E/A-Besitzerspeicherort** aus. Diese Funktion ist nur verfügbar, wenn Sie vSAN Cluster als Stretched Cluster konfiguriert haben. Sie ermöglicht Ihnen die Angabe des Site-Standorts für das Hosting des iSCSI-Zieldiensts für ein Ziel. Dies hilft bei der Vermeidung des standortübergreifenden iSCSI-Datenverkehrs. Wenn Sie die Richtlinie als HFT>=1 festlegen, ändert sich der E/A-Besitzerspeicherort im Falle eines Site-Ausfalls in die alternative Site. Nach der Wiederherstellung des Site-Fehlers wird der E/A-Besitzerspeicherort gemäß Konfiguration automatisch auf den ursprünglichen E/A-Besitzerspeicherort zurückgesetzt. Sie können eine der folgenden Optionen auswählen, um den Speicherort der Site festzulegen:

- **Entweder**: Hostet den iSCSI-Zieldienst entweder auf der bevorzugten oder der sekundären Site.
- **Bevorzugt**: Hostet den iSCSI-Zieldienst auf der bevorzugten Site.
- **Sekundär**: Hostet den iSCSI-Zieldienst auf der sekundären Site.

3 Klicken Sie auf **OK**.

#### Ergebnisse

Das iSCSI-Ziel wird erstellt und im Bereich der vSAN iSCSI-Ziele zusammen mit Informationen wie IQN, E/A-Besitzerhost usw. aufgelistet.

#### Nächste Schritte

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.

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.

b Klicken Sie auf die Registerkarte „iSCSI-Ziele“ und wählen Sie ein Ziel aus.

c Klicken Sie im Abschnitt „vSAN-iSCSI-LUNs“ auf **Hinzufügen**. Das Dialogfeld **LUN zu Ziel hinzufügen** wird angezeigt.

d 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.

3 Klicken Sie auf **Hinzufügen**.

## Ändern der Größe einer LUN auf einem iSCSI-Ziel

Je nach Ihren Anforderungen können Sie eine Online-LUN vergrößern. Die Online-Größenanpassung der LUN ist nur dann aktiviert, wenn alle Hosts im Cluster auf vSAN 6.7 Update 3 oder höher aktualisiert wurden.

### Verfahren

1 Navigieren Sie im vSphere Client zum vSAN-Cluster.

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

3 Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.

4 Klicken Sie auf die Registerkarte **iSCSI-Ziele** und wählen Sie ein Ziel aus.

5 Wählen Sie im Abschnitt „vSAN-iSCSI-LUNs“ eine LUN aus und klicken Sie auf **Bearbeiten**. Das Dialogfeld „LUN bearbeiten“ wird angezeigt.

6 Vergrößern Sie die LUN entsprechend Ihren Anforderungen.

7 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.

**Hinweis** Die Initiatoren außerhalb der Initiatorgruppe können nicht auf das Ziel zugreifen, wenn die Initiatorgruppe für die Zugriffssteuerung auf dem iSCSI-Ziel erstellt wurde. Die vorhandenen Verbindungen von diesen Initiatoren gehen verloren und können erst wiederhergestellt werden, wenn sie zur Initiatorgruppe hinzugefügt wurden. Sie müssen die aktuellen Initiatorverbindungen überprüfen und sicherstellen, dass alle autorisierten Initiatoren vor der Gruppenerstellung zur Initiatorgruppe hinzugefügt werden.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

   a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.

   b Klicken Sie auf die Registerkarte „Initiatorgruppe“ und dann auf **Hinzufügen**. Das Dialogfeld **Neue Initiatorgruppe** wird angezeigt.

c Geben Sie einen Namen für die iSCSI-Initiatorgruppe ein.

d (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)

3 Klicken Sie auf **OK** oder **Erstellen**.

#### Nächste Schritte

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.

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.

b Wählen Sie die Registerkarte **Initiatorgruppen** aus.

c Klicken Sie im Abschnitt „Zugängliche Ziele“ auf **Hinzufügen**. Das Dialogfeld **Zugängliche Ziele hinzufügen** wird angezeigt.

d Wählen Sie ein Ziel aus der Liste der verfügbaren Ziele aus.

3 Klicken Sie auf **Hinzufügen**.

## Deaktivieren Sie den iSCSI-Zieldienst

Sie können den vSAN iSCSI-Zieldienst deaktivieren. Durch deaktivieren des vSAN iSCSI-Zieldiensts werden die LUNs/Ziele nicht gelöscht. Wenn Sie Speicherplatz zurückfordern möchten, löschen Sie die LUNs/Ziele manuell, bevor Sie den vSAN iSCSI-Zieldienst deaktivieren.

### Voraussetzungen

Arbeitslasten, die auf iSCSI-LUNs ausgeführt werden, werden beendet, wenn Sie den iSCSI-Zieldienst deaktivieren. Stellen Sie vor dem Deaktivieren sicher, dass keine Arbeitslasten auf iSCSI-LUNs ausgeführt werden.

### Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dienste**.
2. Klicken Sie in der Zeile vSAN-iSCSI-Zieldienst auf **BEARBEITEN**.

   Der Assistent „vSAN-iSCSI-Zieldienst bearbeiten“ wird geöffnet.
3. Klicken Sie auf den Schieberegler **vSAN-iSCSI-Zieldienst aktivieren**, um ihn zu beenden, und klicken Sie auf **Übernehmen**.

### Ergebnisse

Der vSAN iSCSI-Zieldienst ist deaktiviert.

### Nächste Schritte

## 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.

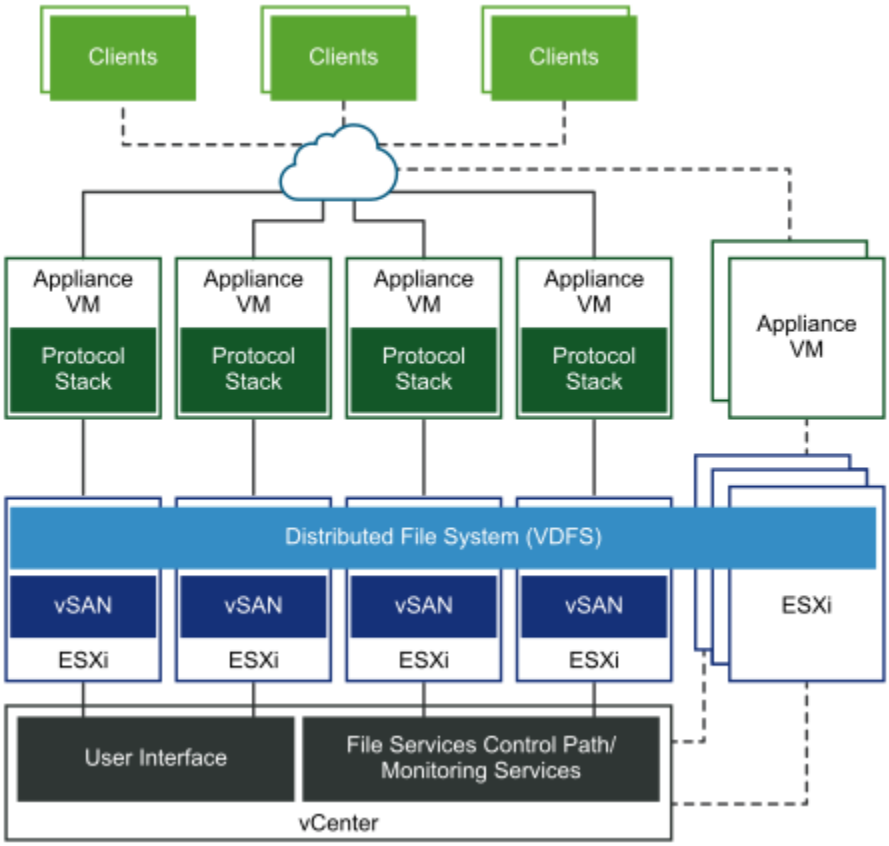
### Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf **Überwachen** und wählen Sie **Virtuelle Objekte** aus. Die iSCSI-Ziele werden auf der Seite aufgelistet.
3. Wählen Sie ein Ziel aus und klicken Sie auf **Platzierungsdetails anzeigen**. Die physische Platzierung zeigt an, wo sich die Datenkomponenten des Ziels befinden.
4. Klicken Sie auf **Gruppenkomponenten nach Hostplatzierung**, um die Hosts anzuzeigen, die den iSCSI-Datenkomponenten zugeordnet sind.

# vSAN-Dateidienst

Nutzen Sie den vSAN-Dateidienst, um im vSAN-Datenspeicher Dateifreigaben zu erstellen, auf die Client-Arbeitsplätze oder VMs zugreifen können. Auf die in einer Dateifreigabe gespeicherten Daten kann von jedem Gerät zugegriffen werden, das über Zugriffsrechte verfügt.

Der vSAN-Dateidienst ist eine Schicht über vSAN, die dazu dient, Dateifreigaben bereitzustellen. Momentan werden SMB-, NFS v3- und NFS v4.1-Dateifreigaben unterstützt. Der vSAN-Dateidienst besteht aus dem verteilten vSAN-Dateisystem (vDFS), das das zugrunde liegende skalierbare Dateisystem bereitstellt, indem vSAN-Objekte, eine Speicherdienstplattform, die belastbare Dateiserver-Endpoints und eine Control Plane für die Bereitstellung, Verwaltung und Überwachung bereitstellt, zusammengefasst werden. Dateifreigaben werden auf Freigabebasis in die vorhandene speicherrichtlinienbasierte Verwaltung von vSAN integriert. Der vSAN-Dateidienst bietet die Möglichkeit, die Dateifreigaben direkt auf dem vSAN-Cluster zu hosten.




Wenn Sie den vSAN-Dateidienst konfigurieren, erstellt vSAN ein einziges verteiltes VDFS-Dateisystem für den Cluster, der intern für Verwaltungszwecke verwendet wird. Auf jedem Host wird eine Dateidienst-VM (FSVM) platziert. Die FSVMs verwalten Dateifreigaben im vSAN-Datenspeicher. Jede FSVM enthält einen Dateiserver, der sowohl den NFS- als auch den SMB-Dienst bereitstellt.

Bei der Aktivierung des Dateidienst-Workflows muss ein Pool mit statischen IP-Adressen angegeben werden. Eine der IP-Adressen wird als primäre IP-Adresse festgelegt. Die primäre IP-Adresse kann über SMB- und NFS v4.1-Verweise für den Zugriff auf alle Freigaben im Dateidienst-Cluster verwendet werden. Für jede im IP-Pool angegebene IP-Adresse wird ein Dateiserver gestartet. Eine Dateifreigabe wird nur von einem einzelnen Dateiserver exportiert. Die Dateifreigaben werden jedoch gleichmäßig auf alle Dateiserver verteilt. Für die Bereitstellung von Computerressourcen für die Verwaltung von Zugriffsanforderungen, muss die Anzahl der IP-Adressen der Anzahl der Hosts im vSAN-Cluster entsprechen.

Der vSAN-Dateidienst unterstützt Stretched Cluster und Cluster mit zwei Knoten. Der Cluster mit zwei Knoten sollte zwei Datenknoten-Server am gleichen Standort oder Büro und den Zeugen an einem entfernten oder geteilten Standort haben.

Weitere Informationen zu Cloudnativer Speicher (CNS)-Dateivolumen finden Sie in der Dokumentation zum *VMware vSphere Container Storage Plug-in* und in der Dokumentation zu *Konfiguration und Verwaltung von vSphere with Tanzu*.

## Einschränkungen und Überlegungen

Beachten Sie Folgendes, wenn Sie den vSAN-Dateidienst konfigurieren:

- Mit vSAN 7.0 U3 werden Dateidienst-VMs ausgeschaltet und nicht mehr gelöscht, wenn der vSAN-Cluster in den Wartungsmodus wechselt.
- vSAN 7.0 Update 3 unterstützt Konfigurationen mit zwei Knoten und Stretched Cluster.
- vSAN 7.0 Update 3 unterstützt 64 Dateiserver in einer 64-Host-Konfiguration.
- vSAN 7.0 Update 3 unterstützt 100 Dateifreigaben.
- Wenn in Versionen vor vSAN 7.0 Update 3 ein Host in den Wartungsmodus wechselt, wird der Protokollstapelcontainer auf eine andere FSVM verschoben. Die FSVM auf dem Host, der in den Wartungsmodus gewechselt ist, wird gelöscht. Nachdem der Host den Wartungsmodus verlassen hat, wird eine neue FSVM bereitgestellt.

  Die Dateidienst-VMs werden ausgeschaltet und gelöscht, wenn der vSAN-Cluster in den Wartungsmodus wechselt. Sie werden neu erstellt, wenn der Host den Wartungsmodus verlässt.
- Das interne Docker-Netzwerk der vSAN-Dateidienst-VM kann sich ohne Warnung oder Neukonfiguration mit dem Kundennetzwerk überschneiden.

  Es besteht ein bekannter Konflikt, wenn sich das angegebene Dateidienstnetzwerk mit dem internen Docker-Netzwerknetzwerk (172.17.0.0/16) überschneidet. Dies führt zu Problemen beim Routing des Datenverkehrs zum richtigen Endpoint.

  Als Problemumgehung geben Sie ein anderes Dateidienstnetzwerk an, sodass es sich nicht mit dem internen Docker-Netzwerk (172.17.0.0/16) überschneidet.

## Konfigurieren von Dateidiensten

Sie können die Dateidienste konfigurieren, mit denen Sie Dateifreigaben in Ihrem vSAN-Datenspeicher erstellen können. Sie können die vSAN-Dateidienste auf einem regulären vSAN-Cluster, einem Stretched vSAN-Cluster oder einem vSAN-ROBO-Cluster aktivieren.

### Voraussetzungen

Stellen Sie sicher, dass Folgendes konfiguriert ist, bevor Sie die vSAN-Dateidienste aktivieren:

Alle ESXi-Hosts im vSAN-Cluster müssen folgende Mindestanforderungen an die Hardware erfüllen:

- CPU mit 4 Kernen
- 10 GB physischer Arbeitsspeicher

Sie müssen sicherstellen, dass das Netzwerk als vSAN-Dateidienstnetzwerk vorbereitet wird:

- Bei Verwendung eines auf Standard-Switches basierenden Netzwerks werden der promiskuitive Modus und gefälschte Übertragungen im Rahmen des Aktivierungsvorgangs der vSAN-Dateidienste aktiviert.
- Bei Verwendung eines DVS-basierten Netzwerks werden vSAN-Dateidienste auf DVS-Version 6.6.0 oder höher unterstützt. Erstellen Sie eine dedizierte Portgruppe für vSAN-Dateidienste im DVS. MacLearning und gefälschte Übertragungen werden im Rahmen der Aktivierung der vSAN-Dateidienste für eine angegebene DVS-Portgruppe aktiviert.
- **Wichtig** Stellen Sie bei Verwendung eines NSX-basierten Netzwerks sicher, dass MacLearning für die bereitgestellte Netzwerkentität in der NSX-Administrationskonsole aktiviert ist und alle Hosts und Dateidienstknoten mit dem gewünschten NSX-T-Netzwerk verbunden sind.

Weisen Sie statische IP-Adressen als Dateiserver-IPs über das vSAN-Dateidienstnetzwerk zu, wobei mit jeder IP zentral auf vSAN-Dateifreigaben zugegriffen werden kann.

- Für optimale Leistung muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.
- Alle statischen IP-Adressen müssen aus demselben Subnetz stammen.
- Jede statische IP-Adresse verfügt über einen zugehörigen FQDN, der Teil der Forward- und Reverse-Lookup-Zonen im DNS-Server sein sollte.

Wenn Sie eine Kerberos-basierte SMB- oder NFS-Dateifreigabe erstellen möchten, benötigen Sie Folgendes:

- AD-Domäne (Microsoft Active Directory) zum Bereitstellen von Authentifizierung bei der Erstellung einer SMB- oder NFS-Dateifreigabe mit Kerberos-Sicherheit.
- (Optional) Active Directory-Organisationseinheit zum Erstellen aller Computerobjekte des Dateiservers.
- Ein Domänenbenutzer im Verzeichnisdienst mit ausreichenden Berechtigungen zum Erstellen und Löschen von Computerobjekten.

Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dienste**.
2. Klicken Sie in der Zeile „Dateidienst“ auf **Aktivieren**.

   Der Assistent zum Konfigurieren des Dateidienstes wird geöffnet.
3. Prüfen Sie die Checkliste auf der Einführungsseite und klicken Sie auf **Weiter**.

4 Wählen Sie auf der Seite „Dateidienst-Agent“ eine der folgenden Optionen aus, um die OVF-Datei herunterzuladen.

| Option | Beschreibung |
| --- | --- |
| **Automatischer Ansatz** | Mit dieser Option sucht das System nach der OVF-Datei und lädt sie herunter.<br>**Hinweis**<br>■ Stellen Sie sicher, dass Sie den Proxy und die Firewall so konfiguriert haben, dass vCenter auf die folgende Website zugreifen und die entsprechende JSON-Datei herunterladen kann.<br>https://download3.vmware.com/software/VSANOVF/FsOvfMapping.json<br>Weitere Informationen zum Konfigurieren des vCenter-DNS, der IP-Adresse und der Proxy-Einstellungen finden Sie unter *vCenter Server Appliance-Konfiguration*.<br>■ Wenn bereits eine OVF-Datei heruntergeladen wurde und zur Verfügung steht, sind die folgenden Optionen verfügbar:<br>■ **Aktuelle OVF verwenden**: Ermöglicht Ihnen die Verwendung der bereits verfügbaren OVF-Datei.<br>■ **Neueste OVF automatisch laden**: Ermöglicht dem System, die neueste OVF-Datei zu suchen und herunterzuladen. |
| **Manueller Ansatz** | Mit dieser Option können Sie nach einer OVF-Datei suchen, die bereits in Ihrem lokalen System verfügbar ist.<br>**Hinweis** Wenn Sie diese Option auswählen, müssen Sie alle folgenden Dateien hochladen:<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf` |

5 Geben Sie auf der Seite „Domäne“ die folgenden Informationen ein und klicken Sie auf **Weiter**:

- **Dateidienstdomäne**: Der Domänenname muss mindestens zwei Zeichen lang sein. Das erste Zeichen muss ein Buchstabe oder eine Zahl sein. Die übrigen Zeichen können Buchstaben, Zahlen, Unterstriche (_), Punkte (.) und Bindestriche (-) sein.

- **DNS-Server**: Geben Sie einen gültigen DNS-Server ein, um die ordnungsgemäße Konfiguration der Dateidienste sicherzustellen.
- **DNS-Suffixe**: Geben Sie das DNS-Suffix an, das mit den Dateidiensten verwendet wird. Alle anderen DNS-Suffixe, von denen aus die Clients auf diese Dateiserver zugreifen können, müssen ebenfalls enthalten sein. Dateidienste unterstützt keine DNS-Domäne mit einer einzelnen Bezeichnung wie „app“, „wiz“, „com“ usw. Ein Domänenname, der den Dateidiensten zugeordnet ist, sollte das Format „thisdomain.registerdrootdnsname“ aufweisen. DNS-Name und Suffix müssen den Best Practices entsprechen, die unter https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain ausführlich erläutert sind.
- **Verzeichnisdienst**: Konfigurieren Sie eine Active Directory-Domäne für die vSAN-Dateidienste zur Authentifizierung. Wenn Sie planen, eine SMB-Dateifreigabe oder eine NFS v4.1-Dateifreigabe mit Kerberos-Authentifizierung zu erstellen, müssen Sie eine AD-Domäne für die vSAN-Dateidienste konfigurieren.

  Geben Sie die entsprechenden Werte in die folgenden Textfelder ein, um die Active Directory-Domäne für die vSAN-Dateidienste zu konfigurieren:

| Option | Beschreibung |
| --- | --- |
| **AD-Domäne** | Der vollqualifizierte Domänenname, der vom Dateiserver verknüpft wurde. |
| **Organisationseinheit (optional)** | Enthält das Computerkonto, das von den vSAN-Dateidiensten erstellt wird. Erstellen Sie in einer Organisation mit komplexen Hierarchien das Computerkonto in einem angegebenen Container, indem Sie einen Schrägstrich verwenden, um Hierarchien zu bezeichnen (z. B. organizational_unit/inner_organizational_unit).<br>**Hinweis** Standardmäßig erstellen die vSAN-Dateidienste das Computerkonto im Computer-Container. |

| Option | Beschreibung |
| --- | --- |
| **AD-Benutzername** | Der Benutzername, der zum Verbinden und Konfigurieren des Active Directory-Diensts verwendet werden soll.<br>Mit diesem Benutzernamen wird Active Directory in der Domäne authentifiziert. Ein Domänenbenutzer authentifiziert den Domänencontroller und erstellt vSAN-Dateidienste-Computerkonten, zugehörige SPN-Einträge und DNS-Einträge (bei Verwendung von Microsoft DNS). Als Best Practice wird empfohlen, ein dediziertes Dienstkonto für die Dateidienste zu erstellen.<br>Ein Domänenbenutzer im Verzeichnisdienst mit den folgenden ausreichenden Berechtigungen zum Erstellen und Löschen von Computerobjekten:<br>■ (Optional) Hinzufügen/Aktualisieren von DNS-Einträgen |
| **Kennwort** | Kennwort für den Benutzernamen des Active Directory in der Domäne. Die vSAN-Dateidienste verwenden das Kennwort, um sich bei AD zu authentifizieren und das Computerkonto für die vSAN-Dateidienste zu erstellen. |

**Hinweis**

- vSAN-Dateidienste unterstützen Folgendes nicht:
  - Schreibgeschützte Domänencontroller (RODC) zum Beitritt zu Domänen, da der RODC keine Computerkonten erstellen kann. Als Best Practice für die Sicherheit muss vorab eine dedizierte Organisationseinheit im Active Directory erstellt werden, und der hier erwähnte Benutzername muss diese Organisation kontrollieren.
  - Namespace-Verknüpfung entfernen.
  - Leerzeichen in Namen von Organisationseinheiten (OUs).
  - Umgebungen mit mehreren Domänen und einer einzelnen Active Directory Forest-Struktur.
- Für den Active Directory-Benutzernamen werden nur englische Zeichen unterstützt.
- Es wird nur eine einzelne AD-Domänenkonfiguration unterstützt. Die Dateiserver können jedoch in eine gültige DNS-Unterdomäne gelegt werden. Beispielsweise kann eine AD-Domäne mit dem Namen `example.com` den Dateiserver-FQDN `name1.eng.example.com` aufweisen.
- Vorab erstellte Computerobjekte für Dateiserver werden nicht unterstützt. Stellen Sie sicher, dass der hier angegebene Benutzer über ausreichende Rechte für die Organisationseinheit verfügt.
- Die vSAN-Dateidienste aktualisieren die DNS-Datensätze für die Dateiserver, wenn Active Directory auch als DNS-Server verwendet wird und der Benutzer über ausreichende Berechtigungen zum Aktualisieren der DNS-Datensätze verfügt. Die vSAN-Dateidienste verfügen auch über eine Integritätsprüfung, um anzugeben, ob die Forward- und Reverse-Suchvorgänge nach Dateiservern ordnungsgemäß funktionieren. Wenn jedoch andere proprietäre Lösungen als DNS-Server verwendet werden, muss der Vi-Admin diese DNS-Datensätze aktualisieren.

6 Geben Sie auf der Seite „Netzwerk“ die folgenden Informationen ein und klicken Sie auf **Weiter**:
   - Netzwerk
   - Protokoll
   - Subnetzmaske
   - Gateway

7 Geben Sie auf der Seite „IP-Pool“ die folgenden Informationen ein, wählen Sie eine **primäre IP-Adresse** aus und klicken Sie auf **Weiter**.
   - **IP-Adresse**
   - **DNS-Name**

- **Affinität der Site**: Diese Option ist verfügbar, wenn Sie vSAN-Dateidienste auf einem Stretched Cluster konfigurieren. Mit dieser Option können Sie die Platzierung des Dateiservers auf der **bevorzugten** oder **sekundären** Site konfigurieren. Dies hilft bei der Verringerung der Latenz des seitenübergreifenden Datenverkehrs. Der Standardwert ist **Beide**. Das bedeutet, dass keine Regel für die Affinität der Site auf den Dateiserver angewendet wird.

  **Hinweis** Wenn Ihr Cluster ein ROBO-Cluster ist, stellen Sie sicher, dass der Wert für die Affinität der Site auf **Beide** eingestellt ist.

  Bei einem Ausfall einer Site nimmt der zu dieser Site gehörende Dateiserver einen Failover auf die andere Site vor. Der Dateiserver führt bei der Wiederherstellung ein Failback zur verbundenen Site durch. Konfigurieren Sie mehr Dateiserver für eine Site, wenn an einer bestimmten Site mehr Arbeitslasten zu erwarten sind.

  **Hinweis** Wenn der Dateiserver SMB-Dateifreigaben enthält, erfolgt kein automatisches Failback, selbst wenn der Standortausfall wiederhergestellt ist.

Beachten Sie beim Konfigurieren der IP-Adressen und DNS-Namen Folgendes:

- Um eine ordnungsgemäße Konfiguration der Dateidienste zu gewährleisten, muss es sich bei den IP-Adressen, die Sie auf der Seite „IP-Pool“ eingeben, um statische Adressen handeln, und der DNS-Server muss über Datensätze für diese IP-Adressen verfügen. Um eine optimale Leistung zu erzielen, muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.
- Sie können bis zu 32 IP-Adressen eingeben.
- Sie können die folgenden Optionen nutzen, um die Textfelder für die IP-Adresse und den Namen des DNS-Servers automatisch auszufüllen:

  **AUTOMATISCH AUSFÜLLEN**: Diese Option wird angezeigt, nachdem Sie die erste IP-Adresse in das Textfeld „IP-Adresse“ eingegeben haben. Klicken Sie auf die Option „AUTOMATISCH AUSFÜLLEN“, um die übrigen Felder automatisch mit fortlaufenden IP-Adressen auszufüllen, die auf der Subnetzmaske und der Gateway-Adresse der IP-Adresse basieren, die Sie in der ersten Zeile eingegeben haben. Sie können die automatischen ausgefüllten IP-Adressen bearbeiten.

**DNS SUCHEN**: Diese Option wird angezeigt, nachdem Sie die erste IP-Adresse in das Textfeld „IP-Adresse“ eingegeben haben. Klicken Sie auf die Option „DNS SUCHEN“, um den zu den IP-Adressen gehörenden FQDN automatisch abzurufen und in die Spalte „IP-Adresse“ einzufügen.

**Hinweis**

- Für die FQDNs gelten alle gültigen Regeln. Weitere Informationen finden Sie unter https://tools.ietf.org/html/rfc953.
- Der erste Teil des FQDN, der auch als NetBIOS-Name bezeichnet wird, darf maximal 15 Zeichen lang sein.

Die FQDNs werden nur unter den folgenden Bedingungen automatisch abgerufen:

- Sie müssen auf der Seite „Domäne“ einen gültigen DNS-Server eingegeben haben.
- Die auf der Seite „IP-Pool“ angegebenen IP-Adressen müssen statische Adressen sein und der DNS-Server muss Datensätze für diese IP-Adressen besitzen.

8 Überprüfen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.

### Ergebnisse

Die OVF-Datei wird heruntergeladen und bereitgestellt. Die Domäne für die Dateidienste wird erstellt und die vSAN-Dateidienste werden aktiviert. Dateiserver werden mit den IP-Adressen gestartet, die während der Konfiguration der vSAN-Dateidienste zugewiesen wurden.

- Die OVF-Datei wird heruntergeladen und bereitgestellt.
- Die Domäne für die Dateidienste wird erstellt und die vSAN-Dateidienste werden aktiviert.
- Die Dateiserver werden mit den IP-Adressen gestartet, die während der Konfiguration der vSAN-Dateidienste zugewiesen wurden.
- Auf jedem Host wird eine Dateidienste-VM (FSVM) platziert.

**Hinweis** Die FSVMs werden von den vSAN-Dateidiensten verwaltet. Führen Sie auf den FSVMs keine Vorgänge durch.

## Bearbeiten des vSAN-Dateidiensts

Sie können die Einstellungen einer vSAN-Dateifreigabe bearbeiten und neu konfigurieren.

### Voraussetzungen

- Wenn Sie ein Upgrade von vSAN 7.0 auf Version 7.0 Update 1 durchführen, können Sie die Dateifreigaben für SMB und NFS Kerberos erstellen. Dies erfordert die Konfiguration der Active Directory-Domäne für den vSAN-Dateidienst.
- Wenn aktive Freigaben vorhanden sind, ist das Ändern der Active Directory-Domäne nicht zulässig, da diese Aktion die Benutzerberechtigungen für die aktiven Freigaben stören kann.

- Wenn Ihr Active Directory-Kennwort geändert wurde, können Sie die Konfigurationseinstellungen für Active Directory bearbeiten und das neue Kennwort bereitstellen.

  **Hinweis** Diese Aktion kann zu geringfügigen Unterbrechungen der Inflight-E/A-Vorgänge für die Dateifreigaben führen.

**Verfahren**

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dienste**.
2. Klicken Sie in der Zeile „Dateidienst“ auf **Bearbeiten**.

   Der Assistent zum Konfigurieren des Dateidienstes wird geöffnet.
3. Nehmen Sie die entsprechenden Konfigurationsänderungen vor. Sie können die folgenden Änderungen an der vSAN-Dateidienstkonfiguration vornehmen:

| Seite | Bearbeitbare Felder |
|---|---|
| Domäne | Sie können die folgenden domänenbezogenen Informationen bearbeiten:<br>■ Dateidienstdomäne<br>■ DNS-Server<br>■ DNS-Suffixe<br>■ Verzeichnisdienst<br>**Hinweis** Das Ändern von Domäneninformationen ist eine Aktion, die Unterbrechungen nach sich zieht. Möglicherweise müssen dadurch alle Clients neue URLs verwenden, um erneut eine Verbindung mit den Dateifreigaben herzustellen. |
| Netzwerk | Sie können die folgenden netzwerkbezogenen Informationen bearbeiten:<br>■ Subnetzmaske<br>■ Gateway |
| IP-Pool | Sie können die statischen IP-Adressen und DNS-Namen bearbeiten, außer der primären IP-Adresse und des primären DNS-Namens. |

   Überprüfen Sie nach dem Vornehmen der erforderlichen Änderungen die Änderungen auf der Seite „Überprüfen“ und klicken Sie auf **Beenden**.

**Ergebnisse**

Die Änderungen werden auf die Konfiguration des vSAN-Dateidiensts angewendet.

## Erstellen einer Dateifreigabe

Sofern der vSAN-Dateidienst aktiviert ist, können Sie im vSAN-Datenspeicher eine oder mehrere Dateifreigaben erstellen. Der vSAN-Dateidienst bietet keine Unterstützung für die Verwendung dieser Dateifreigaben als Datenspeicher in ESXi.

Voraussetzungen

Wenn Sie eine SMB-Dateifreigabe oder eine NFS v4.1-Dateifreigabe mit Kerberos-Sicherheit erstellen, stellen Sie sicher, dass Sie den vSAN-Dateidienst in einer AD-Domäne konfiguriert haben.

**Überlegungen zum Namen und zur Nutzung von Freigaben**

- Benutzernamen mit Nicht-ASCII-Zeichen können für den Zugriff auf Freigabedaten verwendet werden.
- Freigabenamen dürfen nicht länger als 80 Zeichen sein und dürfen englische Zeichen, Ziffern und Bindestriche enthalten. Jedem Bindestrich muss eine Zahl oder ein Buchstabe vorangestellt und nachgestellt werden. Aufeinanderfolgende Bindestriche sind nicht zulässig.
- Bei Freigaben vom Typ „SMB“ können Datei und Verzeichnisse beliebige Unicode-kompatible Zeichenfolgen enthalten.
- Bei reinen NFS v4-Freigaben können die Datei und die Verzeichnisse beliebige UTF-8-kompatible Zeichenfolgen enthalten.
- Wenn es sich um reine NFS v3- und NFS v3+NFS v4-Freigaben handelt, können Dateien und Verzeichnisse nur ASCII-kompatible Zeichenfolgen enthalten.
- Das Migrieren von Freigabedaten von älteren NFS v3- auf neue vSAN-Dateidienstfreigaben mit NFS v4 erfordert lediglich die Konvertierung aller Datei-und Verzeichnisnamen in die UTF-8-Kodierung. Für denselben Zweck gibt es auch Drittanbietertools.

Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateifreigaben**.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen von Dateifreigaben wird geöffnet.
3. Geben Sie auf der Seite „Allgemein“ die folgenden allgemeinen Informationen ein und klicken Sie auf **Weiter**.
   - **Name:** Geben Sie einen Namen für die Dateifreigabe ein.
   - **Protokoll**: Wählen Sie ein geeignetes Protokoll aus. Der vSAN-Dateidienst unterstützt die Dateisystemprotokolle „SMB“ und „NFS“.

     Wenn Sie das Protokoll **SMB** verwenden, können Sie auch die SMB-Dateifreigabe konfigurieren, sodass nur die verschlüsselten Daten mit der Option **Protokollverschlüsselung** akzeptiert werden.

Wenn Sie das Protokoll **NFS** auswählen, können Sie die Dateifreigabe so konfigurieren, dass entweder **NFS 3**, **NFS 4** oder sowohl **NFS 3 als auch NFS 4**-Versionen unterstützt werden. Wenn Sie die Version **NFS 4** auswählen, können Sie entweder **AUTH_SYS** oder die **Kerberos**-Sicherheit festlegen.

**Hinweis** Das SMB-Protokoll und die Kerberos-Sicherheit für das NFS-Protokoll können nur konfiguriert werden, wenn der vSAN-Dateidienst mit Active Directory konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von Dateidiensten.

- Mit dem KMU-Protokoll können Sie mit der Option **Zugriffsbasierte Enumeration** die Dateien und Ordner ausblenden, für die der Benutzer des Freigabeclients keine Zugriffsberechtigung hat.
- **Speicherrichtlinie**: Wählen Sie eine geeignete Speicherrichtlinie aus.
- **Affinität der Site**: Diese Option ist verfügbar, wenn Sie eine Dateifreigabe auf einem Stretched Cluster erstellen. Mit dieser Option können Sie die Dateifreigabe auf einem Dateiserver platzieren, der zu der von Ihnen gewählten Site gehört. Verwenden Sie diese Option, wenn Sie eine geringe Latenz beim Zugriff auf die Dateifreigabe bevorzugen. Der Standardwert ist **Beide**. Das bedeutet, dass die Dateifreigabe auf einer Site mit geringerem Datenverkehr entweder auf der bevorzugten oder der sekundären Site angewendet wird.
- **Speicherplatzkontingente**: Sie können folgende Werte festlegen:
  - **Warnungsschwellenwert für Freigabe**: Wenn die Freigabe diesen Grenzwert erreicht, wird eine Warnmeldung angezeigt.
  - **Harte Kontingentgrenze freigeben**: Sobald die Freigabe diesen Grenzwert erreicht, wird eine neue Blockzuteilung verweigert.
- **Bezeichnungen**: Eine Bezeichnung ist ein Schlüssel-Wert-Paar, das Ihnen bei der Organisation von Dateifreigaben hilft. Sie können Bezeichnungen an die einzelnen Dateien anhängen und diese dann anhand der Bezeichnungen filtern. Ein Bezeichnungsschlüssel ist eine Zeichenfolge aus 1 bis 250 Zeichen. Ein Bezeichnungswert ist eine maximal 1.000 Zeichen lange Zeichenfolge. Der vSAN-Dateidienst unterstützt bis zu 5 Bezeichnungen pro Freigabe.

4 Auf der Seite „Netzzugriffssteuerung“ finden Sie Optionen, mit denen Sie den Zugriff auf die Dateifreigabe definieren können. Die Optionen für die Netzzugriffssteuerung sind nur für NFS-Freigaben verfügbar. Wählen Sie eine der folgenden Optionen aus, und klicken Sie auf **Weiter**:

- **Kein Zugriff**: Wählen Sie diese Option aus, um den Zugriff auf die Dateifreigabe von allen IP-Adressen zu verhindern.
- **Zugriff von beliebiger IP-Adresse zulassen**: Wählen Sie diese Option aus, um den Zugriff auf die Dateifreigabe für alle IP-Adressen freizugeben.

- **Internetzugriff anpassen**: Wählen Sie diese Option aus, um Berechtigungen für bestimmte IP-Adressen zu definieren. Mit dieser Option können Sie festlegen, ob eine bestimmte IP-Adresse auf die Dateieingabe zugreifen, diese ändern oder ausschließlich lesen kann. Sie können außerdem für jede IP-Adresse **Root-Squashing** aktivieren oder deaktivieren. Sie können die IP-Adressen in den folgenden Formaten eingeben:
  - Als einzelne IP-Adresse. Beispiel: 123.23.23.123
  - Als IP-Adresse mit einer Subnetzmaske. Beispiel: 123.23.23.0/8
  - Als Bereich, indem Sie eine durch einen Bindestrich (-) getrennte Start-IP-Adresse und End-IP-Adresse eingeben. Beispiel: 123.23.23.123-123.23.23.128
  - Ein Sternchen (*), um alle Clients einzubeziehen.

5 Überprüfen Sie die Einstellungen auf der Seite „Überprüfen“ und klicken Sie dann auf **Beenden**.

Im vSAN-Datenspeicher wird eine neue Dateifreigabe erstellt.

## Dateifreigaben anzeigen

Sie können die Liste der vSAN-Dateifreigaben anzeigen.

Um die Liste der vSAN-Dateifreigaben anzuzeigen, navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

Eine Liste der vSAN-Dateifreigaben wird angezeigt. Für jede Dateifreigabe werden Informationen wie Speicherrichtlinie, harte Kontingentgrenze, Nutzung über Kontingent, tatsächliche Nutzung und so weiter angezeigt.

## Zugreifen auf Dateifreigaben

Sie können über einen Host-Client auf eine Dateifreigabe zugreifen.

### Zugreifen auf eine NFS-Dateifreigabe

Sie können über einen Host-Client auf eine Dateifreigabe zugreifen, indem Sie ein Betriebssystem verwenden, das mit NFS-Dateisystemen kommuniziert. Für RHEL-basierte Linux-Distributionen ist die NFS 4.1-Unterstützung in RHEL 7.3 und CentOS 7.3-1611 mit Kernel 3.10.0-514 oder höher verfügbar. Für Debian-basierte Linux-Distributionen ist die NFS 4.1-Unterstützung in Linux-Kernel-Version 4.0.0 oder höher verfügbar. Alle NFS-Clients müssen eindeutige Hostnamen besitzen, damit NFS v4.1 funktioniert. Sie können den Linux-Befehl „mount“ mit der primären IP verwenden, um eine vSAN-Dateifreigabe für den Client zu mounten. Beispiel: `mount -t nfs4 -o minorversion=1,sec=sys <primary ip>:/vsanfs/<share name>`. NFS v3-Unterstützung ist für RHEL-basierte und für Debian-basierte Linux-Distributionen verfügbar. Sie können den Linux-Befehl „mount“ verwenden, um eine vSAN-Dateifreigabe für den Client zu mounten. Beispiel: Mounten Sie `-t nfs vers=3 <nfsv3_access_point> <localmount_point>`.

**Beispiel**

Beispiele für v4.1-Befehle zum Überprüfen der NFS-Dateifreigabe über einen Host-Client:

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

## Zugreifen auf eine NFS Kerberos-Dateifreigabe

Ein Linux-Client, der auf eine NFS Kerberos-Freigabe zugreift, sollte über ein gültiges Kerberos-Ticket verfügen.

**Beispiele für v4.1-Befehle zum Überprüfen der NFS Kerberos-Dateifreigabe über einen Host-Client:**

Eine NFS Kerberos-Freigabe kann mithilfe des folgenden Befehls bereitgestellt werden:

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=krb5/krb5i/krb5p <primary ip
address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

### Ändern der Zuständigkeit für eine NFS Kerberos-Freigabe

Sie müssen sich mit dem AD-Domänenbenutzernamen abmelden, um die Zuständigkeit einer Freigabe zu ändern. Der in der Dateidienstkonfiguration angegebene AD-Domänenbenutzername fungiert als sudo-Benutzer für die Kerberos-Dateifreigabe.

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[fsadmin@ocalhost ~]# chown user1 /mnt/TestShare-0
[user1@localhost ~]# ls -l /mnt/TestShare-0
total 0
drwxr-xr-x. 1 user1 domain  users 0 Feb 19 18:35 bar
-rw-r--r--. 1 user1 domain users 0 Feb 19 18:35 foo
```

## Zugreifen auf eine SMB-Dateifreigabe

Sie können über einen Windows-Client auf eine SMB-Dateifreigabe zugreifen.

### Voraussetzungen

Stellen Sie sicher, dass der Windows-Client mit der Active Directory-Domäne verbunden ist, die mit dem vSAN-Dateidienst konfiguriert ist.

### Verfahren

1 Kopieren Sie den SMB-Dateifreigabepfad mithilfe des folgenden Verfahrens:

   a Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

   b Wählen Sie die SMB-Dateifreigabe aus, auf die Sie über den Windows-Client zugreifen möchten.

   c Klicken Sie auf **PFAD KOPIEREN** > **SMB**.

   Der Pfad für die SMB-Dateifreigabe wird in Ihre Zwischenablage kopiert.

2 Melden Sie sich beim Windows-Client als normaler Active Directory-Domänenbenutzer an.

3 Greifen Sie über den von Ihnen kopierten Pfad auf die SMB-Dateifreigabe zu.

## Bearbeiten einer Dateifreigabe

Sie können die Einstellungen einer vSAN-Dateifreigabe bearbeiten.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

2 Wählen Sie die Dateifreigabe aus, die Sie ändern möchten, und klicken Sie auf **BEARBEITEN**.

3 Nehmen Sie auf der Seite „Dateifreigabe bearbeiten“ die entsprechenden Änderungen der Einstellungen für die Dateifreigabe vor und klicken Sie auf **Beenden**.

### Ergebnisse

Die Einstellungen der Dateifreigabe werden aktualisiert.

**Hinweis** vSAN erlaubt keinen Wechsel des Dateifreigabeprotokolls zwischen SMB und NFS.

## Verwalten der SMB-Dateifreigabe

Der vSAN-Dateidienst unterstützt zur Verwaltung der SMB-Freigaben auf dem vSAN-Cluster das Snap-In der gemeinsam genutzten Ordner für die Microsoft Management Console (MMC).

Mit dem MMC-Tool können Sie die folgenden Aufgaben für SMB-Freigaben des vSAN-Dateisystems ausführen:

- Verwalten Sie die Zugriffssteuerungsliste (ACL).
- Schließen Sie die geöffneten Dateien.
- Zeigen Sie aktive Sitzungen an.
- Zeigen Sie die geöffneten Dateien an.
- Schließen Sie Clientverbindungen.

Verfahren

1 Kopieren Sie den MMC-Befehl mithilfe des folgenden Verfahrens:

   a Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

   b Wählen Sie die SMB-Dateifreigabe aus, die Sie über den Windows-Client mithilfe des MMC-Tools verwalten möchten.

   c Klicken Sie auf **MMC-BEFEHL KOPIEREN**.

   Der MMC-Befehlsspeicher wird in Ihre Zwischenablage kopiert.

2 Melden Sie sich beim Windows-Client als Dateiserver-Admin-Benutzer an. Sie können einen Benutzer als Dateiserver-Admin-Benutzer konfigurieren, wenn Sie den Dateidienst aktivieren. Ein Dateidienst-Admin-Benutzer verfügt über alle Berechtigungen auf dem Dateiserver.

3 Geben Sie im Suchfeld in der Taskleiste „Ausführen“ ein und wählen Sie dann **Ausführen** aus.

4 Führen Sie im Feld „Ausführen“ den von Ihnen kopierten MMC-Befehl aus, um mit dem MMC-Tool auf die SMB-Freigabe zuzugreifen und sie zu verwalten.

## Löschen einer Dateifreigabe

Wenn Sie eine Dateifreigabe nicht länger benötigen, können Sie sie löschen. Wenn Sie eine Dateifreigabe löschen, werden auch alle mit dieser Dateifreigabe verknüpften Snapshots gelöscht.

Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

2 Wählen Sie die Dateifreigabe aus, die Sie ändern möchten, und klicken Sie auf **LÖSCHEN**.

3 Klicken Sie im Dialogfeld „Dateifreigaben löschen“ auf **LÖSCHEN**.

# vSAN-Snapshot des verteilten Dateisystems

Ein Snapshot bietet eine platzsparende und zeitbezogene Archivierung der Daten. Er bietet die Möglichkeit, Daten aus einer Datei oder einem Satz von Dateien abzurufen, wenn eine Datei versehentlich gelöscht wurde. Ein Snapshot auf Dateisystemebene liefert Ihnen Informationen über die Dateien, die geändert wurden, und die an der Datei vorgenommenen Änderungen. Er bietet Ihnen einen automatisierten Dateiwiederherstellungsservice und ist im Vergleich zur traditionellen bandbasierten Sicherungsmethode effizienter. Ein Snapshot allein bietet keine vollständige Lösung zur Notfallwiederherstellung, aber er kann von den Backup-Benutzern verwendet werden, um die geänderten Dateien (inkrementelle Sicherung) an einen anderen physischen Speicherort zu kopieren.

vSAN-Dateidienste verfügen über eine integrierte Funktion, mit der Sie ein Point-in-Time-Image der vSAN-Dateifreigabe erstellen können. Wenn der vSAN-Dateidienst aktiviert ist, können Sie bis zu 32 Snapshots pro Freigabe erstellen. Ein vSAN-Dateifreigabe-Snapshot ist ein Dateisystem-Snapshot, der ein Point-in-Time-Image einer vSAN-Dateifreigabe liefert.

**Hinweis** vSAN-Snapshot des verteilten Dateisystems wird von Version 7.0 Update 2 oder höher unterstützt.

## Einen Snapshot erstellen

Wenn der vSAN-Dateidienst aktiviert ist, können Sie einen oder mehrere Snapshots erstellen, die ein Point-in-Time-Image der vSAN-Dateifreigabe bieten. Sie können maximal 32 Snapshots pro Dateifreigabe erstellen.

### Voraussetzungen

Sie sollten eine vSAN-Dateifreigabe erstellt haben.

### Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

   Eine Liste der vSAN-Dateifreigaben wird angezeigt.

2. Wählen Sie die Dateifreigabe aus, für die Sie einen Snapshot erstellen möchten, und klicken Sie dann auf **SNAPSHOTS NEUER SNAPSHOT**.

   Das Dialogfeld zum Erstellen eines neuen Snapshots wird angezeigt.

3. Geben Sie im Dialogfeld „Neuer Snapshot“ einen Namen für den Snapshot ein und klicken Sie auf **Erstellen**.

### Ergebnisse

Es wird ein Point-in-Time-Snapshot für die ausgewählte Dateifreigabe erstellt.

### Einen Snapshot anzeigen

Sie können die Liste der Snapshots sowie die Informationen wie Datum und Uhrzeit der Erstellung des Snapshots sowie die zugehörige Größe anzeigen.

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

Eine Liste der vSAN-Dateifreigaben wird angezeigt.

2 Wählen Sie eine Dateifreigabe und klicken Sie auf **Snapshots**.

#### Ergebnisse

Eine Liste der Snapshots für diese Dateifreigabe wird angezeigt. Sie können Informationen wie Datum und Uhrzeit der Snapshot-Erstellung sowie die Größe des Snapshots anzeigen.

### Löschen eines Snapshots

Wenn Sie einen Snapshot nicht länger benötigen, können Sie ihn löschen.

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dateidienstfreigaben**.

Eine Liste der vSAN-Dateifreigaben wird angezeigt.

2 Wählen Sie eine Dateifreigabe aus und klicken Sie auf **Snapshots**.

Eine Liste der Snapshots davon, die zu der von Ihnen ausgewählten Dateifreigabe gehört, wird angezeigt.

3 Wählen Sie den Snapshot aus, den Sie löschen möchten, und klicken Sie **LÖSCHEN**.

## Neuverteilen der Arbeitslast auf vSAN-Dateidiensthosts

Unter „Skyline-Integrität“ wird der Integritätsstatus des Arbeitslastausgleichs für alle Hosts angezeigt, die Teil der vSAN-Dateidienstinfrastruktur sind.

Wenn die Arbeitslast eines Hosts nicht gleichmäßig verteilt ist, können Sie dies korrigieren, indem Sie die Arbeitslast neu verteilen.

#### Voraussetzungen

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie dann auf **Überwachen** > **vSAN** > **Skyline-Integrität**.

2 Erweitern Sie unter „Skyline-Integrität“ den Eintrag **Dateidienst** und klicken Sie dann auf **Infrastrukturzustand**.

   Auf der Registerkarte „Infrastrukturzustand“ wird eine Liste aller Hosts angezeigt, die Teil der vSAN-Dateidienstinfrastruktur sind. Für jeden Host wird der Status des Arbeitslastausgleichs angezeigt. Wenn es bei der Arbeitslast eines Hosts zu einem Ungleichgewicht kommt, wird eine Warnung in der Spalte **Beschreibung** angezeigt.

3 Klicken Sie auf **UNGLEICHGEWICHT STANDARDISIEREN** und dann auf **NEU VERTEILEN**, um das Ungleichgewicht zu beheben.

   Bevor Sie mit der Neuverteilung fortfahren, sollten Sie Folgendes beachten:

   - Während der Neuverteilung werden Container in den Hosts mit einer unausgeglichenen Arbeitslast möglicherweise auf andere Hosts verschoben. Die Neuverteilungsaktivität kann sich auch auf die anderen Hosts im Cluster auswirken.
   - Während des Neuverteilungsvorgangs werden die Arbeitslasten, die auf NFS-Freigaben ausgeführt werden, nicht unterbrochen. Allerdings kommt es zu Unterbrechungen der E/A-Vorgänge für SMB-Freigaben, die sich in den von verschobenen Containern befinden.

**Ergebnisse**

Die Arbeitslast des Hosts ist ausgeglichen und der Status des Arbeitslastausgleichs wird grün.

## Rückfordern von Speicherplatz mit Aufhebung der Zuordnung

vSAN 6.7 Update 2 und höher unterstützt UNMAP-Befehle, mit denen Sie Speicherplatz zurückgewinnen können, der den gelöschten Dateien im Dateisystem zugeordnet ist, das vom Gast auf dem - vSAN Objekt erstellt wurde.

Durch Löschen oder Entfernen von Dateien und Snapshots wird Speicherplatz im Dateisystem freigegeben. Dieser freie Speicherplatz wird einem Speichergerät zugewiesen, bis er vom Dateisystem freigegeben oder die Zuordnung aufgehoben wird. vSAN unterstützt die Rückforderung von freiem Speicherplatz, die auch als Aufhebung der Zuordnung bezeichnet wird. Sie können Speicherplatz im VDFS freigeben, wenn Sie Dateifreigaben und Snapshots löschen, Dateifreigaben und Snapshots konsolidieren usw. Sie können die Zuordnung von Speicherplatz aufheben, wenn Sie Dateien oder Snapshots löschen.

Die Funktion der Aufhebung von Zuordnungen (Unmap) ist standardmäßig deaktiviert. Um die Aufhebung der Zuordnung auf einem vSAN-Cluster zu aktivieren, verwenden Sie den folgenden RVC-Befehl:

```
vsan.unmap_support –enable
```

Wenn Sie die Aufhebung der Zuordnung auf einem vSAN-Cluster aktivieren, müssen Sie alle VMs aus- und danach wieder einschalten. VMs müssen für die Durchführung von Unmap-Vorgängen die virtuelle Hardwareversion 13 oder höhere Versionen verwenden.

## Upgrade des Dateidiensts

Ein Upgrade des Dateidienstes wird rollierend durchgeführt. Während des Upgrades erfolgt ein Failover der Dateiserver-Container, die auf den virtuellen Maschinen ausgeführt werden, auf denen ein Upgrade durchgeführt wird, auf andere virtuelle Maschinen. Der Zugriff auf die Dateifreigaben bleibt während des Upgrades erhalten. Während des Upgrades kann es beim Zugriff auf die Dateifreigaben zu Unterbrechungen kommen.

### Voraussetzungen

Stellen Sie sicher, dass für Folgendes ein Upgrade erfolgt:

- ESXi-Hosts
- vCenter Server
- vSAN-Festplattenformat

### Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Konfigurieren** > **vSAN** > **Dienste**.
2. Klicken Sie unter „vSAN-Dienste“ in der Zeile „Dateidienst“ auf **UPGRADE ÜBERPRÜFEN**.
3. Wählen Sie im Dialogfeld „Upgrade des Dateidiensts“ eine der folgenden Bereitstellungsoptionen aus und klicken Sie auf **UPGRADE**.

| Option | Aktion |
| --- | --- |
| **Automatischer Ansatz** | Dies ist die Standardoption. Mit dieser Option sucht das System nach der OVF-Datei und lädt sie herunter. Das Upgrade kann nach dem Start nicht mehr abgebrochen werden.<br>**Hinweis** vSAN benötigt für diese Option eine Internetverbindung. |
| **Manueller Ansatz** | Mit dieser Option können Sie nach einer OVF-Datei suchen, die bereits in Ihrem lokalen System verfügbar ist. Das Upgrade kann nach dem Start nicht mehr abgebrochen werden.<br>**Hinweis** Wenn Sie diese Option auswählen, müssen Sie die folgenden Dateien hochladen:<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk`<br>■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf` |

## Leistung überwachen

Sie können die Leistung von NFS und SMB-Dateifreigaben überwachen.

### Voraussetzungen

Stellen Sie sicher, dass der vSAN-Leistungsdienst aktiviert ist. Wenn Sie den vSAN-Leistungsdienst zum ersten Mal nutzen, wird eine Meldung angezeigt, die Sie auffordert, diesen zu aktivieren. Weitere Informationen zum vSAN-Leistungsdienst finden Sie im *vSAN-Überwachungs- und Fehlerbehebungshandbuch*.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie dann auf **Überwachen** > **vSAN** > **Leistung**.

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

3 Wählen Sie eine der folgenden Optionen aus:

| Option | Aktion |
|---|---|
| **Zeitraum** | ■ Wählen Sie **Letzte** aus, um die Anzahl der Stunden auszuwählen, für die Sie den Leistungsbericht anzeigen möchten.<br>■ Wählen Sie **BENUTZERDEFINIERT** aus, um das Datum und die Uhrzeit auszuwählen, für die Sie den Leistungsbericht anzeigen möchten.<br>■ Wählen Sie **SPEICHERN** aus, um die aktuelle Einstellung als Option zur Liste „Zeitraum“ hinzuzufügen. |
| **Dateifreigabe** | Wählen Sie die Dateifreigabe aus, für die Sie den Leistungsbericht generieren und anzeigen möchten. |

4 Klicken Sie auf **ERGEBNISSE ANZEIGEN**.

### Ergebnisse

Durchsatz-, IOPS- und die Latenzmetriken des vSAN-Dateidienstes für den ausgewählten Zeitraum werden angezeigt.

Weitere Informationen zu vSAN-Leistungsdiagrammen finden Sie im VMware Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2144493.

## Überwachen der Kapazität

Sie können sowohl die Kapazität von nativen als auch von CNS-verwalteten Dateifreigaben überwachen.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Überwachen** > **vSAN** > **Kapazität**.

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

3 Erweitern Sie **Benutzerobjekte** im Abschnitt „Nutzungsaufschlüsselung vor Deduplizierung und Komprimierung“.

### Ergebnisse

Die Kapazitätsinformationen für die Dateifreigabe werden angezeigt.

Weitere Informationen zur Überwachung der vSAN-Kapazität finden Sie im *vSAN-Überwachungs- und Fehlerbehebungshandbuch*.

## Integrität überwachen

Sie können sowohl den Zustand des vSAN-Dateidienstes als auch der Dateifreigabeobjekte überwachen.

### Anzeigen der Integrität des vSAN-Dateidienstes

Sie können den Zustand des vSAN-Dateidienstes überwachen.

#### Voraussetzungen

Stellen Sie sicher, dass der vSAN-Leistungsdienst aktiviert ist.

#### Verfahren

1. Navigieren Sie zum vSAN-Cluster und klicken Sie auf **Überwachen** > **vSAN**.
2. Erweitern Sie im Abschnitt „Skyline-Integrität“ **Dateidienst**.
3. Klicken Sie auf die folgenden Parameter für die Dateidienstintegrität, um den Status anzuzeigen.

| Option | Aktion |
|---|---|
| **Infrastrukturzustand** | Zeigt den Infrastrukturzustand pro ESXi-Host an. Klicken Sie für weitere Informationen auf die Registerkarte **Info**. |
| **Integrität des Dateiservers** | Zeigt den Zustand des Dateiservers an. Klicken Sie für weitere Informationen auf die Registerkarte **Info**. |
| **Freigabeintegrität** | Zeigt den Zustand der Dateidienstfreigabe an. Klicken Sie für weitere Informationen auf die Registerkarte **Info**. |

### Überwachen der Integrität von Dateifreigabeobjekten

Sie können den Zustand von Dateifreigabeobjekten überwachen.

Um den Zustand eines Dateifreigabeobjekts anzuzeigen, navigieren Sie zum vSAN-Cluster und klicken Sie auf **Überwachen** > **vSAN** > **Virtuelle Objekte**.

Im Abschnitt „PLATZIERUNGSDETAILS ANZEIGEN“ werden die Geräteinformationen angezeigt, wie Name, Bezeichner oder UUID, Anzahl der für jede virtuelle Maschine verwendeten Geräte und wie diese über Hosts hinweg gespiegelt werden.

# 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.

**Verfahren**

1 Navigieren Sie 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. Klicken Sie auf **...** und dann auf **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.

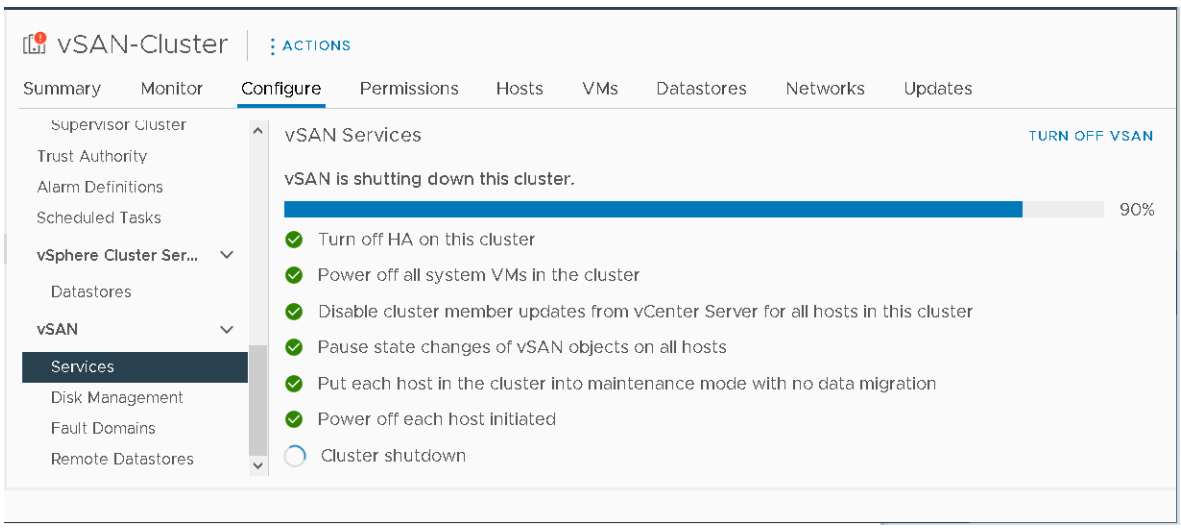
5 Erstellen Sie die All-Flash-Festplattengruppen auf jedem Host.

# Herunterfahren und Neustarten des vSAN-Clusters

Sie können den gesamten vSAN Cluster herunterfahren, um eine Wartung oder Fehlerbehebung durchzuführen.

Verwenden Sie zum Herunterfahren des vSANClusters den Assistenten zum Herunterfahren des Clusters. Der Assistent führt die erforderlichen Schritte aus und weist Sie darauf hin, wenn eine Benutzeraktion erforderlich ist. Sie können den Cluster bei Bedarf auch manuell herunterfahren.

**Hinweis** Wenn Sie einen Stretched Cluster herunterfahren, bleibt der Zeugenhost aktiv.



# Herunterfahren des vSAN-Clusters mithilfe des Assistenten zum Herunterfahren des Clusters

Verwenden Sie den Assistenten zum Herunterfahren von Clustern, um den vSAN-Cluster zu Wartungszwecken oder zur Fehlerbehebung ordnungsgemäß herunterzufahren. Der Assistent zum Herunterfahren von Clustern ist mit vSAN 7.0 Update 3 und höheren Versionen verfügbar.

**Hinweis** Wenn Sie mit einer vSphere with Tanzu-Umgebung arbeiten, müssen Sie beim Herunterfahren und Starten der Komponenten die angegebene Reihenfolge einhalten. Weitere Informationen finden Sie unter „Herunterfahren und Starten von VMware Cloud Foundation“ im *VMware Cloud Foundation-Betriebshandbuch*.

### Verfahren

1 Bereiten Sie den vSAN-Cluster für das Herunterfahren vor.

   a Überprüfen Sie den vSAN-Integritätsdienst, um zu bestätigen, dass der Cluster fehlerfrei ist.

   b Schalten Sie alle virtuellen Maschinen (VMs) aus, die im vSAN-Cluster gespeichert sind, mit Ausnahme von vCenter Server-VMs, vCLS-VMs und Dateidienst-VMs. Wenn vCenter Server im vSAN-Cluster gehostet wird, schalten Sie die vCenter Server-VM nicht aus.

   c Wenn es sich um einen HCI Mesh-Servercluster handelt, schalten Sie alle auf dem Cluster gespeicherten Client-VMs aus. Wenn die vCenter Server-VM des Client-Clusters in diesem Cluster gespeichert ist, migrieren Sie die VM oder schalten Sie sie aus. Sobald dieser Server-Cluster heruntergefahren ist, ist der Zugriff auf den freigegebenen Datenspeicher für Clients nicht mehr möglich.

   d Vergewissern Sie sich, dass alle Neusynchronisierungsaufgaben abgeschlossen sind.

      Klicken Sie auf die Registerkarte **Überwachen** und wählen Sie **vSAN** > **Neusynchronisieren von Objekten** aus.

   **Hinweis** Wenn sich ein Mitgliedshost im Sperrmodus befindet, fügen Sie das Root-Konto des Hosts zur Liste der Ausnahmebenutzer des Sicherheitsprofils hinzu. Weitere Informationen finden Sie unter Sperrmodus unter *vSphere-Sicherheit*.

2 Klicken Sie mit der rechten Maustaste auf den vSAN-Cluster im vSphere Client und wählen Sie das Menü **Cluster herunterfahren** aus.

   Sie können auch auf der Seite „vSAN-Dienste“ auf **Cluster herunterfahren** klicken.

3 Überprüfen Sie im Assistenten für das Herunterfahren des Clusters, ob die Vorabprüfungen für das Herunterfahren mit grünen Häkchen versehen sind. Beheben Sie alle Probleme mit roten Ausrufezeichen. Klicken Sie auf **Weiter**.

   Wenn die vCenter Server Appliance auf dem vSAN-Cluster bereitgestellt wird, zeigt der Assistent zum Herunterfahren den Hinweis auf vCenter Server an. Notieren Sie sich die IP-Adresse des Orchestrierungshosts, falls Sie sie während des Neustarts des Clusters benötigen. Klicken Sie auf **Weiter**.

4 Geben Sie einen Grund für das Herunterfahren ein und klicken Sie auf **Herunterfahren**.

   Auf der Seite „vSAN-Dienste“ werden Informationen zum Herunterfahren angezeigt.

5 Überwachen Sie den Vorgang zum Herunterfahren.

   vSAN führt die Schritte zum Herunterfahren des Clusters, zum Ausschalten der System-VMs und zum Ausschalten der Hosts aus.

## Neustart des vSAN-Clusters

Sie können einen vSAN-Cluster neu starten, der zur Wartung oder Fehlerbehebung heruntergefahren wurde.

### Verfahren

1 Schalten Sie die Cluster-Hosts ein.

   Wenn der vCenter Server im vSAN-Cluster gehostet wird, warten Sie, bis vCenter Server neu gestartet wurde.

2 Klicken Sie mit der rechten Maustaste auf den vSAN-Cluster im vSphere Client und wählen Sie das Menü **Neustart des Clusters** aus.

   Sie können auch auf der Seite „vSAN-Dienste“ auf **Neustart des Clusters** klicken.

3 Klicken Sie im Dialogfeld „Neustart des Clusters“ auf **Neu starten**.

   Auf der Seite „vSAN-Dienste“ werden Informationen zum Neustart angezeigt.

4 Nachdem der Cluster neu gestartet wurde, überprüfen Sie den vSAN-Integritätsdienst und beheben Sie alle ausstehenden Probleme.

## Manuelles Herunterfahren und Neustarten des vSAN-Clusters

Sie können den gesamten vSAN-Cluster manuell herunterfahren, um eine Wartung oder Fehlerbehebung durchzuführen.

Verwenden Sie den Assistenten zum Herunterfahren von Clustern, es sei denn, Ihr Workflow erfordert ein manuelles Herunterfahren. Wenn Sie den vSAN-Cluster manuell herunterfahren, deaktivieren Sie vSAN auf dem Cluster nicht.

**Hinweis** Wenn Sie mit einer vSphere with Tanzu-Umgebung arbeiten, müssen Sie beim Herunterfahren und Starten der Komponenten die angegebene Reihenfolge einhalten. Weitere Informationen finden Sie unter „Herunterfahren und Starten von VMware Cloud Foundation“ im *VMware Cloud Foundation-Betriebshandbuch*.

### Verfahren

1 Fahren Sie den vSAN-Cluster herunter.

a Überprüfen Sie den vSAN-Integritätsdienst, um zu bestätigen, dass der Cluster fehlerfrei ist.

b Schalten Sie alle im vSAN-Cluster ausgeführten virtuellen Maschinen (VMs) aus, wenn vCenter Server nicht im Cluster gehostet wird. Wenn vCenter Server im vSAN-Cluster gehostet wird, schalten Sie die vCenter Server-VM nicht aus.

c Klicken Sie auf die Registerkarte **Konfigurieren** und deaktivieren Sie HA. Dies führt dazu, dass der Cluster das Herunterfahren von Hosts nicht als Fehler registriert.

Aktivieren Sie für vSphere 7.0 U1 und höher den vCLS-Retreat-Modus.
Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/80472.

d Vergewissern Sie sich, dass alle Neusynchronisierungsaufgaben abgeschlossen sind.

Klicken Sie auf die Registerkarte **Überwachen** und wählen Sie **vSAN** > **Neusynchronisieren von Objekten** aus.

e Wenn vCenter Server im vSAN-Cluster gehostet wird, schalten Sie die vCenter Server-VM aus.

Notieren Sie sich den Host, auf dem die vCenter Server-VM ausgeführt wird. Dies ist der Host, auf dem Sie die vCenter Server-VM neu starten müssen.

f Deaktivieren Sie die Aktualisierung der Clustermitglieder von vCenter Server, indem Sie den folgenden Befehl auf den ESXi-Hosts im Cluster ausführen. Stellen Sie sicher, dass Sie den folgenden Befehl auf allen Hosts ausführen.

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

g Anmelden bei einem beliebigen Host im Cluster außer dem Zeugenhost.

h Führen Sie den folgenden Befehl nur auf diesem Host aus. Wenn Sie den Befehl auf mehreren Hosts gleichzeitig ausführen, kann dies dazu führen, dass eine Race-Bedingung zu unerwarteten Ergebnissen führt.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

Der Befehl gibt Folgendes zurück und aus:

```
Die Clustervorbereitung ist erfolgt.
```

**Hinweis**

- Der Cluster ist nach dem erfolgreichen Abschluss des Befehls vollständig partitioniert.
- Wenn ein Fehler auftritt, beheben Sie das Problem basierend auf der Fehlermeldung und versuchen Sie erneut, den vCLS-Retreat-Modus zu aktivieren.
- Wenn im Cluster fehlerhafte oder getrennte Hosts vorhanden sind, entfernen Sie die Hosts und führen Sie die Ausführung des Befehls erneut aus.

i Versetzen Sie alle Hosts mit dem Modus **Keine Aktion** in den Wartungsmodus. Wenn der vCenter Server ausgeschaltet ist, verwenden Sie den folgenden Befehl, um die ESXi-Hosts mit dem Modus **Keine Aktion** in den Wartungsmodus zu versetzen.

```
esxcli system maintenanceMode set -e true -m noAction
```

Führen Sie diesen Schritt auf allen Hosts aus.

Um das Risiko der Nichtverfügbarkeit von Daten zu vermeiden, wenn der Modus **Keine Aktion** gleichzeitig auf mehreren Hosts verwendet wird, gefolgt von einem Neustart mehrerer Hosts, lesen Sie den VMware-Knowledge-Base-Artikel unter https://kb.vmware.com/s/article/60424. Informationen zur Durchführung eines gleichzeitigen Neustarts aller Hosts im Cluster mithilfe eines integrierten Tools finden Sie im VMware-Knowledge-Base-Artikel unter https://kb.vmware.com/s/article/70650.

j Nachdem alle Hosts erfolgreich in den Wartungsmodus gelangt sind, führen Sie alle erforderlichen Wartungsaufgaben durch und schalten Sie die Hosts aus.

2 Starten Sie den vSAN-Cluster neu.

a Schalten Sie die ESXi-Hosts ein.

Schalten Sie die physische Box ein, in der ESXi installiert ist. Der ESXi-Host wird gestartet, sucht nach den VMs und arbeitet wie gewohnt.

Wenn Hosts nicht neu gestartet werden können, müssen Sie die Hosts manuell wiederherstellen oder die ungültigen Hosts aus dem vSAN-Cluster verschieben.

b Wenn alle Hosts nach dem Einschalten wieder zurück sind, müssen Sie alle Hosts aus dem Wartungsmodus nehmen. Wenn der vCenter Server ausgeschaltet ist, verwenden Sie den folgenden Befehl auf den ESXi-Hosts, um den Wartungsmodus zu verlassen.

```
esxcli system maintenanceMode set -e false
```

Führen Sie diesen Schritt auf allen Hosts aus.

c Sie können sich bei einem der Hosts im Cluster mit einem anderen als dem Zeugenhost melden.

d Führen Sie den folgenden Befehl nur auf diesem Host aus. Wenn Sie den Befehl auf mehreren Hosts gleichzeitig ausführen, kann dies dazu führen, dass eine Race-Bedingung zu unerwarteten Ergebnissen führt.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

Der Befehl gibt Folgendes zurück und aus:

```
Neustart/Einschalten des Clusters wurde erfolgreich abgeschlossen.
```

e Stellen Sie sicher, dass alle Hosts im Cluster verfügbar sind, indem Sie auf jedem Host den folgenden Befehl ausführen.

```
esxcli vsan cluster get
```

f Aktivieren Sie die Aktualisierung der Clustermitglieder von vCenter Server, indem Sie den folgenden Befehl auf den ESXi-Hosts im Cluster ausführen. Stellen Sie sicher, dass Sie den folgenden Befehl auf allen Hosts ausführen.

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

g Starten Sie die vCenter Server-VM neu, wenn sie ausgeschaltet ist. Warten Sie, bis die vCenter Server-VM eingeschaltet ist und ausgeführt wird. Informationen zum Deaktivieren des vCLS-Retreat-Modus finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/80472.

h Stellen Sie erneut sicher, dass alle Hosts im vSAN-Cluster teilnehmen, indem Sie auf jedem Host den folgenden Befehl ausführen.

```
esxcli vsan cluster get
```

i Starten Sie die restlichen VMs über vCenter Server neu.

j Überprüfen Sie den vSAN-Integritätsdienst und beheben Sie alle ausstehenden Probleme.

k (Optional) Wenn für den vSAN-Cluster vSphere-Verfügbarkeit aktiviert ist, müssen Sie vSphere-Verfügbarkeit manuell neu starten, um den folgenden Fehler zu vermeiden: `vSphere HA-Primäragent nicht gefunden`.

Um vSphere-Verfügbarkeit manuell neu zu starten, wählen Sie den vSAN-Cluster aus und navigieren Sie zu:

1 **Konfigurieren** > **Dienste** > **vSphere-Verfügbarkeit** > **BEARBEITEN** > **vSphere HA deaktivieren**

2 **Konfigurieren** > **Dienste** > **vSphere-Verfügbarkeit** > **BEARBEITEN** > **vSphere HA aktivieren**

3 Wenn im Cluster fehlerhafte oder getrennte Hosts vorhanden sind, müssen Sie die Hosts aus dem vSAN-Cluster wiederherstellen oder entfernen. Versuchen Sie, die obigen Befehle erst dann erneut zu verwenden, wenn der vSAN-Integritätsdienst alle verfügbaren Hosts im grünen Status zeigt.

Wenn Sie einen vSAN-Cluster mit drei Knoten haben, kann der Befehl `reboot_helper.py recover` bei einem Ausfall eines Hosts nicht funktionieren. Gehen Sie als Administrator folgendermaßen vor:

a Entfernen Sie die Informationen des Fehlerhosts vorübergehend aus der Liste „Unicast-Agent“.

b Fügen Sie den Host hinzu, nachdem Sie den folgenden Befehl ausgeführt haben.

```
reboot_helper.py recover
```

Im Folgenden finden Sie die Befehle zum Entfernen und zum Hinzufügen des Hosts zu einem vSAN-Cluster:

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p
12321
```

# Geräteverwaltung in einem vSAN-Cluster

6

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 enthält 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 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. Das Verhältnis hängt von den Anforderungen und der Arbeitslast des Clusters ab. Ziehen Sie für einen Hybrid-Cluster die Verwendung eines Verhältnisses zwischen Flash-Cache und belegter Kapazität von mindestens 10 Prozent in Betracht (ohne Replikate wie beispielsweise Spiegel).

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.

Jede Festplattengruppe enthält ein einzelnes Flash-Cache-Gerät. Sie können mehrere Festplattengruppen manuell erstellen und für jede Gruppe ein Flash-Cache-Gerät beanspruchen.

**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.

### Festplatten für vSAN Direct beanspruchen

Verwenden Sie vSAN Direct, um statusbehafteten Diensten den Zugriff auf rohen, lokalen Nicht-vSAN-Speicher über einen direkten Pfad zu ermöglichen.

Sie können lokale Hostgeräte für vSAN Direct anfordern und diese Geräte mithilfe vSAN verwalten und überwachen. Auf jedem lokalen Gerät erstellt vSAN Direct einen unabhängigen VMFS-Datenspeicher und stellt ihn Ihrer statusbehafteten Anwendung zur Verfügung.

Jeder lokale vSAN Direct-Datenspeicher erscheint als vSAN-D-Datenspeicher.

## 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.

**Hinweis** Nur die vSAN-Datenpersistenzplattform kann den vSAN Direct-Speicher verbrauchen. Die vSAN-Datenpersistenzplattform bietet ein Framework für Softwaretechnologiepartner zur Integration in die VMware-Infrastruktur. Jeder Partner muss sein eigenes Plug-In für VMware-Kunden entwickeln, um die Vorteile der vSAN-Datenpersistenzplattform nutzen zu können. Die Plattform ist erst betriebsbereit, wenn auch die übergeordnet ausgeführte Partnerlösung betriebsbereit ist. Weitere Informationen finden Sie unter *vSphere mit Tanzu-Konfiguration und -Verwaltung*.

### Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Klicken Sie auf **Ungenutzte Festplatten beanspruchen**.

5 Gruppieren Sie nach Host.

6 Wählen Sie die zu beanspruchenden Festplatten aus.

- Wählen Sie das für die Cacheebene zu verwendende Flash-Gerät aus.
- Wählen Sie die für die Kapazitätsebene zu verwendenden Festplatten aus.

7 Klicken Sie auf **Erstellen** oder auf **OK**, um Ihre Auswahl zu bestätigen.

#### Ergebnisse

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.

Bei dieser Methode wählen Sie Geräte zum Erstellen einer Festplattengruppe für den vSAN-Cluster aus. Sie benötigen für jede Festplattengruppe ein Cache-Gerät und mindestens ein Kapazitätsgerät.

**Hinweis** Nur die vSAN-Datenpersistenzplattform kann den vSAN Direct-Speicher verbrauchen. Die vSAN-Datenpersistenzplattform bietet ein Framework für Softwaretechnologiepartner, das in die VMware-Infrastruktur integriert werden kann. Jeder Partner muss sein eigenes Plug-In für VMware-Kunden entwickeln, um die Vorteile der vSAN-Datenpersistenzplattform nutzen zu können. Die Plattform ist erst betriebsbereit, wenn auch die übergeordnet ausgeführte Partnerlösung betriebsbereit ist. Weitere Informationen finden Sie unter *vSphere mit Tanzu-Konfiguration und -Verwaltung*.

#### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Klicken Sie auf **Ungenutzte Festplatten beanspruchen**.

5 Wählen Sie Geräte aus, die Festplattengruppen hinzugefügt werden sollen.

- Bei Hybrid-Festplattengruppen muss jeder Host, der Speicher bereitstellt, ein Flash-Cache-Gerät und ein oder mehrere Geräte mit Festplattenkapazität beisteuern. Pro Festplattengruppe kann nur ein Cache-Gerät hinzugefügt werden.
  - Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf **Für Cache-Schicht beanspruchen**.
  - Wählen Sie ein HDD-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf **Für Kapazitätsschicht beanspruchen**.

- Klicken Sie auf **Erstellen** oder **OK**.

- Bei All-Flash-Festplattengruppen muss jeder Host, der Speicher bereitstellt, ein Flash-Cache-Gerät und ein oder mehrere Geräte mit Flash-Kapazität beisteuern. Pro Festplattengruppe kann nur ein Cache-Gerät hinzugefügt werden.
  - Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf **Für Cache-Schicht beanspruchen**.
  - Wählen Sie ein Flash-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf **Für Kapazitätsschicht beanspruchen**.
  - Klicken Sie auf **Erstellen** oder **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.

## Festplatten für vSAN Direct beanspruchen

Sie können lokale Speichergeräte als vSAN Direct für die Verwendung mit der vSAN-Datenpersistenzplattform beanspruchen.

**Hinweis** Nur die vSAN-Datenpersistenzplattform kann den vSAN Direct-Speicher verbrauchen. Die vSAN-Datenpersistenzplattform bietet ein Framework für Softwaretechnologiepartner zur Integration in die VMware-Infrastruktur. Jeder Partner muss sein eigenes Plug-In für VMware-Kunden entwickeln, um die Vorteile der vSAN-Datenpersistenzplattform nutzen zu können. Die Plattform ist erst betriebsbereit, wenn auch die übergeordnet ausgeführte Partnerlösung betriebsbereit ist. Weitere Informationen finden Sie unter *vSphere mit Tanzu-Konfiguration und -Verwaltung*.

Verfahren

1. Navigieren Sie im vSphere Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Festplattenverwaltung**.
4. Klicken Sie auf **Ungenutzte Festplatten beanspruchen**.
5. Wählen Sie im Assistenten „Ungenutzte Festplatten beanspruchen“ die Registerkarte „vSAN Direct“ aus.
6. Wählen Sie ein anzufordernde Gerät aus und aktivieren Sie das Kontrollkästchen **Für vSAN Direct beanspruchen**.

   **Hinweis** Für Ihren vSAN-Cluster beanspruchte Geräte werden auf der Registerkarte „vSAN Direct“ angezeigt.

7 Klicken Sie auf **Erstellen**.

### Ergebnisse

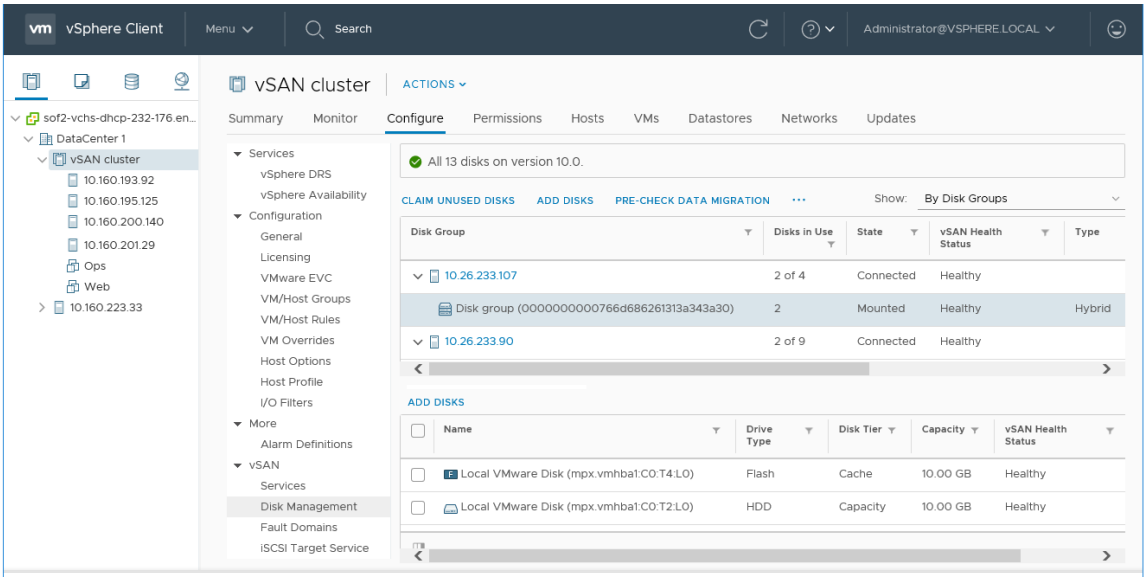
Für jedes von Ihnen beanspruchte Gerät erstellt vSAN einen neuen vSAN Direct-Datenspeicher.

### Nächste Schritte

Sie können auf die Registerkarte „Datenspeicher“ klicken, um alle vSAN Direct-Datenspeicher in Ihrem Cluster anzuzeigen.

# 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. Sie können auch Festplatten hinzufügen oder entfernen, die mit vSAN Direct beansprucht werden.




## 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.

### Verfahren

1 Navigieren Sie 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 **Festplatten hinzufügen**.

5 Wählen Sie das hinzuzufügende Gerät aus und klicken Sie auf **Hinzufügen**.

Wenn Sie ein verwendetes Gerät hinzufügen, das verbleibende Daten oder Partitionsinformationen enthält, müssen Sie das Gerät zuerst bereinigen. Informationen zum Entfernen von Partitionsinformationen aus Geräten finden Sie unter Entfernen der Partition von Geräten. 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)*.

### Nächste Schritte

Stellen Sie sicher, dass die Integritätsprüfung für die vSAN-Datenträgerverteilung grün ist. Wenn die Integritätsprüfung für die Datenträgerverteilung eine Warnung ausgibt, führen Sie eine manuelle Neuverteilung außerhalb der Spitzenzeiten durch. Weitere Informationen finden Sie unter „Manuelle Neuverteilung“ in *vSAN-Überwachung und -Fehlerbehebung*.

## Überprüfen der Datenmigrationsfunktionen einer Festplatte oder einer Festplattengruppe

Verwenden Sie die Vorabprüfung der Datenmigration, um die Auswirkungen von Datenmigrationsoptionen zu ermitteln, wenn Sie eine Festplatte oder Festplattengruppen unmounten oder aus dem vSAN-Cluster entfernen.

Führen Sie die Vorabprüfung der Datenmigration aus, bevor Sie eine Festplatte oder eine Festplattengruppe aus dem vSAN-Cluster unmounten oder entfernen. Die Testergebnisse enthalten Informationen, mit denen Sie die Auswirkungen auf die Clusterkapazität, die vorhergesagten Integritätsprüfungen und alle abweichenden Objekte ermitteln können. Bei einem Fehlschlagen des Vorgangs stellt die Vorabprüfung Informationen zu den Ressourcen bereit, die benötigt werden.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

2 Klicken Sie auf die Registerkarte „Überwachen“.

3 Klicken Sie unter vSAN auf **Vorabprüfung der Datenmigration**.

4 Wählen Sie eine Festplatte oder Festplattengruppe aus, wählen Sie eine Datenmigrationsoption aus und klicken Sie auf **Vorabprüfung**.

vSAN führt die Tests für die Vorabprüfung der Datenmigration aus.

5 Zeigen Sie die Testergebnisse an.

Die Ergebnisse der Vorabprüfung zeigen, ob Sie die Festplatte oder die Festplattengruppe sicher unmounten oder entfernen können.

- Auf der Registerkarte „Objektübereinstimmung und Zugriffsfähigkeit“ werden Objekte angezeigt, die nach der Datenmigration Probleme aufweisen können.

- Auf der Registerkarte „Clusterkapazität“ werden die Auswirkungen der Datenmigration auf den vSAN-Cluster vor und nach der Durchführung des Vorgangs angezeigt.
- Auf der Registerkarte „Systemzustand“ werden die Integritätsprüfungen angezeigt, die unter Umständen von der Datenmigration betroffen sind.

#### Nächste Schritte

Wenn die Vorabprüfung angibt, dass Sie das Gerät unmounten oder entfernen können, klicken Sie auf die Option, um den Vorgang fortzusetzen.

## 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 und 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

Führen Sie die Vorabprüfung für die Datenmigration auf dem Gerät oder der Festplattengruppe aus, bevor Sie sie aus dem Cluster entfernen. Weitere Informationen finden Sie unter

#### Verfahren

1. Navigieren Sie 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, klicken Sie auf **...** und dann auf **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 **Festplatten entfernen**.<br>c Wählen Sie einen Datenevakuierungsmodus aus. |

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

Die Daten werden von den ausgewählten Geräten oder der Festplattengruppe evakuiert.

## Erneutes Erstellen einer Festplattengruppe

Wenn Sie eine Festplattengruppe im vSAN-Cluster neu erstellen, werden die vorhandenen Festplatten aus der Festplattengruppe entfernt und die Festplattengruppe wird gelöscht. vSAN erstellt die Festplattengruppe mit denselben Festplatten neu.

Bei der Neuerstellung einer Festplattengruppe auf einem vSAN-Cluster verwaltet vSAN den Vorgang für Sie. vSAN evakuiert Daten von allen Festplatten in der Festplattengruppe, entfernt die Festplattengruppe und erstellt die Festplattengruppe mit denselben Festplatten.

### Verfahren

1 Navigieren Sie im vSphere Client zum vSAN-Cluster.

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

3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Wählen Sie unter „Festplattengruppen“ die Festplattengruppe aus, die Sie neu erstellen möchten.

5 Klicken Sie auf **...** und dann auf **Neu erstellen**.

Das Dialogfeld „Festplattengruppe neu erstellen“ wird angezeigt.

6 Wählen Sie einen Datenmigrationsmodus aus und klicken Sie auf **Neu erstellen**.

### Ergebnisse

Alle Daten, die sich auf den Festplatten befinden, werden evakuiert. Die Festplattengruppe wird aus dem Cluster entfernt und neu erstellt.

## 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*.

### Verfahren

1. Navigieren Sie 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 |
|---|---|
| **LED einschalten** | Aktiviert die Locator-LED des ausgewählten Speichergeräts. Sie können Locator-LEDs über die Registerkarte **Verwalten** aktivieren, indem Sie auf **Speicher > Speichergeräte** klicken. |
| **LED 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.

Flash-Geräte werden möglicherweise nicht als solche erkannt, wenn sie für den RAID 0-Modus statt für den Passthrough-Modus aktiviert sind. 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.

### Verfahren

1 Navigieren Sie 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 in der Liste aus und klicken Sie auf **Als Flash-Festplatte markieren**.

7 Klicken Sie auf **Ja**, um Ihre Änderungen zu speichern.

Als Laufwerktyp 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.

### Verfahren

1. Navigieren Sie 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 in der Liste aus und klicken Sie auf das Symbol **Als HDD-Festplatte 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.

### Verfahren

1. Navigieren Sie 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 im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie in der Geräteliste ein oder mehrere Remotegeräte aus, die Sie als lokale Geräte markieren möchten, und klicken Sie auf das Symbol **Als lokal markieren**.

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.

### Verfahren

1 Navigieren Sie 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 im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.

6 Wählen Sie eines oder mehrere Geräte aus, die Sie als Remotegeräte markieren möchten, und klicken Sie auf **Als Remote 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.

### Verfahren

1 Navigieren Sie 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 **Festplatten hinzufügen**.

6 Wählen Sie das Kapazitätsgerät aus, das Sie zur Festplattengruppe hinzufügen möchten.

7 Klicken Sie auf **OK** oder **Hinzufügen**.

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.

### Verfahren

1 Navigieren Sie 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** die Option **Nicht geeignet** aus.

6 Wählen Sie ein Gerät aus der Liste aus und klicken Sie auf **Partitionen löschen**.

7 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Das Gerät ist bereinigt und enthält keine Partitionsinformationen mehr.

# 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 enthält 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.

vSAN 6.7 Update 1 und höher unterstützt Befehle zur Aufhebung der SCSI-Zuordnung (SCSI Unmap), mit denen Sie den Speicherplatz zurückgewinnen können, der einem gelöschten vSAN-Objekt zugeordnet ist.

Sie können Deduplizierung und Komprimierung auf einem vSAN-Cluster nutzen, um duplizierte Daten zu entfernen und den zum Speichern von Daten erforderlichen Speicherplatz zu verringern. Sie können auch vSAN nur mit Komprimierung nutzen, um die Speicheranforderungen zu reduzieren, ohne die Serverleistung zu beeinträchtigen.

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. Sowohl RAID 5 als auch RAID 6 ermöglichen gegenüber RAID 1 klar definierte Speicherplatzeinsparungen. Mit Deduplizierung und Komprimierung sind weitere Einsparungen möglich.

# Rückfordern von Speicherplatz mit SCSI Unmap

vSAN 6.7 Update 1 und höher unterstützt SCSI UNMAP-Befehle, mit denen Sie Speicherplatz zurückgewinnen können, der den gelöschten Dateien im Dateisystem zugeordnet ist, das vom Gast auf dem vSAN-Objekt erstellt wurde.

Durch Löschen oder Entfernen von Dateien wird Speicherplatz im Dateisystem freigegeben. Dieser freie Speicherplatz wird einem Speichergerät zugewiesen, bis er vom Dateisystem freigegeben oder die Zuordnung aufgehoben wird. vSAN unterstützt die Rückforderung von freiem Speicherplatz, die auch als Aufhebung der Zuordnung (Unmap) bezeichnet wird. Sie können Speicherplatz innerhalb des vSAN-Datenspeichers freigeben, wenn Sie eine VM löschen oder migrieren, einen Snapshot konsolidieren usw.

Durch die Rückgewinnung von Speicherplatz können ein höherer Host-Flash-E/A-Durchsatz erreicht und die Flash-Lebensdauer verbessert werden.

vSAN unterstützt auch die Befehle vom Typ „SCSI UNMAP“, die direkt von einem Gastbetriebssystem ausgegeben werden, um Speicherplatz zurückzufordern. vSAN unterstützt Offline- und Inline-Unmap-Vorgänge. Unter einem Linux-Betriebssystem werden Offline-Unmap-Vorgänge mit dem Befehl **`fstrim(8)`** durchgeführt, und Inline-Unmap-Vorgänge werden durchgeführt, wenn der Befehl **`mount -o discard`** verwendet wird. Unter Windows-Betriebssystemen führt NTFS standardmäßig Inline-Unmap-Vorgänge durch.

Die Funktion der Aufhebung von Zuordnungen (Unmap) ist standardmäßig deaktiviert. Um die Aufhebung von Zuordnungen auf einem vSAN-Cluster zu aktivieren, verwenden Sie den folgenden RVC-Befehl: **`vsan.unmap_support –enable`**

Wenn Sie die Aufhebung von Zuordnungen auf einem vSAN-Cluster aktivieren, müssen Sie alle VMs aus- und danach wieder einschalten. VMs müssen für die Durchführung von Unmap-Vorgängen die virtuelle Hardwareversion 13 oder höhere Versionen verwenden.

# 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. Verwenden Sie vSAN nur mit Komprimierung für Arbeitslasten, die nicht von der Deduplizierung profitieren, wie z. B. die Online-Transaktionsverwaltung.

Die Deduplizierung erfolgt inline, wenn Daten von der Cache-Ebene zurück auf die Kapazitätsebene geschrieben werden. Der Deduplizierungsalgorithmus verwendet eine feste Blockgröße und wird innerhalb jeder Festplattengruppe angewendet. Redundante Kopien eines Blocks innerhalb derselben Festplattengruppe werden dedupliziert.

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

**Hinweis** vSAN nur mit Komprimierung wird auf Festplattenebene angewendet.

Sie können Deduplizierung und Komprimierung beim Erstellen eines vSAN-All-Flash-Clusters oder beim Bearbeiten eines vorhandenen vSAN-All-Flash-Clusters aktivieren. Weitere Informationen zum Erstellen und Bearbeiten von vSAN-Clustern finden Sie unter „Aktivieren von vSAN“ in *vSAN-Planung und -Bereitstellung*.

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. Vermeiden Sie es, diese Vorgänge 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.

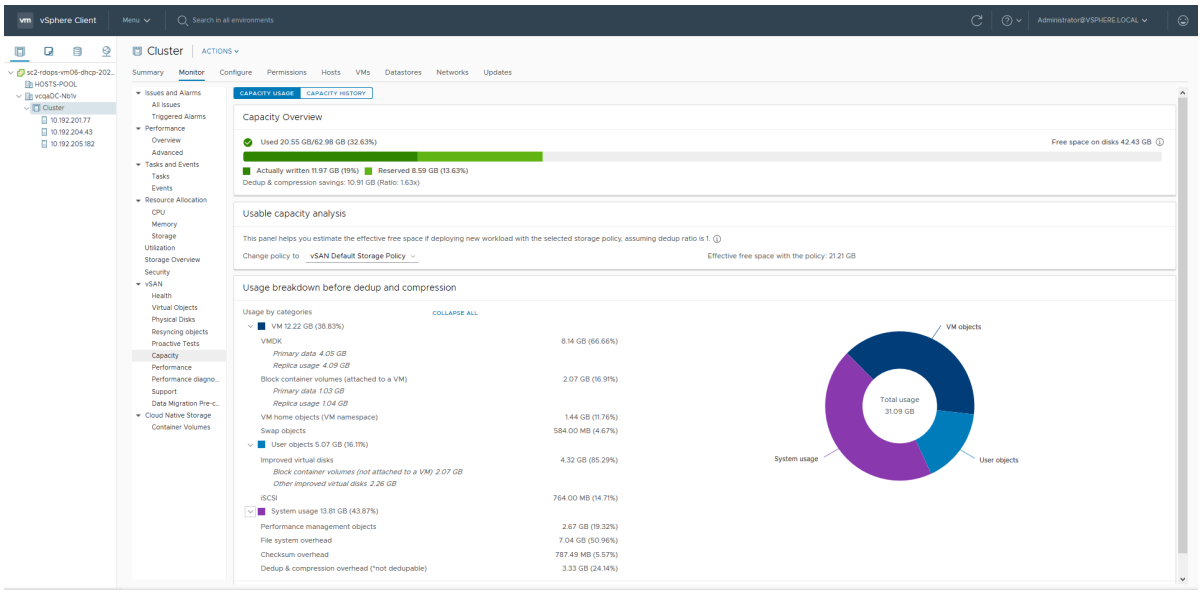
## Verwalten von Festplatten in einem Cluster mit Deduplizierung und Komprimierung

Beachten Sie beim Verwalten von Festplatten in einem Cluster mit aktivierter Deduplizierung und Komprimierung die folgenden Richtlinien. Diese Richtlinien gelten nicht für vSAN nur mit Komprimierung.

- Fügen Sie einer Festplattengruppe keine Festplatten hinzu. Fügen Sie für effizientere Deduplizierung und Komprimierung eine Festplattengruppe hinzu, um die Speicherkapazität des Clusters zu erhöhen.
- Wenn Sie eine 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 im Vorhinein die Aufschlüsselung der Nutzung in der vSAN-Kapazitätsüberwachung anzeigen.




Sie können die Aufschlüsselung der Nutzung vor der Deduplizierung und Komprimierung anzeigen, wenn Sie die vSAN-Kapazität im vSphere 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.
- 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.

### Verfahren

1. Navigieren Sie zu einem neuen All-Flash-vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
   a. Klicken Sie, um die Speichereffizienz zu bearbeiten.
   b. Wählen Sie eine Speichereffizienzoption aus: Deduplizierung und Komprimierung oder nur Komprimierung.
   c. (Optional) Wählen Sie **Verringerte Redundanz zulassen** aus. Bei Bedarf reduziert vSAN die Schutzebene Ihrer VMs durch Aktivieren von Deduplizierung und Komprimierung. Weitere Informationen finden Sie unter Reduzieren der VM-Redundanz für vSAN-Cluster.

4 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 All-Flash-vSAN-Cluster bearbeiten.

### Voraussetzungen

Erstellen Sie einen All-Flash-vSAN-Cluster.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

3 Wählen Sie unter „vSAN“ die Option **Dienste** aus.

   a Klicken Sie, um die Speicherplatzeffizienz zu bearbeiten.

   b Wählen Sie eine Speichereffizienzoption aus: Deduplizierung und Komprimierung oder nur Komprimierung.

   c (Optional) Wählen Sie **Verringerte Redundanz zulassen** aus. Bei Bedarf reduziert vSAN die Schutzebene Ihrer VMs durch Aktivieren von Deduplizierung und Komprimierung. Weitere Informationen finden Sie unter Reduzieren der VM-Redundanz für vSAN-Cluster.

4 Klicken Sie auf **Übernehmen**, um Ihre Konfigurationsänderungen zu speichern.

### Ergebnisse

Während des Aktivierens von Deduplizierung und Komprimierung aktualisiert vSAN das Festplattenformat aller Festplattengruppen 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.

### Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

   a Wählen Sie unter „vSAN“ die Option **Dienste** aus.

   b Klicken Sie auf **Bearbeiten**.

   c Deaktivieren Sie die Deduplizierung und Komprimierung.

   d (Optional) Wählen Sie **Verringerte Redundanz zulassen** aus. Bei Bedarf reduziert vSAN die Schutzebene Ihrer VMs durch Deaktivierung von Deduplizierung und Komprimierung. Siehe Reduzieren der VM-Redundanz für vSAN-Cluster.

3 Klicken Sie auf **Übernehmen** oder **OK**, um die Konfigurationsänderungen zu speichern.

### Ergebnisse

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-Ebene 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 von **Zu tolerierende Fehler** auf den Wert 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 | Zu tolerierende Fehler | 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 die **Fehlertoleranzmethode** auf **RAID-5/6 (Erasure Coding) – Kapazität** und den Wert für **Zu tolerierende Fehler** auf 1 fest. Um RAID 6 zu verwenden, legen Sie die **Fehlertoleranzmethode** auf **RAID-5/6 (Erasure Coding) – Kapazität** und den Wert für **Zu tolerierende Fehler** auf 2 fest. RAID 5- oder RAID 6-Erasure Coding unterstützt nicht den Wert 3 für **Zu tolerierende Fehler**.

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.

**Hinweis** In einem vSAN Stretched Cluster wird die **Fehlertoleranzmethode** von **RAID-5/6 (Erasure Coding) – Kapazität** nur auf die Einstellung **Site-Ausfalltoleranz** angewendet.

Weitere Informationen zum Konfigurieren von Richtlinien finden Sie unter Kapitel 4 Verwenden von vSAN-Speicherrichtlinien.

# 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.
- Sie können weitere Speichereinsparungen vornehmen, wenn Sie Deduplizierung und Komprimierung auf dem vSAN-Cluster aktivieren.

# Verwenden der Verschlüsselung in einem vSAN-Cluster

8

Sie können in Ihrem vSAN-Cluster die data-in-transit-Verschlüsselung und in Ihrem vSAN-Datenspeicher die data-at-rest-Verschlüsselung verwenden.

vSAN kann in der Übertragung befindliche Daten zwischen den Hosts im vSAN-Cluster verschlüsseln. Die data-in-transit-Verschlüsselung schützt Daten, während sie sich um den vSAN-Cluster bewegen.

vSAN kann ruhende Daten im vSAN-Datenspeicher verschlüsseln. Die Verschlüsselung ruhender Daten schützt Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.

Dieses Kapitel enthält die folgenden Themen:



## Verschlüsselung in Übertragung begriffener vSAN-Daten

vSAN kann in Übertragung begriffene Daten verschlüsseln, während sie zwischen Hosts in Ihrem vSAN bewegt werden.

vSAN kann in Übertragung begriffene Daten zwischen den Hosts im Cluster verschlüsseln. Wenn Sie die Verschlüsselung in Übertragung begriffener Daten aktivieren, verschlüsselt vSAN den gesamten Daten- und Metadatenverkehr zwischen Hosts.

Die Verschlüsselung in Übertragung begriffener vSAN-Daten weist die folgenden Merkmale auf:

- vSAN verwendet bei in Übertragung begriffenen Daten eine AES 256-Bit-Verschlüsselung.
- Die Verschlüsselung in Übertragung begriffener vSAN-Daten steht nicht in Zusammenhang mit der Verschlüsselung ruhender Daten. Sie können beide Optionen separat aktivieren oder deaktivieren.
- Die Weiterleitungsgeheimhaltung wird für die Verschlüsselung in Übertragung begriffener vSAN-Daten erzwungen.
- Der Datenverkehr zwischen Datenhosts und Zeugenhosts ist verschlüsselt.
- Der Dateidienst-Datenverkehr zwischen dem VDFS-Proxy und dem VDFS-Server ist verschlüsselt.
- Die Verbindungen zwischen den Hosts der vSAN-Dateidienste sind verschlüsselt.

vSAN verwendet symmetrische Schlüssel, die dynamisch generiert und gemeinsam von den Hosts genutzt werden. Die Hosts generieren dynamisch einen Verschlüsselungsschlüssel, wenn Sie eine Verbindung herstellen und Sie verwenden den Schlüssel, um den gesamten Datenverkehr zwischen den Hosts zu verschlüsseln. Sie benötigen keinen Schlüsselverwaltungsserver, um die Verschlüsselung in Übertragung begriffener Daten auszuführen.

Jeder Host wird authentifiziert, wenn er dem Cluster beitritt. So wird sichergestellt, dass Verbindungen nur für vertrauenswürdige Hosts zulässig sind. Wenn Sie einen Host aus dem Cluster entfernen, wird das zugehörige Authentifizierungszertifikat entfernt.

Die Verschlüsselung in Übertragung begriffener vSAN-Daten ist eine clusterweite Einstellung. Wenn sie aktiviert ist, wird der gesamte Daten- und Metadatenverkehr während der Übertragung zwischen den Hosts verschlüsselt.

## Aktivieren der Verschlüsselung in Übertragung begriffener Daten auf einem vSAN-Cluster

Sie können die Verschlüsselung in Übertragung begriffener Daten aktivieren, indem Sie die Konfigurationsparameter eines vSAN-Clusters bearbeiten.

### Verfahren

1. Navigieren Sie zu einem vorhandenen Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus und klicken Sie unter „Verschlüsselung in Übertragung begriffener Daten“ auf die Schaltfläche **Bearbeiten**.
4. Klicken Sie, um die **Verschlüsselung in Übertragung begriffener Daten** zu aktivieren, und wählen Sie ein Intervall für die erneute Schlüsselerstellung aus.
5. Klicken Sie auf **Übernehmen**.

### Ergebnisse

Die Verschlüsselung in Übertragung begriffener Daten ist auf dem vSAN-Cluster aktiviert. vSAN verschlüsselt alle Daten, die über Hosts und über Verbindungen zwischen den Hosts der Dateidienste im Cluster verschoben werden.

# Verschlüsselung ruhender vSAN-Daten

vSAN kann ruhende Daten in Ihrem vSAN-Datenspeicher verschlüsseln.

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 ruhender Daten schützt Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.

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

Die Verschlüsselung ruhender Daten erfordert einen externen Schlüsselverwaltungsserver (KMS) oder einen vSphere Native Key Provider. Weitere Informationen zur vSphere-Verschlüsselung finden Sie unter *vSphere-Sicherheit*.

Sie können einen externen Schlüsselverwaltungsserver (Key Management Server, KMS), das vCenter Server-System und Ihre ESXi-Hosts verwenden, um Daten in Ihrem vSAN-Cluster zu verschlüsseln. 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.

## Funktionsweise der Verschlüsselung ruhender Daten

Wenn Sie die Verschlüsselung ruhender Daten 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 Datenträgerdaten im branchenüblichen AES-256-XTS-Modus. Jeder Datenträger verfügt über einen anderen zufällig erzeugten Datenverschlüsselungsschlüssel (Data Encryption Key, DEK).
- Jeder ESXi-Host verwendet den KEK, um seine DEKs zu verschlüsseln, und speichert den verschlüsselten DEKs auf dem Datenträger. Der Host speichert den KEK nicht auf dem Datenträger. 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. Sie können ein Kennwort zum Verschlüsseln des Zufallsschlüssels angeben.

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

### Verschlüsselungsschlüsselpersistenz

In vSAN 7.0 Update 3 und höher kann die Verschlüsselung ruhender Daten auch dann weiter funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Wenn die Schlüsselpersistenz aktiviert ist, bleiben die Verschlüsselungsschlüssel auf den ESXi-Hosts auch nach einem Neustart persistent.

Jeder ESXi-Host erhält die Verschlüsselungsschlüssel anfänglich und speichert sie in seinem Schlüssel-Cache. Wenn der ESXi-Host über ein vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM) verfügt, werden die Verschlüsselungsschlüssel im TPM über Neustarts hinweg beibehalten. Der Host muss keine Verschlüsselungsschlüssel anfordern. Verschlüsselungsvorgänge können fortgesetzt werden, wenn der Schlüsselserver nicht verfügbar ist, da die Schlüssel im TPM beibehalten wurden.

Verwenden Sie die folgenden Befehle, um die Schlüsselpersistenz auf einem Clusterhost zu aktivieren.

```
esxcli system settings encryption set --mode=TPM
```

```
esxcli system security keypersistence enable
```

Weitere Informationen zur Persistenz von Verschlüsselungsschlüsseln finden Sie unter „Schlüsselpersistenz – Übersicht“ in *vSphere-Sicherheit*.

### Verwenden von vSphere Native Key Provider

vSAN 7.0 Update 2 unterstützt vSphere Native Key Provider. Wenn Ihre Umgebung für einen vSphere Native Key Provider eingerichtet ist, können Sie ihn zum Verschlüsseln virtueller Maschinen in Ihrem vSAN-Cluster verwenden. Weitere Informationen finden Sie unter „Konfigurieren und Verwalten von vSphere Native Key Provider“ in *vSphere-Sicherheit*.

vSphere Native Key Provider benötigt keinen externen Schlüsselverwaltungsserver (Key Management Server, KMS). vCenter Server generiert den Verschlüsselungsschlüssel und sendet ihn an die ESXi-Hosts. Die ESXi-Hosts generieren dann Datenverschlüsselungsschlüssel.

**Hinweis** Wenn Sie vSphere Native Key Provider verwenden, stellen Sie sicher, dass Sie den nativen Schlüsselanbieter sichern, um sicherzustellen, dass die Neukonfigurationsaufgaben reibungslos ausgeführt werden.

vSphere Native Key Provider kann mit einer bestehenden Schlüsselserver-Infrastruktur koexistieren.

## Design-Überlegungen für die Verschlüsselung ruhender Daten

Halten Sie sich beim Arbeiten mit der Verschlüsselung ruhender Daten an die folgenden 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 Stretched Cluster ist nicht Teil der vSAN-Verschlüsselung. Der Zeugenhost speichert keine Kundendaten, sondern nur Metadaten wie Größe und UUID des vSAN-Objekts und der Komponenten.

  **Hinweis** Wenn der Zeugenhost eine Appliance ist, die auf einem anderen Cluster ausgeführt wird, können Sie die darauf gespeicherten Metadaten verschlüsseln. Aktivieren Sie die Verschlüsselung ruhender Daten (Data-at-Rest) auf dem Cluster, der den Zeugenhost enthält.
- Erstellen Sie eine Richtlinie bezüglich Core-Dumps. Core-Dumps sind verschlüsselt, da sie vertrauliche Informationen 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 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.

## Einrichten des Standard-Schlüsselanbieters

Verwenden Sie einen Standard-Schlüsselanbieter, um die Schlüssel zu verteilen, die den vSAN-Datenspeicher verschlüsseln.

Bevor Sie den vSAN-Datenspeicher verschlüsseln können, müssen Sie einen Standard-Schlüsselanbieter 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 Schlüsselanbieter bereit.

Der KMS muss den Key Management Interoperability Protocol (KMIP) 1.1-Standard unterstützen. Details finden Sie in *vSphere-Kompatibilitätstabellen*.

### Hinzufügen eines KMS zu vCenter Server

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

vCenter Server erstellt einen Standard-Schlüsselanbieter, wenn Sie die erste KMS-Instanz hinzufügen. Stellen Sie sicher, dass Sie denselben Schlüsselanbieternamen verwenden, wenn Sie den Schlüsselanbieter 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 Schlüsselanbieter als Standard festzulegen. Sie können die Standardeinstellung später ändern.
- Nachdem vCenter Server den ersten Schlüsselanbieter erstellt hat, können Sie dem Schlüsselanbieter KMS-Instanzen desselben Anbieters hinzufügen und alle KMS-Instanzen so konfigurieren, dass ihre jeweiligen Schlüssel miteinander synchronisiert werden. Verwenden Sie die von Ihrem KMS-Anbieter dokumentierte Methode.
- Sie können den Schlüsselanbieter mit nur einer KMS-Instanz einrichten.
- Wenn Ihre Umgebung KMS-Lösungen anderer Anbieter unterstützt, können Sie mehrere Schlüsselanbieter hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass der Schlüssel-Verwaltungsserver in *vSphere-Kompatibilitätstabellen* und KMIP 1.1-konform 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.

Verfahren

1. Melden Sie sich beim vCenter Server an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter „Sicherheit“ auf **Schlüsselanbieter**.
4. Klicken Sie auf **Standardschlüsselanbieter hinzufügen**, geben Sie Informationen zum Schlüsselanbieter ein und klicken Sie auf **Schlüsselanbieter hinzufügen**.

   Sie können auf **KMS hinzufügen** klicken, um weitere Schlüsselmanagementserver hinzuzufügen.
5. Klicken Sie auf **Vertrauenswürdigkeit**.

   vCenter Server fügt den Schlüsselanbieter hinzu und zeigt den Status als „Verbunden“ an.

### Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten

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

#### Voraussetzungen

Fügen Sie den Standardschlüsselanbieter hinzu.

#### Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.
3. Wählen Sie den Schlüsselanbieter aus.

   Der KMS für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie den KMS aus.
5. Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.
6. Wählen Sie die entsprechende Option für den Server aus und befolgen Sie die entsprechenden Schritte.

| Option | Informationen hierzu finden Sie unter |
|---|---|
| **CA-Root-Zertifikat von vCenter Server** | Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters. |
| **vCenter Server-Zertifikat** | Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters. |
| **Zertifikat und privaten Schlüssel hochladen** | Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters. |
| **Neue Zertifikatssignieranforderung** | Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters. |

### Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das 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.

#### Verfahren

1. Navigieren Sie zum vCenter Server.
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 im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.
5. Wählen Sie **vCenter-Zertifikat der Stammzertifizierungsstelle herunterladen** aus und klicken Sie auf **Weiter**.

   Im Dialogfeld „Root-CA-Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.
6. Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie das Zertifikat als Datei herunter.
7. Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf sein System hochzuladen.

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

#### Nächste Schritte

Schließen Sie den Zertifikatsaustausch ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

### Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) 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.

Verfahren

1 Navigieren Sie zum vCenter Server.

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 im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **vCenter-Zertifikat** aus und klicken Sie auf **Weiter**.

   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.

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

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

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

### Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass vCenter Server eine Zertifikatsignierungsanforderung (CSR) generiert und 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.

Verfahren

1 Navigieren Sie zum vCenter Server.

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 im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **Neue Zertifikatsignierungsanforderung (CSR)** aus und klicken Sie auf **Weiter**.

6 Kopieren Sie im Dialogfeld das vollständige Zertifikat aus dem Textfeld in die Zwischenablage oder laden es als Datei herunter.

   Klicken Sie auf die Schaltfläche **Neue CSR generieren** des Dialogfelds nur dann, wenn Sie explizit eine Zertifikatsignierungsanforderung generieren möchten.

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

8 Wenn Sie das signierte Zertifikat vom KMS-Anbieter erhalten, klicken Sie erneut auf **Schlüsselanbieter**, wählen Sie den Schlüsselanbieter aus und wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **Signiertes CSR-Zertifikat hochladen** aus.

9 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 **Hochladen**.

#### Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Siehe Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

### Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das KMS-Serverzertifikat und den privaten Schlüssel in 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.

#### Verfahren

1 Navigieren Sie zum vCenter Server.

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 im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **KMS-Zertifikat und privater Schlüssel** aus und klicken Sie auf **Weiter**.

6 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.

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

8 Klicken Sie auf **Vertrauenswürdige Verbindung einrichten**.

#### Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

## Festlegen des Standardschlüsselanbieters

Sie müssen den Standardschlüsselanbieter festlegen, wenn Sie nicht den ersten Schlüsselanbieter als Standardschlüsselanbieter verwenden oder wenn in Ihrer Umgebung mehrere Schlüsselanbieter verwendet werden und der Standardschlüsselanbieter von Ihnen entfernt wird.

#### Voraussetzungen

Stellen Sie als Best Practice sicher, dass auf der Registerkarte **Schlüsselanbieter** für den Verbindungsstatus „Verbunden“ und ein grünes Häkchen angezeigt werden.

#### Verfahren

1 Navigieren Sie zum vCenter Server.

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

3 Wählen Sie den Schlüsselanbieter aus.

4 Klicken Sie auf **Als Standard festlegen**.

Ein Bestätigungsdialogfeld wird angezeigt.

5 Klicken Sie auf **Als Standard festlegen**.

Der Schlüsselanbieter wird als aktueller Standardschlüsselanbieter angezeigt.

## Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter

Sofern Sie im Dialogfeld **Standardschlüsselanbieter hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS herzustellen, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikatsaustausch 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 das Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** explizit als vertrauenswürdig fest.

- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat in vCenter Server hoch, indem Sie die Option **vCenter für KMS vertrauenswürdig machen** verwenden.

**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.

### Verfahren

1. Navigieren Sie zum vCenter Server.
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 den KMS aus.
5. Wählen Sie eine der folgenden Optionen im Dropdown-Menü **Vertrauensstellung herstellen** aus.

| Option | Aktion |
|---|---|
| **vCenter für KMS vertrauenswürdig machen** | Klicken Sie im daraufhin angezeigten Dialogfeld auf **Vertrauenswürdigkeit**. |
| **KMS-Zertifikat hochladen** | a Fügen Sie im angezeigten Dialogfeld entweder das Zertifikat ein oder klicken Sie auf **Datei hochladen** und navigieren Sie zur Zertifikatsdatei.<br>b Klicken Sie auf **Hochladen**. |

## Aktivieren der Verschlüsselung ruhender Daten auf einem neuen vSAN-Cluster

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

### Voraussetzungen

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

### Verfahren

1. Navigieren Sie zu einem vorhandenen Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus und klicken Sie unter „Verschlüsselung“ auf die Schaltfläche **Bearbeiten**.
4. Aktivieren Sie im Dialogfeld **vSAN-Dienste** die Option **Verschlüsselung** und wählen Sie einen KMS-Cluster oder Schlüsselanbieter aus.

   **Hinweis** Verwenden Sie das Kontrollkästchen **Restdaten löschen**, um Restdaten von Geräten zu löschen, bevor Sie die vSAN-Verschlüsselung aktivieren. Stellen Sie sicher, dass dieses Kontrollkästchen deaktiviert ist, sofern Sie vorhandene Daten nicht von den Speichergeräten löschen möchten, wenn Sie einen Cluster verschlüsseln, der VM-Daten enthält. Auf diese Weise wird sichergestellt, dass sich die unverschlüsselten Daten nach dem Aktivieren der vSAN-Verschlüsselung nicht mehr auf den Geräten befinden. Diese Einstellung ist für Neuinstallationen, bei denen keine VM-Daten auf den Speichergeräten vorhanden sind, nicht erforderlich.
5. Schließen Sie die Clusterkonfiguration ab.

### Ergebnisse

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

## Generieren neuer Verschlüsselungsschlüssel zur Verschlüsselung ruhender Daten

Sie können neue Verschlüsselungsschlüssel für ruhende Daten 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 Schlüsselanbieter eingerichtet und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.

Verfahren

1. Navigieren Sie zum vSAN-Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
4. Klicken Sie auf **Neue Verschlüsselungsschlüssel generieren**.
5. Klicken Sie auf **Übernehmen**, 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 Verschlüsselung ruhender Daten auf einem vorhandenen vSAN-Cluster

Sie können die Verschlüsselung ruhender Daten 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 Standard-Schlüsselanbieter konfiguriert und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.
- Der Modus für Festplattenbeanspruchung des Clusters muss auf „manuell“ festgelegt sein.

Verfahren

1. Navigieren Sie zum vSAN-Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter vSAN die Option **Dienste** aus.

4 Klicken Sie unter „Verschlüsselung“ auf die Schaltfläche **Bearbeiten**.

5 Aktivieren Sie im Dialogfeld „vSAN-Dienste“ die Option **Verschlüsselung** und wählen Sie einen KMS-Cluster oder Schlüsselanbieter aus.

6 (Optional) Wenn die Speichergeräte in Ihrem Cluster sensible Daten enthalten, aktivieren Sie die Option **Restdaten löschen**.

   Diese Einstellung sorgt dafür, dass vSAN vorhandene Daten von den Speichergeräten löscht, während sie verschlüsselt werden. Mit dieser Option nimmt möglicherweise die Zeit zum Verarbeiten der einzelnen Festplatten zu. Aktivieren Sie die Option daher nur, wenn auf den Festplatten unerwünschte Daten vorhanden sind.

7 Klicken Sie auf **Übernehmen**.

#### Ergebnisse

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 ruhender Daten 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 vCenter Server 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-Datenspeicher

Falls auf einem vSAN-Cluster die Verschlüsselung ruhender Daten aktiviert ist, sind die Core-Dumps im `vm-support`-Paket verschlüsselt. Sie können das Paket 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 ruhender Daten für den vSAN-Datenspeicher 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.

### Verfahren

1. Melden Sie sich bei vCenter Server mithilfe von vSphere 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.

### Verfahren

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. 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.

Dieses Kapitel enthält die folgenden Themen:

- vSAN-Build-Empfehlungen für vSphere Lifecycle Manager

# 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 durchführen.

**Tabelle 9-1. Voraussetzungen für das Upgrade**

| Voraussetzungen für das Upgrade | Beschreibung |
|---|---|
| Software, Hardware, Treiber, Firmware und Speicher-E/A-Controller | Vergewissern Sie sich, dass die neue Version von vSAN die Software- und Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller unterstützt, die Sie verwenden möchten. Die unterstützten Elemente sind auf der Website des VMware-Kompatibilitätshandbuchs unter http://www.vmware.com/resources/compatibility/search.php aufgelistet. |
| vSAN-Version | Stellen Sie sicher, dass Sie die neueste Version von vSAN verwenden. Sie können kein Upgrade von einer Beta-Version auf die neue vSAN-Version vornehmen. 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*. |

Tabelle 9-1. Voraussetzungen für das Upgrade (Fortsetzung)

| Voraussetzungen für das Upgrade | Beschreibung |
|---|---|
| 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 konvertierenden Festplattengruppen) 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 freie Kapazität 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. Wenn ein Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, wird die Clusterkapazität automatisch reduziert. Der Mitgliedshost trägt keinen Speicher mehr zum Cluster bei, und die Kapazität auf dem Host steht nicht mehr für Daten zur Verfügung. Informationen zu verschiedenen Evakuierungsmodi finden Sie in der Dokumentation *Verwalten von VMware vSAN*. |
| 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 Lifecycle Manager verwenden, um den Upgradevorgang zu automatisieren und zu testen. Wenn Sie allerdings den vSphere Lifecycle Manager zum Aktualisieren von vSAN verwenden, lautet der Standardevakuierungsmodus **Datenzugriff sicherstellen**. Bei Verwendung des Modus **Datenzugriff sicherstellen** sind Ihre Daten nicht 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 in der Dokumentation *Verwalten von VMware vSAN*. |
| 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.
- Informationen dazu, ob Ihre Hardware die Anforderungen für vSAN erfüllt, finden Sie unter *vSAN-Planung und -Bereitstellung*.

vSAN 6.5 und neuere Versionen ermöglichen 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 Witness-Servers in einem ausgeweiteten oder aus zwei Hosts bestehenden Cluster

Der Witness-Server in einem ausgeweiteten oder aus zwei Hosts bestehenden Cluster befindet sich außerhalb des vSAN-Clusters, wird jedoch vom selben vCenter Server verwaltet. Sie können denselben Vorgang, den Sie für einen vSAN-Datenhost verwenden, auch zum Aktualisieren des Witness-Servers verwenden.

Führen Sie ein Upgrade des Zeugenhosts durch, bevor Sie die Datenhosts aktualisieren.

Die Verwendung von vSphere Lifecycle 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 Lifecycle Manager so, dass er den Witness-Server 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.

Die Details und die Ebene der Unterstützung für ein Upgrade auf ESXi 7.0 hängen vom zu aktualisierenden Host und von der verwendeten Upgrade-Methode ab. Stellen Sie sicher, dass der Upgrade-Pfad von Ihrer aktuellen Version von ESXi auf die Version, auf die Sie ein Upgrade durchführen möchten, unterstützt wird. Weitere Informationen finden Sie in den VMware-Produktinteroperabilitätstabellen unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Statt ein direktes Upgrade auf vCenter Server durchzuführen, können Sie auch einen anderen Computer für das Upgrade verwenden. Detaillierte Anweisungen und Upgrade-Optionen finden Sie in der Dokumentation zum *vCenter Server-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.

Sie können Folgendes verwenden, um ein Upgrade der ESXi-Hosts im vSAN-Cluster durchzuführen:

- vSphere Lifecycle Manager: vSphere Lifecycle Manager ermöglicht Ihnen ein Upgrade der ESXi-Hosts im vSAN-Cluster mithilfe von Images oder Baselines. Der Standard-Evakuierungsmodus lautet **Möglichkeit des Datenzugriffs sicherstellen**. Wenn Sie diesen Modus verwenden und während des Upgrades von vSAN ein Fehler auftritt, kann dies dazu führen, dass auf einige Daten nicht mehr zugegriffen werden kann, bis einer der Hosts wieder online ist. Informationen zum Arbeiten mit Evakuierungsmodi und Wartungsmodi finden Sie unter Arbeiten mit dem Wartungsmodus. Weitere Informationen zu Upgrades und Updates finden Sie in der Dokumentation *Verwalten des Host- und Cluster-Lebenszyklus*.
- Esxcli-Befehl: Sie können Komponenten, Basis-Images und Add-ons als neue Softwareleistung verwenden, um ESXi 7.0-Hosts mithilfe des manuellen Upgrades zu aktualisieren oder zu patchen.

Wenn Sie ein Upgrade eines vSAN-Clusters mit konfigurierten Fehlerdomänen durchführen, aktualisiert vSphere Lifecycle Manager einen Host innerhalb einer einzelnen Fehlerdomäne und fährt dann mit dem nächsten Host fort. Dadurch wird sichergestellt, dass für den Cluster dieselben vSphere-Versionen auf allen Hosts ausgeführt werden. Wenn Sie ein Upgrade für einen Stretched Cluster ausführen, aktualisiert vSphere Lifecycle Manager alle Hosts der bevorzugten Site und fährt dann mit dem Host auf der sekundären Site fort. Dadurch wird sichergestellt, dass für den Cluster dieselben vSphere-Versionen auf allen Hosts ausgeführt werden. Weitere Informationen zum Upgrade eines Stretched Clusters finden Sie in der Dokumentation *Verwalten des Host- und Cluster-Lebenszyklus*.

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. Detaillierte Anweisungen und Upgrade-Optionen finden Sie in der Dokumentation zum *VMware ESXi-Upgrade*.

### Nächste Schritte

1. (Optional) Führen Sie ein Upgrade des vSAN-Festplattenformats durch. Siehe Upgrade des vSAN-Festplattenformats mit RVC.
2. Prüfen Sie die Hostlizenz. In den meisten Fällen müssen Sie Ihre Hostlizenz neu anwenden. 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 Client oder vSphere Lifecycle 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. |

Tabelle 9-2. Upgrade-Fortschritt (Fortsetzung)

| Prozentsatz des Abschlusses | Beschreibung |
|---|---|
| 15% - 95% | Entfernen und Neuformatieren von Festplattengruppen beim Upgrade von vSAN-Versionen vor Version 3.0. 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 Upgradevorgang über die Seite „Neusynchronisieren von Komponenten“ überwachen. Siehe *vSAN-Überwachung und -Fehlerbehebung*. 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 Bereich „Kürzlich bearbeitete Aufgaben“ der Statusleiste können Sie 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 einem Wert für **Zu tolerierende Fehler** von mehr als 0 (null) 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 **Zu tolerierende Fehler** 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.

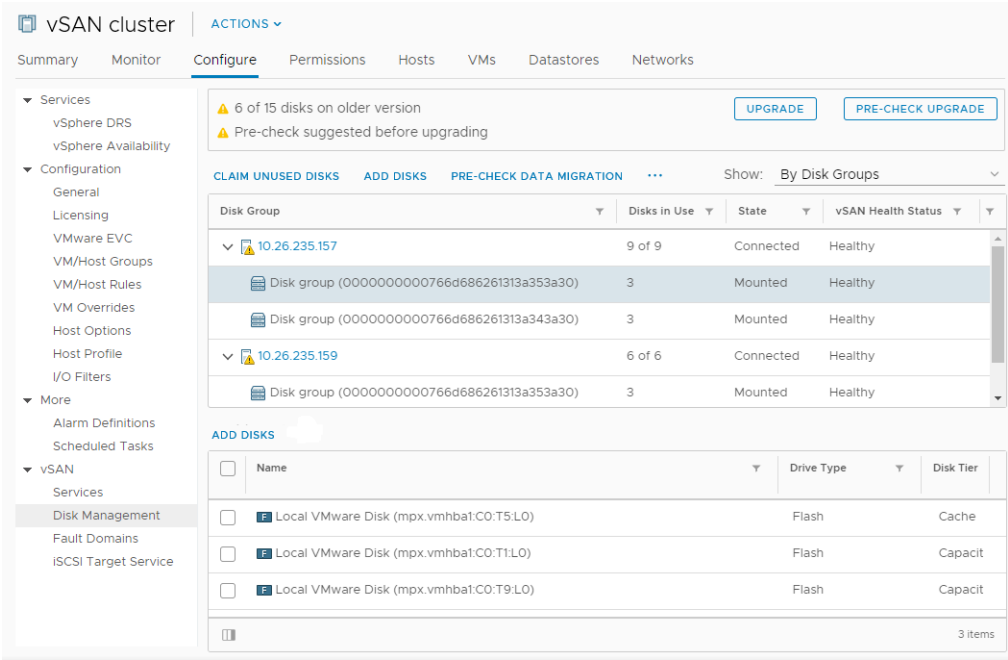
  Darüber hinaus müssen Sie sicherstellen, dass ausreichend freier Speicherplatz verfügbar ist. Der Speicherplatz muss der logischen verbrauchten Kapazität der größten Festplattengruppe entsprechen. Diese Kapazität muss auf einer Festplattengruppe separat von der zu migrierenden Festplattengruppe verfügbar 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 über den vSphere Client

Nachdem Sie ein Upgrade der vSAN-Hosts durchgeführt haben, können Sie das Festplattenformat aktualisieren.




**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. Siehe Bearbeiten von vSAN-Einstellungen.

### 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 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. Wenn ein beliebiger Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, steht die Kapazität des Mitgliedshosts nicht mehr im Cluster bereit. Die Clusterkapazität wird verringert und das Upgrade des Clusters schlägt möglicherweise fehl.
- Stellen Sie sicher, dass aktuell keine Komponentenneuerstellungsaufgaben im vSAN-Cluster ausgeführt werden. Informationen zur vSAN-Neusynchronisierung finden Sie unter *vSphere-Überwachung und -Leistung*.

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter vSAN **Festplattenverwaltung** aus.
4. (Optional) Klicken Sie 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 auf **Upgrade durchführen**.
6. Klicken Sie im Dialogfeld „Upgrade“ auf **Ja**, um das Upgrade des Festplattenformats durchzuführen.

Ergebnisse

Das Festplattenformat wurde von vSAN erfolgreich aktualisiert. Die Spalte „Datenträgerformat-Version“ zeigt die Festplattenformat-Version der Speichergeräte im Cluster an.

Wenn beim Upgrade ein Fehler auftritt, können Sie die Seite „Neusynchronisieren von Objekten“ 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“ 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.

Verfahren

1. Melden Sie sich mit RVC bei Ihrem vCenter Server an.
2. Führen Sie den folgenden RVC-Befehl aus, um den Festplattenstatus anzuzeigen: `vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

   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 folgenden RVC-Befehl aus: `vsan.ondisk_upgrade <path to vsan cluster>`

   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 folgenden RVC-Befehl aus, um zu überprüfen, ob für die Objektversionen ein Upgrade auf das neue Festplattenformat durchgeführt wurde: `vsan.obj_status_report`

## 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.

### Verfahren

1 Navigieren Sie 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.

# Informationen zum vSAN-Objektformat

Der Arbeitsspeicherplatz, den vSAN zum Durchführen der Richtlinienänderung oder anderer derartiger Vorgänge für ein Objekt, das von vSAN 7.0 oder früher erstellt wurde, benötigt, ist der vom größten Objekt im Cluster verwendete Speicherplatz. Dies ist in der Regel schwer zu planen. Daher sollten Sie 30 Prozent des freien Speicherplatzes im Cluster beibehalten, vorausgesetzt, dass es unwahrscheinlich ist, dass das größte Objekt im Cluster mehr als 25 Prozent des Speicherplatzes verbraucht und 5 Prozent des Speicherplatzes reserviert sind, um sicherzustellen, dass der Cluster aufgrund von Richtlinienänderungen nicht voll wird. In vSAN 7.0 U1 und höher werden alle Objekte in einem neuen Format erstellt. Dadurch kann mit dem von vSAN benötigten Arbeitsspeicherplatz eine Richtlinienänderung für ein Objekt durchgeführt werden, wenn 255 GB pro Host für Objekte unter 8 TB und 765 GB pro Host für Objekte mit 8 TB oder mehr vorhanden sind.

Nach dem Upgrade eines Clusters auf vSAN 7.0 U1 oder höher von vSAN 7.0 oder früheren Versionen müssen die mit der älteren Version erstellten Objekte mit mehr als 255 GB im neuen Format neu geschrieben werden, bevor vSAN mit den neuen Anforderungen an den freien Speicherplatz Vorgänge für ein Objekt ausführen kann. Nach einem Upgrade wird eine Systemzustandswarnung für das neue Objektformat angezeigt, wenn Objekte vorhanden sind, die in das neue Objektformat korrigiert werden müssen. Zudem kann der Systemzustand standardisiert werden, indem eine Aufgabe für ein neues Layout gestartet wird, um diese Objekte zu korrigieren. Die Systemzustandswarnung liefert Informationen zur Anzahl der zu korrigierenden Objekte und zur Menge der Daten, die neu geschrieben werden. Während der Vorgang für das neue Layout ausgeführt wird, kann der Cluster etwa 20 Prozent an Leistung verlieren. Das Dashboard für die Neusynchronisierung enthält genauere Informationen zur Dauer dieses Vorgangs.

# 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.

**Verfahren**

1. Navigieren Sie 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. |

Tabelle 9-3. Optionen des Upgradebefehls (Fortsetzung)

| Optionen | Beschreibung |
|---|---|
| `--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 Lifecycle Manager

vSAN generiert System-Baselines und Baseline-Gruppen, die Sie mit vSphere Lifecycle Manager verwenden können. vSphere Lifecycle Manager umfasst in vSphere 7.0 die System-Baselines, die Update Manager in früheren vSphere-Versionen zur Verfügung gestellt hat. Darüber hinaus sind neue Funktionalitäten für die Image-Verwaltung für Hosts enthalten, auf denen ESXi 7.0 und höher ausgeführt wird.

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.

System-Baselines für vSAN 6.7.1 bis vSAN 7.0 können auch Gerätetreiber und Firmware-Updates umfassen. Diese Updates unterstützen die für Ihren Cluster empfohlene ESXi-Software.

In vSAN 6.7.3 und höher können Sie auswählen, ob Build-Empfehlungen ausschließlich für die aktuelle ESXi-Version oder für die aktuellste unterstützte ESXi-Version bereitgestellt werden. Eine Build-Empfehlung für die aktuelle Version enthält alle Patches und Treiber-Updates für diese Version.

In vSAN 7.0 und höher enthalten vSAN-Build-Empfehlungen Updates für Patches und verwendete Treiber. Um die Firmware auf vSAN 7.0-Clustern zu aktualisieren, müssen Sie über vSphere Lifecycle Manager ein Image verwenden.

## vSAN-System-Baselines

vSAN-Build-Empfehlungen werden über vSAN-System-Baselines für vSphere Lifecycle 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.

vSAN-System-Baselines können von zertifizierten Anbietern bereitgestellte benutzerdefinierte ISO-Images umfassen. Wenn Hosts in Ihrem vSAN-Cluster OEM-spezifische benutzerdefinierte ISO-Dateien aufweisen, können von vSAN empfohlene System-Baselines benutzerdefinierte ISO-Dateien vom selben Anbieter umfassen. vSphere Lifecycle Manager kann keine Empfehlung für benutzerdefinierte ISO-Dateien generieren, die nicht von vSAN unterstützt werden. Wenn Sie ein angepasstes Software-Image ausführen, das den Anbieternamen im Image-Profil des Hosts überschreibt, kann vSphere Lifecycle Manager keine System-Baseline empfehlen.

vSphere Lifecycle 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 vSphere Lifecycle 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.

Wenn Sie nicht über eine Internetverbindung verfügen, können Sie den vSAN-Versionskatalog direkt auf den vCenter Server hochladen. Klicken Sie im vSphere Client auf **Konfigurieren > vSAN > Aktualisieren** und klicken Sie im Abschnitt „Versionskatalog“ auf **Aus Datei hochladen**. Sie können den neuesten vSAN-Versionskatalog herunterladen.

Mit vSphere Lifecycle Manager können Sie für Ihren vSAN-Cluster empfohlene Speicher-Controller-Treiber importieren. Anbieter von Speicher-Controllern stellen ein Software-Verwaltungstool zur Verfügung, das vSAN zum Aktualisieren von Controller-Treibern nutzen kann. Falls das Verwaltungstool auf ESXi-Hosts nicht zur Verfügung steht, können Sie es herunterladen.

## Arbeiten mit vSAN-Build-Empfehlungen

vSphere Lifecycle Manager überprüft die installierten ESXi-Versionen anhand der Informationen in der Hardwarekompatibilitätsliste (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, kann vSAN ein Upgrade auf die neueste Version empfehlen, da sie nicht schlechter als der aktuelle Status ist.

**Hinweis** vSphere Lifecycle Manager verwendet den vSAN-Integritätsdienst beim Durchführen der Standardisierungs-Vorabprüfung für Hosts in einem vSAN-Cluster. Der vSAN-Integritätsdienst ist nicht verfügbar auf Hosts, auf denen ESXi 6. 0 Update 1 oder früher ausgeführt wird. Wenn vSphere Lifecycle Manager ein Upgrade von Hosts durchführt, auf denen ESXi 6.0 Update 1 oder eine frühere Version ausgeführt wird, schlägt das Upgrade des letzten Hosts im vSAN-Cluster möglicherweise fehl. Wenn die Standardisierung aufgrund von vSAN-Integritätsproblemen fehlgeschlagen ist, können Sie das Upgrade trotzdem abschließen. Verwenden Sie den vSAN-Integritätsdienst zum Beheben von Integritätsproblemen auf dem Host und deaktivieren Sie anschließend den Wartungsmodus für den Host, um den Upgrade-Workflow abzuschließen.

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 6.7 Update 2 aus, und die Hardware ist in der HCL für 6.7 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 7.0 Update 3 unterstützt. vSAN empfiehlt ein Upgrade auf Version 7.0 Update 3.

**Beispiel 3**

Ein vSAN-Cluster führt Version 6.7 Update 2 aus, und die Hardware ist nicht in der HCL für diese Version enthalten. vSAN empfiehlt ein Upgrade auf Version 7.0 Update 3, obwohl die Hardware nicht in der HCL für 7.0 Update 3 enthalten ist. vSAN empfiehlt das Upgrade, da der neue Status nicht schlechter als der aktuelle Status ist.

**Beispiel 4**

Ein vSAN-Cluster führt Version 6.7 Update 2 aus, und die Hardware ist in der HCL für 6.7 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 7.0 Update 3 unterstützt, wobei die ausgewählte Baseline-Einstellung nur für Patches gilt. vSAN empfiehlt ein Upgrade auf Version 7.0 Update 3, einschließlich der erforderlichen kritischen Patches für die Version.

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 Webbrowser oder RVC bei VMware Customer Connect 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

vSphere Lifecycle Manager ist ein Erweiterungsdienst in vCenter Server 7.0 und höher.

vSAN erfordert Internetzugriff für die Aktualisierung von Versionsmetadaten, die Überprüfung des VMware-Kompatibilitätshandbuchs und zum Herunterladen von ISO-Images aus VMware Customer Connect.

vSAN erfordert gültige Anmeldedaten zum Herunterladen von ISO-Images für Upgrades aus VMware Customer Connect. Für Hosts, auf denen Version 6.0 Update 1 und früher ausgeführt wird, müssen Sie für die Eingabe der **VMware Customer Connect**-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.

Um die Anmeldedaten von **VMware Customer Connect** über RVC einzugeben, führen Sie den folgenden Befehl aus: **`vsan.login_iso_depot -u`** *<username>* **`-p`** *<password>*