Verwalten von VMware vSAN

Update 3
20. August 2019
VMware vSphere 6.7
VMware vSAN 6.7

vmware®

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

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

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

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

Inhalt

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.

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*.

vSphere Client und vSphere Web Client

Die Anweisungen in diesem Handbuch beziehen sich auf den vSphere Client (eine HTML5-basierte Benutzeroberfläche). Sie können die Anweisungen auch nutzen, um die Aufgaben mithilfe des vSphere Web Client (einer Flex-basierten Benutzeroberfläche) durchzuführen.

Für Aufgaben, bei denen sich der Workflow zwischen dem vSphere Client und dem vSphere Web Client erheblich unterscheidet, sind doppelte Prozeduren vorhanden. Die Schritte der einzelnen Prozeduren beziehen sich auf die jeweilige Client-Benutzeroberfläche. Im Titel der Prozeduren, die sich auf den vSphere Web Client beziehen, ist vSphere Web Client angegeben.

Hinweis In vSphere 6.7 Update 3 sind fast alle Funktionen des vSphere Web Client im vSphere Client implementiert. Eine aktuelle Liste aller nicht unterstützten Funktionen finden Sie im Handbuch Funktionsaktualisierungen für den vSphere Client.

Einführung in vSAN

1

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

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

Konfigurieren und Verwalten eines vSAN-Clusters

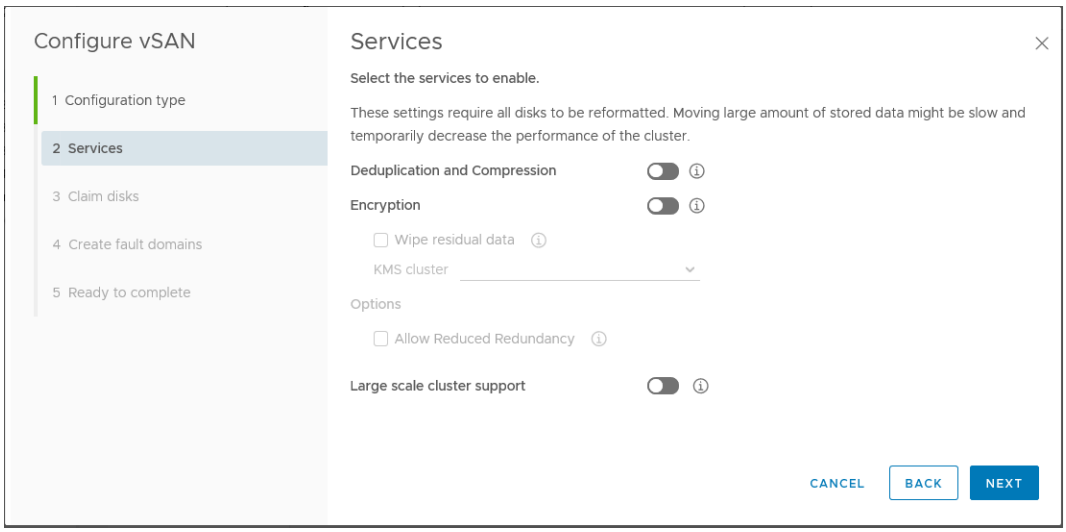
2

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 Assistenten zum Konfigurieren von vSAN im HTML5-basierten vSphere Client für die grundlegende Konfiguration Ihres vSAN-Clusters verwenden.



Voraussetzungen

Erstellen Sie einen Cluster und fügen Sie diesem Hosts hinzu, bevor Sie den Assistenten zum Konfigurieren von vSAN verwenden, um die grundlegende Konfiguration durchzuführen.

Verfahren

1 Navigieren Sie im vSphere Client zu einem vorhandenen Cluster.

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

3 Wählen Sie unter vSAN die Option **Dienste** aus und klicken Sie auf die Schaltfläche **Konfigurieren**.

4 Wählen Sie den Konfigurationstyp aus und klicken Sie auf **Weiter**.

- Cluster auf einer Site. Alle Hosts auf einer Site mit gemeinsam ausgeübten Witness-Funktionen.
- vSAN-Cluster mit zwei Hosts. Ein Host auf jeder Site und ein Witness-Server auf einer anderen Site.
- Stretched Cluster. Zwei aktive Daten-Sites mit einer gleichmäßigen Anzahl an Hosts und Speichergeräten und einem Witness-Server an einem dritten Standort.

5 Konfigurieren Sie auf der Seite **Dienste** vSAN-Dienste und klicken Sie auf **Weiter**.

a (Optional) Aktivieren Sie **Deduplizierung und Komprimierung** auf dem Cluster.

b (Optional) Aktivieren Sie **Verschlüsselung** und wählen Sie einen KMS aus.

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

d (Optional) Aktivieren Sie die Unterstützung großer Cluster für maximal 64 Hosts im vSAN-Cluster.

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

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

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

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

b Definieren Sie bei Auswahl von **Stretched Cluster konfigurieren** Fehlerdomänen für den Cluster, wählen Sie einen Witness-Server aus und beanspruchen Sie Festplatten für den Witness-Server.

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

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

Weitere Informationen zu Stretched Clustern finden Sie unter „Einführung in Stretched Cluster“ im Handbuch *vSAN-Planung und -Bereitstellung*.

8 Überprüfen Sie auf der Seite **Bereit zum Abschließen** 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

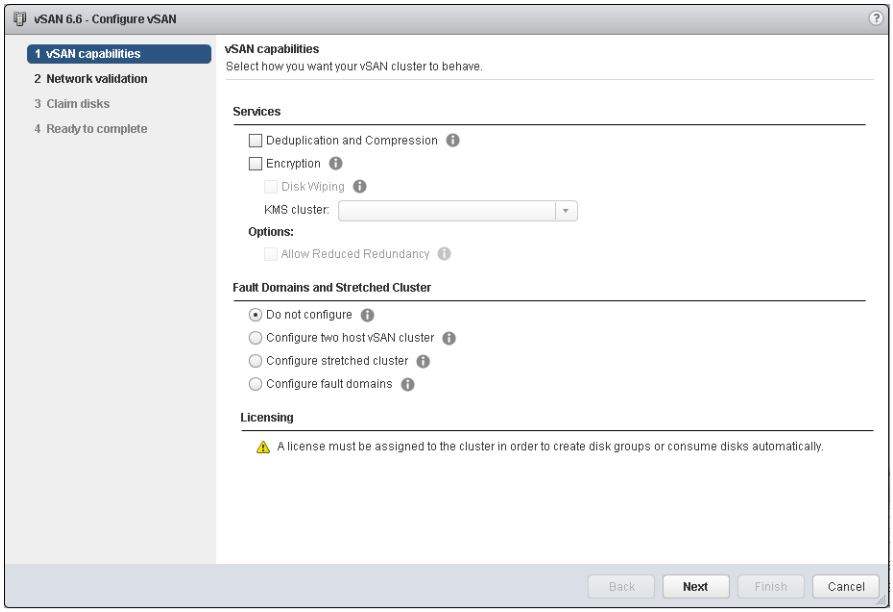
Vergewissern Sie sich, dass der Datenspeicher für vSAN erstellt wurde. Siehe Anzeigen des vSAN-Datenspeichers.

Vergewissern Sie sich, dass der Speicheranbieter für vSAN registriert ist. Siehe Anzeigen von vSAN-Speicheranbietern.

Beanspruchen Sie die Speichergeräte oder erstellen Sie Festplattegruppen. Siehe *Verwalten von VMware vSAN*.

Konfigurieren eines Clusters für vSAN mit dem vSphere Web Client

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



Voraussetzungen

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

Verfahren

1. Navigieren Sie im vSphere Web Client zu einem vorhandenen Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Allgemein** aus und klicken Sie auf die Schaltfläche **Konfigurieren**.

4 Wählen Sie **vSAN-Funktionen** aus.

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

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

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

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

Option	Beschreibung
Nicht konfigurieren	Für einen vSAN-Cluster an einem einzelnen Standort verwendete Standardeinstellung.
vSAN-Cluster mit 2 Hosts	Bietet Fault Tolerance für einen Cluster, der über zwei Hosts an einer Außenstelle und einen Witness-Server in der Hauptniederlassung verfügt. Legen Sie die Richtlinie **Primäre Ebene von zu tolerierenden Fehlern** auf 1 fest.
Ausgeweiteter Cluster	Unterstützt zwei aktive Sites mit einer gleichmäßigen Anzahl an Hosts und Speichergeräten und einen Witness-Server an einer dritten Site.
Fehlerdomänen konfigurieren	Unterstützt Fehlerdomänen, die Sie zum Gruppieren von vSAN-Hosts verwenden können, die möglicherweise gemeinsam fehlschlagen. Weisen Sie jeder Fehlerdomäne mindestens einen Host zu.

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

5 Klicken Sie auf **Weiter**.

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

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

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

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

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

   b Definieren Sie bei Auswahl von **Ausgeweiteten Cluster konfigurieren** Fehlerdomänen für den Cluster, wählen Sie einen Witness-Server aus und beanspruchen Sie Festplatten für den Witness-Server.

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

   Weitere Informationen zu Fehlerdomänen und ausgeweiteten Clustern finden Sie unter *Verwalten von VMware vSAN*.

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

Aktivieren von vSAN für einen vorhandenen Cluster

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

Voraussetzungen

Vergewissern Sie sich, dass Ihre Umgebung alle Anforderungen erfüllt. Siehe „Anforderungen für die Aktivierung von vSAN“ in *Verwalten von VMware vSAN*.

Verfahren

1 Navigieren Sie zu einem vorhandenen Host-Cluster.

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

Option	Beschreibung
vSphere Client	a Wählen Sie unter „vSAN“ die Option **Dienste** aus. b (Optional) Aktivieren Sie die Deduplizierung und Komprimierung auf dem Cluster. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt. c (Optional) Aktivieren Sie die Verschlüsselung auf dem Cluster und wählen Sie einen KMS-Server aus. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt. d (Optional) Wählen Sie „Verringerte Redundanz zulassen“ als Datenmigrationsoption aus. Falls erforderlich, wird vSAN während der Aktivierung von Deduplizierung und Komprimierung oder Verschlüsselung die Schutzebene Ihrer VMs absenken.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**. c (Optional) Wählen Sie das Kontrollkästchen **Deduplizierung und Komprimierung** aus, wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren möchten. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt. d (Optional) Wenn Sie auf dem Cluster die Verschlüsselung aktivieren möchten, aktivieren Sie das Kontrollkästchen **Verschlüsselung** und wählen Sie einen KMS-Server aus. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt.

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

Nächste Schritte

Beanspruchen Sie die Speichergeräte oder erstellen Sie Festplattegruppen. Siehe *Verwalten von VMware vSAN*.

Deaktivieren von vSAN

Sie können vSAN für einen Host-Cluster deaktivieren.

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

Voraussetzungen

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

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

Option	Beschreibung
vSphere Client	a Wählen Sie unter „vSAN“ die Option **Dienste** aus. b Klicken Sie auf **vSAN ausschalten**. c Bestätigen Sie Ihre Auswahl im Dialogfeld „vSAN ausschalten“.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**. c Deaktivieren Sie das vSAN-Kontrollkästchen **Einschalten**.

Bearbeiten von vSAN-Einstellungen

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

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

Verfahren

1 Navigieren Sie zum vSAN-Host-Cluster.

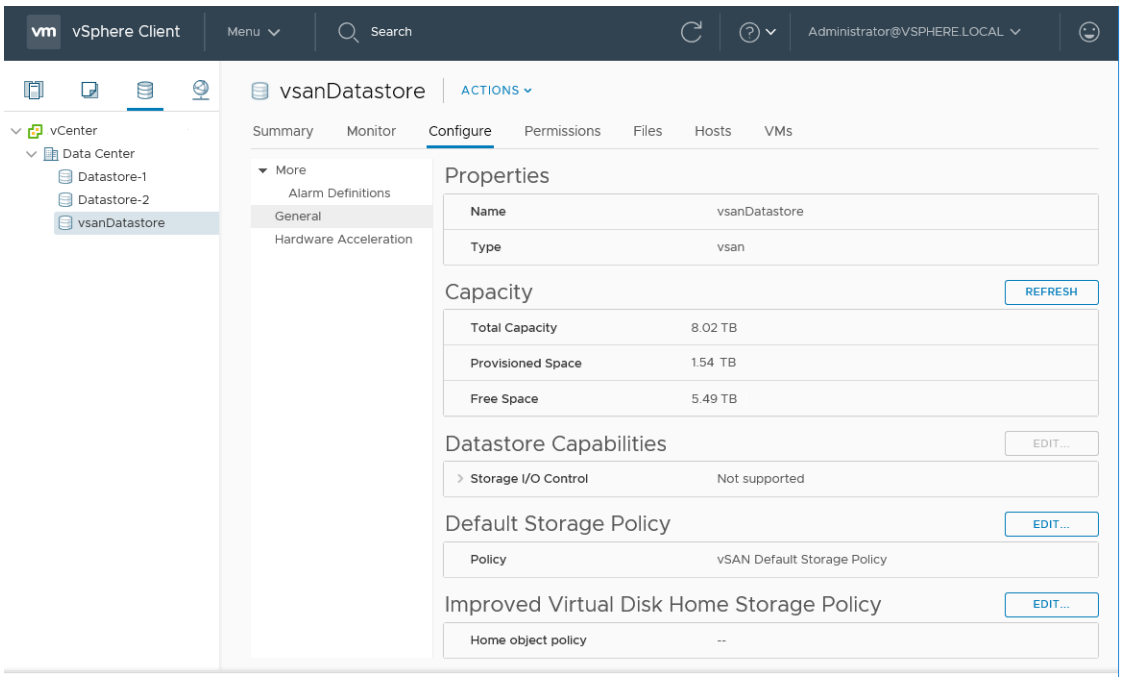
2 Klicken Sie auf die Registerkarte **Konfigurieren**.

Option	Beschreibung
vSphere Client	a Wählen Sie unter „vSAN“ die Option **Dienste** aus. b Klicken Sie für den Dienst, den Sie konfigurieren möchten, auf die Schaltfläche **Bearbeiten**. ■ Aktivieren oder deaktivieren Sie Deduplizierung und Komprimierung. ■ Konfigurieren Sie die vSAN-Verschlüsselung. ■ Konfigurieren Sie den vSAN-Leistungsdienst. ■ Konfigurieren Sie den iSCSI-Zieldienst. ■ 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.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**. c (Optional) Wählen Sie das Kontrollkästchen **Deduplizierung und Komprimierung** aus, wenn Sie Deduplizierung und Komprimierung auf dem Cluster aktivieren möchten. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt. d (Optional) Wenn Sie auf dem Cluster die Verschlüsselung aktivieren möchten, aktivieren Sie das Kontrollkästchen **Verschlüsselung** und wählen Sie einen KMS-Server aus. vSAN führt automatisch ein Upgrade des Festplattenformats aus, was zu einer rollierenden Neuformatierung jeder Festplattengruppe im Cluster führt.

3 Klicken Sie auf **OK** oder 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 NFS-, VMFS- und 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. b Klicken Sie auf **Hochladen**. c Suchen Sie nach dem hochzuladenden Element auf dem lokalen Computer 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. b Klicken Sie auf **Hochladen**. 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

3

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 die Option **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt, und sie hat einen einzelnen Disk-Stripe pro Objekt sowie eine schnell („thin“) bereitgestellte virtuelle Festplatte.

Das VM-Auslagerungsobjekt und das VM-Snapshot-Arbeitsspeicherobjekt sind nicht an die einer VM zugeordneten Speicherrichtlinien gebunden. Diese Objekte werden mit der auf 1 festgelegten Option **Primäre Ebene von zu tolerierenden Fehlern** konfiguriert. Diese Objekte haben nicht dieselbe Verfügbarkeit wie andere Objekte, denen eine Richtlinie mit einem anderen Wert für **Primäre Ebene von zu tolerierenden Fehlern** zugewiesen wurde.

Tabelle 3-1. Speicherrichtlinienregeln

Funktionalität	Beschreibung
Primäre Ebene von zu tolerierenden Fehlern (PFTT)	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. Wenn Sie beim Bereitstellen einer virtuellen Maschine keine Speicherrichtlinie auswählen, weist vSAN diese Richtlinie als VM-Standardspeicherrichtlinie zu. 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. Der Standardwert ist 1. Der Höchstwert ist 3. **Hinweis** Wenn vSAN eine einzelne Spiegelkopie von VM-Objekten nicht schützen soll, können Sie **PFTT** auf 0 festlegen. Beim Host können allerdings ungewöhnliche Verzögerungen beim Wechseln in den Wartungsmodus auftreten. Die Verzögerungen treten auf, weil vSAN das Objekt vom Host evakuieren muss, um den Wartungsvorgang erfolgreich abschließen zu können. Wenn Sie **PFTT** auf 0 festlegen, sind Ihre Daten nicht geschützt und Sie verlieren eventuell Daten, wenn beim vSAN-Cluster ein Gerätefehler auftritt. **Hinweis** Wenn Sie eine Speicherrichtlinie erstellen und keinen Wert für **PFTT** 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. In einem Stretched Cluster definiert diese Regel die Anzahl der Siteausfälle, die ein VM-Objekt tolerieren kann. Sie können die Option **PFTT** zusammen mit der Option **SFTT** verwenden, um für Objekte innerhalb Ihrer Datensites einen lokalen Fehlerschutz anzubieten. Der Höchstwert für einen Stretched Cluster ist 1.
Sekundäre Ebene von zu tolerierenden Fehlern (SFTT)	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 **PFTT** definierten tolerierbaren Site-Ausfälle erreicht ist. Wenn **PFTT** auf 1 und **SFTT** auf 2 festgelegt und eine Site nicht verfügbar ist, kann der Cluster zwei weitere Hostausfälle tolerieren. Der Standardwert ist 1. Der Höchstwert ist 3.
Datenbelegung	In einem Stretched Cluster steht diese Regel nur dann zur Verfügung, wenn die Option **Primäre Ebene von zu tolerierenden Fehlern** auf 0 festgelegt ist. Sie können die Regel **Datenbelegung** auf **Keine**, **Bevorzugt** oder **Sekundär** festlegen. Diese Regel ermöglicht es Ihnen, die VM-Objekte auf eine ausgewählte Site oder einen ausgewählten Host im Stretched Cluster zu begrenzen. Der Standardwert ist „Keine“.

Tabelle 3-1. Speicherrichtlinienregeln (Fortsetzung)

Funktionalität	Beschreibung
Fehlertoleranzmethode	Gibt an, ob die Datenreplizierungsmethode für Leistung und Kapazität optimiert wird. Bei Auswahl von **RAID-1 (Spiegelung) - Leistung** verwendet vSAN mehr Festplattenspeicher, um die Objektkomponenten zu platzieren. Die Verwendung dieser Option führt jedoch zu verbesserten Leistung beim Zugreifen auf die Objekte. Bei Auswahl von **RAID-5/6 (Erasure Coding) - Kapazität** verwendet vSAN weniger Festplattenspeicher, die Leistung nimmt jedoch ab. Sie können RAID 5 verwenden, indem Sie das Attribut **RAID-5/6 (Erasure Coding) - Kapazität** für Cluster mit vier oder mehr Fehlerdomänen anwenden und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festlegen. Sie können RAID 6 verwenden, indem Sie das Attribut **RAID-5/6 (Erasure Coding) - Kapazität** für Cluster mit sechs oder mehr Fehlerdomänen anwenden und **Primäre Ebene von zu tolerierenden Fehlern** auf 2 festlegen. In Stretched Clustern mit konfigurierter Option **Sekundäre Ebene von zu tolerierenden Fehlern** gilt diese Regel nur für die **Sekundäre Ebene von zu tolerierenden Fehlern**. Weitere Informationen zu RAID 5 oder RAID 6 finden Sie unter Verwenden von RAID 5- oder RAID 6-Erasure Coding.
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. Der Standardwert ist 1. Der Höchstwert ist 12. Ändern Sie diesen Standard-Striping-Wert nicht. 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.

Tabelle 3-1. Speicherrichtlinienregeln (Fortsetzung)

Funktionalität	Beschreibung
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. 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. 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. Der Standardwert ist 0%. Der Höchstwert ist 100%. **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. 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.
Bereitstellung erzwingen	Wenn die Option auf **Ja** festgelegt ist, wird das Objekt bereitgestellt, auch wenn die in der Speicherrichtlinie angegebenen Richtlinien **Primäre Ebene von zu tolerierenden Fehlern**, **Anzahl der Festplatten-Stripes pro Objekt** und **Flash Read Cache-Reservierung** vom Datenspeicher nicht erfüllt werden können. Verwenden Sie diesen Parameter in Bootstrapping-Szenarien und bei Ausfällen, wenn keine Standardbereitstellung mehr möglich ist. 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.

Tabelle 3-1. Speicherrichtlinienregeln (Fortsetzung)

Funktionalität	Beschreibung
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: ■ Thin Provisioning (Standard) ■ 25 % Reservierung ■ 50 % Reservierung ■ 75 % Reservierung ■ Thick Provisioning
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. 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. 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. 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. 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. 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.

Host-Affinität

Mithilfe der Speicherrichtlinie für die vSAN-Host-Affinität können Sie eine einzelne Datenkopie auf dem lokalen Host einer VM speichern.

Die Speicherrichtlinie für die vSAN-Host-Affinität passt die Effizienz und Widerstandsfähigkeit von vSAN für Shared-Nothing-Anwendungen der nächsten Generation an. Wenn Sie diese Richtlinie verwenden, behält vSAN nur eine Kopie der Daten bei, die auf dem lokalen Host, auf dem die VM ausgeführt wird, gespeichert werden. Diese Richtlinie wird als Bereitstellungsoption für Big Data (Hadoop, Spark), NoSQL und ähnliche Anwendungen bereitgestellt, die die Datenredundanz auf der Anwendungsschicht aufrechterhalten.

Die vSAN-Host-Affinität weist spezifische Anforderungen und Richtlinien auf, die VMware-Validierung zur Gewährleistung einer ordnungsgemäßen Bereitstellung erfordern. Die Richtlinie für die vSAN-Host-Affinität muss auf alle VMs im Cluster angewendet werden. Eine Kombination mit anderen Richtlinien im selben Cluster ist nicht möglich. vSAN-Verschlüsselung und -Deduplizierung können nicht zusammen mit der Richtlinie für die vSAN-Host-Affinität verwendet werden. Die Optionen „DRS“ und „HA“ von vSphere müssen deaktiviert werden, um ein automatisiertes Verschieben von VMs zu vermeiden.

An dieser Funktion interessierte Administratoren müssen sich an VMware wenden, um eine Anfrage zu ihrer Bereitstellungsabsicht einzureichen. Vor der Genehmigung von Support und Verwendung in der Produktion überprüft VMware die Anfrage, um sicherzustellen, dass Ihre Bereitstellung die Anforderungen erfüllt. VMware bietet für Bereitstellungen, für die keine ausdrückliche Genehmigung vorliegt, keinen Support. Weitere Informationen erhalten Sie von Ihrem VMware-Repräsentanten.

Anzeigen von vSAN-Speicheranbietern

Durch die Aktivierung von vSAN wird ein Speicheranbieter für jeden Host im vSAN-Cluster automatisch konfiguriert und registriert.

vSAN-Speicheranbieter sind integrierte Softwarekomponenten, die Datenspeicherfunktionen an vCenter Server übermitteln. Eine Speicherfunktion wird in der Regel durch ein Schlüssel-Wert-Paar dargestellt, wobei der Schlüssel eine spezielle Eigenschaft ist, die vom Datenspeicher angeboten wird. Der Wert ist eine Zahl oder ein Bereich, den der Datenspeicher für ein bereitgestelltes Objekt, z. B. ein VM-Home-Namespace-Objekt oder eine virtuelle Festplatte, zur Verfügung stellen kann. Außerdem können Sie Tags verwenden, um benutzerdefinierte Speicherfunktionen zu erstellen, und bei der Definition einer Speicherrichtlinie für eine virtuelle Maschine auf diese verweisen. Informationen zur Verwendung und Anwendung von Tags für Datenspeicher finden Sie in der Dokumentation *vSphere-Speicher*.

Die Speicheranbieter des vSAN berichten eine Reihe von zugrunde liegenden Speicherfunktionen an vCenter Server. Sie kommunizieren auch mit der Ebene des vSAN, um über die Speicheranforderungen der virtuellen Maschinen zu berichten. Weitere Informationen zu Speicheranbietern finden Sie in der Dokumentation *vSphere-Speicher*.

Das vSAN registriert einen getrennten Speicheranbieter für jeden Host im Cluster für vSAN über die folgende URL:

http://*host_ip*:8080/version.xml

wobei *host_ip* die tatsächliche IP des Hosts ist.

Überprüfen Sie, dass die Speicheranbieter registriert sind.

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 3-2. Spezifikationen für die vSAN-Standardspeicherrichtlinie

Spezifikation	Einstellung
Primäre Ebene von zu tolerierenden Fehlern	1
Anzahl der Festplatten-Stripes pro Objekt	1
Die Flash Read Cache-Reservierung oder die Flash-Kapazität für den Lesecache	0
Reservierter Objektspeicherplatz	Thin Provisioning
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. Informationen zum Erstellen einer benutzerdefinierten VM-Speicherrichtlinie finden Sie unter Definieren einer Speicherrichtlinie für vSAN mit dem vSphere Client.

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**.

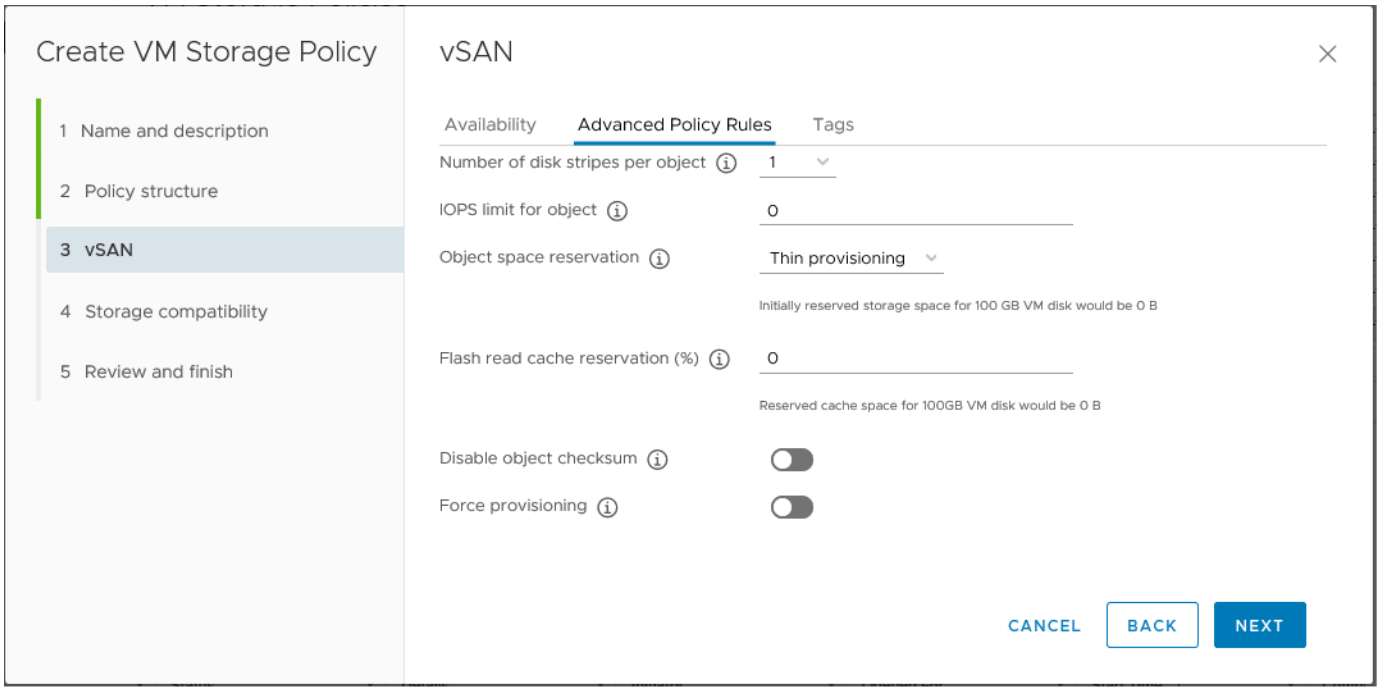
   Die Speicherrichtlinie wird als Standardrichtlinie angewendet, wenn Sie neue virtuelle Maschinen bereitstellen, ohne für einen Datenspeicher explizit eine Speicherrichtlinie festzulegen.

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**.

      Verfügbarkeitsoptionen definieren die Regeln für die primäre und sekundäre Ebene der zu tolerierenden Ausfälle sowie die Regeln für die 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:

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

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

   c 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, die mit dieser Richtlinie übereinstimmen, und klicken Sie auf **Weiter**.

   Ein geeigneter Datenspeicher muss nicht alle Regelsätze der Richtlinie erfüllen. Der Datenspeicher muss mindestens einen Regelsatz und alle Regeln innerhalb dieses Regelsatzes erfüllen. Stellen Sie sicher, dass der Datenspeicher für vSAN die in der Speicherrichtlinie festgelegten Anforderungen erfüllt und in der Liste kompatibler Datenspeicher angezeigt wird.

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

Ergebnisse

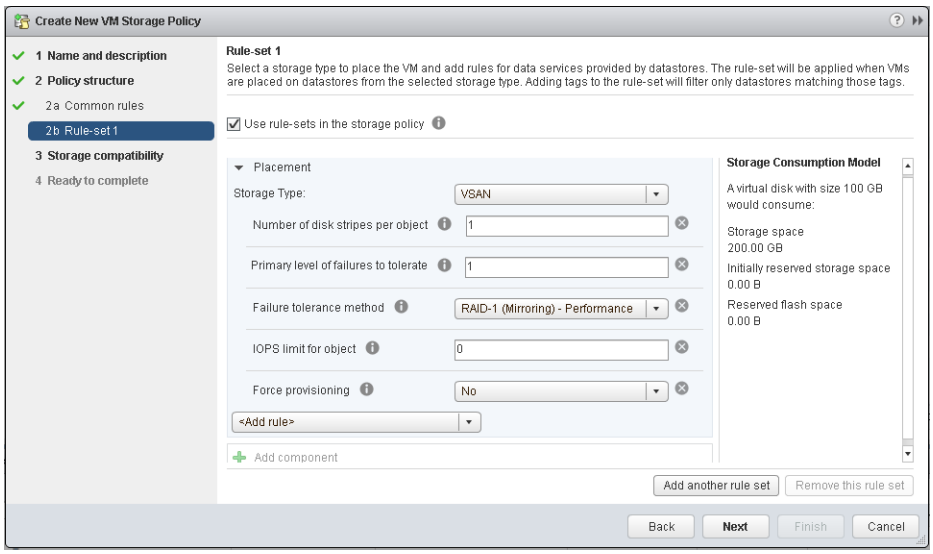
Die neue Richtlinie wird zur Liste hinzugefügt.

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*.

Definieren einer Speicherrichtlinie für vSAN mit dem vSphere Web 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. Weitere Informationen hierzu finden Sie unter Anzeigen von vSAN-Speicheranbietern.
- Stellen Sie sicher, dass die VM-Speicherrichtlinien aktiviert sind. Informationen zu Speicherrichtlinien finden Sie in der Dokumentation zu *vSphere-Speicher*.
- Erforderliche Berechtigungen: **Profilgesteuerter Speicher.Ansicht des profilgesteuerten Speichers** und **Profilgesteuerter Speicher.Update des profilgesteuerten Speichers**

Verfahren

1. Klicken Sie auf der Startseite des vSphere Web Client auf **Richtlinien und Profile** und dann auf **VM-Speicherrichtlinien**.
2. Klicken Sie auf das Symbol **Neue VM-Speicherrichtlinie erstellen** ( ).
3. Wählen Sie auf der Seite „Name und Beschreibung“ einen vCenter Server aus.

4 Geben Sie einen Namen und eine Beschreibung für die Speicherrichtlinie ein und klicken Sie auf **Weiter**.

5 Klicken Sie auf der Seite „Richtlinienstruktur“ auf **Weiter**.

6 Klicken Sie auf der Seite **Gemeinsame Regeln für von Hosts bereitgestellte Datendienste** auf **Weiter**.

7 Definieren Sie auf der Seite „Regelsatz 1“ den ersten Regelsatz.

   a Aktivieren Sie das Kontrollkästchen **Regelsätze in der Speicherrichtlinie verwenden**.

   b Wählen Sie **VSAN** aus dem Dropdown-Menü **Speichertyp** aus.

   Die Seite wird beim Hinzufügen von Regeln für den vSAN-Datenspeicher erweitert.

   c Wählen Sie im Dropdown-Menü **Regel hinzufügen** eine Regel aus.

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

   Über das Speicherbelegungsmodell können Sie die verfügbare Größe der virtuellen Festplatte und den entsprechenden Flash-Cache und die Kapazitätsanforderungen einschließlich des reservierten Speicherplatzes überprüfen, die von Ihren virtuellen Maschinen potenziell genutzt würden, wenn Sie die angegebene Speicherrichtlinie anwenden.

   d (Optional) Fügen Sie Tag-basierte Funktionen hinzu.

8 (Optional) Klicken Sie auf die Schaltfläche **Weiteren Regelsatz hinzufügen**, um einen weiteren Regelsatz hinzuzufügen.

9 Klicken Sie auf **Weiter**.

10 Überprüfen Sie auf der Seite „Speicherkompatibilität“ die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen, und klicken Sie auf **Weiter**.

   Ein geeigneter Datenspeicher muss nicht alle Regelsätze der Richtlinie erfüllen. Der Datenspeicher muss mindestens einen Regelsatz und alle Regeln innerhalb dieses Regelsatzes erfüllen. Stellen Sie sicher, dass der Datenspeicher für vSAN die in der Speicherrichtlinie festgelegten Anforderungen erfüllt und in der Liste kompatibler Datenspeicher angezeigt wird.

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

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

4

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 nicht automatisch Daten an das neu hinzugefügte Gerät. Um vSAN für Verteilung von Daten auf kürzlich hinzugefügte Geräte zu aktivieren, müssen Sie den Cluster unter Verwendung von Ruby vSphere Console (RVC) manuell neu verteilen. Siehe „Manuelle Neuverteilung“ 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. Siehe „Design-Überlegungen für Flash-Caching-Geräte in vSAN“ in *Verwalten von VMware vSAN*.
- 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 „Manuelle Neuverteilung“ in *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 zum Schnellstart finden Sie unter „Verwenden von Schnellstart zum Konfigurieren und Erweitern eines vSAN-Clusters“ in *vSAN-Planung und -Bereitstellung*.

Hinweis Wenn Sie auf einem Host im Cluster vCenter Server ausführen, muss der Host nicht in den Wartungsmodus versetzt werden, wenn Sie ihn unter Verwendung des Schnellstart-Workflows einem Cluster hinzufügen. Auf dem Host, der die vCenter Server-VM enthält, muss ESXi 6.5 EP2 oder höher ausgeführt werden. Auf demselben Host kann auch ein Platform Services Controller ausgeführt werden. Alle anderen VMs auf dem Host müssen ausgeschaltet sein.

Voraussetzungen

Der Workflow Schnellstart muss für Ihren vSAN-Cluster verfügbar sein.

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 **Hinzufügen**, 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 **Konfigurieren**, um den Assistenten für die Clusterkonfiguration zu öffnen.
   a. (Optional) Geben Sie auf der Seite „vMotion-Datenverkehr“ Informationen zur IP-Adresse für den vMotion-Datenverkehr ein.
   b. Geben Sie auf der Seite „Speicher-Datenverkehr“ Informationen zur IP-Adresse für den Speicher-Datenverkehr ein.
   c. (Optional) Wählen Sie auf der Seite „Festplatten beanspruchen“ die Festplatten auf jedem neuen Host.

d (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.

e 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. 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. 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*.

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-Übereinstimmung überprüfen** ( ).

      Wenn Sie bestimmte Details zu den Parametern anzeigen möchten, die zwischen dem Host, bei dem eine Nichtübereinstimmung gefunden wurde, und dem Hostprofil voneinander abweichen, klicken Sie auf die Registerkarte **Überwachen** und wählen Sie die Übereinstimmungsansicht aus. Erweitern Sie die Objekthierarchie und wählen Sie den nicht übereinstimmenden Host aus. Die abweichenden Parameter werden in der Übereinstimmungsansicht unterhalb der Hierarchie angezeigt.

      Verwenden Sie bei einem Übereinstimmungsfehler die Standardisierungsaktion, um die Hostprofileinstellungen auf den Host anzuwenden. Dabei werden alle vom Hostprofil verwalteten Parameter in die in dem Hostprofil vorhandenen Werte geändert, das dem Host zugeordnet ist.

   c Wenn Sie bestimmte Details zu den Parametern anzeigen möchten, die zwischen dem Host, bei dem eine Nichtübereinstimmung gefunden wurde, und dem Hostprofil voneinander abweichen, klicken Sie auf die Registerkarte **Überwachen** und wählen Sie die Übereinstimmungsansicht aus.

   d Erweitern Sie die Objekthierarchie und wählen Sie den fehlerhaften Host aus.

      Die abweichenden Parameter werden in der Übereinstimmungsansicht unterhalb der Hierarchie angezeigt.

5 Standardisieren Sie den Host, um Übereinstimmungsfehler zu beheben.

   a Wählen Sie die Registerkarte **Überwachen** aus und klicken Sie auf **Übereinstimmung**.

   b Klicken Sie mit der rechten Maustaste auf den Host bzw. die Hosts, den bzw. die Sie standardisieren möchten, und wählen Sie **Alle vCenter-Aktionen > Hostprofile > Standardisieren** aus.

      Sie können die Benutzereingabeparameter für die Hostprofil-Richtlinien aktualisieren oder ändern, indem Sie den Host anpassen.

   c Klicken Sie auf **Weiter**.

   d Überprüfen Sie die erforderlichen Aufgaben, um das Hostprofil zu standardisieren, und klicken Sie auf **Beenden**.

   Der Host ist Teil des vSAN-Clusters, und seine Ressourcen sind für den vSAN-Cluster zugänglich. Der Host kann auch auf alle vorhandenen Speicher-E/A-Richtlinien von vSAN im vSAN-Cluster zugreifen.

Arbeiten mit dem Wartungsmodus

Bevor Sie einen Host, der zu einem Cluster für vSAN gehört, herunterfahren, neu starten oder trennen, müssen Sie den Host in den Wartungsmodus versetzen.

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

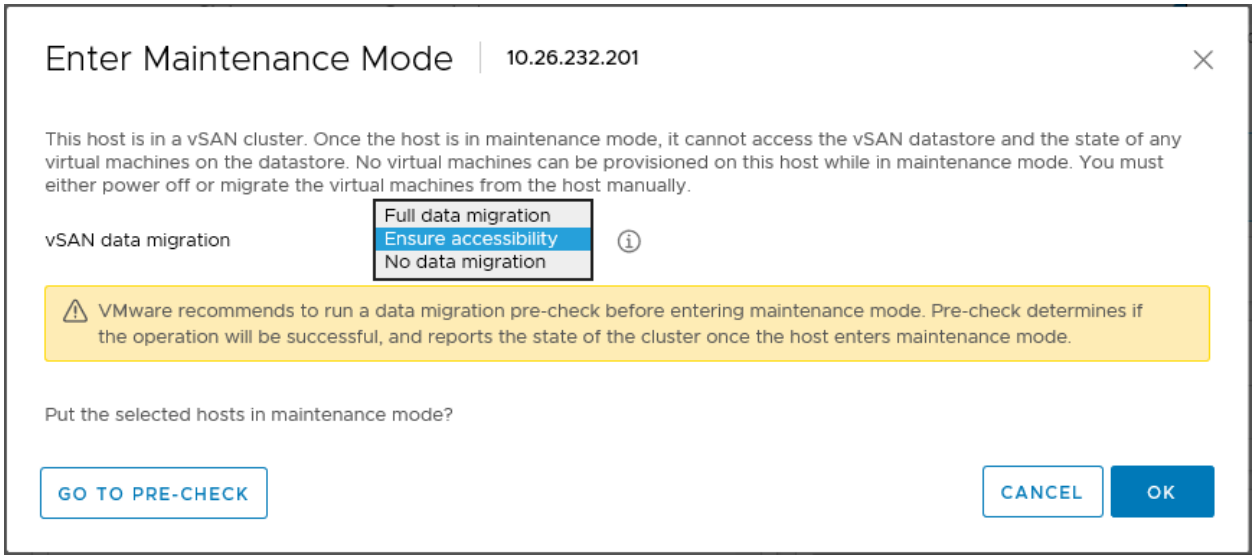
- Wenn Sie einen ESXi-Host in den Wartungsmodus versetzen, müssen Sie einen Datenevakuierungsmodus wie zum Beispiel **Zugriff sicherstellen** oder **Vollständige Datenmigration** auswählen.
- Wenn ein beliebiger Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, wird die Clusterkapazität 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 die Ressourcen verfügbar sind und für die **Primäre Ebene von zu tolerierenden Fehlern** der Wert 1 oder höher festgelegt wurde. In diesem Modus werden alle Komponenten vom Host migriert und je nach der Menge der Daten auf dem Host kann die Migration länger dauern. Im Modus **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 **Primäre Ebene von zu tolerierenden Fehlern** 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.

Führen Sie die Vorabprüfung der Datenmigration aus, um die Auswirkungen auf den Cluster zu überprüfen, wenn Sie den Host in den Wartungsmodus versetzen.



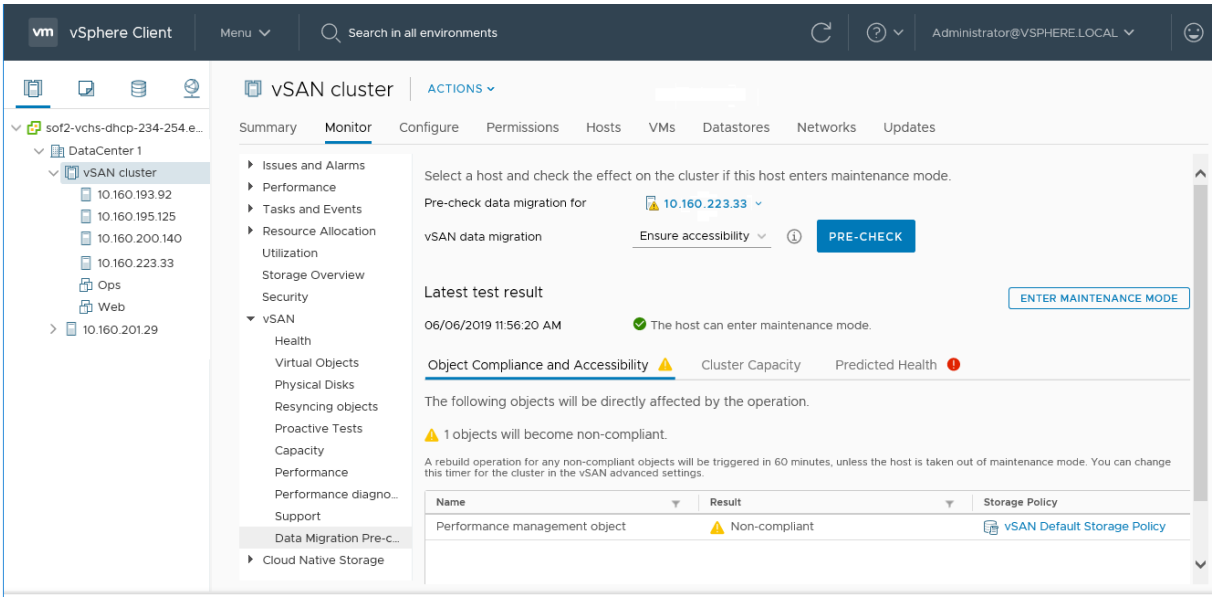
Das Dialogfeld „Wartungsmodus bestätigen“ bietet Informationen hinsichtlich Ihrer Wartungsaktivitäten. Sie können die Auswirkungen einer jeden Datenevakuierungsoption anzeigen.

- 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 Mitglieds

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. In der Regel muss nur ein Teil der Daten verlagert werden. Die virtuelle Maschine ist jedoch möglicherweise während der Verlagerung nicht mehr vollständig mit einer VM-Speicherrichtlinie kompatibel. Dies bedeutet, dass sie möglicherweise keinen Zugriff auf alle Replikate hat. Wenn ein Fehler auftritt, während sich der Host im Wartungsmodus befindet und **Primäre Ebene von zu tolerierenden Fehlern** auf 1 festgelegt ist, können im Cluster Datenverluste auftreten. **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. Dieser Evakuierungsmodus führt zur größten Menge an Datenübertragungen und verbraucht die meiste Zeit und die meisten Ressourcen. Alle Komponenten im lokalen Speicher des ausgewählten Hosts werden anderswo im Cluster migriert. Wenn der Host in den Wartungsmodus wechselt, haben alle virtuellen Maschinen Zugriff auf ihre Speicherkomponenten und halten weiterhin die ihnen zugewiesenen Speicherrichtlinien ein. **Hinweis** Bei Objekten mit reduziertem Verfügbarkeitszustand behält dieser Modus diesen Übereinstimmungsstatus bei und gibt keine Garantie, dass die Objekte kompatibel werden. 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. Siehe „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“ in *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 **Primäre Ebene von zu tolerierenden Fehlern** für den Cluster hängt von der Anzahl der Ausfälle ab, die eine virtuelle Maschine tolerieren kann. Wenn das Attribut **Primäre Ebene von zu tolerierenden Fehlern** (PFFT) für eine virtuelle Maschine auf 1 `(PFTT=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 **Primäre Ebene von zu tolerierenden Fehlern** auf N `(PFTT=n)` festgelegt ist, benötigt vSAN mindestens `2*n+1` Fault Domains im Cluster. Wenn virtuelle Maschinen in einem Cluster mit Fault Domains und dieser Richtlinie bereitgestellt sind, werden die Kopien der damit verknüpften VM-Objekte auf verschiedenen Racks gespeichert.

Für die Unterstützung der Festlegung von PFTT 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 **Primäre Ebene von zu tolerierenden Fehlern** konfigurieren. Wenn Sie das Attribut **Primäre Ebene von zu tolerierenden Fehlern** 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**.

Option	Beschreibung
vSphere Client	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.
vSphere Web Client	a Wählen Sie den zu verschiebenden Host aus und klicken Sie auf das Symbol **Hosts aus Fehlerdomäne verschieben**. b Klicken Sie auf **Ja**.

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**.

Option	Beschreibung
vSphere Client	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.
vSphere Web Client	a Wählen Sie die Fehlerdomäne aus und klicken Sie auf das Symbol **Ausgewählte Fehlerdomäne umbenennen**. 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**.

Option	Beschreibung
vSphere Client	a Klicken Sie auf das Symbol „Aktionen“ auf der rechten Seite der Fehlerdomäne und wählen Sie **Löschen** aus. b Klicken Sie auf **Löschen**, um den Vorgang zu bestätigen.
vSphere Web Client	a Wählen Sie die zu löschende Fault Domain aus und klicken Sie auf das Symbol **Ausgewählte Fault Domains entfernen** (✖). b Klicken Sie auf **Ja**, 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.

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 WFSC-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 Mappings).

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 iSCSI Target Usage Guide.

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.

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

Option	Beschreibung
vSphere Client	a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**. b Klicken Sie auf **Aktivieren**, um den vSAN-iSCSI-Zieldienst zu aktivieren. c Bearbeiten Sie die Konfiguration des vSAN-iSCSI-Zieldiensts. Sie können gegenwärtig das Standardnetzwerk, den TCP-Port und die Authentifizierungsmethode auswählen. Sie können auch eine vSAN-Speicherrichtlinie auswählen.
vSphere Web Client	a Klicken Sie unter „vSAN“ auf **iSCSI-Ziele**. b Klicken Sie auf die Schaltfläche **Bearbeiten** des vSAN-iSCSI-Zieldiensts. c Aktivieren Sie das Kontrollkästchen „vSAN-iSCSI-Zieldienst aktivieren“. Sie können gegenwärtig das Standardnetzwerk, den TCP-Port und die Authentifizierungsmethode auswählen. Sie können auch eine vSAN-Speicherrichtlinie auswählen.

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

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**.

Option	Beschreibung
vSphere Client	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. Sie können auch das Netzwerk, den TCP-Port und die Authentifizierungsmethode für dieses Ziel bearbeiten.
vSphere Web Client	a Klicken Sie unter „vSAN“ auf **iSCSI-Ziele**. b Klicken Sie im Abschnitt „vSAN-iSCSI-Ziele“ auf das Symbol **Neues iSCSI-Ziel hinzufügen**. Das Dialogfeld „Neues iSCSI-Ziel“ wird angezeigt. Der Ziel-IQN wird automatisch generiert. c Geben Sie einen Ziel-Alias ein. Sie können auch das Netzwerk, den TCP-Port und die Authentifizierungsmethode für dieses Ziel bearbeiten. d (Optional) Klicken Sie zum Definieren der LUN für das Ziel auf das Kontrollkästchen „Erste LUN zum iSCSI-Ziel hinzufügen“ und geben Sie die Größe der LUN ein.

3 Klicken Sie auf **OK**.

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**.

Option	Beschreibung
vSphere Client	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.
vSphere Web Client	a Klicken Sie unter „vSAN“ auf **iSCSI-Ziele**. b Wählen Sie ein Ziel aus und klicken Sie auf die Registerkarte „LUNs“ im Seitenabschnitt „Zieldetails“. c Klicken Sie auf das Symbol **Neue iSCSI-LUN zum Ziel 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.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

Option	Beschreibung
vSphere Client	a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**. b Klicken Sie auf die Registerkarte „Initiatorgruppen“ und anschließend auf das Symbol **Neue iSCSI-Initiatorgruppe 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)
vSphere Web Client	a Klicken Sie unter „vSAN“ auf **iSCSI-Initiatorgruppen**. b Klicken Sie im Abschnitt „vSAN-iSCSI-Initiatorgruppen“ auf das Symbol **Neue iSCSI-Initiatorgruppe hinzufügen**. Das Dialogfeld „Neue vSAN-iSCSI-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**.

Option	Beschreibung
vSphere Client	a Klicken Sie unter vSAN auf **iSCSI-Zieldienst**. b Wählen Sie die Registerkarte **Initiatorgruppen** aus. c Klicken Sie im Abschnitt „Zugängliche Ziele“ auf das Symbol **Neues zugängliches Ziel für iSCSI-Initiatorgruppe hinzufügen** (✚). Das Dialogfeld **Zugängliche Ziele hinzufügen** wird angezeigt. d Wählen Sie ein Ziel aus der Liste der verfügbaren Ziele aus.
vSphere Web Client	a Klicken Sie unter „vSAN“ auf **iSCSI-Ziele**. b Wählen Sie die Registerkarte „Initiatorgruppen“ aus. c Wählen Sie im Abschnitt „Gruppendetails“ die Registerkarte „Zugängliche Ziele“ aus. d Klicken Sie auf das Symbol **Neues zugängliches Ziel für iSCSI-Initiatorgruppe hinzufügen**. Das Dialogfeld „Zugängliche Ziele hinzufügen“ wird angezeigt. e Wählen Sie auf der Registerkarte „Filter“ aus der Liste der verfügbaren Ziele ein Ziel aus. Die Registerkarte „Ausgewählte Objekte“ zeigt die derzeit ausgewählten Ziele an.

3 Klicken Sie auf **Hinzufügen**.

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

- Navigieren Sie zum vSAN-Cluster.

Option	Beschreibung
vSphere Client	a Klicken Sie auf **Überwachen** und wählen Sie **Virtuelle Objekte** aus. Die iSCSI-Ziele werden auf der Seite aufgelistet. b Wählen Sie ein Ziel aus und klicken Sie auf **Platzierungsdetails anzeigen**. Die physische Platzierung zeigt an, wo sich die Datenkomponenten des Ziels befinden. c Klicken Sie auf **Komponenten nach Hostplatzierung gruppieren**, um die Hosts anzuzeigen, die den iSCSI-Datenkomponenten zugeordnet sind.
vSphere Web Client	a Klicken Sie auf **Überwachen** und wählen Sie **vSAN** aus. b Klicken Sie auf **iSCSI-Ziele**. iSCSI-Ziele und -LUNs werden oben auf der Seite aufgelistet. c Klicken Sie auf einen Ziel-Alias und zeigen Sie dessen Status an. Die Registerkarte „Platzierung physischer Festplatten“ unten auf der Seite zeigt an, wo sich die Datenkomponenten des Ziels befinden. Die Registerkarte „Übereinstimmungsfehler“ zeigt fehlgeschlagene Komponenten an. d Klicken Sie auf eine LUN und zeigen Sie deren Status an. Die Registerkarte „Platzierung physischer Festplatten“ unten auf der Seite zeigt an, wo sich die Datenkomponenten der LUN befinden. Die Registerkarte „Übereinstimmungsfehler“ zeigt fehlgeschlagene Komponenten an.

Migrieren eines hybriden vSAN-Clusters auf einen All-Flash-Cluster

Sie können die Festplattengruppen in einem hybriden vSAN-Cluster auf All-Flash-Festplattengruppen migrieren.

Der hybride vSAN-Cluster verwendet Magnetplattenspeicher für die Kapazitätsschicht und Flash-Geräte für die Cache-Ebene. Sie können die Konfiguration der Festplattengruppen im Cluster so ändern, dass Flash-Geräte auf der Cache-Ebene und der Kapazitätsebene verwendet werden.

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.

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
```

Ausschalten eines vSAN-Clusters

Sie können einen vSAN-Cluster ausschalten, um Wartungsaufgaben oder Upgrades durchzuführen.

Voraussetzungen

Falls die vCenter Server-VM auf dem vSAN-Cluster ausgeführt wird, migrieren Sie die VM auf den ersten Host oder erfassen Sie den Host, auf dem sie gerade ausgeführt wird.

Verfahren

1 Schalten Sie alle virtuellen Maschinen aus, die auf dem vSAN-Cluster ausgeführt werden.

   Wenn der vCenter Server auf dem vSAN-Cluster ausgeführt wird, muss die vCenter Server-VM zuletzt ausgeschaltet werden.

2 Versetzen Sie alle ESXi-Hosts, aus denen sich der Cluster zusammensetzt, in den Wartungsmodus.

   Siehe Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus

3 Schalten Sie die ESXi-Hosts aus.

Geräteverwaltung in einem vSAN-Cluster

5

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.

Beanspruchen von Festplatten für den vSAN-Cluster

Sie können mehrere Geräte aus den Hosts auswählen und vSAN erstellt Standardfestplattengruppen.

Wenn Sie die Kapazität von Hosts erhöhen oder neue Hosts mit Kapazität hinzufügen, können Sie zum Erhöhen der Kapazität des vSAN-Datenspeichers die neuen Geräte auswählen. In einem reinen Flash-Cluster können Sie die Flash-Geräte zur Nutzung als Kapazität markieren.

Nachdem vSAN Geräte beansprucht hat, wird der gemeinsam genutzte vSAN-Datenspeicher erstellt. Die Gesamtgröße des Datenspeichers spiegelt die Kapazität aller Kapazitätsgeräte in Festplattengruppen auf allen Hosts im Cluster wider. Ein geringer Kapazitäts-Overhead wird für Metadaten verwendet.

Erstellen einer Festplattengruppe auf einem vSAN-Host

Sie können bestimmte Cache-Geräte manuell mit bestimmten Kapazitätsgeräten kombinieren, um Festplattengruppen auf einem bestimmten Host zu definieren.

Bei dieser Methode wählen Sie manuell Geräte zum Erstellen einer Festplattengruppe für einen Host aus. Sie können der Festplattengruppe ein Cache- und mindestens ein Kapazitätsgerät hinzufügen.

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 und klicken Sie auf **Festplattengruppe erstellen**.
   - Wählen Sie das für den Cache zu verwendende Flash-Gerät aus.

- Wählen Sie den Typ der zu verwendenden Kapazitätsfestplatten aus. Ihre Auswahl richtet sich dabei nach dem Typ der Festplattengruppe, die Sie erstellen möchten (HDD für Hybrid oder Flash für All-Flash).
- Wählen Sie die Geräte aus, die Sie für die Kapazität verwenden möchten.

5 Klicken Sie auf **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.

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 zum Hinzufügen zur Festplattengruppe aus.

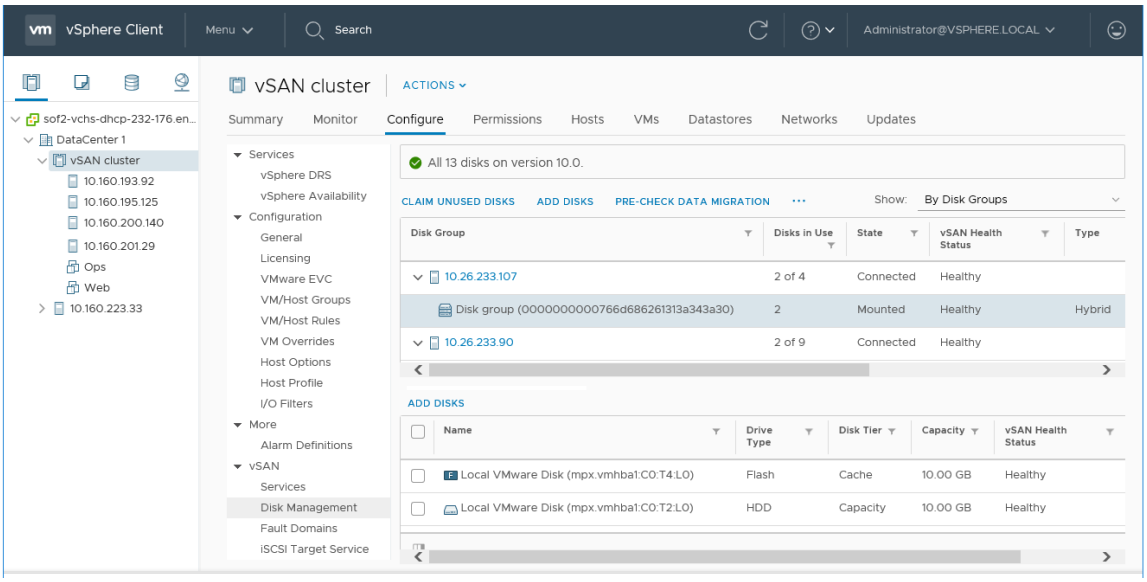
- Bei Hybrid-Festplattengruppen muss jeder Host, der Speicher bereitstellt, ein Flash-Cache-Gerät und ein oder mehrere Geräte mit Festplattenkapazität beisteuern. Pro Festplattengruppe kann nur ein Cache-Gerät hinzugefügt werden.
  - Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird,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

Arbeiten mit einzelnen Geräten

Sie können verschiedene Geräteverwaltungsaufgaben im vSAN-Cluster durchführen, wie zum Beispiel Hinzufügen von Geräten zu einer Festplattengruppe, Entfernen von Geräten aus einer Festplattengruppe, Aktivieren oder Deaktivieren von Locator-LEDs und Markieren von Geräten.



Hinzufügen von Geräten zu einer Festplattengruppe

Wenn Sie vSAN für die Beanspruchung von Festplatten im manuellen Modus konfigurieren, können Sie zusätzliche lokale Geräte zu vorhandenen Festplattengruppen hinzufügen.

Die Geräte müssen denselben Typ wie die vorhandenen Geräte in den Festplattengruppen aufweisen, also beispielsweise SSD oder Magnetfestplatten.

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*.

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

- Sie können den vSAN-Host durch Auswählen der Option **Vollständige Datenmigration** oder der Option **Datenzugriff sicherstellen** in den Wartungsmodus versetzen, wenn Sie ein Gerät oder eine Festplattengruppe löschen möchten. Wenn Sie die Option **Keine Datenmigration** aus dem Dropdown-Menü auswählen, sind Ihre Daten möglicherweise einem Risiko ausgesetzt, falls während der Evakuierung ein Fehler auftritt.

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**. b Wählen Sie einen Datenevakuierungsmodus aus.
Ausgewählte Festplatte entfernen	a Wählen Sie unter „Festplattengruppen“ die Festplattengruppe aus, die das zu entfernende Gerät enthält. b Wählen Sie unter „Festplatten“ das zu entfernende Gerät aus und klicken Sie auf das Symbol **Festplatten entfernen**. c Wählen Sie einen Datenevakuierungsmodus aus.

Sie können die evakuierten Daten auf eine andere Festplatte oder Festplattengruppe auf demselben Host verschieben.

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

Die Daten werden aus den ausgewählten Geräten oder einer Festplattengruppe evakuiert und sind nicht mehr für vSAN verfügbar.

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.

Option	Beschreibung
vSphere Client	Klicken Sie auf **Partitionen löschen**.
vSphere Web Client	Klicken Sie auf das Symbol **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

6

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 aktivieren, um doppelt vorhandene Daten zu vermeiden und den zum Speichern von Daten erforderlichen Speicherplatz zu verringern.

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

Sie können Deduplizierung und Komprimierung sowie RAID 5- oder RAID 6-Erasure Coding verwenden, um noch mehr Speicherplatz zu gewinnen. 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 höhere Versionen unterstützen SCSI-UNMAP-Befehle, mit denen Sie den einem gelöschten vSAN-Objekt zugeordneten Speicherplatz zurückfordern können.

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-Unmap- 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.

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

Sie können Deduplizierung und Komprimierung beim Erstellen eines neuen vSAN-All-Flash-Clusters oder beim Bearbeiten eines vorhandenen vSAN-All-Flash-Clusters aktivieren. Weitere Informationen zum Erstellen und Bearbeiten 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.

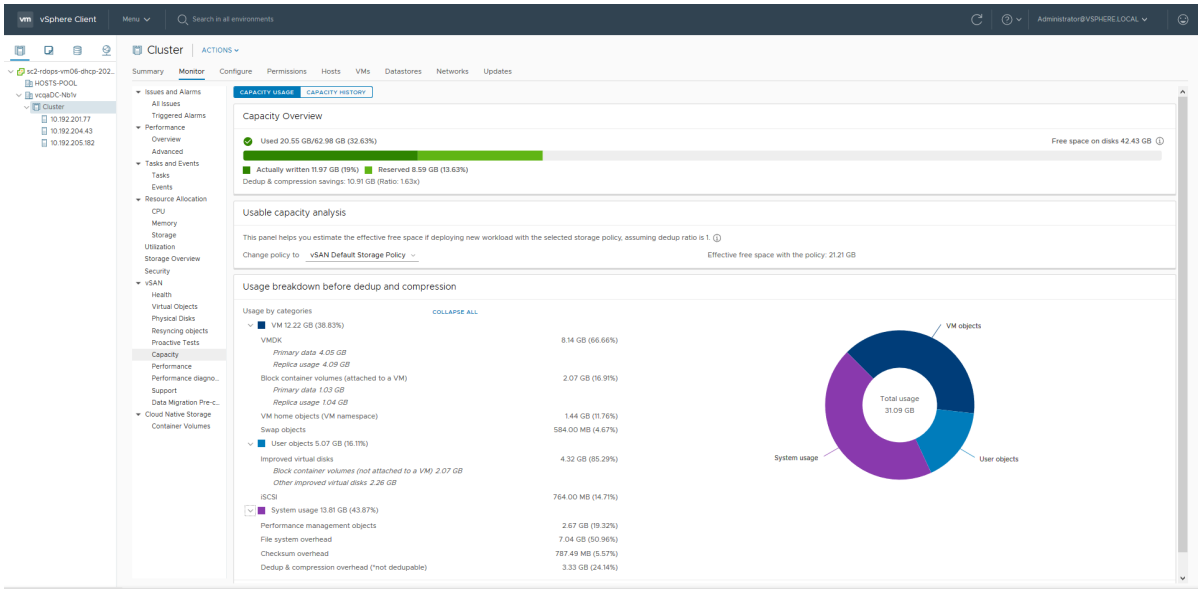
Verwalten von Festplatten in einem Cluster mit Deduplizierung und Komprimierung

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

- 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**.

Option	Beschreibung
vSphere Client	a Wählen Sie unter vSAN die Option **Dienste** aus und klicken Sie auf **Bearbeiten**. b Aktivieren Sie Deduplizierung und 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.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie auf die Schaltfläche **vSAN konfigurieren**. c Konfigurieren Sie die Deduplizierung und Komprimierung auf dem Cluster. 1 Aktivieren Sie auf der Seite **vSAN-Funktionen** das Kontrollkästchen **Aktivieren** unter „Deduplizierung und Komprimierung“. 2 Aktivieren Sie verringerte Redundanz für Ihre VMs. Siehe Reduzieren der VM-Redundanz für vSAN-Cluster. d Geben Sie auf der Seite **Festplatten beanspruchen** an, welche Festplatten für den vSAN-Cluster beansprucht werden sollen. 1 Wählen Sie ein Flash-Gerät aus, das als Kapazitätsgerät eingesetzt wird, und klicken Sie auf das Symbol **Für Kapazitätsschicht beanspruchen** (). 2 Wählen Sie ein Flash-Gerät aus, das als Cache-Gerät eingesetzt wird, und klicken Sie auf das Symbol **Für Cache-Schicht beanspruchen** ().

3 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**.

Option	Beschreibung
vSphere Client	a Wählen Sie unter „vSAN“ die Option **Dienste** aus. b Klicken Sie auf **Bearbeiten**. c Aktivieren Sie Deduplizierung und Komprimierung. d (Optional) Wählen Sie **Verringerte Redundanz zulassen** aus. Bei Bedarf reduziert vSAN die Schutzebene Ihrer VMs durch Aktivieren von Deduplizierung und Komprimierung. Siehe Reduzieren der VM-Redundanz für vSAN-Cluster.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**. c Konfigurieren Sie die Deduplizierung und Komprimierung auf dem Cluster. 1 Legen Sie die Deduplizierung und Komprimierung auf **Aktiviert** fest. 2 Aktivieren Sie verringerte Redundanz für Ihre VMs. Siehe Reduzieren der VM-Redundanz für vSAN-Cluster.

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

Option	Beschreibung
vSphere Client	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.
vSphere Web Client	a Wählen Sie unter vSAN die Option **Allgemein**. b Klicken Sie im Bereich „vSAN ist eingeschaltet“ auf die Schaltfläche **Bearbeiten**. c Deaktivieren Sie die Deduplizierung und Komprimierung. 1 Legen Sie den Modus für das Beanspruchen von Festplatten auf **Manuell** fest. 2 Legen Sie die Deduplizierung und Komprimierung auf **Deaktiviert** fest.

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-Schicht entfernen, wird die gesamte Festplattengruppe entfernt. Das Entfernen einer Festplatte auf der Cache-Schicht bei aktivierter Deduplizierung und Komprimierung löst eine Evakuierung der Daten aus.
- Deduplizierung und Komprimierung sind auf der Ebene der Festplattengruppe implementiert. Sie können eine Kapazitätsfestplatte nicht aus einem Cluster mit aktivierter Deduplizierung und Komprimierung entfernen. Sie müssen die gesamte Festplattengruppe entfernen.
- Wenn eine Kapazitätsfestplatte ausfällt, ist die gesamte Festplattengruppe nicht mehr verfügbar. Beheben Sie dieses Problem, indem Sie die fehlerhafte Komponente sofort identifizieren und ersetzen. Verwenden Sie beim Entfernen der fehlerhaften Festplattengruppe die Option „Keine Datenmigration“.

Verwenden von RAID 5- oder RAID 6-Erasure Coding

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

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

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

Tabelle 6-1. Zum Speichern und Schützen von Daten auf verschiedenen RAID-Ebenen erforderliche Kapazität

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

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

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

Hinweis In einem ausgeweiteten vSAN-Cluster wird die **Fehlertoleranzmethode** von **RAID-5/6 (Erasure Coding) – Kapazität** nur für **Sekundäre Ebene von zu tolerierenden Fehlern** angewendet.

Weitere Informationen zum Konfigurieren von Richtlinien finden Sie unter Kapitel 3 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 auf einem vSAN-Cluster

7

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

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

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

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

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

Dieses Kapitel enthält die folgenden Themen:

Funktionsweise der vSAN-Verschlüsselung

Wenn Sie die Verschlüsselung aktivieren, verschlüsselt vSAN alles, was sich im vSAN-Datenspeicher befindet. Alle Dateien werden verschlüsselt, sodass alle virtuellen Maschinen

und ihre entsprechenden Daten geschützt sind. Nur Administratoren mit Berechtigungen zum Verschlüsseln können Verschlüsselungs- und Entschlüsselungsaufgaben durchführen.

vSAN verwendet Verschlüsselungsschlüssel wie folgt:

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

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

Design-Überlegungen für vSAN-Verschlüsselung

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

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

Das Kennwort verschlüsselt Core-Dumps erneut, die interne Schlüssel zur Verwendung von auf diesem Kennwort basierenden Schlüsseln verwenden. Sie können das Kennwort zu einem späteren Zeitpunkt zum Entschlüsseln und Verschlüsseln von Core-Dumps verwenden, die möglicherweise im Support-Paket enthalten sind. Nicht verschlüsselte Core-Dumps oder Protokolle sind davon nicht betroffen.

- Das von Ihnen während der `vm-support`-Paketerstellung angegebene Kennwort wird in vSphere-Komponenten nicht dauerhaft gespeichert. Sie müssen Ihre Kennwörter für Support-Pakete selbst speichern bzw. diese notieren.

Festlegen des KMS-Clusters

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

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

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

Hinzufügen eines KMS zu vCenter Server

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

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

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

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

Voraussetzungen

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

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 dann auf **Schlüsselmanagementserver**.
4. Klicken Sie auf **Hinzufügen**, geben Sie im Assistenten die KMS-Informationen an und klicken Sie auf **Hinzufügen**.

Option	Wert
KMS-Cluster	Wählen Sie für einen neuen Cluster **Neuen Cluster erstellen** aus. Wenn ein Cluster vorhanden ist, können Sie diesen Cluster auswählen.
Clustername	Name des KMS-Clusters. Sie können diesen Namen für die Verbindung zum KMS verwenden, wenn Ihre vCenter Server-Instanz ausfällt.
Serveralias	Alias für den KMS. Sie können diesen Alias für die Verbindung zum KMS verwenden, wenn Ihre vCenter Server-Instanz ausfällt.
Serveradresse	IP-Adresse oder FQDN des KMS.
Serverport	Port, an dem vCenter Server eine Verbindung zum KMS herstellt.
Proxy-Adresse	Optionale Proxy-Adresse für die Verbindung zum KMS.
Proxyport	Optionaler Proxyport für die Verbindung zum KMS.
Benutzername	Einige KMS-Anbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann einen Benutzernamen an, wenn Ihr KMS diese Funktion unterstützt und Sie beabsichtigen, ihn zu verwenden.
Kennwort	Einige KMS-Anbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann ein Kennwort an, wenn Ihr KMS diese Funktion unterstützt und Sie beabsichtigen, es zu verwenden.

Herstellen einer vertrauenswürdigen Verbindung durch den Austausch von Zertifikaten

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

Voraussetzungen

Fügen Sie den KMS-Cluster hinzu.

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. Klicken Sie auf **vertrauenswürdige Verbindung mit KMS einrichten**.
5. Wählen Sie die entsprechenden Option für den Server aus und durchlaufen Sie die Schritte.

Option	Informationen hierzu finden Sie unter
CA-Root-Zertifikat	Verwenden der Root-CA-Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung.
Zertifikat	Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung.
Neue Zertifikatssignieranforderung	Verwenden der Option „Neue Zertifikatsignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung.
Zertifikat und privaten Schlüssel hochladen	Verwenden der Option zum Hochladen des Zertifikats und des privaten Schlüssels, um eine vertrauenswürdige Verbindung herzustellen.

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

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

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

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

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

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

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

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

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

Nächste Schritte

Schließen Sie den Zertifikatsaustausch ab. Weitere Informationen hierzu finden Sie unter Einrichten der vertrauenswürdigen Verbindung.

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung

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

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

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

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

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

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

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

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten der vertrauenswürdigen Verbindung.

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

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

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

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

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

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

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

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

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

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Siehe Einrichten der vertrauenswürdigen Verbindung.

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

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

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

Voraussetzungen

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

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 **Zertifikat und privater Schlüssel hochladen** und klicken Sie auf **OK**.
5. Fügen Sie das Zertifikat, das Sie vom KMS-Anbieter erhalten haben, in das obere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Zertifikatsdatei hochzuladen.
6. Fügen Sie die Schlüsseldatei in das untere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Schlüsseldatei hochzuladen.
7. Klicken Sie auf **OK**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten der vertrauenswürdigen Verbindung.

Festlegen des Standard-KMS-Clusters

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

Voraussetzungen

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

Verfahren

1. Navigieren Sie zum vCenter Server-System.

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

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

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

4 Klicken Sie auf **Ja**.

   Das Wort `default` erscheint neben dem Clusternamen.

Einrichten der vertrauenswürdigen Verbindung

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

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

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

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

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

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

Aktivieren der Verschlüsselung auf einen neuen vSAN-Cluster

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

Voraussetzungen

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

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 aus.

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

5 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.

Neue Verschlüsselungsschlüssel generieren

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

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

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

Voraussetzungen

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

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 vSAN-Verschlüsselung auf einem vorhandenen vSAN-Cluster

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

Voraussetzungen

- Erforderliche Rechte:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**
- Sie müssen einen KMS-Cluster eingerichtet und eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS hergestellt haben.
- Der Modus für Festplattenbeanspruchung des Clusters muss auf „manuell“ festgelegt sein.

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 aus.
6. (Optional) Wenn die Speichergeräte in Ihrem Cluster vertrauliche Daten enthalten, aktivieren Sie die Option **Festplatten vor Verwendung 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 **Akzeptieren**.

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

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

Core-Dumps auf ESXi-Hosts

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

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

Core-Dumps und vm-support-Pakete

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

Core-Dumps auf vCenter Server-Systemen

Ein Core-Dump auf einem vCenter Server-System ist nicht verschlüsselt. vCenter Server enthält bereits potenziell vertrauliche Informationen. Stellen Sie mindestens sicher, dass das Windows-System, auf dem vCenter Server ausgeführt wird, bzw. der vCenter Server Appliance geschützt ist. Alternativ können Sie Core-Dumps für das vCenter Server-System ausschalten. Weitere Informationen in den Protokolldateien können zum Ermitteln der Ursache des Problems dienlich sein.

Abrufen eines vm-support-Pakets für einen ESXi-Host in einem verschlüsselten vSAN-Cluster

Falls auf einem vSAN-Cluster die Verschlüsselung aktiviert ist, sind die Core-Dumps im `vm-support`-Paket verschlüsselt. Sie können das Paket erfassen und ein Kennwort angeben, falls Sie davon ausgehen, dass der Core-Dump zu einem späteren Zeitpunkt entschlüsselt werden muss.

Das `vm-support`-Paket enthält u. a. Protokolldateien und Core-Dump-Dateien.

Voraussetzungen

Informieren Sie Ihren Supportmitarbeiter darüber, dass die Verschlüsselung für den vSAN-Cluster aktiviert ist. Der Supportmitarbeiter bittet Sie möglicherweise darum, Core-Dumps zu entschlüsseln, um relevante Informationen zu extrahieren.

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Beachten Sie die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens, um den Schutz vertraulicher Daten wie Hostschlüssel zu gewährleisten.

Verfahren

1. Melden Sie sich unter Verwendung des Flex-basierten vSphere Web Client bei vCenter Server 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 encryptedZdumpdecryptedZdump
```

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 zdumpEncryptedzdumpUnencrypted`

Upgrade des vSAN-Clusters

8

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 Dokumentation *vSphere-Upgrade*.

2 Aktualisieren Sie die ESXi-Hosts. Weitere Informationen hierzu finden Sie unter 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. Weitere Informationen hierzu finden Sie unter Upgrade des vSAN-Festplattenformats mit RVC.

Dieses Kapitel enthält die folgenden Themen:

Vor dem Upgrade von vSAN

Planen und entwerfen Sie ein ausfallsicheres Upgrade. Bevor Sie versuchen, vSAN zu aktualisieren, stellen Sie sicher, dass Ihre Umgebung die vSphere-Hardware- und -Softwareanforderungen erfüllt.

Voraussetzungen für das Upgrade

Berücksichtigen Sie die Aspekte, die den allgemeinen Upgradevorgang verzögern können. Richtlinien und Best Practices finden Sie in der Dokumentation zum *vSphere-Upgrade*.

Prüfen Sie die wichtigsten Voraussetzungen, bevor Sie ein Upgrade des Clusters auf vSAN 6.7.3 durchführen.

Tabelle 8-1. Voraussetzungen für das Upgrade

Voraussetzungen für das Upgrade	Beschreibung
Software, Hardware, Treiber, Firmware und Speicher-E/A-Controller	Vergewissern Sie sich, dass vSAN 6.7.3 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. Ein Upgrade von einer Beta-Version auf vSAN 6.7.3 ist nicht möglich. Wenn Sie ein Upgrade von einer Beta-Version durchführen, müssen Sie vSAN erneut bereitstellen.
Festplattenspeicher	Stellen Sie sicher, dass ausreichend Speicherplatz verfügbar ist, um das Upgrade der Softwareversion fertig zu stellen. Die Menge des benötigten Festplattenspeichers für die vCenter Server-Installation hängt von Ihrer vCenter Server-Konfiguration ab. Richtlinien zum erforderlichen Festplattenspeicher für ein vSphere-Upgrade finden Sie in der Dokumentation zum *vSphere-Upgrade*.
vSAN-Festplattenformat	Stellen Sie sicher, dass genügend Kapazität für das Upgrade des Festplattenformats verfügbar ist. Wenn der freie Speicherplatz auf den Festplattengruppen (ohne die zu konvertierenden Festplattengruppen) geringer ist als die verbrauchte Kapazität der größten Festplattengruppe, müssen Sie **Verringerte Redundanz zulassen** als Datenmigrationsoption auswählen. 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 unter Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus.

Tabelle 8-1. Voraussetzungen für das Upgrade (Fortsetzung)

Voraussetzungen für das Upgrade	Beschreibung
vSAN-Hosts	Stellen Sie sicher, dass Sie die vSAN-Hosts in den Wartungsmodus versetzt und die Option **Datenzugriff sicherstellen** oder **Alle Daten evakuieren** ausgewählt haben. Sie können den vSphere Update Manager verwenden, um den Upgradevorgang zu automatisieren und zu testen. Wenn Sie allerdings den vSphere Update Manager zum Aktualisieren von vSAN verwenden, lautet der Standardevakuierungsmodus **Datenzugriff sicherstellen**. Bei Verwendung des Modus **Datenzugriff sicherstellen** sind Ihre Daten nicht geschützt. Falls während des Upgrades von vSAN ein Fehler auftritt, kann dies einen unerwarteten Datenverlust zur Folge haben. Der Modus **Datenzugriff sicherstellen** ist jedoch schneller als der Modus **Alle Daten evakuieren**, weil nicht alle Daten auf einen anderen Host im Cluster verschoben werden müssen. Informationen zu verschiedenen Evakuierungsmodi finden Sie unter Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus.
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 „Hardwareanforderungen für vSAN“ in *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.

Aktualisieren Sie den Witness-Server erst, wenn alle Datenhosts aktualisiert wurden und den Wartungsmodus verlassen haben.

Die Verwendung von vSphere Update Manager zur gleichzeitigen Aktualisierung von Hosts kann unter Umständen dazu führen, dass der Witness-Server gleichzeitig mit einem der Datenhosts aktualisiert wird. Um diese Probleme bei der Aktualisierung zu vermeiden, konfigurieren Sie vSphere Update 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. Statt ein In-Place-Upgrade auf vCenter Server durchzuführen, können Sie auch eine andere Maschine für das Upgrade verwenden. Detaillierte Anweisungen und verschiedene Upgrade-Optionen finden Sie in der Dokumentation zum *vSphere-Upgrade*.

Aktualisieren der ESXi-Hosts

Nach dem Upgrade von vCenter Server müssen Sie beim Upgrade des vSAN-Clusters als nächstes ein Upgrade der ESXi-Hosts für die Verwendung der aktuellen Version durchführen.

Wenn der vSAN-Cluster mehrere Hosts enthält und Sie diese mit vSphere Update Manager aktualisieren, ist **Datenzugriff sicherstellen** der Standardevakuierungsmodus. Wenn Sie diesen Modus verwenden und 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 finden Sie unter Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus.

Vor dem Aktualisieren der ESXi-Hosts sollten Sie die Informationen zu empfohlenen Vorgehensweisen im *vSphere Upgrade*-Handbuch lesen. VMware bietet verschiedene ESXi-Upgrade-Optionen. Wählen Sie die Upgrade-Option aus, die für den Hosttyp, den Sie aktualisieren, am besten geeignet ist. Weitere Informationen zu verschiedenen Upgrade-Optionen finden Sie in der *vSphere Upgrade*-Dokumentation.

Voraussetzungen

- Prüfen Sie, ob Sie ausreichend Festplattenspeicherplatz zum Aktualisieren der ESXi-Hosts haben. Hinweise zu den Festplattenspeicherplatzanforderungen finden Sie in der *vSphere Upgrade*-Dokumentation.
- Stellen Sie sicher, dass Sie die neueste Version von ESXi verwenden. Sie können das neueste ESXi-Installationsprogramm von der VMware-Website für Produktdownloads unter https://my.vmware.com/web/vmware/downloads herunterladen.
- Stellen Sie sicher, dass Sie die neueste Version von vCenter Server verwenden.
- Prüfen Sie die Kompatibilität der Netzwerkkonfiguration, des E/A-Controllers des Speichers, des Speichergeräts und der Sicherungssoftware.
- Prüfen Sie, ob Sie die virtuellen Maschinen gesichert haben.
- Verwenden Sie den Distributed Resource Scheduler (DRS), um Ausfallzeiten virtueller Maschinen während der Aktualisierung zu verhindern. Stellen Sie sicher, dass die Automatisierungsebene für jede virtuelle Maschine auf **Vollautomatisiert** eingestellt ist, damit der DRS virtuelle Maschinen migrieren kann, wenn Hosts in den Wartungsmodus versetzt werden. Sie können aber auch alle virtuellen Maschinen ausschalten oder eine manuelle Migration durchführen.

Verfahren

1. Versetzen Sie den Host, den Sie aktualisieren möchten, in den Wartungsmodus.

   Sie müssen Ihren Upgrade-Pfad mit ESXi 5.5-Hosts oder höher im vSAN-Cluster beginnen.

   a. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus > In den Wartungsmodus wechseln** aus.

   b. Wählen Sie je nach Ihren Anforderungen den Evakuierungsmodus **Datenzugriff sicherstellen** bzw. **Alle Daten evakuieren** aus und warten Sie, bis der Host in den Wartungsmodus gewechselt ist.

      Wenn Sie den Host mit vSphere Update Manager aktualisieren oder mit einem 3-Host-Cluster arbeiten, ist **Datenzugriff sicherstellen** als Standardevakuierungsoption verfügbar. Dieser Modus ist schneller als der Modus **Alle Daten evakuieren**. Im Modus **Datenzugriff sicherstellen** sind Ihre Daten allerdings nicht vollständig geschützt. Ein Hostausfall während des Betriebs im Wartungsmodus kann dazu führen, dass auf einige Daten nicht mehr zugegriffen werden kann, bis einer der Hosts wieder online ist.

2. Laden Sie die Software auf den Datenspeicher Ihres ESXi-Hosts hoch und stellen Sie sicher, dass die Datei im Verzeichnis innerhalb des Datenspeichers verfügbar ist. Sie können beispielsweise die Software auf `/vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip` hochladen.

3 Führen Sie den `esxcli`-Befehl `install -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check` aus. Verwenden Sie den `esxcli`-Software-VIB, um diesen Befehl auszuführen.

   Wenn der ESXi-Host erfolgreich installiert wurde, wird sinngemäß die folgende Meldung eingeblendet:

   `Die Aktualisierung wurde erfolgreich abgeschlossen, aber das System muss neu gestartet werden, damit die Änderungen wirksam werden.`

4 Starten Sie Ihren ESXi-Host manuell neu.

   a Navigieren Sie zum ESXi-Host in der Bestandsliste.

   b Klicken Sie mit der rechten Maustaste auf den Host, wählen Sie **Einschalten > Neustart** aus, klicken Sie auf **Ja**, um den Vorgang zu bestätigen, und warten Sie dann auf den Neustart des Hosts.

   c Klicken Sie mit der rechten Maustaste auf den Host, wählen Sie **Verbindung > Trennen** und dann **Verbindung > Verbinden** aus, um den Host zu verbinden.

      Zum Aktualisieren der restlichen Hosts im Cluster wiederholen Sie die Schritte für jeden Host.

      Wenn der vSAN-Cluster mehrere Hosts enthält, können Sie mit vSphere Update Manager die restlichen Hosts aktualisieren.

5 Beenden Sie den Wartungsmodus.

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 Update Manager.

Informationen zum vSAN-Festplattenformat

Das Upgrade des Festplattenformats ist optional. Ihr Cluster vSAN wird auch dann reibungslos ausgeführt, wenn Sie eine vorherige Festplattenformatversion verwenden.

Für optimale Ergebnisse sollten Sie jedoch ein Upgrade der Objekte auf das neue Festplattenformat durchführen. Das neue Festplattenformat stellt den kompletten Funktionssatz von vSAN für Ihre Umgebung bereit.

Je nach der Größe von Festplattengruppen kann das Upgrade des Festplattenformats zeitaufwändig sein, da jeweils nur eine Festplattengruppe aktualisiert. Für das Upgrade jeder Festplattengruppe werden alle Daten von jedem Gerät evakuiert und die Festplattengruppe wird aus dem vSAN-Cluster entfernt. Die Festplattengruppe wird dann wieder zu vSAN mit dem neuen Festplattenformat hinzugefügt.

Hinweis Sobald Sie das Festplattenformat aktualisiert haben, können Sie weder ein Rollback der Software auf den Hosts durchführen noch dem Cluster bestimmte ältere Hosts hinzufügen.

Wenn Sie ein Upgrade des Festplattenformats starten, führt vSAN mehrere Operationen durch, die Sie auf der Seite „Neusynchronisieren von Komponenten“ überwachen können. In der Tabelle wird jeder Vorgang zusammengefasst, der beim Upgrade des Festplattenformats durchgeführt wird.

Tabelle 8-2. 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. ■ Alle Hosts sind verbunden. ■ Alle Hosts weisen die richtige Softwareversion auf. ■ Alle Festplatten sind in einem ordnungsgemäßen Zustand. ■ 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 8-2. 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 „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“ in *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 **Alle Daten evakuieren** auswählen, kann die Evakuierung für Objekte mit **Primäre Ebene von zu tolerierenden Fehlern** größer 0 (null) fehlschlagen. Ein Cluster mit drei Hosts kann eine Festplattengruppe, die vollständig evakuiert wird, mit den Ressourcen von nur zwei Hosts nicht neu schützen. Sie werden unter Umständen aufgefordert, eine weitere Festplattengruppe zu einem vorhandenen Host hinzuzufügen.

  Für einen Cluster mit drei Hosts können Sie die Datenmigrationsoption **Zugriff 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.

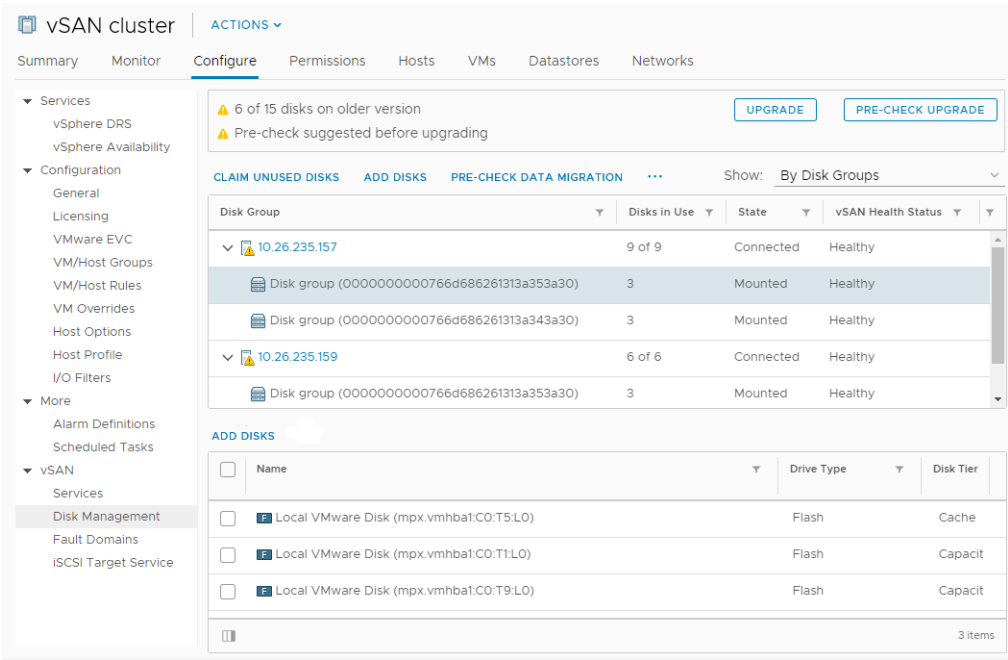
- Sorgen Sie bei einem Upgrade eines Clusters mit drei Hosts oder beim Upgrade eines Clusters mit begrenzten Ressourcen dafür, dass die virtuellen Maschinen in einem reduzierten Redundanzmodus betrieben werden können. Führen Sie den RVC-Befehl mit der Option `vsan.ondisk_upgrade --allow-reduced-redundancy` 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.

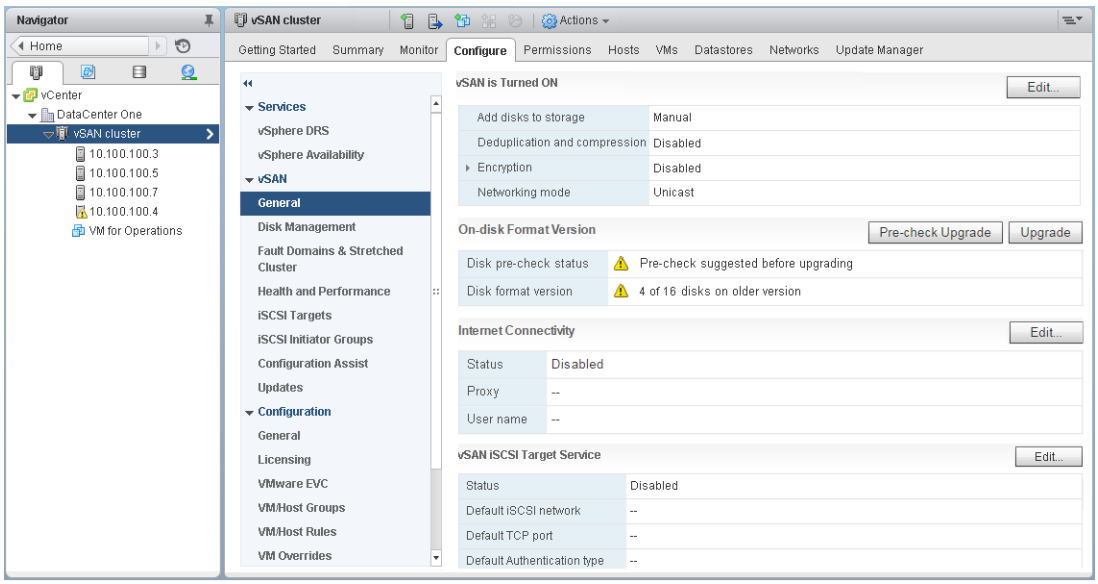
Ergebnisse

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 dem vSphere Web Client

Nachdem Sie ein Upgrade der vSAN-Hosts durchgeführt haben, können Sie das Upgrade des Festplattenformats durchführen.



Hinweis Wenn Sie die Verschlüsselung oder die Deduplizierung und Komprimierung auf einem vorhandenen vSAN-Cluster aktivieren, wird das Festplattenformat automatisch auf die neueste Version aktualisiert. Dieser Vorgang ist nicht erforderlich. Sie können die zweimalige Neuformatierung der Festplattengruppen vermeiden. Siehe Bearbeiten von vSAN-Einstellungen.

Voraussetzungen

- Stellen Sie sicher, dass Sie die aktualisierte Version von vCenter Server verwenden.
- Stellen Sie sicher, dass Sie die neueste Version von ESXi-Hosts verwenden.
- Stellen Sie sicher, dass die Festplatten einen ordnungsgemäßen Status aufweisen. Navigieren Sie in vSphere Web Client zur Seite „Festplattenverwaltung“, um den Objektstatus zu überprüfen.
- Stellen Sie sicher, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, zertifiziert und auf der VMware-Kompatibilitätshandbuch-Website unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind.

- Stellen Sie sicher, dass ausreichend freier Speicherplatz vorhanden ist, um das Upgrade des Festplattenformats durchzuführen. Führen Sie den RVC-Befehl `vsan.whatif_host_failures` aus, um festzustellen, ob ausreichend Kapazität zum Abschließen des Upgrades vorhanden ist, oder um eine Neuerstellung der Komponenten vorzunehmen, falls beim Upgrade ein Fehler auftritt.
- Stellen Sie sicher, dass sich Ihre Hosts nicht im Wartungsmodus befinden. Versetzen Sie Ihre Hosts beim Upgrade des Festplattenformats nicht in den Wartungsmodus. 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. Siehe „Überwachen der Neusynchronisierungsaufgaben im vSAN-Cluster“ in *vSAN-Überwachung und -Fehlerbehebung*.

Verfahren

1. Navigieren Sie im vSphere Web Client zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter vSAN die Option **Allgemein**.
4. (Optional) Klicken Sie unter **Datenträgerformat-Version** auf **Upgrade der Vorabprüfung**.

   Die Vorabprüfung zum Upgrade analysiert den Cluster, um Probleme aufzudecken, die ein erfolgreiches Upgrade möglicherweise verhindern. Einige der überprüften Punkte sind der Hoststatus, der Festplattenstatus, der Netzwerkstatus und der Objektstatus. Upgradeprobleme werden im Textfeld **Status der Festplattenvorabprüfung** angezeigt.
5. Klicken Sie unter **Datenträgerformat-Version** auf **Upgrade**.
6. Klicken Sie im Dialogfeld „Upgrade“ auf **Ja**, um das Upgrade des Festplattenformats durchzuführen.

Ergebnisse

vSAN erstellt jede Festplattengruppe im Cluster neu. Die Spalte „Datenträgerformat-Version“ zeigt die Festplattenformat-Version der Speichergeräte im Cluster an. Die Spalte **Datenträger mit veralteter Version** zeigt die Anzahl der Geräte an, die das neue Format verwenden. Bei erfolgreichem Upgrade lautet die Anzahl der **Datenträger mit veralteter Version** 0 (null).

Wenn beim Upgrade ein Fehler auftritt, können Sie die Seite „Neusynchronisieren von Komponenten“ im vSphere Web Client aufrufen. Warten Sie, bis die gesamte Neusynchronisierung abgeschlossen ist, und führen Sie das Upgrade erneut aus. Sie können die Cluster-Integrität auch mit dem Integritätsdienst überprüfen. Wenn Sie alle bei den Integritätsprüfungen aufgetretenen Fehler behoben haben, können Sie das Upgrade erneut ausführen.

Upgrade des vSAN-Festplattenformats mit RVC

Nachdem Sie ein Upgrade der vSAN-Hosts durchgeführt haben, können Sie die RVC (Ruby vSphere Console) verwenden, um mit dem Upgrade des Festplattenformats fortzufahren.

Voraussetzungen

- Stellen Sie sicher, dass Sie die aktualisierte Version von vCenter Server verwenden.
- Stellen Sie sicher, dass auf den ESXi-Hosts im vSAN-Cluster Version 6.5 oder höher ausgeführt wird.
- Stellen Sie sicher, dass die Festplatten auf der Seite „Festplattenverwaltung“ 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**.

Die aktuelle Festplattenformatversion wird oben auf der Seite angezeigt.

Überprüfen des vSAN-Cluster-Upgrades

Das vSAN-Cluster-Upgrade ist erst abgeschlossen, wenn Sie sich vergewissert haben, dass Sie die neueste Version von vSphere verwenden und dass vSAN zur Nutzung zur Verfügung steht.

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 8-3. Optionen des Upgradebefehls

Optionen	Beschreibung
`--hosts_and_clusters`	Hiermit geben Sie die Pfade zu allen Hostsystemen im Cluster oder den Computing-Ressourcen des Clusters an.
`--ignore-objects, -i`	Hiermit überspringen Sie das vSAN-Objektupgrade. Sie können mit dieser Befehlsoption auch die Versionsaktualisierung von Objekten eliminieren. Bei Verwendung dieser Befehlsoption verwenden Objekte weiterhin die aktuelle Version des Festplattenformats.
`--allow-reduced-redundancy, -a`	Mit dieser Option entfernen Sie die Anforderung, dass die Menge an freiem Speicherplatz während des Festplatten-Upgrades der Größe einer Festplattengruppe entsprechen muss. Mit dieser Option werden virtuelle Maschinen während des Upgrades in einem Modus mit reduzierter Redundanz betrieben. Das bedeutet, dass bestimmte virtuelle Maschinen möglicherweise vorübergehend keine Fehler tolerieren und dass ein Ausfall zu Datenverlust führen kann. vSAN stellt die vollständige Übereinstimmung und Redundanz nach Abschluss des Upgrades wieder her.
`--force, -f`	Verwenden Sie diese Option, um „force-proceed“ zu aktivieren und alle Bestätigungsanfragen automatisch zu beantworten.
`--help, -h`	Hiermit werden die Hilfeoptionen angezeigt.

Informationen zum Verwenden der RVC-Befehle finden Sie im *Referenzhandbuch zu RVC-Befehlen*.

vSAN-Build-Empfehlungen für vSphere Update Manager

vSAN generiert System-Baselines und Baseline-Gruppen, die mit vSphere Update Manager verwendet werden. Sie können diese empfohlenen Baselines verwenden, um Software, Patches und Erweiterungen für Hosts in Ihrem vSAN-Cluster zu aktualisieren.

vSAN 6.6.1 und höher generiert automatisierte Build-Empfehlungen für vSAN-Cluster. vSAN kombiniert Informationen im VMware-Kompatibilitätshandbuch und im vSAN-Versionskatalog mit Informationen zu den installierten ESXi-Versionen. Diese empfohlenen Updates stellen die beste verfügbare Version bereit, um die Hardware in einem unterstützten Status zu halten.

System-Baselines für vSAN 6.7.1 und höher 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 Update Manager so konfigurieren, dass Build-Empfehlungen nur für die aktuelle ESXi-Version oder für die neueste unterstützte ESXi-Version generiert werden. Eine Build-Empfehlung für die aktuelle Version enthält alle Patches und Treiber-Updates für diese Version.

vSAN-System-Baselines

vSAN-Build-Empfehlungen werden über vSAN-System-Baselines für Update Manager bereitgestellt. Diese System-Baselines werden von vSANverwaltet. Sie sind schreibgeschützt und können nicht angepasst werden.

vSAN generiert eine Baseline-Gruppe für jeden vSAN-Cluster. vSAN-System-Baselines werden im Bereich **Baselines** der Registerkarte „Baselines und Gruppen“ aufgelistet. Sie können weiterhin Ihre eigenen Baselines erstellen und standardisieren.

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. Update 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 Update Manager keine System-Baseline empfehlen.

Update Manager prüft automatisch jeden vSAN-Cluster, um die Übereinstimmung anhand der Baseline-Gruppe zu überprüfen. Um ein Upgrade Ihres Clusters durchzuführen, müssen Sie die System-Baseline manuell über den Update Manager standardisieren. Sie können die vSAN-System-Baseline auf einem einzelnen Host oder auf dem gesamten Cluster standardisieren.

vSAN-Versionskatalog

Der vSAN-Versionskatalog verwaltet Informationen zu verfügbaren Versionen, zur bevorzugten Reihenfolge der Versionen und zu kritischen Patches, die für die jeweilige Version erforderlich sind. Der vSAN-Versionskatalog wird in der VMware Cloud gehostet.

vSAN benötigt für den Zugriff auf den Versionskatalog eine Internetverbindung. Sie müssen nicht beim Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für vSAN registriert sein, um Zugriff auf den Versionskatalog zu erhalten.

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

Arbeiten mit vSAN-Build-Empfehlungen

Update 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 Update 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 Update 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 6.0 Update 2 aus, und die Hardware ist in der HCL für 6.0 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 6.7 Update 3 unterstützt. vSAN empfiehlt ein Upgrade auf Version 6.7 Update 3.

Beispiel 3

Ein vSAN-Cluster führt Version 6.0 Update 2 aus, und die Hardware ist nicht in der HCL für diese Version enthalten. vSAN empfiehlt ein Upgrade auf Version 6.7 Update 3, obwohl die Hardware nicht in der HCL für 6.7 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 6.0 Update 2 aus, und die Hardware ist in der HCL für 6.0 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 6.7 Update 3 unterstützt, wobei die ausgewählte Baseline-Einstellung nur für Patches gilt. vSAN empfiehlt ein Upgrade auf Version 6.0 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 My VMware an.
- Das VMware-Kompatibilitätshandbuch oder der vSAN-Versionskatalog wird aktualisiert.

Die Systemdiagnose für die vSAN-Build-Empfehlung zeigt den aktuellen Build an, der für den vSAN-Cluster empfohlen wird. Sie kann Sie auch bezüglich etwaiger Probleme mit der Funktion warnen.

Systemanforderungen

Update Manager muss auf Windows-vCenter Servermanuell installiert werden.

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

vSAN erfordert gültige Anmeldedaten zum Herunterladen von ISO-Images für Upgrades aus My VMware. Für Hosts, auf denen Version 6.0 Update 1 und früher ausgeführt wird, müssen Sie für die Eingabe der My VMware-Anmeldedaten RVC verwenden. Für Hosts, auf denen eine höhere Version der Software ausgeführt wird, können Sie sich über die Systemdiagnose für die ESX-Build-Empfehlung anmelden.

Führen Sie zum Eingeben der My VMware-Anmeldedaten über RVC den folgenden Befehl aus:
`vsan.login_iso_depot -u` *<Benutzername>* **`-p`** *<Kennwort>*