Verwalten von VMware vSAN

Update 3

VMware vSphere 8.0
VMware vSAN 8.0

vmware
by Broadcom

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

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

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

Inhalt

Informationen zum Verwalten von VMware vSAN

In *Verwalten von VMware vSAN* wird beschrieben, wie Sie einen vSAN-Cluster in einer VMware vSphere®-Umgebung konfigurieren und verwalten.

Darüber hinaus wird in *Verwalten von VMwarevSAN* erläutert, wie die lokalen physischen Speicherressourcen, die als Speicherkapazitätsgeräte in einem vSAN-Cluster dienen, verwaltet werden und wie Speicherrichtlinien für virtuelle Maschinen, die für vSAN-Datenspeicher bereitgestellt werden, definiert werden.

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

Zielgruppe

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

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

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

Aktualisierte Informationen

1

Dieses Dokument wird mit jeder Produktversion oder bei Bedarf aktualisiert.

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

Revision	Beschreibung
25. Juli 2024	■ Die Lizenzierungsinformationen für vSAN Max in Freigeben von Remote-vSAN-Datenspeichern wurden aktualisiert. ■ Informationen zum Wiederherstellen gelöschter VMs wurden in Wiederherstellen einer VM aus einem vSAN-Snapshot hinzugefügt. ■ Weitere kleinere Updates.
25. Juni 2024	Erstversion.

Was ist vSAN?

2

Bei VMware vSAN handelt es sich um eine Software-Ebene, die nativ als Teil des ESXi-Hypervisors ausgeführt wird.

vSAN fasst lokale oder direkt angeschlossene Kapazitätsgeräte eines Hostclusters zusammen und erstellt einen einzelnen Speicherpool, der von allen Hosts im vSAN-Cluster verwendet wird. vSAN unterstützt VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, wie etwa HA, vMotion und DRS. Dadurch wird ein externer gemeinsam genutzter Speicher überflüssig, und außerdem werden die Speicherkonfiguration und Aktivitäten zum Bereitstellen von virtuellen Maschinen vereinfacht.

Lesen Sie als Nächstes die folgenden Themen:

- vSAN-Konzepte
- vSAN-Begriffe und -Definitionen
- Unterschiede zwischen vSAN und herkömmlichem Speicher

vSAN-Konzepte

VMware vSAN verwendet einen softwaredefinierten Ansatz zum Erstellen von gemeinsam genutztem Speicher für virtuelle Maschinen.

Mit VMware Virtual SAN werden die lokalen physischen Speicherressourcen von ESXi-Hosts virtualisiert und in Speicherpools verwandelt, die unterteilt und virtuellen Maschinen und Anwendungen gemäß ihren Servicequalitätsanforderungen zugewiesen werden können. vSAN ist direkt im ESXi-Hypervisor implementiert.

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

Sie können vSAN auf vorhandenen Host-Clustern und beim Erstellen neuer Cluster aktivieren. vSAN fasst alle verfügbaren lokalen Kapazitätsgeräte zu einem einzelnen, von allen Hosts im vSAN-Cluster gemeinsam genutzten Datenspeicher zusammen. Sie können den Datenspeicher erweitern, indem Sie dem Cluster Kapazitätsgeräte oder Hosts mit Kapazitätsgeräten hinzufügen. vSAN funktioniert am besten, wenn alle ESXi-Hosts im Cluster bei allen Clustermitgliedern ähnliche oder identische Konfigurationen zu verwenden, einschließlich

ähnlicher oder identischer Speicherkonfigurationen. Mit dieser konsistenten Konfiguration werden ausgeglichene Speicherkomponenten der virtuellen Maschine auf allen Geräten und Hosts im Cluster sichergestellt. Die Hosts ohne lokale Geräte können auch teilnehmen und ihre virtuellen Maschinen im Datenspeicher von vSAN ausführen.

In der vSAN Original Storage Architecture (OSA) muss jeder Host, der Speichergeräte zum vSAN-Datenspeicher beiträgt, mindestens ein Gerät für den Flash-Cache und mindestens ein Gerät für die Kapazität bereitstellen. Die Geräte auf dem beitragenden Host bilden eine oder mehrere Datenträgergruppen. Jede Datenträgergruppe enthält ein Flash-Zwischenspeichergerät und ein oder mehrere Kapazitätsgeräte für dauerhaften Speicher. Jeder Host kann für die Verwendung mehrerer Datenträgergruppen konfiguriert werden.

In der vSAN Express Storage Architecture (ESA) tragen alle von vSAN beanspruchten Speichergeräte zur Kapazität und Leistung bei. Die von vSAN beanspruchten Speichergeräte eines jeden Hosts bilden einen Speicherpool. Der Speicherpool stellt die Menge an Caching und Kapazität dar, die der Host für den vSAN-Datenspeicher bereitstellt.

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

Merkmale von vSAN

Die folgenden Merkmale gelten für vSAN sowie für die zugehörigen Cluster und Datenspeicher.

vSAN enthält zahlreiche Funktionen zum Hinzufügen von Ausfallsicherheit und Effizienz in Ihrer Datenverarbeitungs- und Speicherumgebung.

Tabelle 2-1. Funktionen von vSAN

Unterstützte Funktionen	Beschreibung
Unterstützung von gemeinsam genutztem Speicher	vSAN unterstützt VMware-Funktionen, die gemeinsam genutzten Speicher erfordern, wie HA, vMotion und DRS. Beispiel: Wenn ein Host überlastet wird, kann DRS die virtuellen Maschinen zu anderen Hosts im Cluster migrieren.
On-Disk-Format	Das vSAN-Format für virtuelle Datenträgerdateien unterstützt für jeden vSAN-Cluster eine stark skalierbare Snapshot- und Klonverwaltung. Informationen zur Anzahl der pro vSAN-Cluster unterstützten VM-Snapshots und -Klone finden Sie unter *Maximalwerte für die Konfiguration von vSphere* https://configmax.esp.vmware.com/home.
Reine Flash- und Hybrid-Konfigurationen	vSAN kann für reine Flash- oder Hybrid-Cluster konfiguriert werden.
Fehlerdomänen	vSAN unterstützt das Konfigurieren von Fehlerdomänen, um Hosts vor Rack- oder Gehäuseausfällen zu schützen, wenn der vSAN-Cluster sich über mehrere Racks oder Blade-Server-Gehäuse in einem Datencenter erstreckt.
Dateidienst	Mit dem vSAN-Dateidienst können Sie Dateifreigaben im vSAN-Datenspeicher erstellen, auf die Client-Arbeitsplätze oder VMs zugreifen können.

Tabelle 2-1. Funktionen von vSAN (Fortsetzung)

Unterstützte Funktionen	Beschreibung
iSCSI-Zieldienst	Mit dem iSCSI-Zieldienst von vSAN können Hosts und physische Arbeitslasten, die sich außerhalb des vSAN-Clusters befinden, auf den vSAN-Datenspeicher zugreifen.
vSAN Stretched Cluster und vSAN-Cluster mit zwei Knoten	vSAN unterstützt Stretched Cluster, die sich über zwei geografische Standorte erstrecken.
Unterstützung für Windows Server Failover Cluster (WSFC)	vSAN 6.7 Update 3 und höher bietet Unterstützung für dauerhafte SCSI-3-Reservierungen (SCSI-3 Persistent Reservations, SCSI3-PR) auf der Ebene eines virtuellen Datenträgers, die von Windows Server Failover Cluster (WSFC) benötigt wird, um Zugriff auf einen gemeinsamen Datenträger zwischen Knoten zu vermitteln. Aufgrund der Unterstützung von SCSI-3 PRs kann WSFC mit einer Datenträgerressource konfiguriert werden, die zwischen VMs auf vSAN-Datenspeichern nativ freigegeben wird. Aktuell werden die folgenden Konfigurationen unterstützt: ■ Maximal 6 Anwendungsknoten pro Cluster. ■ Maximal 64 freigegebene virtuelle Datenträger pro Knoten. **Hinweis** Microsoft SQL Server 2012 oder höher unter Microsoft Windows Server 2012 oder höher wurde für vSAN qualifiziert.
vSAN-Integritätsdienst	Der vSAN-Integritätsdienst enthält vorkonfigurierte Tests zur Systemdiagnoseprüfung, um die Ursache von Problemen bei Clusterkomponenten zu überwachen, zu beheben und zu diagnostizieren und um potenzielle Risiken zu erkennen.
vSAN-Leistungsdienst	Der vSAN-Leistungsdienst beinhaltet statistische Diagramme, die zum Überwachen von IOPS, Durchsatz, Latenz und Überlastung verwendet werden. Sie können die Leistung eines Clusters, Hosts, einer Datenträgergruppe, eines Datenträgers und von VMs von vSAN überwachen.
Integration in vSphere-Speicherfunktionen	vSAN ist in den vSphere-Datenverwaltungsfunktionen integriert, die ursprünglich mit dem VMFS- und NFS-Speicher verwendet wurden. Zu diesen Funktionen gehören Snapshots, verknüpfte Klone und vSphere Replication.
VM-Speicherrichtlinien	vSAN arbeitet mit VM-Speicherrichtlinien, um einen VM-zentrierten Ansatz für die Speicherverwaltung zu unterstützen. Wenn Sie während der Bereitstellung keine Speicherrichtlinie zuweisen, wird der VM automatisch die Standardspeicherrichtlinie für vSAN zugewiesen.
Schnelle Bereitstellung	vSAN ermöglicht eine schnelle Bereitstellung von Speicher in vCenter Server® während der Erstellung und Bereitstellung einer virtuellen Maschine.

Tabelle 2-1. Funktionen von vSAN (Fortsetzung)

Unterstützte Funktionen	Beschreibung
Deduplizierung und Komprimierung	vSAN führt Deduplizierung und Komprimierung auf Blockebene durch, um Speicherplatz zu sparen. Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-All-Flash-Cluster aktivieren, werden redundante Daten innerhalb jeder Datenträgergruppe reduziert. Deduplizierung und Komprimierung sind als clusterweite Einstellung aktiviert, die Anwendung der Funktionen erfolgt jedoch auf Datenträgergruppenbasis. vSAN nur mit Komprimierung wird auf Datenträgerebene angewendet.
Verschlüsselung ruhender Daten	vSAN bietet Verschlüsselung ruhender Daten. Die Daten werden verschlüsselt, nachdem alle anderen Verarbeitungsvorgänge, z. B. die Deduplizierung, durchgeführt wurden. Die Verschlüsselung ruhender Daten schützt Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.
Verschlüsselung in Übertragung begriffener Daten	vSAN kann in der Übertragung begriffene Daten zwischen den Hosts im Cluster verschlüsseln. Wenn Sie die Verschlüsselung in Übertragung begriffener Daten aktivieren, verschlüsselt vSAN den gesamten Daten- und Metadatenverkehr zwischen Hosts.
SDK-Unterstützung	Das VMware vSAN SDK stellt eine Erweiterung des VMware vSphere Management SDK dar. Es enthält die Dokumentation, Bibliotheken und Codebeispiele, mit denen Entwickler die Installation, Konfiguration, Überwachung und Fehlerbehebung von vSAN automatisieren können.

vSAN-Begriffe und -Definitionen

vSAN führt bestimmte wichtige Begriffe und Definitionen ein.

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

Datenträgergruppe (vSAN Original Storage Architecture)

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

Jede Datenträgergruppe muss über ein Flash-Cache-Gerät und mindestens ein Kapazitätsgerät verfügen. Die für das Caching verwendeten Geräte können nicht über Datenträgergruppen hinweg oder für andere Verwendungszwecke freigegeben werden. Jedes einzelne Caching-Gerät muss für eine einzige Datenträgergruppe dediziert sein. In Hybrid-Clustern werden Flash-Geräte für die Cache-Ebene verwendet. Magnetdatenträger werden hingegen für die Speicherkapazitätsschicht verwendet. In einem reinen Flash-Cluster werden Flash-Geräte für Cache und Kapazität verwendet. Informationen zum Erstellen und Verwalten von Datenträgerngruppen finden Sie unter *Verwalten von VMware vSAN*

Speicherpool (vSAN Express Storage Architecture)

Ein Speicherpool ist eine Darstellung aller Speichergeräte auf einem Host, die von vSAN beansprucht werden. Jeder Host enthält einen Speicherpool. Jedes Gerät im Speicherpool trägt sowohl Kapazität als auch Leistung bei. Die Anzahl der zulässigen Speichergeräte wird durch die Hostkonfiguration bestimmt.

Benötigte Kapazität

Menge an physischer Kapazität, die von einer oder mehreren virtuellen Maschinen zu einem bestimmten Zeitpunkt benötigt wird. Viele Faktoren bestimmen die verbrauchte Kapazität, einschließlich der verbrauchten Größe Ihrer `.vmdk`-Dateien, der Schutzreplikate usw. Die für die Schutzreplikate verwendete Kapazität ist bei der Berechnung der Cachegröße nicht zu berücksichtigen.

Objektbasierter Speicher

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

Hinweis Wenn vSAN Express Storage Architecture aktiviert ist, ist nicht jeder Snapshot ein neues Objekt. Eine Basis-`.vmdk` und ihre Snapshots sind in einem vSAN-Objekt enthalten. Darüber hinaus wird der Digest in vSAN ESA von vSAN-Objekten gestützt.

Wenn vSAN ein Objekt für einen virtuellen Datenträger erstellt und festlegt, wie das Objekt im Cluster verteilt werden soll, werden die folgenden Parameter berücksichtigt:

- vSAN stellt sicher, dass die Anforderungen an den virtuellen Datenträger entsprechend den festgelegten VM-Speicherrichtlinieneinstellungen angewendet werden.
- vSAN überprüft, ob zum Zeitpunkt der Bereitstellung die richtigen Clusterressourcen verwendet werden. Beispielsweise bestimmt vSAN anhand der Schutzrichtlinie die Anzahl der zu erstellenden Replikate. Die Leistungsrichtlinie ermittelt die Menge des jedem Replikat zugeordneten Flash-Lesecache und bestimmt, wie viele Stripes für jedes Replikat erstellt und wo diese im Cluster gespeichert werden.

- vSAN überwacht ständig den Status der Richtlinieneinhaltung des virtuellen Datenträgers und erstellt Berichte dazu. Wenn Sie einen nicht konformen Richtlinienstatus finden, müssen Sie das zugrunde liegende Problem diagnostizieren und beheben.

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

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

vSAN-Datenspeicher

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

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

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

Objekte und Komponenten

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

Ein vSAN-Datenspeicher enthält die folgenden Objekttypen:

VM-Home-Namespace

Das Home-Verzeichnis der virtuellen Maschine, in dem alle Konfigurationsdateien der virtuellen Maschine gespeichert sind, z. B. `.vmx`-Dateien, Protokolldateien, `.vmdk`-Dateien und Snapshot-Delta-Beschreibungsdateien.

VMDK

Eine Datenträgerdatei für eine virtuelle Maschine oder `.vmdk` speichert die Inhalte eines Festplattenlaufwerks einer virtuellen Maschine.

VM-Auslagerungsobjekt

Wird beim Einschalten einer virtuellen Maschine erstellt.

Snapshot-Delta-VMDKs

Werden beim Erstellen von VM-Snapshots angelegt. Solche Delta-Datenträger werden nicht für vSAN Express Storage Architecture erstellt.

Arbeitsspeicherobjekt

Wird beim Erstellen oder Anhalten einer virtuellen Maschine erstellt, wenn die Arbeitsspeicher-Snapshot-Option aktiviert ist.

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

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

Komponentenzustand: Die Zustände „Herabgestuft“ und „Abwesend“

vSAN erkennt die folgenden Fehlerzustände für Komponenten:

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

Objektzustand: „Ordnungsgemäß“ und „Nicht ordnungsgemäß“

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

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

Witness

Ein Witness ist eine Komponente, die nur Metadaten und keine eigentlichen Anwendungsdaten enthält. Wenn eine Entscheidung hinsichtlich der Verfügbarkeit der verbleibenden Datenspeicherkomponenten nach einem potenziellen Ausfall getroffen werden muss, dient der Witness als Entscheidungskriterium. Ein Zeuge verbraucht etwa 2 MB Speicherplatz für Metadaten auf dem vSAN-Datenspeicher, wenn das Datenträgerformat 1.0 verwendet wird, und 4 MB bei Datenträgerformat-Version 2.0 und höher.

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

Speicherrichtlinienbasierte Verwaltung (SPBM)

Wenn Sie vSAN verwenden, können Sie Speicheranforderungen für virtuelle Maschinen wie Leistung und Verfügbarkeit in Form einer Richtlinie definieren. vSAN sorgt dafür, dass den in vSAN-Datenspeichern bereitgestellten virtuellen Maschinen mindestens eine VM-Speicherrichtlinie zugewiesen wird. Wenn Sie die Speicheranforderungen Ihrer virtuellen Maschinen kennen, können Sie benutzerdefinierte Speicherrichtlinien definieren und diese Ihren virtuellen Maschinen zuweisen. Wenn Sie bei der Bereitstellung virtueller Maschinen keine Speicherrichtlinie anwenden, weist vSAN automatisch eine vSAN-Standardrichtlinie zu, die Folgendes festlegt: **Zu tolerierende Fehler** mit dem Wert „1“, ein einziger Datenträger-Stripe für jedes Objekt und ein per Thin Provisioning bereitgestellter virtueller Datenträger. Um die besten Ergebnisse zu erzielen, definieren Sie Ihre eigenen VM-Speicherrichtlinien, selbst wenn die Anforderungen der Richtlinie denjenigen entsprechen, die in der Standardspeicherrichtlinie definiert sind. Informationen zur Arbeit mit vSAN-Speicherrichtlinien finden Sie unter *Verwalten von VMware vSAN*.

vSphere PowerCLI

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

Unterschiede zwischen vSAN und herkömmlichem Speicher

vSAN weist zwar viele gemeinsame Merkmale mit herkömmlichen Speicher-Arrays auf, aber das Verhalten und die Funktionsweise von vSAN sind insgesamt unterschiedlich.

Beispielsweise kann vSAN nur ESXi-Hosts verwalten und verwenden, während eine einzelne vSAN-Instanz einen einzelnen Datenspeicher für den Cluster bereitstellt.

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

- vSAN benötigt keinen externen Netzwerkspeicher für die Remotespeicherung von VM-Dateien, wie beispielsweise auf einem Fibre Channel (FC) oder einem Storage Area Network (SAN).

- Bei Verwendung von herkömmlichem Speicher teilt der Speicheradministrator vorab Speicherplatz auf unterschiedlichen Speichersystemen zu. vSAN konvertiert die lokalen physischen Speicherressourcen der ESXi-Hosts automatisch in einen einzelnen Speicherpool. Diese Pools können unterteilt und virtuellen Maschinen und Anwendungen gemäß ihren Servicequalitätsanforderungen zugewiesen werden.
- vSAN verhält sich nicht wie herkömmliche Speichervolumes, die auf LUNs oder NFS-Freigaben basieren. Der iSCSI-Zieldienst verwendet LUNs zum Aktivieren eines Initiators auf einem Remotehost zum Transportieren von Daten auf Blockebene zu einem Speichergerät im vSAN-Cluster.
- Einige Standardspeicherprotokolle, z. B. FCP, gelten für vSAN nicht.
- vSAN ist nahtlos in vSphere integriert. Im Gegensatz zu herkömmlichem Speicher benötigen Sie für vSAN keine separaten Plug-Ins bzw. keine Speicherkonsole. vSAN können Sie mit dem vSphere Client bereitstellen, verwalten und überwachen.
- vSAN muss nicht von einem eigens dafür vorgesehenen Speicheradministrator verwaltet werden. Stattdessen kann ein vSphere-Administrator eine vSAN-Umgebung verwalten.
- Mit vSAN werden VM-Speicherrichtlinien automatisch zugewiesen, wenn Sie neue VMs bereitstellen. Die Speicherrichtlinien können bei Bedarf dynamisch geändert werden.

Erstellen eines vSAN-Clusters

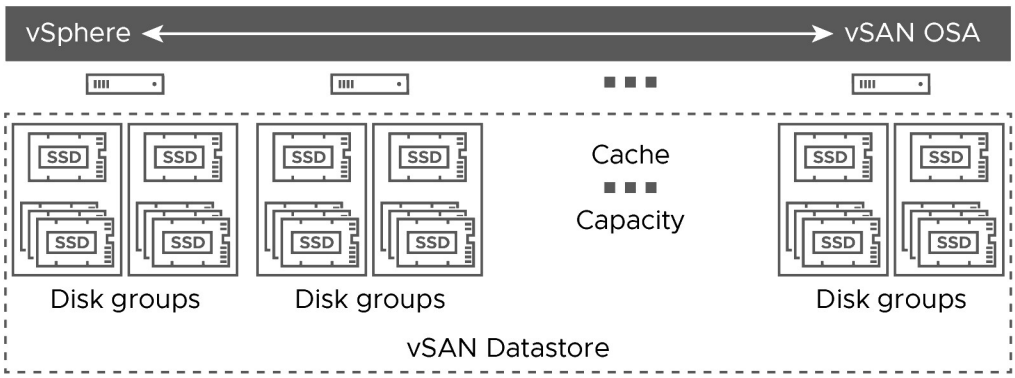
3

Sie können die Speicherarchitektur und die Bereitstellungsoption beim Erstellen eines vSAN-Clusters auswählen.

Wählen Sie die vSAN-Speicherarchitektur aus, die ihren Ressourcen und Ihren Anforderungen am besten entspricht.

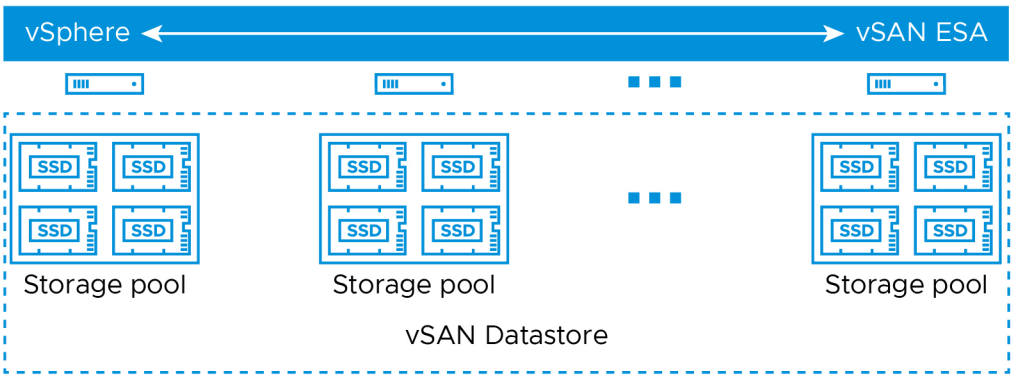
vSAN Original Storage Architecture

vSAN Original Storage Architecture (OSA) wurde für eine Vielzahl von Speichergeräten entwickelt, einschließlich Flash-Solid-State- (SSD) und Magnetdatenträgerlaufwerken (HDD). Jeder Host, der Speicher bereitstellt, enthält eine oder mehrere Datenträgergruppen. Jede Datenträgergruppe enthält ein Flash-Cache- und mindestens ein Kapazitätsgerät.



vSAN Express Storage Architecture

vSAN Express Storage Architecture (ESA) ist für leistungsstarke NVMe-basierte TLC-Flash-Geräte und Hochleistungsnetzwerke konzipiert. Jeder Host, der Speicher bereitstellt, enthält einen einzelnen Speicherpool mit vier oder mehr Flash-Geräten. Jedes Flash-Gerät stellt dem Cluster Zwischenspeicher und Kapazität zur Verfügung.



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

vSAN ReadyNode

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

Benutzerdefinierter vSAN-Cluster

Sie können einen vSAN-Cluster erstellen, indem Sie einzelne Software- und Hardwarekomponenten wie Treiber, Firmware und Speicher-E/A-Controller auswählen, die auf der VMware-Kompatibilitätshandbuch-Website (vSAN Compatibility Guide, VCG) unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind. Sie können beliebige Server, Speicher-E/A-Controller, Kapazitäts- und Flash-Cache-Geräte, Arbeitsspeicher, eine beliebige Anzahl von erforderlichen Kernen pro CPU auswählen, die auf der VCG-Website zertifiziert und aufgelistet sind. Lesen Sie die Kompatibilitätsinformationen auf der VCG-Website durch, bevor Sie Software- und Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller, die von vSAN unterstützt werden, auswählen. Verwenden Sie beim Entwerfen eines vSAN-Clusters nur Geräte, Firmware und Treiber, die auf der VCG-Website aufgelistet sind. Die Verwendung von Software- und Hardwareversionen, die nicht auf der VCG-Website aufgelistet sind, kann zu Clusterfehlern oder unerwarteten Datenverlusten führen. Informationen zum Entwerfen eines vSAN-Clusters finden Sie unter „Entwerfen und Dimensionieren eines vSAN-Clusters“ in *vSAN-Planung und Bereitstellung*.

Lesen Sie als Nächstes die folgenden Themen:

- vSAN-Bereitstellungsoptionen

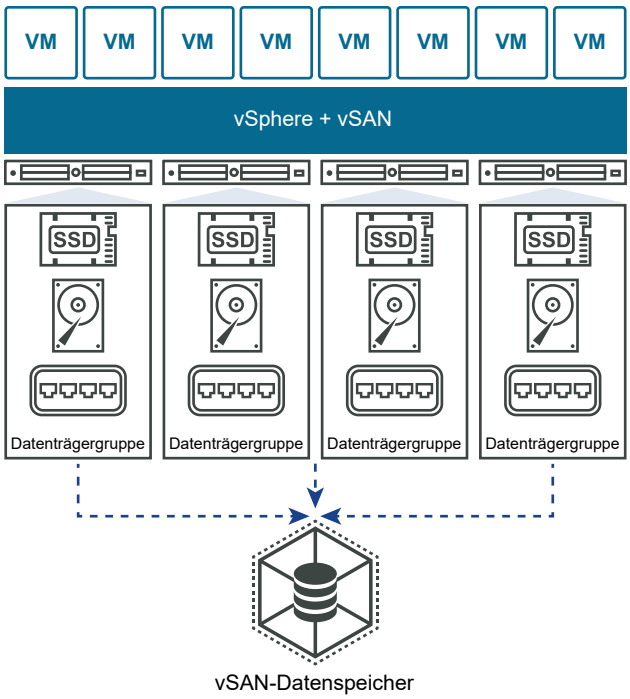
vSAN-Bereitstellungsoptionen

In diesem Abschnitt werden die unterstützten Bereitstellungsoptionen für vSAN-Cluster behandelt.

vSAN-Cluster mit einer Site

Ein vSAN-Cluster mit einer Site besteht aus mindestens drei Hosts. In der Regel befinden sich alle Hosts in einem vSAN-Cluster mit einer Site auf einer einzelnen Site und sind mit demselben Schicht-2-Netzwerk verbunden. Reine Flash-Konfigurationen erfordern 10-GBit-Netzwerkverbindungen, und die vSAN Express Storage Architecture erfordert 25-GBit-Netzwerkverbindungen.

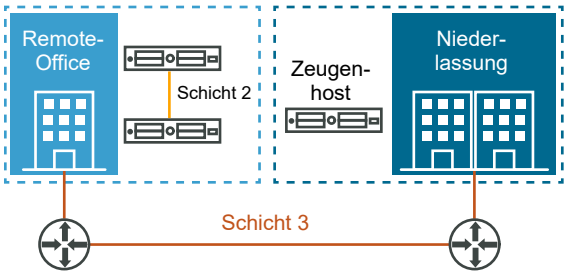
Weitere Informationen finden Sie unter Erstellen eines vSAN-Clusters mit einer Site.



vSAN-Cluster mit zwei Knoten

vSAN-Cluster mit zwei Knoten werden häufig für Remote-Niederlassungen/Zweigbüros verwendet, die in der Regel eine geringe Anzahl Arbeitslasten mit erforderlicher Hochverfügbarkeit aufweisen. Ein vSAN-Cluster mit zwei Knoten besteht aus zwei Hosts an demselben Standort, die mit demselben Netzwerk-Switch oder direkt verbunden sind. Sie können einen vSAN-Cluster mit zwei Knoten konfigurieren, der einen dritten Host als Zeugen nutzt. Dieser Zeugenhost kann sich an einem Remote-Standort, beispielsweise einer Niederlassung, befinden. In der Regel befindet sich der Whitness am Hauptstandort, neben dem vCenter-Server.

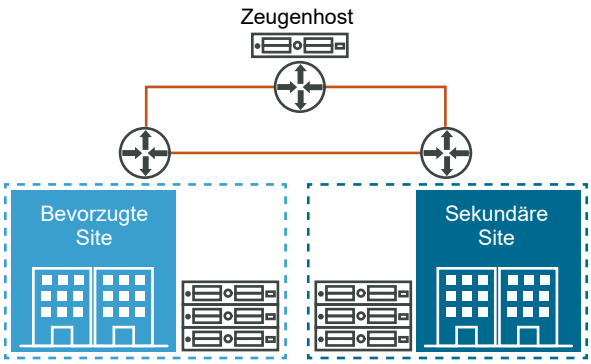
Weitere Informationen finden Sie unter Erstellen eines vSAN Stretched Clusters oder eines Clusters mit zwei Knoten.



Stretched vSAN-Cluster

Ein ausgeweiteter vSAN-Cluster bietet Ausfallsicherheit gegen den Verlust einer ganzen Site. Die Hosts in einem vSAN Stretched Cluster werden gleichmäßig auf zwei Sites verteilt. Die beiden Sites müssen über eine Netzwerklatenz von nicht mehr als fünf Millisekunden (5 ms) verfügen. Ein vSAN-Zeugenhost befindet sich an einer dritten Site, um die Zeugenfunktion bereitzustellen. Der Zeuge fungiert zudem als Tie-Breaker in Szenarien, in denen eine Netzwerkpartition zwischen den beiden Datensites generiert wird. Nur Metadaten, wie z. B. Witness-Komponenten, sind auf dem Witness gespeichert.

Weitere Informationen finden Sie unter Erstellen eines vSAN Stretched Clusters oder eines Clusters mit zwei Knoten.



Integrieren von vSAN in andere VMware-Software

4

Wenn vSAN betriebsbereit ist, erfolgt die Integration in den restlichen VMware-Software-Stack.

Mithilfe der vSphere-Komponenten und -Funktionen wie etwa vSphere vMotion, Snapshots, Klone, Distributed Resource Scheduler (DRS), vSphere High Availability, VMware Site Recovery Manager usw. können Sie weitgehend dieselben Aufgaben wie mit herkömmlichen Speicherlösungen ausführen.

vSphere HA

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

VMware Horizon View

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

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

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

Einschränkungen von vSAN

5

In diesem Thema werden die Einschränkungen von vSAN behandelt.

Wenn Sie mit vSAN arbeiten, beachten Sie folgende Einschränkungen:

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

Konfigurieren und Verwalten eines vSAN-Clusters

6

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

Lesen Sie als Nächstes die folgenden Themen:

- Konfigurieren eines Clusters für vSAN mit dem vSphere Client
- Aktivieren von vSAN für einen vorhandenen Cluster
- vSAN Ausschalten
- Bearbeiten von vSAN-Einstellungen
- Anzeigen des vSAN-Datenspeichers
- Hochladen von Dateien oder Ordnern in vSAN-Datenspeicher
- Herunterladen von Dateien oder Ordnern aus vSAN-Datenspeichern

Konfigurieren eines Clusters für vSAN mit dem vSphere Client

Sie können den vSphere Client verwenden, um vSAN auf einem bestehenden Cluster zu konfigurieren.

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

Voraussetzungen

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

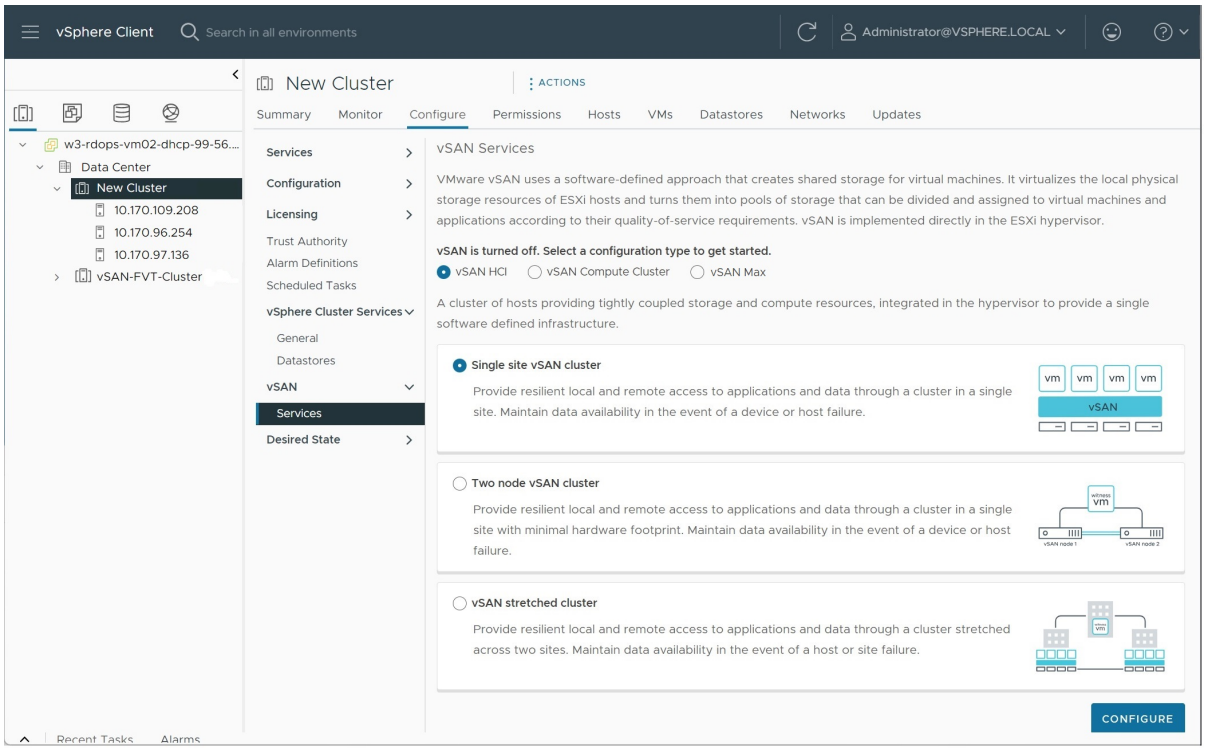
Erstellen Sie einen Cluster und fügen Sie dem Cluster Hosts hinzu, bevor Sie vSAN aktivieren und konfigurieren. Konfigurieren Sie die Porteigenschaften auf jedem Host, um den vSAN-Dienst hinzuzufügen.

Verfahren

1 Navigieren Sie zu einem vorhandenen Host-Cluster.

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

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



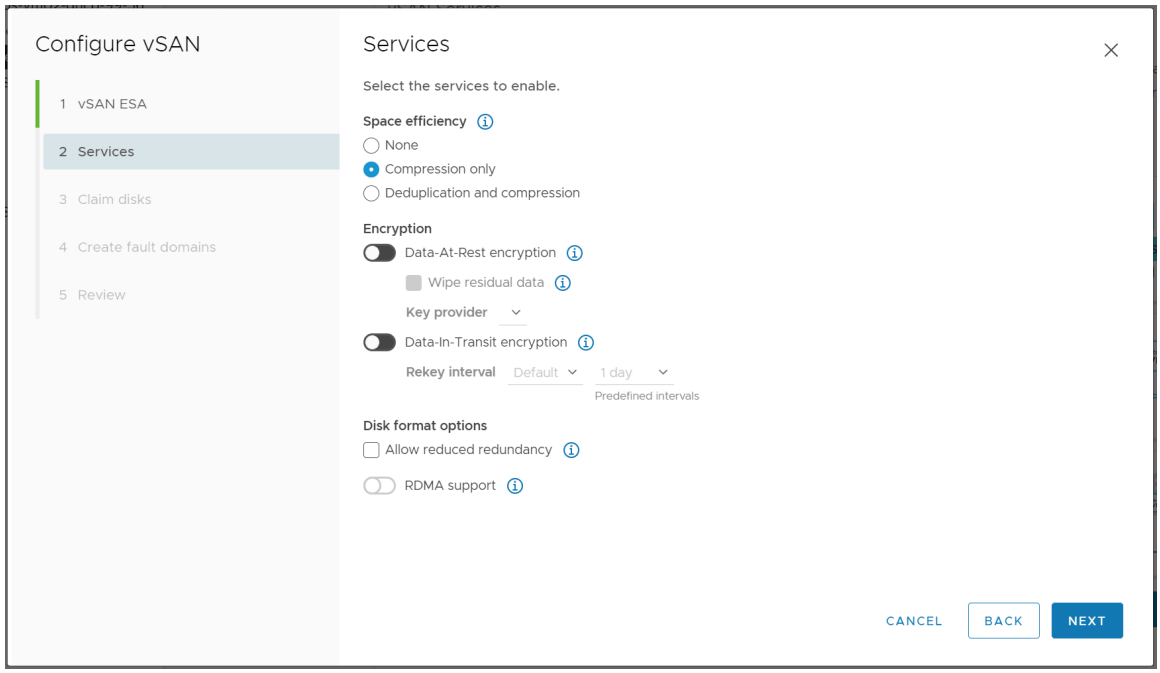
a Wählen Sie einen HCI-Konfigurationstyp aus.

- **vSAN HCI** stellt Computing- und Speicherressourcen bereit. Der Datenspeicher kann von Clustern im selben Datencenter und von Remote-vCentern verwalteten Clustern gemeinsam genutzt werden.
- **vSAN-Computing-Cluster** stellt nur vSphere-Computing-Ressourcen bereit. Er kann Datenspeicher mounten, die von vSAN Max-Clustern im selben Datencenter und von Remote-vCentern bereitgestellt werden.

- **vSAN Max** (vSAN ESA-Cluster) stellt Speicherressourcen, aber keine Computing-Ressourcen bereit. Der Datenspeicher kann von Client-vSphere-Clustern und vSAN-Clustern im selben Datencenter und von Remote-vCentern gemountet werden.

b Wählen Sie eine Bereitstellungsoption aus (vSAN-Cluster mit einer Site, vSAN-Cluster mit zwei Knoten oder vSAN Stretched Cluster).

c Klicken Sie auf **Konfigurieren**, um den Assistenten „vSAN konfigurieren“ zu öffnen.



4 Wählen Sie vSAN ESA aus, wenn Ihr Cluster kompatibel ist, und klicken Sie auf **Weiter**.

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

Konfigurieren Sie Datenverwaltungsfunktionen, einschließlich Deduplizierung und Komprimierung, Verschlüsselung ruhender Daten und Verschlüsselung in Übertragung begriffener Daten. Wählen Sie RDMA (Remote Direct Memory Access) aus, wenn Ihr Netzwerk dies unterstützt.

6 Beanspruchen Sie Datenträger für den vSAN-Cluster, und klicken Sie auf **Weiter**.

Bei der vSAN Original Storage Architecture (vSAN OSA) benötigt jeder Host, der Speicher bereitstellt, mindestens ein Flash-Gerät für den Cache und ein oder mehrere Geräte für die Kapazität. Bei vSAN Express Storage Architecture (vSAN ESA) benötigt jeder Host, der Speicher bereitstellt, ein oder mehrere Flash-Geräte.

7 Erstellen Sie Fehlerdomänen, um Hosts zu gruppieren, die gleichzeitig ausfallen können.

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

Ergebnisse

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

Nächste Schritte

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.

Aktivieren von vSAN für einen vorhandenen Cluster

Sie können vSAN auf einem vorhandenen Cluster aktivieren und Funktionen und Dienste konfigurieren.

Voraussetzungen

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

Verfahren

1. Navigieren Sie zu einem vorhandenen Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
   a. Wählen Sie einen Konfigurationstyp aus (vSAN-Cluster mit einer Site, vSAN-Cluster mit zwei Knoten oder vSAN Stretched Cluster).
   b. Wählen Sie **Ich benötige einen lokalen vSAN-Datenspeicher** aus, wenn Sie Datenträgergruppen oder Speicherpools zu den Clusterhosts hinzufügen möchten.
   c. Klicken Sie auf **Konfigurieren**, um den Assistenten „vSAN konfigurieren“ zu öffnen.
4. Wählen Sie vSAN ESA aus, wenn Ihr Cluster kompatibel ist, und klicken Sie auf **Weiter**.
5. Konfigurieren Sie die zu verwendenden vSAN-Dienste, und klicken Sie auf **Weiter**.

   Konfigurieren Sie Datenverwaltungsfunktionen, einschließlich Deduplizierung und Komprimierung, Verschlüsselung ruhender Daten und Verschlüsselung in Übertragung begriffener Daten. Wählen Sie RDMA (Remote Direct Memory Access) aus, wenn Ihr Netzwerk dies unterstützt.

6 Beanspruchen Sie Datenträger für den vSAN-Cluster, und klicken Sie auf **Weiter**.

   Bei der vSAN Original Storage Architecture (vSAN OSA) benötigt jeder Host, der Speicher bereitstellt, mindestens ein Flash-Gerät für den Zwischenspeicher und ein oder mehrere Geräte für die Kapazität. Bei vSAN Express Storage Architecture (vSAN ESA) benötigt jeder Host, der Speicher bereitstellt, ein oder mehrere Flash-Geräte.

7 Erstellen Sie Fehlerdomänen, um Hosts zu gruppieren, die gleichzeitig ausfallen können.

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

vSAN Ausschalten

Sie können vSAN für einen Host-Cluster deaktivieren.

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

Voraussetzungen

Stellen Sie sicher, dass sich die Hosts im Wartungsmodus befinden. Weitere Informationen finden Sie unter Versetzen eines Mitglieds des Clusters für vSAN in den Wartungsmodus.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

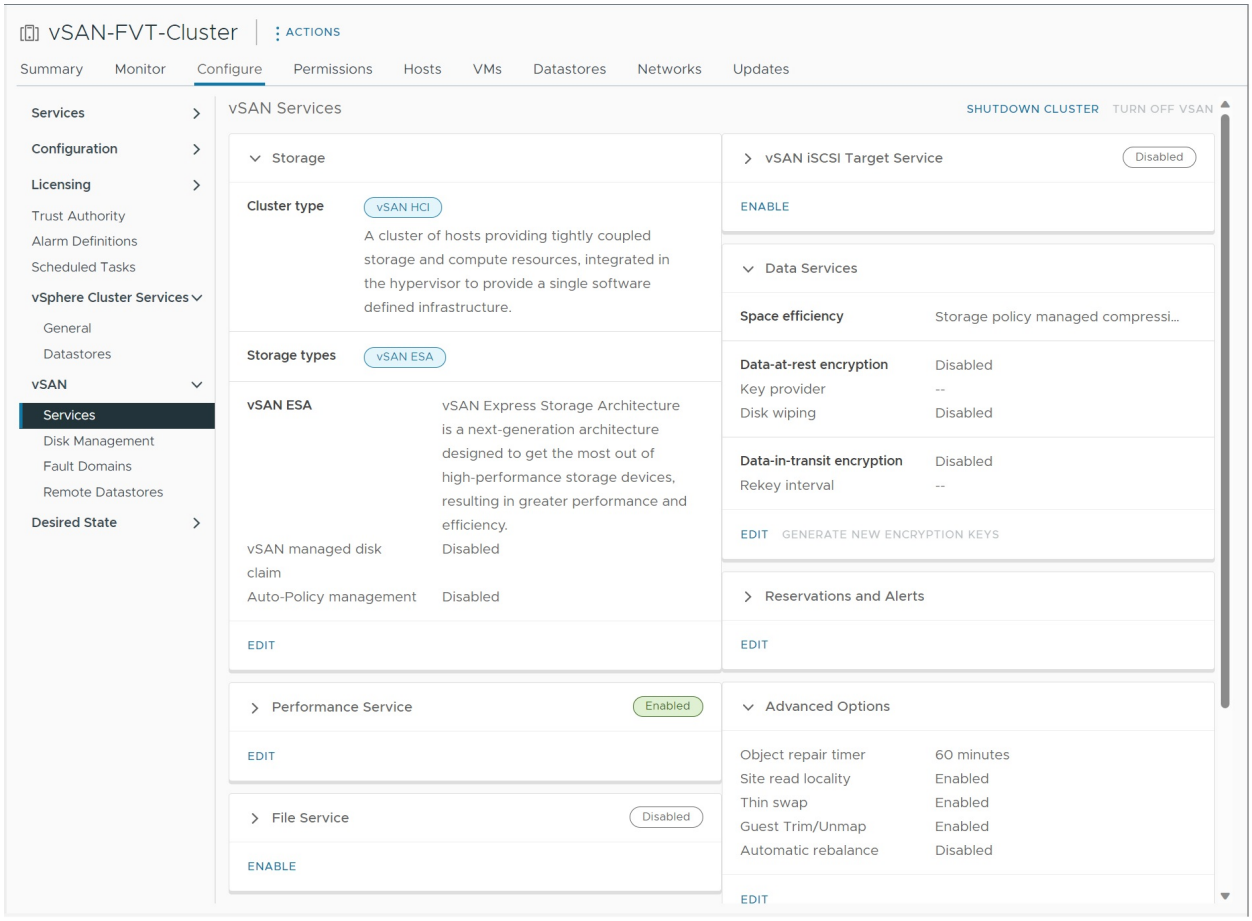
4 Klicken Sie auf **vSAN ausschalten**.

5 Bestätigen Sie Ihre Auswahl im Dialogfeld „vSAN ausschalten“.

Bearbeiten von vSAN-Einstellungen

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

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



Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

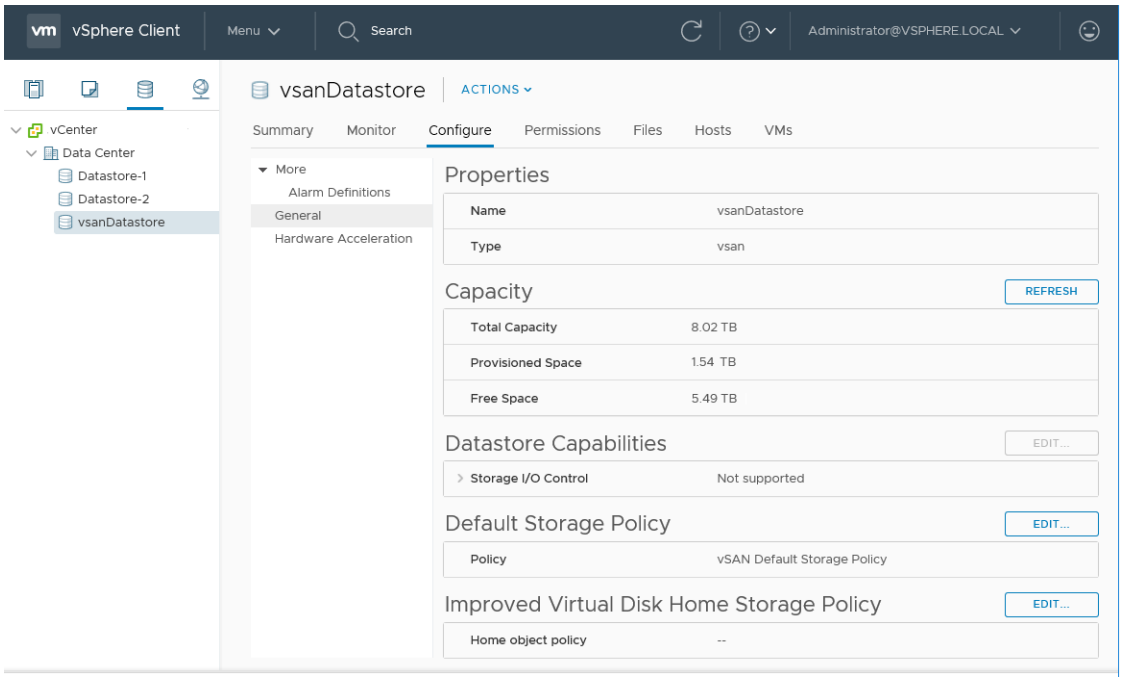
      - Konfigurieren Sie den Speicher. Klicken Sie auf **Remote-Datenspeicher bereitstellen**, um Speicher aus anderen vSAN-Clustern zu verwenden.
      - Konfigurieren Sie den vSAN-Leistungsdienst. Weitere Informationen finden Sie unter „Überwachen der vSAN-Leistung“ in *vSAN-Überwachung und -Fehlerbehebung*.
      - Aktivieren Sie den Dateidienst. Weitere Informationen finden Sie unter „vSAN-Dateidienst“ unter *Verwalten von VMware vSAN*.
      - Konfigurieren Sie vSAN-Netzwerkoptionen. Weitere Informationen finden Sie unter „Konfigurieren des vSAN-Netzwerks“ in *vSAN-Planung und -Bereitstellung*.
      - Konfigurieren Sie den iSCSI-Zieldienst. Weitere Informationen finden Sie unter „Verwenden des vSAN-iSCSI-Zieldiensts“ in *Verwalten von VMware vSAN*.
      - Konfigurieren Sie Datendienste, einschließlich Deduplizierung und Komprimierung, Verschlüsselung ruhender Daten und Verschlüsselung in Übertragung begriffener Daten.
      - Konfigurieren Sie vSAN Data Protection. Bevor Sie vSAN Data Protection verwenden können, müssen Sie den vSAN Snapshot Service bereitstellen. Weitere Informationen finden Sie unter „Bereitstellen der Snapshot Service-Appliance“ in *Verwalten von VMware vSAN*.
      - Konfigurieren Sie Kapazitätsreservierungen und -warnungen. Weitere Informationen finden Sie unter „Übersicht über reservierte Kapazität“ in *vSAN-Überwachung und -Fehlerbehebung*.
      - Konfigurieren Sie erweiterte Optionen:
         - Objektreparatur-Timer
         - Site-Lesebelegung für vSAN Stretched Cluster
         - Bereitstellung von Thin-Auslagerung
         - Unterstützung großer Cluster für maximal 64 Hosts
         - Automatische Neuverteilung
      - Aktivieren Sie den vSAN-Verlaufsintegritätsdienst.

   c Ändern Sie die Einstellungen Ihren Anforderungen entsprechend.

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

Anzeigen des vSAN-Datenspeichers

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



Voraussetzungen

Konfigurieren Sie vSAN und Datenträgergruppen oder Speicherpools.

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 Magnetdatenträger für die Kapazität verwendet.

   Ein Teil der Kapazität wird für Metadaten zugeteilt.

   - Version 1.0 des Datenträgerformats fügt etwa 1 GB pro Kapazitätsgerät hinzu.
   - Version 2.0 des Datenträgerformats fügt Kapazitäts-Overhead hinzu, normalerweise nicht mehr als 1-2 Prozent Kapazität pro Gerät.

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

Nächste Schritte

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

Hochladen von Dateien oder Ordnern in vSAN-Datenspeicher

Sie können VMDK-Dateien in einen vSAN-Datenspeicher hochladen.

Sie können auch Ordner in einen vSAN-Datenspeicher hochladen. Weitere Informationen zu Datenspeichern finden Sie unter *vSphere Storage*. Wenn Sie eine VMDK-Datei in einen vSAN-Datenspeicher hochladen, gelten die folgenden Überlegungen:

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

Verfahren

1 Navigieren Sie zum vSAN-Datenspeicher.

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

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

7

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.

Lesen Sie als Nächstes die folgenden Themen:

- Informationen zu vSAN-Richtlinien
- Vorgehensweise zur Verwaltung von Richtlinienänderungen in vSAN
- Anzeigen von vSAN-Speicheranbietern
- Definition der vSAN-Standardspeicherrichtlinien
- Ändern der Standardspeicherrichtlinie für vSAN-Datenspeicher
- Definieren einer Speicherrichtlinie für vSAN mit dem vSphere Client

Informationen zu vSAN-Richtlinien

vSAN-Speicherrichtlinien definieren Speicheranforderungen für virtuelle Maschinen.

Diese Richtlinien legen fest, wie die VM-Speicherobjekte bereitgestellt und innerhalb des Datenspeichers zugeteilt werden, um den erforderlichen Service-Level zu garantieren. Wenn Sie vSAN auf einem Host-Cluster aktivieren, wird ein einzelner vSAN-Datenspeicher erstellt und dem Datenspeicher wird eine standardmäßige Speicherrichtlinie zugeteilt.

Wenn Sie die Speicheranforderungen Ihrer virtuellen Maschinen kennen, können Sie eine Speicherrichtlinie erstellen, die die vom Datenspeicher angekündigten Funktionen referenziert. Sie können mehrere Richtlinien erstellen, um verschiedene Anforderungstypen bzw. -klassen zu erfassen.

Jeder in vSAN-Datenspeichern bereitgestellten virtuellen Maschinen wird mindestens eine VM-Speicherrichtlinie zugewiesen. Speicherrichtlinien können Sie beim Erstellen oder Bearbeiten von virtuellen Maschinen zuweisen.

Hinweis Falls Sie einer virtuellen Maschine keine Speicherrichtlinie zuweisen, weist vSAN eine Standardrichtlinie zu. Bei der Standardrichtlinie ist der Wert für **Zu tolerierende Fehler** auf 1 festgelegt und sie hat einen einzelnen Datenträger-Stripe pro Objekt sowie einen schnell (thin) bereitgestellten virtuellen Datenträger.

Das VM-Auslagerungsobjekt und das VM-Snapshot-Arbeitsspeicherobjekt sind an die einer VM zugeordneten Speicherrichtlinien gebunden, wobei **Zu tolerierende Fehler** auf „1“ festgelegt ist. Sie weisen nicht dieselbe Verfügbarkeit wie andere Objekte auf, denen eine Richtlinie mit einem anderen Wert für **Zu tolerierende Fehler** zugewiesen wurde.

Hinweis Wenn vSAN Express Storage Architecture aktiviert ist, ist nicht jeder Snapshot ein neues Objekt. Eine Basis-VMDK und ihre Snapshots sind in einem vSAN-Objekt enthalten. Darüber hinaus wird in vSAN ESA der Digest durch ein vSAN-Objekt gesichert. Dies unterscheidet sich von vSAN Original Storage Architecture.

Tabelle 7-1. Speicherrichtlinie – Verfügbarkeit

Funktionalität	Beschreibung
Zu tolerierende Fehler (Failures to Tolerate, FTT)	Definiert die Anzahl von Host- und Gerätefehlern, die ein Objekt einer virtuellen Maschine tolerieren kann. Für `n` tolerierte Fehler werden alle geschriebenen Daten an `n+1` Stellen gespeichert. Dazu zählen auch Paritätskopien bei Verwendung von RAID-5 oder RAID-6. 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. Sie können eine Datenreplikationsmethode auswählen, die für Leistung oder Kapazität optimiert ist. RAID-1 (Spiegelung) verwendet mehr Datenträgerspeicher, um die Objektkomponenten zu platzieren. Die Verwendung dieser Option führt jedoch zu verbesserter Leistung beim Zugriff auf die Objekte. RAID-5/6 (Erasure Coding) verwendet weniger Datenträgerspeicher, die Leistung nimmt jedoch ab. Sie können eine der folgenden Optionen auswählen: ■ **Keine Datenredundanz**: Geben Sie diese Option an, wenn vSAN eine einzelne Spiegelkopie von VM-Objekten nicht schützen soll. Dies bedeutet, dass Ihre Daten ungeschützt sind und Sie möglicherweise Daten verlieren, wenn beim vSAN-Cluster ein Gerätefehler auftritt. Beim Host können 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. ■ **Keine Datenredundanz mit Hostaffinität**: Geben Sie diese Option nur an, wenn Sie vSAN-SNA-Arbeitslasten (Shared Nothing Architecture) auf der vSAN-Datenpersistenzplattform ausführen möchten. ■ **1 Fehler – RAID-1 (Spiegelung)**: Geben Sie diese Option an, wenn Ihr VM-Objekt einen Host- oder Gerätefehler tolerieren kann. Zum Schutz eines VM-Objekts mit 100 GB durch RAID-1 (Spiegelung) mit einem FTT von 1 werden 200 GB benötigt. ■ **1 Fehler – RAID-5 (Erasure Coding)**: Geben Sie diese Option an, wenn Ihr VM-Objekt einen Host- oder Gerätefehler tolerieren kann. Für vSAN OSA: Zum Schutz eines VM-Objekts von 100 GB durch RAID-5 (Erasure Coding) mit einem FTT von 1 werden 133,33 GB benötigt. **Hinweis** Wenn Sie vSAN Express Storage Architecture verwenden, erstellt vSAN basierend auf der Clustergröße ein optimiertes RAID-5-Format. Wenn die Anzahl der Hosts im Cluster kleiner als 6 ist, erstellt vSAN ein RAID-5-Format (2+1). Wenn die Anzahl der Hosts größer als 6 ist, erstellt vSAN ein RAID-6 (4+1)-Format. Wenn der Cluster größer oder kleiner wird, passt vSAN das Format 24 Stunden nach der Konfigurationsänderung automatisch wieder an. ■ **2 Fehler – RAID-1 (Spiegelung)**: Geben Sie diese Option an, wenn Ihr VM-Objekt bis zu zwei Gerätefehler tolerieren kann. Da Sie mit RAID-1 (Spiegelung) einen FTT-Wert von 2 benötigen, entsteht ein Kapazitäts-Overhead. Zum Schutz eines VM-Objekts mit 100 GB durch RAID-1 (Spiegelung) mit einem FTT von 2 werden 300 GB benötigt.

Tabelle 7-1. Speicherrichtlinie – Verfügbarkeit (Fortsetzung)

Funktionalität	Beschreibung
	■ **2 Fehler – RAID-6 (Erasure Coding)**: Geben Sie diese Option an, wenn Ihre VM-Objekte bis zu zwei Gerätefehler tolerieren können. Zum Schutz eines VM-Objekts von 100 GB durch RAID-6 (Erasure Coding) mit einem FTT von 2 werden 150 GB benötigt. Weitere Informationen finden Sie unter Verwenden von RAID 5- oder RAID 6-Erasure Coding in einem vSAN-Cluster. ■ **3 Fehler – RAID-1 (Spiegelung)**: Geben Sie diese Option an, wenn Ihre VM-Objekte bis zu drei Gerätefehler tolerieren können. Zum Schutz eines VM-Objekts mit 100 GB durch RAID-1 (Spiegelung) mit einem FTT von 3 werden 400 GB benötigt. **Hinweis** Wenn Sie eine Speicherrichtlinie erstellen und keinen Wert für **FTT** angeben, erstellt vSAN eine einzelne Spiegelkopie der VM-Objekte. Sie kann einen einzelnen Ausfall tolerieren. Wenn allerdings mehrere Komponenten ausfallen, sind Ihre Daten möglicherweise gefährdet.
Ausfalltoleranz von Site	Diese Regel legt fest, ob ein Standard-, Stretched- oder 2-Knoten-Cluster verwendet werden soll. Bei Verwendung eines vSAN Stretched Clusters können Sie festlegen, ob die Daten an beiden Sites oder nur an einer Site gespiegelt werden. Bei einem vSAN Stretched Cluster können Sie die Daten auf der bevorzugten oder sekundären Site für Hostaffinität aufbewahren. ■ **Keine – Standardcluster** ist der Standardwert. Dies bedeutet, dass es keine Site-Ausfalltoleranz gibt. ■ **Hostspiegelung – Cluster mit zwei Knoten** definiert die Anzahl zusätzlicher Fehler, die ein Objekt tolerieren kann, nachdem die mit FTT definierte Anzahl von Fehlern erreicht ist. vSAN führt eine Objektspiegelung auf Datenträgerebene durch. Jeder Datenhost muss über mindestens drei Datenträgergruppen oder drei Datenträger in einem Speicherpool verfügen, um diese Regel verwenden zu können. ■ **Site-Spiegelung – Stretched Cluster** definiert die Anzahl der zusätzlichen Hostfehler, die ein Objekt tolerieren kann, nachdem die mit FTT definierte Anzahl von Fehlern erreicht ist. ■ **Null – Daten auf der bevorzugten Site aufbewahren (Stretched Cluster)**. Wenn die Objekte in einem vSAN Stretched Cluster nicht über Site-Ausfalltoleranz verfügen sollen und Sie die Objekte nur an der Site zugänglich machen möchten, die als bevorzugt konfiguriert ist, verwenden Sie diese Option. ■ **Null – Daten auf der sekundären Site aufbewahren (Stretched Cluster)**. Wenn die Objekte in einem vSAN Stretched Cluster nicht über Site-Ausfalltoleranz verfügen sollen und Sie die Objekte nur auf der sekundären Site zugänglich machen möchten, verwenden Sie diese Option. Diese Objekte sind nicht von den Ausfällen des Inter-Switch Link (ISL) oder des Zeugenhosts betroffen. Sie bleiben zugänglich, wenn auf die von der Richtlinie ausgewählte Site zugegriffen werden kann. ■ **Null – Stretched Cluster**. Wenn Sie diese Option wählen, garantiert vSAN nicht, dass auf die Objekte zugegriffen werden kann, wenn eine der Sites ausfällt. Solche Objekte können zu viel ISL-Bandbreite verbrauchen und die Latenz für Objekte erhöhen, die

Tabelle 7-1. Speicherrichtlinie – Verfügbarkeit (Fortsetzung)

Funktionalität	Beschreibung
	die Richtlinie für die Site-Spiegelung verwenden. Verwenden Sie diese Richtlinie nur, wenn Sie die anderen Richtlinien während eines vorübergehenden Zustands, bei dem eine Kapazitätsbeschränkung (CPU/Arbeitsspeicher/Speicher) im Cluster besteht, nicht verwenden können.

Tabelle 7-2. Speicherrichtlinie – Speicherregeln

Funktionalität	Beschreibung
Verschlüsselungsdienste	Definiert die Verschlüsselungsoptionen für die VMs, die Sie in Ihrem Datenspeicher bereitstellen. Wählen Sie eine der folgenden Optionen aus: ■ **Verschlüsselung ruhender Daten**: Geben Sie diese Option an, wenn Sie die Verschlüsselung auf die Daten anwenden möchten, die in Ihrem Datenspeicher gespeichert sind. ■ **Keine Verschlüsselung**: Geben Sie diese Option an, wenn Sie keine Verschlüsselung auf Ihre Daten anwenden möchten. ■ **Keine Voreinstellung**: Geben Sie diese Option an, wenn Sie keine Verschlüsselungsregeln explizit anwenden möchten. Durch Auswahl dieser Option wendet vSAN beide Regeln auf Ihre VMs an.
Speicherplatzeffizienz	Definiert die Speichereffizienzoptionen für die VMs, die Sie in Ihrem Datenspeicher bereitstellen. Wählen Sie eine der folgenden Optionen aus: ■ **Deduplizierung und Komprimierung**: Geben Sie diese Option an, wenn Sie sowohl Deduplizierung als auch Komprimierung für Ihre Daten anwenden möchten. ■ **Nur Komprimierung**: Geben Sie diese Option an, wenn Sie nur die Komprimierung auf Ihre Daten anwenden möchten. **Hinweis** Bei vSAN Original Storage Architecture ist die Komprimierung eine Einstellung auf Clusterebene. Bei vSAN Express Storage Architecture erfolgt „nur Komprimierung“ auf Objektebene. Dies bedeutet, dass Sie die Komprimierung für eine VM, aber nicht für eine andere VM im selben Cluster verwenden können. ■ **Keine Speicherplatzeffizienz**: Geben Sie diese Option an, wenn Sie keine Komprimierung auf Ihre Objekte anwenden möchten. ■ **Keine Voreinstellung**: Geben Sie diese Option an, wenn Sie explizit keine Regeln zum Platzsparen anwenden möchten. Durch Auswahl dieser Option wendet vSAN alle Regeln zum Platzsparen auf Ihre VMs an.
Speicherebene	Geben Sie die Storage-Ebene für alle VMs mit der definierten Speicherrichtlinie an. Wählen Sie eine der folgenden Optionen aus: ■ **All Flash**: Geben Sie diese Option an, wenn Sie Ihre VMs mit einer All-Flash-Umgebung kompatibel machen wollen. ■ **Hybrid**: Geben Sie diese Option an, wenn Sie Ihre VMs nur mit einer hybriden Umgebung kompatibel machen wollen. ■ **Keine Voreinstellung**: Geben Sie diese Option an, wenn Sie keine expliziten Regeln für die Speicherebene anwenden möchten. Durch Auswahl dieser Option macht vSAN die VMs sowohl mit Hybrid- als auch mit All-Flash-Umgebungen kompatibel.

Tabelle 7-3. Speicherrichtlinie – Erweiterte Richtlinienregeln

Funktionalität	Beschreibung
Anzahl der Datenträger-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 Datenträger-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.
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 eines Datenträgers 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.
Reservierter Objektspeicherplatz	Prozentsatz der logischen Größe des Datenträgerobjekts 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

Tabelle 7-3. Speicherrichtlinie – Erweiterte Richtlinienregeln (Fortsetzung)

Funktionalität	Beschreibung
Flash Read Cache-Reservierung (%)	Die als Lesecache reservierte Flash-Kapazität für das virtuelle Maschinenobjekt. Wird als Prozentsatz der logischen Größe des Datenträgerobjekts 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 Flash Read Cache-Reservierung wird nur für Hybrid Storage-Konfigurationen unterstützt. Verwenden Sie dieses Attribut nicht, wenn Sie eine VM-Speicherrichtlinie für einen All-Flash-Cluster oder für einen vSAN ESA-Cluster definieren. 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-Datenträgerspeicherplatz für zu viele Reservierungen verschwendet werden. Diese Cache-Reservierungen stehen dann nicht zur Verfügung, um die Arbeitslasten zu unterstützen, die zu gegebener Zeit den erforderlichen Speicherplatz benötigen. Diese Speicherverschwendung und Nichtverfügbarkeit können zu einem Leistungsabfall führen.

Tabelle 7-3. Speicherrichtlinie – Erweiterte Richtlinienregeln (Fortsetzung)

Funktionalität	Beschreibung
Objektprüfsumme	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. **Hinweis** Bei vSAN Express Storage Architecture ist die Objektprüfsumme immer aktiviert und kann nicht deaktiviert werden.
Bereitstellung erzwingen	Wenn die Option auf **Ja** festgelegt ist, wird das Objekt bereitgestellt, auch wenn die in der Speicherrichtlinie angegebenen Richtlinien für **Zu tolerierende Fehler**, **Anzahl der Datenträger-Stripes pro Objekt** und **Flash Read Cache-Reservierung** vom Datenspeicher nicht erfüllt werden können. Verwenden Sie diesen Parameter in Bootstrapping-Szenarien und bei Ausfällen, wenn keine Standardbereitstellung mehr möglich ist. 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.

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 *vSAN-Planung und -Bereitstellung*.

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 RAID-5-Richtlinie in RAID-6 auf einem Cluster mit fünf Hosts.

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

Anzeigen von vSAN-Speicheranbietern

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

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

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

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

```
https://<VC fqdn>:<VC https port>/vsan/vasa/version.xml
```

Überprüfen Sie, dass die Speicheranbieter registriert sind.

Verfahren

1 Navigieren Sie zu vCenter Server.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicheranbieter**.

Ergebnisse

Die Speicheranbieter für vSAN werden in der Liste aufgeführt.

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.

Definition der vSAN-Standardspeicherrichtlinien

Für vSAN muss den auf den vSAN-Datenspeichern bereitgestellten virtuellen Maschinen mindestens eine Speicherrichtlinie zugewiesen werden.

Wenn Sie bei der Bereitstellung einer virtuellen Maschine nicht explizit eine Speicherrichtlinie zuweisen, weist vSAN der virtuellen Maschine eine Standardspeicherrichtlinie zu. Jede Standardrichtlinie enthält vSAN-Regelsätze und einen Satz elementarer Speicherfunktionen, die in der Regel zur Platzierung von virtuellen Maschinen verwendet werden, die auf vSAN-Datenspeichern bereitgestellt wurden.

Tabelle 7-4. Spezifikationen für die vSAN-Standardspeicherrichtlinie

Spezifikation	Einstellung
Zu tolerierende Fehler	1
Anzahl der Datenträger-Stripes pro Objekt	1
Die Flash Read Cache-Reservierung oder die Flash-Kapazität für den Lesecache	0
Reservierter Objektspeicherplatz	0 **Hinweis** Durch das Festlegen des reservierten Objektspeicherplatzes auf 0 wird der virtuelle Datenträger standardmäßig schnell (thin) bereitgestellt.
Bereitstellung erzwingen	Nein

Wenn Sie einen vSAN Express Storage Architecture-Cluster verwenden, können Sie je nach Clustergröße eine der hier aufgeführten ESA-Richtlinien verwenden.

Tabelle 7-5. vSAN ESA-Spezifikationen für die Standardspeicherrichtlinie – RAID-5

Spezifikation	Einstellung
Zu tolerierende Fehler	1
Anzahl der Datenträger-Stripes pro Objekt	1
Die Flash Read Cache-Reservierung oder die Flash-Kapazität für den Lesecache	0
Reservierter Objektspeicherplatz	Thin Provisioning
Bereitstellung erzwingen	Nein

Hinweis RAID-5 in vSAN ESA unterstützt drei Hostcluster. Wenn Sie die automatische Richtlinienverwaltung aktivieren, muss der Cluster über vier Hosts verfügen, um RAID-5 verwenden zu können.

Tabelle 7-6. vSAN ESA-Spezifikationen für die Standardspeicherrichtlinie – RAID-6

Spezifikation	Einstellung
Zu tolerierende Fehler	2
Anzahl der Datenträger-Stripes pro Objekt	1
Die Flash Read Cache-Reservierung oder die Flash-Kapazität für den Lesecache	0
Reservierter Objektspeicherplatz	Thin Provisioning
Bereitstellung erzwingen	Nein

Hinweis Für RAID-6 sind mindestens 6 Hosts im Cluster erforderlich.

Sie können die Konfigurationseinstellungen für die VM-Standardspeicherrichtlinie prüfen, wenn Sie zu **VM-Speicherrichtlinien** > Name der Standardspeicherrichtlinie > **Regelsatz 1: VSAN** navigieren.

Um optimale Ergebnisse zu erzielen, sollten Sie Ihre eigenen VM-Speicherrichtlinien erstellen und verwenden, selbst wenn die Anforderungen der Richtlinie mit den in der Standardspeicherrichtlinie definierten identisch sind. In einigen Fällen müssen Sie bei dem Vergrößern eines Clusters die Standardspeicherrichtlinie ändern, um die Anforderungen des Service Level Agreements für VMware Cloud on AWS einzuhalten.

Wenn Sie einem Datenspeicher eine benutzerdefinierte Speicherrichtlinie zuweisen, wendet vSAN die Einstellungen für die benutzerdefinierte Richtlinie auf den angegebenen Datenspeicher an. Nur eine Speicherrichtlinie kann die Standardrichtlinie für den vSAN-Datenspeicher sein.

Merkmale der vSAN-Standardspeicherrichtlinie

Die folgenden Merkmale gelten für die Standardspeicherrichtlinien des vSAN-Datenspeichers.

- Eine Standardspeicherrichtlinie des vSAN-Datenspeichers 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 eine vSAN-Standardspeicherrichtlinie, wobei **Bereitstellung erzwingen** auf **Ja** festgelegt ist.

- Eine vSAN-Standardrichtlinie gilt nur für vSAN-Datenspeicher. Sie können eine Standardspeicherrichtlinie nicht auf Nicht-vSAN-Datenspeicher wie NFS- oder VMFS-Datenspeicher anwenden.
- Objekte in einem vSAN Express Storage Architecture-Cluster mit RAID 0- oder RAID 1-Konfiguration verfügen über 3 Datenträger-Stripes, obwohl die Standardrichtlinie nur 1 Datenträger-Stripe definiert.

- Weil die vSAN-Standardspeicherrichtlinie kompatibel mit 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 Standardspeicherrichtlinie nicht löschen.
- Eine Standardspeicherrichtlinie wird zugewiesen, wenn die beim Bereitstellen einer virtuellen Maschine zugewiesene Richtlinie keine spezifischen Regeln für vSAN enthält.

Automatische Richtlinienverwaltung

Cluster mit vSAN Express Storage Architecture können mithilfe der automatischen Richtlinienverwaltung eine optimale Standardspeicherrichtlinie generieren, die auf dem Clustertyp (Standard oder Stretched) und der Anzahl der Hosts basiert. vSAN konfiguriert die **Ausfalltoleranz von Site** und **Zu tolerierende Fehler** auf optimale Einstellungen für den Cluster.

Der Name der automatisch generierten Richtlinie basiert auf dem Clusternamen, wie folgt: *ClusterName – Optimale Standarddatenspeicherrichtlinie*

Wenn Sie die automatische Richtlinie aktivieren, weist vSAN dem vSAN-Datenspeicher eine neue optimale Richtlinie zu. Diese Richtlinie wird dann zur Standardrichtlinie des Datenspeichers für den Cluster.

Zum Aktivieren der automatischen Richtlinienverwaltung verwenden Sie den Schieberegler unter **vSAN > Dienste > Speicher > Bearbeiten**.

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.

Hinweis Sie können auch die verbesserte Home-Speicherrichtlinie für virtuelle Datenträger bearbeiten. Klicken Sie auf **Bearbeiten** und wählen Sie die Home-Speicherrichtlinie aus, die Sie als Speicherrichtlinie für das Home-Objekt 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**.

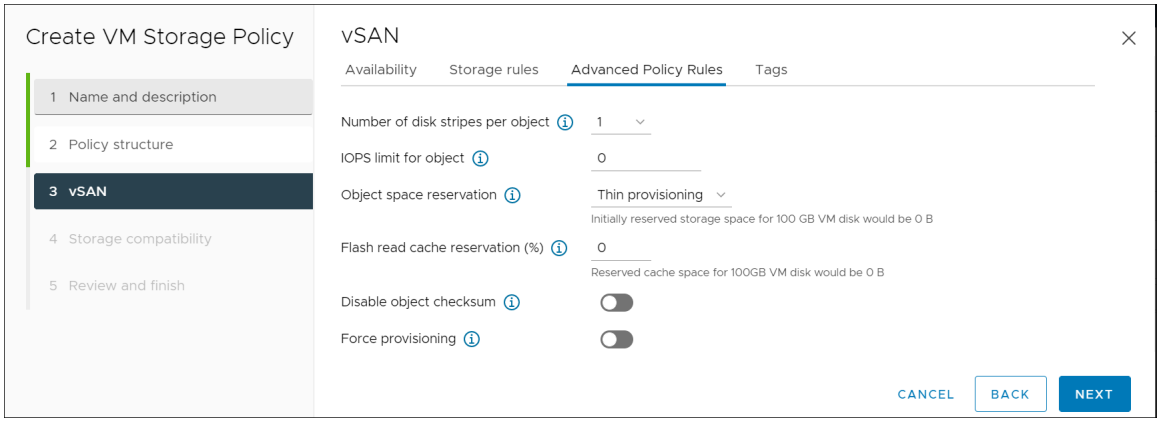
Die Speicherrichtlinie wird als Standardrichtlinie angewendet, wenn Sie neue virtuelle Maschinen bereitstellen, ohne für einen Datenspeicher explizit eine Speicherrichtlinie festzulegen.

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 Datenträger 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 finden Sie unter Anzeigen von vSAN-Speicheranbietern.
- Erforderliche Berechtigungen: **Profilgesteuerter Speicher.Ansicht des profilgesteuerten Speichers** und **Profilgesteuerter Speicher.Update des profilgesteuerten Speichers**

Hinweis Cluster mit vSAN Express Storage Architecture können die automatische Richtlinienverwaltung verwenden. Weitere Informationen finden Sie unter Definition der vSAN-Standardspeicherrichtlinien.

Verfahren

1. Navigieren Sie zu **Richtlinien und Profile** und klicken Sie anschließend auf **VM-Speicherrichtlinien**.
2. Klicken Sie auf **Erstellen**.
3. Wählen Sie auf der Seite „Name und Beschreibung“ einen vCenter Server aus.
4. Geben Sie einen Namen und eine Beschreibung für die Speicherrichtlinie ein und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite „Richtlinienstruktur“ die Option „Regeln für vSAN-Speicher aktivieren“ aus und klicken Sie auf **Weiter**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ergebnisse

Die neue Richtlinie wird zur Liste hinzugefügt.

Nächste Schritte

Weisen Sie diese Richtlinie einer virtuellen Maschine und deren virtuelle Datenträger 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

8

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

Lesen Sie als Nächstes die folgenden Themen:

- Erweitern eines vSAN-Clusters
- Freigeben von Remote-vSAN-Datenspeichern
- Arbeiten mit Mitgliedern des vSAN-Clusters im Wartungsmodus
- Verwalten von Fault Domains in vSAN-Clustern
- Verwenden von vSAN Data Protection
- Verwenden des vSAN-iSCSI-Zieldiensts
- vSAN-Dateidienst
- Migrieren eines hybriden vSAN-Clusters auf einen All-Flash-Cluster
- Herunterfahren und Neustarten des vSAN-Clusters

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.
- Verschieben Sie vorhandene ESXi-Hosts in den vSAN-Cluster und konfigurieren Sie sie mithilfe des Hostprofils. Siehe Konfigurieren von Hosts im vSAN-Cluster mithilfe des Hostprofils.
- Fügen Sie den ESXi-Hosts, die Clustermitglieder sind, neue Kapazitätsgeräte hinzu. Siehe Hinzufügen von Geräten zu einer Datenträgergruppe im vSAN-Cluster.

Erweitern der vSAN-Clusterkapazität und -leistung

Wenn in Ihrem vSAN-Cluster nicht genügend Speicherkapazität vorhanden ist oder Sie eine Leistungsbeeinträchtigung feststellen, können Sie die Kapazität und die Leistung des Clusters erhöhen.

- (Nur für vSAN Original Storage Architecture) Erweitern Sie die Speicherkapazität Ihres Clusters durch Hinzufügen von Speichergeräten zu vorhandenen Datenträgergruppen oder durch Hinzufügen von Datenträgergruppen. Für neue Datenträgergruppen sind Flash-Geräte für den Cache erforderlich. Informationen zum Hinzufügen von Geräten zu Datenträgergruppen finden Sie unter Hinzufügen von Geräten zu einer Datenträgergruppe im vSAN-Cluster. Durch das Hinzufügen von Kapazitätsgeräten ohne Erhöhung des Caches wird möglicherweise das Verhältnis von Cache und Kapazität auf ein nicht unterstütztes Maß reduziert. Weitere Informationen finden Sie unter *vSAN-Planung und -Bereitstellung*.

  Verbessern Sie die Clusterleistung, indem Sie einem vorhandenen Speicher-E/A-Controller oder einem neuen Host mindestens ein Flash-Cache-Gerät und ein Kapazitätsgerät (Flash- oder Magnetdatenträger) hinzufügen. Um dieselbe Auswirkung auf die Leistung zu erzielen, können Sie einen oder mehrere Hosts mit Datenträgergruppen hinzufügen, nachdem vSAN eine automatische Neuverteilung im vSAN-Cluster durchgeführt hat.

- (Nur für vSAN Express Storage Architecture) Erweitern Sie die Speicherkapazität Ihres Clusters, indem Sie Flash-Geräte zu den Speicherpools der vorhandenen Hosts hinzufügen oder einen oder mehrere neue Hosts mit Flash-Geräten hinzufügen.

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. Auch wenn es am besten ist, in Ihren Datenträgergruppen oder Speicherpools dieselben oder ähnliche Geräte zu verwenden, wird jedes in der Hardwarekompatibilitätsliste (HCL) für vSAN aufgeführte Gerät unterstützt. Versuchen Sie, die Kapazität gleichmäßig auf Hosts zu verteilen. Informationen zum Hinzufügen von Geräten zu Datenträgergruppen oder Speicherpools finden Sie unter Erstellen einer Datenträgergruppe oder eines Speicherpools in einem vSAN-Cluster.

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

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

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

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

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

Voraussetzungen

- Der Schnellstart-Workflow muss für Ihren vSAN-Cluster verfügbar sein.
- Die im Schnellstart-Workflow durchgeführte Netzwerkkonfiguration wurde außerhalb des Schnellstart-Workflows geändert.
- Die beim Erstellen des Clusters mit Schnellstart konfigurierten Netzwerkeinstellungen wurden nicht geändert.

Verfahren

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

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

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

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

Hinzufügen eines Hosts zu einem vSAN-Cluster

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

Die Ressourcen des neuen Hosts werden dem Cluster zugeordnet.

Voraussetzungen

- Stellen Sie sicher, dass die Ressourcen, einschließlich Treiber, Firmware und Speicher-E/A-Controller, im VMware-Kompatibilitätshandbuchs unter http://www.vmware.com/resources/compatibility/search.php aufgeführt sind.
- VMware empfiehlt die Erstellung einheitlich konfigurierter Hosts im vSAN-Cluster, um eine gleichmäßige Verteilung von Komponenten und Objekten über die Geräte im Cluster zu erreichen. Es kann jedoch Situationen geben, in denen es in einem Cluster zu einer ungleichmäßigen Verteilung kommt, insbesondere während der Wartung oder bei einem Overcommit der Kapazität des vSAN-Datenspeichers mit übermäßig vielen VM-Bereitstellungen.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

3 Klicken Sie auf **Weiter**.

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

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

Der Host wurde zum Cluster hinzugefügt.

Nächste Schritte

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

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

Konfigurieren von Hosts im vSAN-Cluster mithilfe des Hostprofils

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

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

Voraussetzungen

- Stellen Sie sicher, dass sich der Host im Wartungsmodus befindet.
- Stellen Sie sicher, dass die Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php aufgelistet sind.

Verfahren

1 Erstellen Sie ein Hostprofil.

   a Navigieren Sie zur Ansicht „Hostprofile“.

   b Klicken Sie auf das Symbol **Profil vom Host extrahieren** (✚).

   c Wählen Sie den Host aus, den Sie als Referenzhost verwenden möchten, und klicken Sie auf **Weiter**.

   Der ausgewählte Host muss ein aktiver Host sein.

   d Geben Sie einen Namen und eine Beschreibung für das neue Profil ein und klicken Sie auf **Weiter**.

   e Überprüfen Sie die Zusammenfassung für das neue Hostprofil und klicken Sie auf **Beenden**.

   Das neue Profil wird in der Liste „Hostprofile“ angezeigt.

2 Hängen Sie den Host an das gewünschte Hostprofil an.

   a Wählen Sie in der Profilliste in der Ansicht „Hostprofile“ das Hostprofil aus, das Sie für den vSAN-Host übernehmen möchten.

   b Klicken Sie auf das Symbol **Hosts und Cluster an ein Hostprofil anhängen bzw. davon trennen** ( ).

c Wählen Sie den Host aus der erweiterten Liste aus und klicken Sie auf **Anhängen**, um den Host an das Profil anzuhängen.

Der Host wird zur Liste der verbundenen Elemente hinzugefügt.

d Klicken Sie auf **Weiter**.

e Klicken Sie auf **Beenden**, um das Trennen des Hosts vom Profil abzuschließen.

3 Trennen Sie den referenzierten vSAN-Host vom Hostprofil.

Wenn ein Hostprofil an einen Cluster angehängt wird, wird den Hosts in diesem Cluster ebenfalls das Hostprofil zugewiesen. Wenn das Hostprofil allerdings vom Cluster getrennt wird, bleibt die Verknüpfung zwischen dem Host bzw. den Hosts im Cluster und dem des Hostprofils bestehen.

a Wählen Sie in der Profilliste in der Ansicht „Hostprofile“ das Hostprofil aus, das Sie von einem Host oder Cluster trennen möchten.

b Klicken Sie auf das Symbol **Hosts und Cluster an ein Hostprofil anhängen bzw. davon trennen** ( ).

c Wählen Sie den Host oder Cluster in der erweiterten Liste aus und klicken Sie auf **Trennen**.

d Klicken Sie auf **Alle trennen**, um alle aufgelisteten Hosts und Cluster vom Profil zu trennen.

e Klicken Sie auf **Weiter**.

f Klicken Sie auf **Beenden**, um das Trennen des Hosts vom Hostprofil abzuschließen.

4 Überprüfen Sie die Übereinstimmung des vSAN-Hosts mit dem angehängten Hostprofil und bestimmen Sie, ob es Konfigurationsparameter auf dem Host gibt, die sich von den im Hostprofil angegebenen Konfigurationsparametern unterscheiden.

a Navigieren Sie zu einem Hostprofil.

Auf der Registerkarte **Objekte** werden alle Hostprofile, die Anzahl der an dieses Hostprofil angehängten Hosts sowie eine Zusammenfassung der Ergebnisse der letzten Übereinstimmungsüberprüfung angezeigt.

b Klicken Sie auf das Symbol **Hostprofil-Konformität überprüfen** ( ).

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

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

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

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

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

5 Standardisieren Sie den Host, um Konformitätsfehler zu korrigieren.

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

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

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

c Klicken Sie auf **Weiter**.

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

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

Freigeben von Remote-vSAN-Datenspeichern

Wenn Remote-Datenspeicher freigegeben wird, können vSAN-Cluster ihre Datenspeicher mit anderen Clustern gemeinsam nutzen.

Sie können auf Ihrem lokalen Cluster ausgeführte VMs so bereitstellen, dass sie Speicherplatz auf einem Remote-Datenspeicher verwenden. Wenn Sie eine neue virtuelle Maschine bereitstellen, können Sie einen im Clientcluster bereitgestellten Remote-Datenspeicher auswählen. Weisen Sie alle für den Datenspeicher konfigurierten kompatiblen Speicherrichtlinien zu.

Das Mounten eines Remote-Datenspeichers ist eine clusterweite Konfiguration. Wenn Sie einen Remote-Datenspeicher in einem vSAN-Cluster mounten, ist er für alle Hosts im Cluster verfügbar.

Wenn Sie einen vSAN-Cluster erstellen oder einen vSphere-Cluster für vSAN konfigurieren, können Sie den HCI-Konfigurationstyp auswählen.

- **vSAN HCI** stellt Computing- und Speicherressourcen bereit. Sie kann ihren Datenspeicher über Datencenter und vCenter hinweg freigeben und Datenspeicher von anderen vSAN HCI-Clustern mounten.
- **vSAN-Computing-Cluster** ist ein vSphere-Cluster, der nur Computing-Ressourcen bereitstellt. Er kann Datenspeicher mounten, die von vSAN Max-Clustern bereitgestellt werden.

- **vSAN Max** (nur vSAN ESA) stellt Speicherressourcen, aber keine Computing-Ressourcen bereit. Sein Datenspeicher kann von Remote-vSphere-Clustern oder vSAN HCI-Clustern in Datencentern und vCentern gemountet werden.

Für die vSAN-Datenspeicherfreigabe gelten die folgenden technischen Überlegungen:

- vSAN Original Storage Architecture-Cluster, auf denen Version 8.0 Update 1 oder höher ausgeführt wird, können Datenspeicher zwischen Clustern im selben Datencenter oder zwischen Clustern, die von Remote vCentern verwaltet werden, gemeinsam nutzen, solange sie sich im selben Netzwerk befinden. vSAN Express Storage Architecture-Cluster, auf denen Version 8.0 Update 2 oder höher ausgeführt wird, verfügen über diese Funktion.
- Ein vSAN-HCI- oder vSAN Max-Cluster kann seinen lokalen Datenspeicher für bis zu 10 Clientcluster zur Verfügung stellen.
- Ein Clientcluster kann bis zu fünf Remote-Datenspeicher aus einem oder mehreren vSAN-Serverclustern mounten.
- Ein einzelner Datenspeicher kann auf bis zu 128 vSAN-Hosts gemountet werden, einschließlich der Hosts im lokalen vSAN-Servercluster.
- Alle Objekte, die eine VM erstellen, müssen sich auf demselben Datenspeicher befinden.
- Damit vSphere HA mit vSAN-Datenspeicherfreigabe funktioniert, konfigurieren Sie die folgende Fehlerreaktion für den Datenspeicher mit APD: VMs ausschalten und neu starten.
- Clienthosts, die nicht Teil eines Clusters sind, werden nicht unterstützt. Sie können einen einzelnen hostbasierten rechnergestützten Cluster konfigurieren, aber vSphere HA funktioniert nicht, es sei denn, Sie fügen dem Cluster einen zweiten Host hinzu.
- Die Verschlüsselung in Übertragung begriffener Daten wird nicht unterstützt.

Die folgenden Konfigurationen werden mit vSAN-Datenspeicherfreigabe nicht unterstützt:

- Remotebereitstellung von iSCSI-Volumes oder dauerhaften CNS-Datenträgern. Sie können sie auf dem lokalen vSAN-Datenspeicher, aber nicht auf einem beliebigen vSAN-Remotedatenspeicher verwenden.
- Netzwerke oder Cluster mit Air Gap, die mehrere vSAN-VMkernel-Ports verwenden

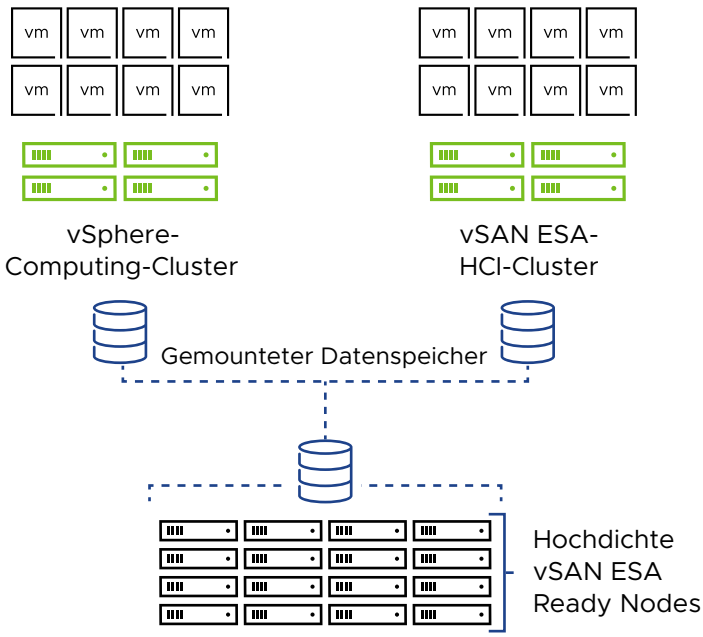
Disaggregierter Speicher mit vSAN Max

vSAN Max ist eine vollständig verteilte, skalierbare gemeinsam genutzte Speicherlösung für vSphere-Cluster und vSAN-Cluster. Die Speicherressourcen sind von den Computing-Ressourcen disaggregiert, sodass Sie Speicher- und Computing-Ressourcen unabhängig voneinander skalieren können.

vSAN Max verwendet vSAN Express Storage Architecture und vSAN Ready Nodes mit hoher Dichte, um Kapazität und Leistung zu erhöhen.

Hinweis vSAN Max kann durch den Erwerb von VMware Cloud Foundation oder des erweiterten Add-On-Angebots für VMware vSphere Foundation bereitgestellt werden. Die Lizenzierung für vSAN Max basiert auf einer Metrik pro TiB, die der Gesamtmenge der für die Umgebungen benötigten Rohspeicherkapazität entspricht.

Ein vSAN Max-Cluster fungiert als Server-Cluster, der nur Speicher bereitstellt. Sie können seinen Datenspeicher in vSphere-Cluster mounten, die als vSAN-Computing-Cluster oder vSAN HCI-Clientcluster konfiguriert sind.



Für vSAN Max-Cluster gelten die folgenden technischen Überlegungen:

- Wird nur auf vSAN Express Storage Architecture unterstützt, die auf vSAN Ready Nodes ausgeführt werden, die für vSAN Max zertifiziert sind.
- Nicht kompatibel mit vSAN Original Storage Architecture.
- Fungiert lediglich als Speicherserver und nicht als Client. Führen Sie keine Arbeitslast-VMs auf Hosts von vSAN Max aus.
- Erfordert mindestens sechs Hosts und 150 TiB pro Host. Um die Leistung zu optimieren, verwenden Sie eine einheitliche Konfiguration von Speichergeräten auf allen Hosts.
- Erfordert 100-GBit/s-Netzwerkverbindungen zwischen Hosts im vSAN Max-Cluster und 10-GBit/s-Verbindungen von Computing-Clients zum vSAN Max-Cluster. Aktivieren Sie für optimale Leistung Unterstützung für Jumbo-Frames (MTU = 9000) und stellen Sie sicher, dass Sie über genügend Ressourcen auf der Netzwerk-Spine verfügen.

- Aktivieren Sie **Automatische Richtlinienverwaltung** (Konfigurieren > vSAN > Dienste > Speicher > Bearbeiten), um ein optimales Maß an Ausfallsicherheit und Speicherplatzeffizienz zu gewährleisten.
- Aktivieren Sie **Automatische Neuverteilung** (Konfigurieren > vSAN > Dienste > Erweiterte Optionen > Bearbeiten), um ein gleichmäßig ausgeglichenes, verteiltes Speichersystem zu gewährleisten.

Hinweis Sie können vSAN Max nur während der Erstellung des Clusters konfigurieren. Sie können einen vorhandenen vSAN-Cluster nicht in vSAN Max konvertieren und vSAN Max nicht in einen vSAN HCI-Cluster konvertieren. Sie müssen vSAN auf dem Cluster deaktivieren und den Cluster neu konfigurieren.

vSAN-Computing-Cluster

Ein vSAN-Computing-Cluster ist ein vSphere-Cluster mit einem kleinen vSAN-Element, das es ihm ermöglicht, einen vSAN Max-Datenspeicher zu mounten. Die Hosts in einem Computing-Cluster verfügen nicht über lokalen Speicher. Sie können die Kapazität, Integrität und Leistung des Remote-Datenspeichers überwachen.

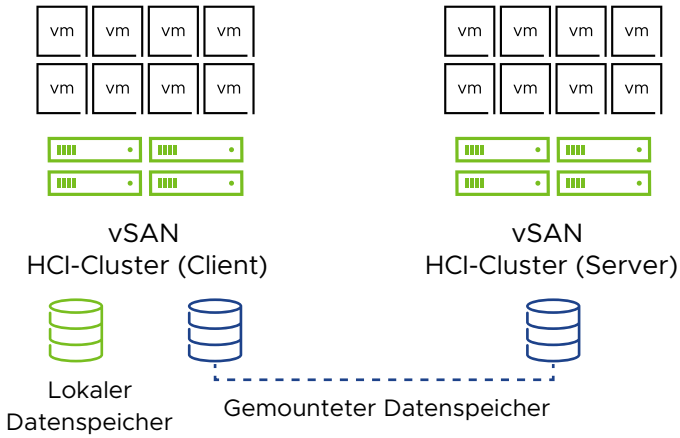
Für vSAN-Computing-Cluster gelten die folgenden technischen Erwägungen:

- vSAN-Netzwerk muss auf Hosts im Computing-Cluster konfiguriert werden.
- Auf Hosts in einem Computing-Cluster können keine Speichergeräte vorhanden sein.
- Auf dem Computing-Cluster können keine Datenverwaltungsfunktionen konfiguriert werden.

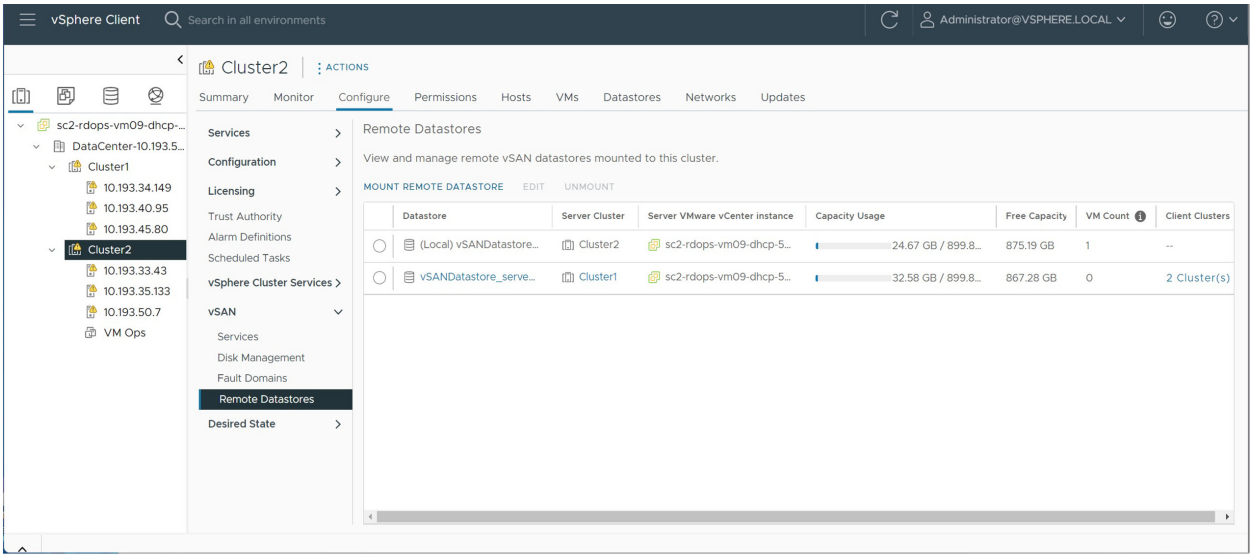
Clusterübergreifende Kapazitätsfreigabe

vSAN HCI-Cluster können ihre Datenspeicher für andere vSAN HCI-Cluster freigeben. Ein vSAN HCI-Cluster kann als Server zur Bereitstellung von Datenspeicher oder als Client fungieren, der Speicher verbraucht.

vSAN Original Storage Architecture und vSAN Express Storage Architecture sind nicht kompatibel und können keine Datenspeicher gemeinsam nutzen. Ein Clientcluster kann keine Datenspeicher aus unterschiedlichen vSAN-Architekturen mounten. Wenn ein Cluster einen Datenspeicher gemountet hat, der vSAN Original Storage Architecture verwendet, kann er keinen Datenspeicher mounten, der vSAN Express Storage Architecture verwendet.



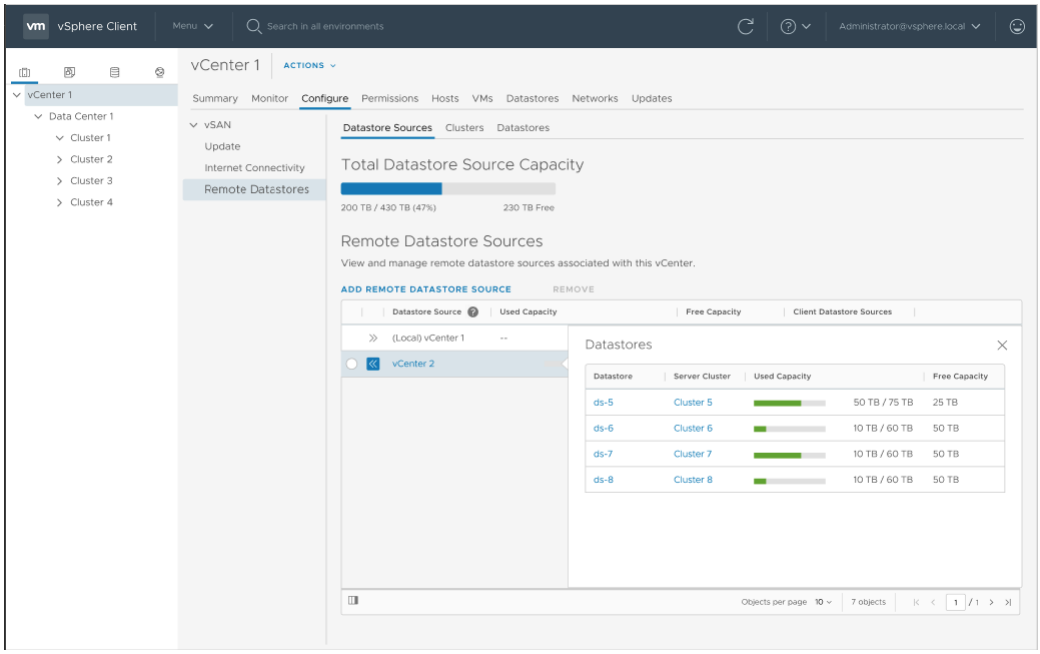
Verwenden Sie die Ansicht „Remote-Datenspeicher“ zur Überwachung und Verwaltung von Remote-Datenspeichern, die auf dem lokalen vSAN-Cluster gemountet sind. Jeder Client vSAN-Cluster kann Remote-Datenspeicher von Server vSAN-Clustern mounten. Jeder kompatible vSAN-Cluster kann auch als Server agieren und anderen vSAN-Clustern erlauben, seine lokalen Datenspeicher zu mounten.



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

Verwenden von Remote-vCentern als Datenspeicherquellen

vSAN HCI- und vSAN Max-Cluster können Remote-Datenspeicher über vCenter hinweg gemeinsam nutzen. Sie können einen Remote-vCenter als Datenspeicherquelle für Cluster auf dem lokalen vCenter hinzufügen. Clientcluster auf dem lokalen vCenter können Datenspeicher mounten, die sich auf dem Remote-vCenter befinden.



Verwenden Sie die Seite „Remote-Datenspeicher“ des vCenters, um Remote-Datenspeicherquellen zu verwalten (**Konfigurieren > vSAN > Remote-Datenspeicher**). Klicken Sie auf die Registerkarten, um auf Informationen über freigegebene Datenspeicher in vCentern zuzugreifen, vCenter als Datenspeicherquellen hinzuzufügen und Datenspeicher in lokalen Clustern zu mounten.

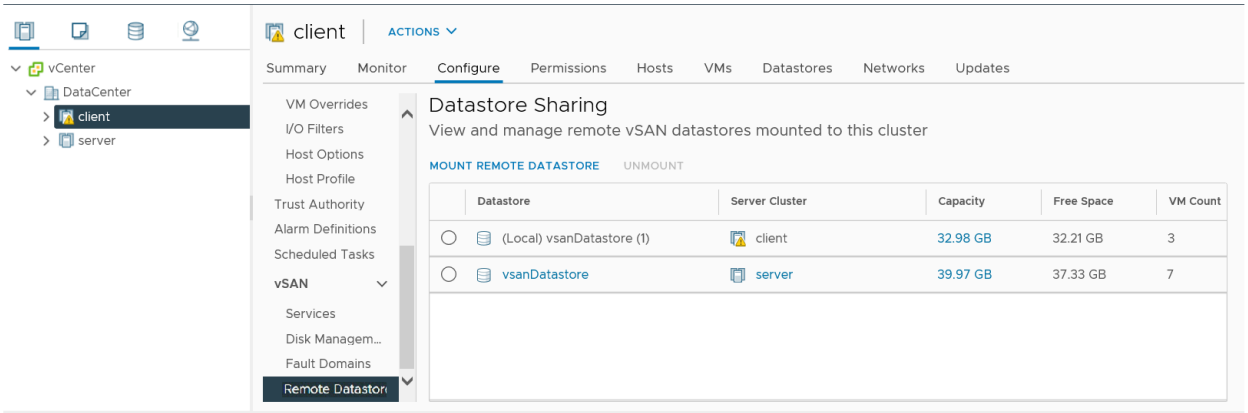
Datenspeicherquellen	Anzeigen und Verwalten von Datenspeicherquellen in Remote-vCentern. Sie können Remote-Datenspeicherquellen für den lokalen vCenter hinzufügen oder entfernen.
Cluster	Anzeigen und Verwalten von Clustern im lokalen vCenter. Sie können Datenspeicher aus Remote-vCentern im ausgewählten Cluster mounten oder unmounten.
Datenspeicher	Zeigen Sie alle unter diesem vCenter verfügbaren Datenspeicher an.

Für eine vCenter-zu-vCenter-Datenspeicherfreigabe gelten die folgenden technischen Überlegungen:

- Jedes vCenter kann bis zu 10 Client-vCenter bedienen.
- Jeder Client vCenter kann bis zu 5 Remote-vCenter-Datenspeicherquellen hinzufügen.
- Wenn eine VM auf einem Clientcluster, der von einem vCenter verwaltet wird, Speicher von einem Server verwendet, der von einem anderen vCenter verwaltet wird, hat die Speicherrichtlinie auf dem vCenter des Clients Vorrang.

Anzeigen von Remote-vSAN-Datenspeichern

Auf der Seite „Remote-Datenspeicher“ können Sie Remote-Datenspeicher anzeigen, die auf dem lokalen vSAN-Cluster gemountet sind, sowie Client-Cluster, die den lokalen Datenspeicher gemeinsam nutzen.



Verfahren

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

Ergebnisse

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

- Server-Cluster, der den Datenspeicher hostet
- vCenter des Server-Clusters (falls zutreffend)
- Kapazitätsnutzung des Datenspeichers
- Freie Kapazität verfügbar
- Die Anzahl VMs, die den Datenspeicher verwenden (Anzahl VMs, die die Rechenressourcen des lokalen Clusters, aber die Speicherressourcen des Serverclusters nutzen)
- Client-Cluster, für die der Datenspeicher bereitgestellt wurde

Nächste Schritte

Auf dieser Seite können Sie Remotedatenspeicher mounten oder unmounten.

Mounten von Remote-vSAN-Datenspeicher

Sie können einen oder mehr Datenspeicher aus anderen vSAN-Clustern mounten.

Verfahren

1. Gehen Sie zum lokalen vSAN-Cluster.
2. Klicken Sie auf die Registerkarte „Konfigurieren“.
3. Klicken Sie unter vSAN auf **Remote-Datenspeicher**.
4. Klicken Sie auf **Remotedatenspeicher mounten**, um den Assistenten zu öffnen.

5 (Optional) Wählen Sie einen Remote-vCenter als Datenspeicherquelle aus.

6 Wählen Sie einen Datenspeicher aus.

7 (Optional) Wenn es sich bei dem Servercluster um einen vSAN Stretched Cluster handelt, konfigurieren Sie Site-Kopplung, um den optimalen Datenpfad zwischen den vSAN HCI-Servern und den Clients auszuwählen.

   Ein vSAN Stretched Cluster kann über ein asymmetrisches Netzwerk verfügen, bei dem die Verbindungen innerhalb der einzelnen Sites eine höhere Bandbreite und geringere Latenz aufweisen als die Verbindungen zwischen den Sites. Ein symmetrisches Netzwerk weist ähnliche Verbindungen innerhalb jeder Site und zwischen den Sites auf.

   a Wählen Sie auf der Seite Netzwerktopologie die Option **Symmetrisch** oder **Asymmetrisch** aus. Wenn Sie Asymmetrisch auswählen, wird die Seite „Site-Kopplung“ angezeigt.

   b Wählen Sie eine Site auf dem Servercluster aus, die mit der entsprechenden Client-Site gekoppelt werden soll. Wählen Sie die Server-Site aus, die physisch näher an den einzelnen Client-Sites liegt oder an sie angrenzt.

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

Ergebnisse

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

Nächste Schritte

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

Unmounten von Remote-vSAN-Datenspeicher

Sie können einen Remote-Datenspeicher von einem vSAN unmounten.

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

Verfahren

1 Gehen Sie zum lokalen vSAN-Cluster.

2 Klicken Sie auf die Registerkarte „Konfigurieren“.

3 Klicken Sie unter vSAN auf **Remote-Datenspeicher**.

4 Wählen Sie einen Remote-Datenspeicher aus und klicken Sie auf **Unmounten**.

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

Ergebnisse

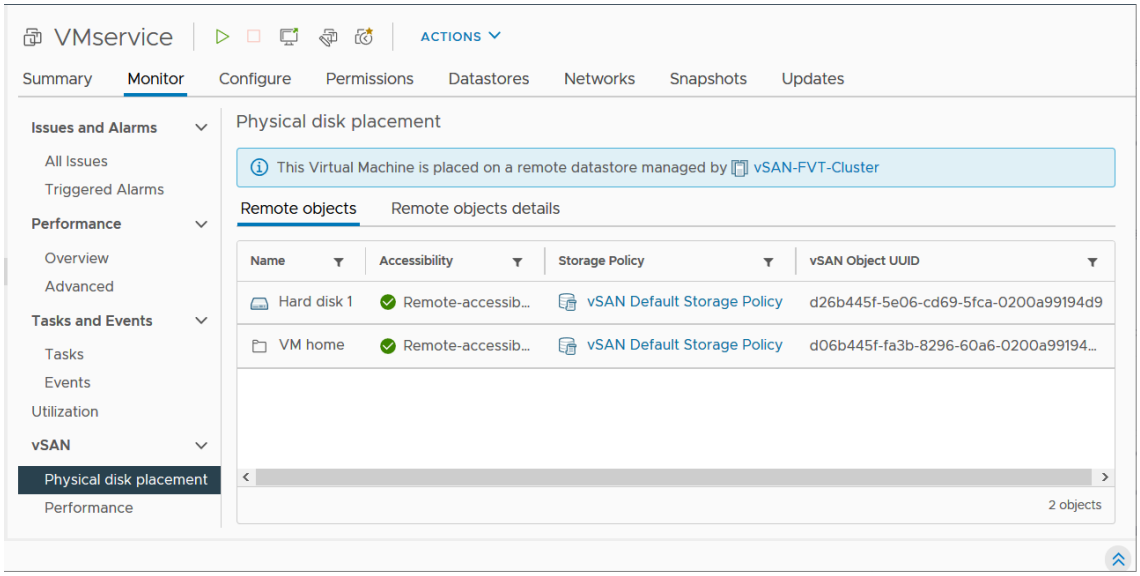
Der ausgewählte Datenspeicher wird von dem lokalen Cluster unmountet.

Überwachen der Datenspeicherfreigabe mit vSphere Client

Sie können den vSphere Client verwenden, um den Status der vSAN-Datenspeicherfreigabevorgänge zu überwachen.

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

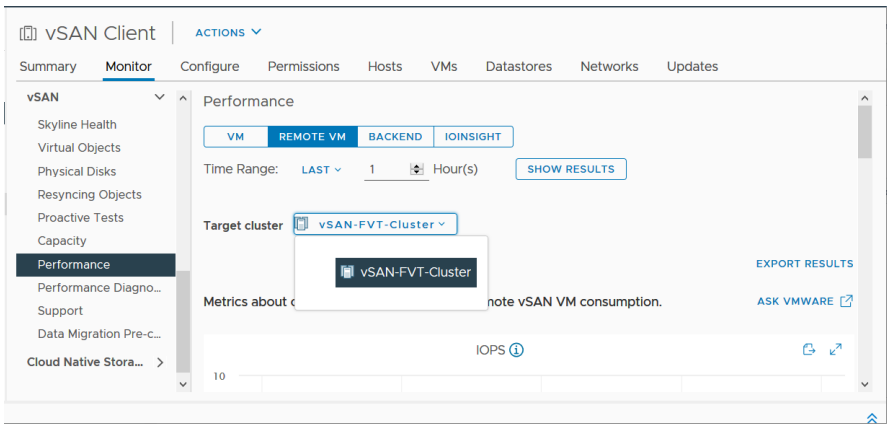
In der Ansicht „Virtuelle Eigenschaften“ wird der Datenspeicher angezeigt, in dem sich virtuelle Objekte befinden. In der Ansicht „Platzierung physischer Datenträger“ für eine VM, die sich auf einem Remote-Datenspeicher befindet, werden Informationen über den zugehörigen Remote-Standort angezeigt.



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

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

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



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

Hinzufügen eines Remote-vCenters als Datenspeicherquelle

Sie können ein Remote-vCenter als Remote-Datenspeicherquelle für Clients auf dem lokalen vCenter hinzufügen.

Verfahren

1. Navigieren Sie im vSphere Client zum vCenter.
2. Wählen Sie **Konfigurieren > vSAN > Remote-Datenspeicher** aus.
3. Klicken Sie auf der Registerkarte „Datenspeicherquellen“ auf **Remote-Datenspeicherquelle hinzufügen**, um den Assistenten zu öffnen.
4. Geben Sie die Informationen zur Angabe des Remote-vCenter ein.
5. Überprüfen Sie die Kompatibilität, überprüfen Sie die Konfiguration und klicken Sie auf **Fertig stellen**.

Ergebnisse

Das Remote-vCenter wird als Datenspeicherquelle hinzugefügt. vSAN Cluster auf diesem vCenter können Remote-Datenspeicher mounten, die sich auf dem Remote-vCenter befinden.

Arbeiten mit Mitgliedern des vSAN-Clusters im Wartungsmodus

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

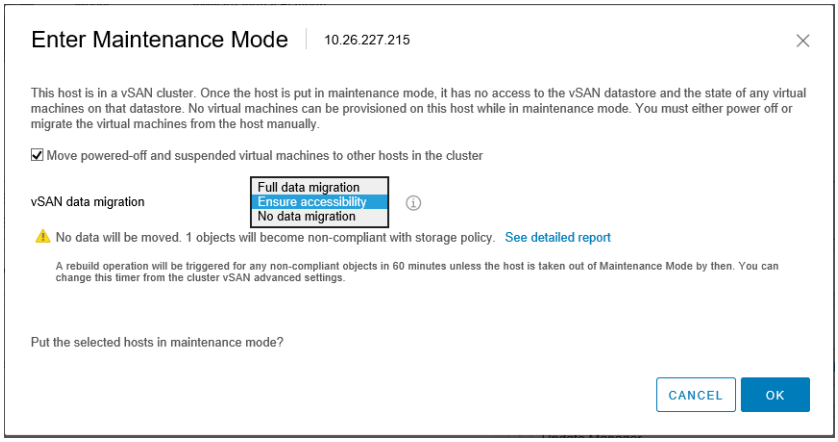
Wenn Sie mit dem Wartungsmodus arbeiten, beachten Sie folgende Einschränkungen:

- Wenn Sie einen ESXi-Host in den Wartungsmodus versetzen, müssen Sie einen Datenevakuierungsmodus wie zum Beispiel **Zugriff sicherstellen** oder **Vollständige Datenmigration** auswählen.
- Wenn ein beliebiger Mitgliedshost eines vSAN-Clusters in den Wartungsmodus wechselt, wird die Clusterkapazität automatisch reduziert, weil der Speicher des Mitgliedshosts im Cluster nicht mehr bereitsteht.
- Die Rechenressourcen einer virtuellen Maschine befinden sich möglicherweise nicht auf dem Host, der in den Wartungsmodus versetzt wird, und der Speicher für virtuelle Maschinen kann sich an beliebiger Stelle im Cluster befinden.
- Der Modus **Zugriff sicherstellen** ist schneller als der Modus **Vollständige Datenmigration**, weil der Modus **Zugriff sicherstellen** nur die Komponenten von den Hosts migriert, die entscheidend für die Ausführung der virtuellen Maschinen sind. Wenn in diesem Modus ein Fehler auftritt, ist die Verfügbarkeit Ihrer virtuellen Maschine davon betroffen. Durch Auswählen des Modus **Zugriff sicherstellen** werden Ihre Daten bei einem Ausfall nicht neu geschützt und eventuell tritt ein unerwarteter Datenverlust auf.
- Wenn Sie den Modus **Vollständige Datenmigration** auswählen, werden Ihre Daten automatisch neu vor einem Ausfall geschützt, wenn Ressourcen verfügbar sind und der Wert für **Zu tolerierende Fehler** auf 1 oder mehr festgelegt wurde. In diesem Modus werden alle Komponenten vom Host migriert und je nach der Menge der Daten auf dem Host kann die Migration länger dauern. Im Modus **Vollständige Datenmigration** können Ihre virtuellen Maschinen Ausfälle tolerieren, selbst während einer geplanten Wartung.
- Wenn Sie einen Cluster mit drei Hosts verwenden, können Sie einen Server nicht mit **Vollständige Datenmigration** in den Wartungsmodus versetzen. Sie sollten einen Cluster mit vier oder mehr Hosts für maximale Verfügbarkeit erstellen.

Vor dem Versetzen eines Hosts in den Wartungsmodus müssen Sie Folgendes prüfen:

- Wenn Sie den Modus **Vollständige Datenmigration** verwenden, stellen Sie sicher, dass der Cluster über genügend Hosts und verfügbare Kapazität verfügt, um die Anforderungen der Richtlinie **Zu tolerierende Fehler** zu erfüllen.
- Stellen Sie sicher, dass auf den restlichen Hosts genügend Flash-Kapazität vorhanden ist, um Flash Read Cache-Reservierungen verarbeiten zu können. Führen Sie den folgenden RVC-Befehl aus, um die aktuell genutzte Kapazität pro Host zu analysieren und um zu ermitteln, ob der Ausfall eines einzelnen Hosts zu einem Speicherplatzmangel auf dem Cluster führen kann und sich auf die Clusterkapazität, die Cachereservierung und die Clusterkomponenten auswirkt: `vsan.whatif_host_failures`. Informationen zu den RVC-Befehlen finden Sie im *Referenzhandbuch zu RVC-Befehlen*.
- Stellen Sie sicher, dass Sie genug Kapazitätsgeräte in den verbleibenden Hosts haben, um Richtlinienanforderungen in Bezug auf Stripe-Breite erfüllen zu können, falls ausgewählt.

- Stellen Sie sicher, dass auf den restlichen Hosts genug freie Kapazität verfügbar ist, um die Menge der Daten verarbeiten zu können, die von dem in den Wartungsmodus wechselnden Host migriert werden müssen.



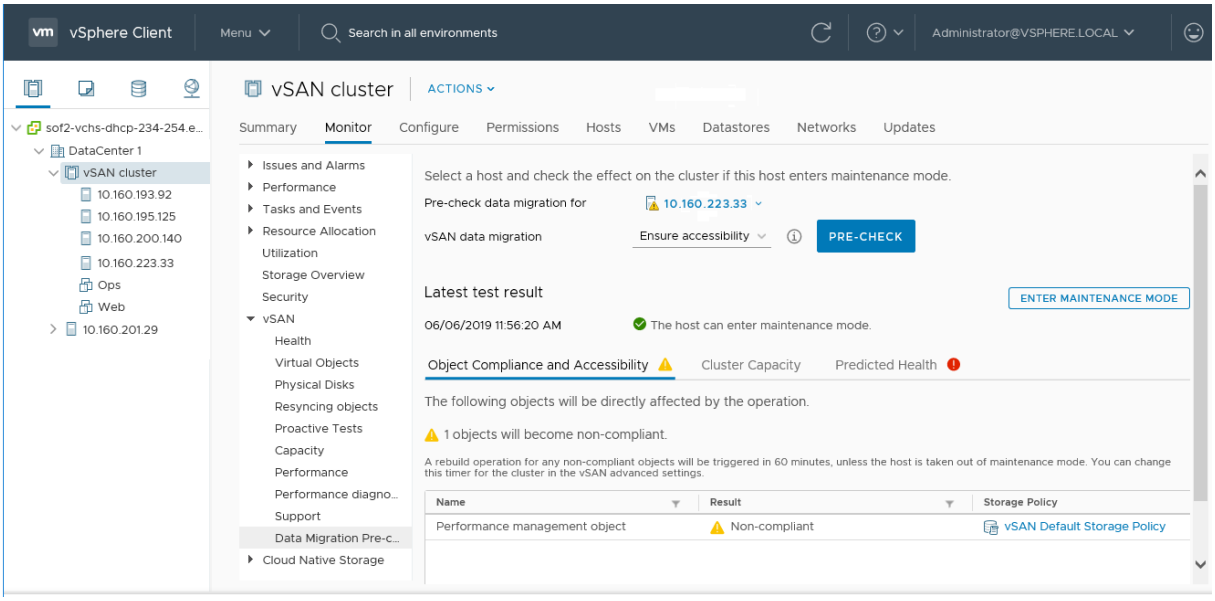
Das Dialogfeld „Wartungsmodus bestätigen“ bietet Informationen hinsichtlich Ihrer Wartungsaktivitäten. Sie können die Auswirkungen einer jeden Datenevakuierungsoption anzeigen.

- Ob es ausreichend Kapazität gibt, um den Vorgang durchzuführen.
- Der Umfang der Daten, der verschoben wird.
- Die Anzahl der Objekte, die dann nicht mehr übereinstimmen.
- Die Anzahl der Objekte, auf die kein Zugriff mehr möglich wird.

Überprüfen der Datenmigrationsfunktionen eines Hosts im vSAN-Cluster

Verwenden Sie die Vorabprüfung der Datenmigration, um die Auswirkungen von Migrationsoptionen 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.

Hinweis Die auf einem Host ausgeführten vSAN-FSVMs (File Service VMs) werden automatisch ausgeschaltet, wenn ein Host im vSAN-Cluster in den Wartungsmodus wechselt.

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 aus dem Cluster entfernen, werden von vSAN gerade so viele Daten migriert, dass nach dem Versetzen des Hosts in den Wartungsmodus der Zugriff auf alle Objekte gewährleistet 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 der Wert für **Zu tolerierende Fehler** 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.

Zum Durchführen einer Aktion vor dem Wechsel in den Wartungsmodus führen Sie folgenden Befehl auf dem Host aus:

```
esxcli system maintenanceMode set --enable 1 --vsanmode=<str>
```

Bei Folgendem handelt es sich um die für vsanmode zulässigen Zeichenfolgenwerte:

- ensureObjectAccessibility – Evakuieren Sie vor dem Wechsel in den Wartungsmodus Daten vom Datenträger, um die Zugriffsfähigkeit von Objekten im vSAN-Cluster sicherzustellen.

  Hinweis Der Standardwert ist „ensureObjectAccessibility“. Dieser Wert wird verwendet, wenn Sie keinen Wert für den vsanmode angeben.

- evacuateAllData – Evakuieren Sie alle Daten vom Datenträger, bevor Sie in den Wartungsmodus wechseln.
- noAction – Verschieben Sie vSAN-Daten nicht vom Datenträger, bevor Sie in den Wartungsmodus wechseln.

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

```
esxcli system maintenanceMode get
```

Zum Beenden des Wartungsmodus führen Sie folgenden Befehl aus:

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

Nächste Schritte

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

Verwalten von Fault Domains in vSAN-Clustern

Fehlerdomänen ermöglichen es Ihnen, sich vor Rack- oder Gehäuseausfällen zu schützen, wenn Ihr vSAN-Cluster über mehrere Racks oder Blade-Server-Gehäuse verteilt ist.

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

Die Richtlinie **Zu tolerierende Fehler** für den Cluster hängt von der Anzahl der Ausfälle ab, die eine virtuelle Maschine tolerieren kann. Wenn das Attribut **Zu tolerierende Fehler** (FTT) für eine virtuelle Maschine auf 1 `(FTT=1)` festgelegt ist, kann vSAN einen einzelnen Ausfall beliebiger Art einer beliebigen Komponente in einer Fehlerdomäne tolerieren, einschließlich des Ausfalls eines ganzen Racks.

Wenn Sie Fault Domains auf einem Rack konfigurieren und eine neue virtuelle Maschine bereitstellen, stellt vSAN sicher, dass Schutzobjekte wie Replikate und Zeugen in verschiedenen Fault Domains platziert werden. Beispiel: Wenn in der Speicherrichtlinie einer virtuellen Maschine der Wert für **Zu tolerierende Fehler** auf „N“ `(FTT=n)` festgelegt ist, benötigt vSAN mindestens `2*n+1` Fehlerdomänen im Cluster. Wenn virtuelle Maschinen in einem Cluster mit Fault Domains und dieser Richtlinie bereitgestellt sind, werden die Kopien der damit verknüpften VM-Objekte auf verschiedenen Racks gespeichert.

Für die Unterstützung der Festlegung von FTT auf 1 sind mindestens drei Fehlerdomänen erforderlich. Konfigurieren Sie vier oder mehr Fault Domains im Cluster, um optimale Ergebnisse zu erhalten. Für einen Cluster mit drei Fault Domains gelten dieselben Einschränkungen wie für einen Cluster mit drei Hosts, wie z. B. die Unmöglichkeit, Daten nach einem Ausfall neu zu schützen oder den Modus **Vollständige Datenmigration** zu verwenden. Informationen zum Entwerfen und Dimensionieren von Fehlerdomänen finden Sie unter „Entwerfen und Dimensionieren von vSAN-Fehlerdomänen“ in *vSAN-Planung und -Bereitstellung*.

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

Wenn ein Rack ausfällt, ist keine Ressource (CPU, Speicher usw.) mehr im Rack für den Cluster verfügbar. Konfigurieren Sie daher kleinere Fehlerdomänen, um die Auswirkungen eines möglichen Rackausfalls zu verringern. Je mehr Fehlerdomänen Sie erstellen, desto höher ist die Gesamtverfügbarkeit der Ressourcen im Cluster nach einem Rackausfall.

Befolgen Sie diese empfohlenen Vorgehensweisen beim Arbeiten mit Fault Domains.

- Konfigurieren Sie mindestens drei Fault Domains im vSAN-Cluster. Konfigurieren Sie vier oder mehr Fault Domains, um optimale Ergebnisse zu erhalten.
- Bei einem Host, der zu keiner Fault Domain gehört, wird davon ausgegangen, dass dieser sich in seiner eigenen Fault Domain mit einem Host befindet.
- Sie brauchen nicht jeden vSAN-Host einer Fault Domain zuzuweisen. Wenn Sie Fault Domains zum Schützen der vSAN-Umgebung verwenden möchten, sollten Sie gleich große Fault Domains erstellen.
- Die Zuweisungen zu Fault Domains bleiben für vSAN-Hosts, die in einen anderen Cluster verschoben werden, erhalten.
- Platzieren Sie beim Entwerfen von Fehlerdomänen eine einheitliche Anzahl an Hosts in jeder Fehlerdomäne.

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

- Sie können einer Fault Domain beliebig viele Hosts hinzufügen. Jede Fault Domain muss mindestens einen Host beinhalten.

Erstellen einer neuen Fault Domain im vSAN-Cluster

Um bei einem Rackausfall die Funktionsfähigkeit der VM-Objekte sicherzustellen, können Sie Hosts in verschiedenen Fault Domains gruppieren.

Wenn Sie eine virtuelle Maschine auf dem Cluster mit Fault Domains bereitstellen, verteilt vSAN Schutzkomponenten wie Zeugen und Repliken der VM-Objekte auf verschiedene Fault Domains. Folglich kann die vSAN-Umgebung komplette Rackausfälle neben dem Ausfall eines einzelnen Hosts, eines Speicherdatenträgers 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 Fehlerdomäne in einem vSAN-Cluster

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 Fehlerdomäne in einem vSAN-Cluster

Je nach Ihren Anforderungen können Sie Hosts aus einer Fault Domain verschieben.

Voraussetzungen

Stellen Sie sicher, dass der Host online ist. Sie können keine Hosts verschieben, die offline sind oder auf die von einer Fault Domain aus nicht zugegriffen werden kann.

Verfahren

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

Ergebnisse

Der ausgewählte Host ist nicht mehr Teil einer Fault Domain. Jeder Host, der nicht Teil einer Fault Domain ist, wird als in einer eigenen Einzelhost-Fault Domain vorhanden betrachtet.

Nächste Schritte

Sie können Hosts zu Fault Domains hinzufügen. Siehe Verschieben von Hosts in eine ausgewählte Fehlerdomäne in einem vSAN-Cluster.

Umbenennen einer Fehlerdomäne in einem vSAN-Cluster

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

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

   b Geben Sie einen neuen Fault Domain-Namen ein.

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

   Der neue Name wird in der Liste der Fault Domains angezeigt.

Entfernen ausgewählter Fehlerdomänen aus einem vSAN-Cluster

Wenn Sie keine Fault Domain mehr brauchen, können Sie sie aus dem vSAN-Cluster entfernen.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

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

Ergebnisse

Alle Hosts in der Fault Domain werden entfernt und die ausgewählte Fault Domain wird im vSAN-Cluster gelöscht. Jeder Host, der nicht Teil einer Fault Domain ist, wird als in einer eigenen Einzelhost-Fault Domain vorhanden betrachtet.

Tolerieren zusätzlicher Ausfälle mit Fehlerdomänen in einem vSAN-Cluster

Fehlerdomänen in einem vSAN-Cluster bieten Ausfallsicherheit und stellen sicher, dass die Daten auch bei richtlinienbedingten Ausfällen verfügbar sind.

Wenn „Anzahl der zu tolerierenden Fehler“ (FTT) auf 1 gesetzt ist, kann das Objekt einen Ausfall tolerieren. Ein vorübergehender Ausfall gefolgt von einem dauerhaften Ausfall kann in einem Cluster zu Datenverlust führen. Eine zusätzliche Fehlerdomäne bietet vSAN die Möglichkeit, eine Haltbarkeitskomponente zu erstellen, ohne zusätzliche FTTs für das Objekt zu haben. vSAN löst diese zusätzliche Komponente bei geplanten und ungeplanten Ausfällen aus. Zu den ungeplanten Ausfällen gehören Netzwerkunterbrechungen, Datenträgerausfälle und Hostausfälle. Zu den geplanten Ausfällen gehört der Eintritt in den Wartungsmodus (EMM). Beispielsweise kann ein 6-Host-Cluster mit RAID 6-Objekt bei einem Hostausfall keine Haltbarkeitskomponente erstellen.

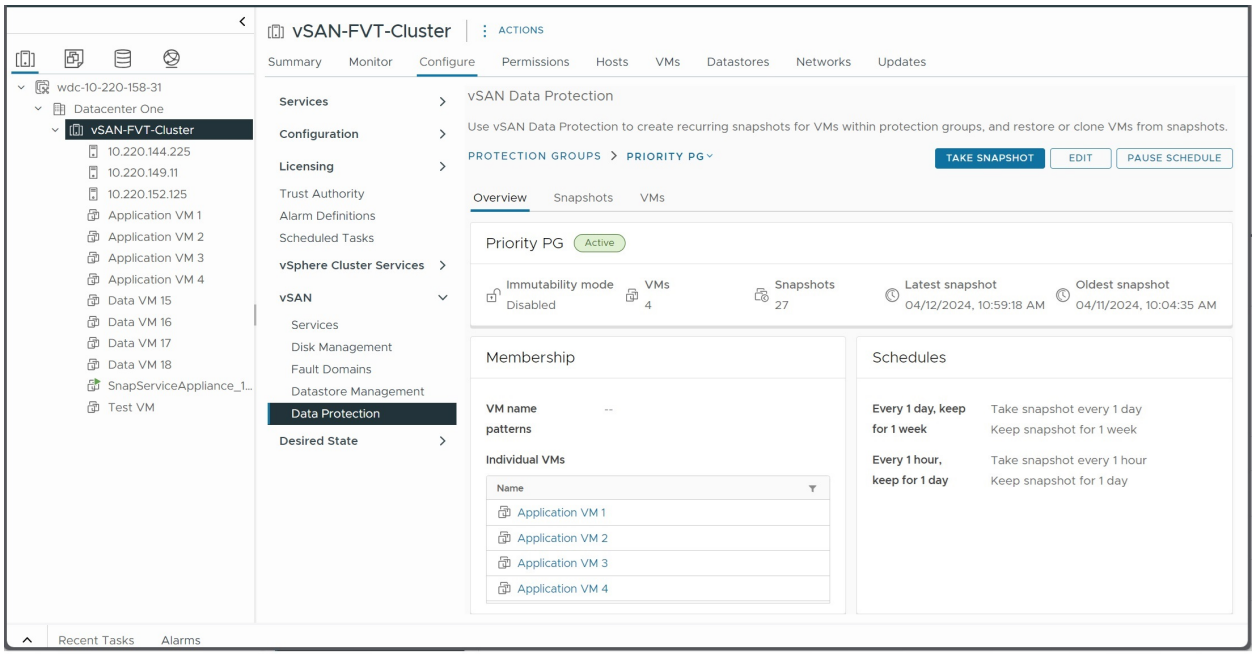
vSAN stellt die Datenverfügbarkeit der Objekte sicher, wenn die Komponenten offline gehen und unerwartet wieder online kommen, basierend auf den in der Speicherrichtlinie festgelegten FTTs. Bei einem Ausfall werden die Schreibvorgänge der ausgefallenen Komponente auf die Haltbarkeitskomponente umgeleitet.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

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

Verwenden von vSAN Data Protection

vSAN Data Protection ermöglicht die schnelle Wiederherstellung von VMs nach Betriebsausfällen oder Ransomware-Angriffen mithilfe nativer Snapshots, die lokal auf dem vSAN-Cluster gespeichert sind.

vSAN Data Protection wird in vSAN HCI-Clustern unterstützt, die von vSAN ESA bereitgestellt werden. vSAN Data Protection verwendet native vSAN-Snapshots, um den aktuellen Zustand Ihrer VMs zu erfassen. Sie können vSAN-Snapshots verwenden, um eine VM auf ihrem vorherigen Zustand zurückzusetzen oder zu Entwicklungs- und Testzwecken zu klonen.



vSAN Data Protection benötigt den VMware Snapshot Service zum Verwalten von vSAN-Snapshots. Stellen Sie die Snapshot Service-Appliance bereit, um vSAN Data Protection im vSphere Client zu aktivieren.

Navigieren Sie mithilfe der folgenden Registerkarten zur Seite „vSAN Data Protection“.

Registerkarte	Beschreibung
Übersicht	Zeigt allgemeine Informationen zu vSAN Data Protection an, einschließlich der Anzahl der Schutzgruppen, des Prozentsatzes der geschützten VMs, der Anzahl der VM-Snapshots und des für Snapshots verwendeten Speicherplatzes.
Schutzgruppen	Zeigt eine Liste der vSAN Data Protection-Gruppen und deren Status an. Wählen Sie eine Schutzgruppe aus, um Snapshots in der Schutzgruppe anzuzeigen, oder bearbeiten Sie die Konfiguration.
VMs	Zeigt eine Liste der VMs im vSAN-Cluster mit Details zum jeweiligen Datenschutzstatus an. Gelöschte VMs mit verfügbaren Snapshots werden hier angezeigt. Sie können eine VM auswählen und die VM durch Klicken wiederherstellen oder klonen.

vSAN-Snapshots

vSAN-Snapshots behalten den Zustand und die Daten einer virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung bei. In diesem lokalen Archiv werden die Daten der VM im damaligen Zustand beibehalten. Sie können eine VM im Zustand zum Zeitpunkt der Snapshot-Erstellung wiederherstellen oder eine verknüpfte Klon-VM erstellen, die dem im Snapshot gespeicherten Zustand entspricht.

Beim Erstellen eines Snapshots wird der Zustand einer VM zu einem bestimmten Zeitpunkt erfasst. vSAN-Snapshots werden nicht stillgelegt und erfassen den aktuellen Ausführungszustand der VM.

Snapshots werden immer für eine einzelne virtuelle Maschine erstellt. Für jede VM ist ein separater Snapshot erforderlich. Sie können manuelle oder geplante Snapshots virtueller Maschinen erstellen, indem Sie sie in Schutzgruppen platzieren.

Jeder vSAN-Snapshot enthält den Zustand des Namespace-Objekts der VM sowie virtuelle Datenträgerobjekte. vSAN erstellt innerhalb geplanter Intervalle Snapshots von VMs in Schutzgruppen. Diese vSAN-Snapshots werden lokal im vSAN-Datenspeicher gespeichert.

Schutzgruppen

Mithilfe von Schutzgruppen können Sie Snapshots für eine oder mehrere VMs planen und verwalten. Sie können VMs zu einer Schutzgruppe hinzufügen, Snapshot-Zeitpläne konfigurieren und Snapshot-Informationen anzeigen.

Wählen Sie eine Schutzgruppe aus und verwalten Sie sie mithilfe der folgenden Registerkarten.

Registerkarte	Beschreibung
Überblick	Zeigt allgemeine Informationen zur Schutzgruppe an, einschließlich einer Liste der Mitglieder-VMs, der Snapshot-Zeitpläne und der Anzahl der erstellten Snapshots.
Snapshots	Zeigt die Snapshot-Serie an, die der Schutzgruppe zugeordnet ist. Sie können einzelne Snapshots aus der Serie auswählen und löschen.
VMs	Zeigt eine Liste der VMs, die Mitglieder der Schutzgruppe sind, sowie die Anzahl der für jede VM verfügbaren Snapshots an.

Wenn Sie eine Schutzgruppe erstellen, fügen Sie Mitglieder-VMs hinzu und konfigurieren Sie einen oder mehrere Snapshot-Zeitpläne. Sie können VMs einzeln hinzufügen oder VM-Namensmuster eingeben, um alle VMs hinzuzufügen, die dem Muster entsprechen. Sie können beide Methoden verwenden, um der Schutzgruppe VMs hinzuzufügen.

Sie können mehrere Snapshot-Zeitpläne definieren, um in regelmäßigen Abständen den Zustand von VMs in einer Schutzgruppe zu erfassen. Wenn neue Snapshots erfasst werden, entfernt vSAN alte Snapshots auf Basis der Aufbewahrungseinstellung aus der Serie. Sie können auch einen manuellen Snapshot erstellen, um den aktuellen Zustand der VMs in der Schutzgruppe zu erfassen.

Aktivieren Sie **Unveränderlichkeitsmodus** in einer Schutzgruppe, um zusätzliche Sicherheit zu gewährleisten. Sie können diese Schutzgruppe nicht bearbeiten oder löschen, die VM-Mitgliedschaft nicht ändern und Snapshots nicht bearbeiten oder löschen. Bei einem unveränderlichen Snapshot handelt es sich um eine schreibgeschützte Kopie von Daten, die selbst von einem Angreifer mit Administratorrechten nicht geändert oder gelöscht werden kann.

Hinweis Sobald der Unveränderlichkeitsmodus in einer Schutzgruppe aktiviert ist, kann dieser nicht mehr von einem Administrator deaktiviert werden.

Sie können Schutzgruppen auf der Registerkarte „Schutzgruppen“ überwachen und ändern. Klicken Sie auf eine Schutzgruppe, um entsprechende Details anzuzeigen.

- Unter **Übersicht** werden allgemeine Informationen zur Schutzgruppe angezeigt, einschließlich VM-Mitgliedschaft, Snapshot-Zeitpläne und Anzahl der Snapshots.
- Unter **Snapshots** wird eine Liste der in der Schutzgruppe verfügbaren Snapshots angezeigt. Sie können einen Snapshot auswählen und auf **>>** klicken, um einzelne Snapshots für jede VM anzuzeigen und Aktionen durchzuführen.
- Unter **VMs** wird eine Liste der VMs in der Schutzgruppe mit Details zu den verfügbaren Snapshots angezeigt. Wählen Sie ein VM-Optionsfeld aus, klicken Sie auf **VM wiederherstellen** oder **VM klonen** und wählen Sie dann einen Snapshot aus.

Klicken Sie auf eine der folgenden Schaltflächen, um Aktionen für die Schutzgruppe durchzuführen.

Aktion	Beschreibung
Snapshot erstellen	Sie können den Standardnamen des Snapshots ändern und den Aufbewahrungszeitraum festlegen. vSAN erstellt einen separaten Snapshot für jede VM in der Schutzgruppe.
Bearbeiten	Sie können VMs hinzufügen oder entfernen, die VM-Namensmuster ändern und die Snapshot-Zeitpläne hinzufügen oder ändern.
Zeitplan anhalten/ Zeitplan fortsetzen	Sie können die für die Schutzgruppe definierten Snapshot-Zeitpläne anhalten. Während die Zeitpläne angehalten werden, werden keine Snapshots erstellt oder gelöscht.

Klicken Sie zum Löschen einer Schutzgruppe neben dem Gruppennamen auf das Symbol **Mehr...** und wählen Sie das Menü **Löschen** aus. Wenn Sie die Schutzgruppe löschen, müssen Sie festlegen, wie die enthaltenen Snapshots verwaltet werden sollen.

- **Snapshots bis zu ihrem Ablaufdatum aufbewahren**. Die Schutzgruppe wird gelöscht, nachdem alle vorhandenen Snapshots abgelaufen sind.
- **Snapshots löschen**. Die Schutzgruppe wird samt vorhandener Snapshots sofort gelöscht.

vSAN und VMware Live Cyber Recovery

VMware Live Cyber Recovery kann vSAN-Snapshots auf der Schutz-Site verwenden, um mit Ransomware infizierte VMs in der Cloud schneller wiederherzustellen. VLCR kann die Wiederherstellungszeiten verkürzen, indem vSAN-Snapshots nur zur Aktualisierung der VM-Deltas auf der Produktions-Site verwendet werden.

Weitere Informationen finden Sie unter „Schnelle Wiederherstellung mithilfe lokaler VMware vSAN-Snapshots“ in *VMware Live Cyber Recovery*.

Bereitstellen der Snapshot Service-Appliance

vSAN Data Protection benötigt den VMware Snapshot Service zum Verwalten von vSAN-Snapshots.

Stellen Sie die Snapshot Service-Appliance unter Verwendung einer Netzwerkverbindung mit niedriger Latenz auf derselben Site wie Ihre vCenter bereit.

Laden Sie die OVA-Datei herunter und stellen Sie sie bereit, um die VMware Snapshot Service-Appliance hinzuzufügen. Das Bereitstellen der Appliance-OVA ist mit dem Bereitstellen einer virtuellen Maschine aus einer Vorlage vergleichbar.

Diese Appliance benötigt ein vertrauenswürdiges vCenter Server-Zertifikat. Klicken Sie auf der vCenter-Startseite auf **Vertrauenswürdige CA-Root-Zertifikate herunterladen**. Extrahieren Sie die Zertifikatsdateien, öffnen Sie **Zertifikate > lin** und kopieren Sie Text aus der Datei mit der Erweiterung „.0“. Detaillierte Anweisungen finden Sie in folgendem KB-Artikel: https://knowledge.broadcom.com/external/article/330833/how-to-download-and-install-vcenter-serv.html

Verfahren

1. Laden Sie die VMware Snapshot Service-Appliance von der Broadcom-Website unter https://support.broadcom.com/group/ecx/downloads herunter.
2. Klicken Sie im vSphere Client mit der rechten Maustaste auf den vSAN-Cluster und wählen Sie **OVF-Vorlage bereitstellen** aus, um den Assistenten zu öffnen.
3. Geben Sie auf der Seite **OVF-Vorlage auswählen** den Speicherort der Appliance-OVA-Datei an und klicken Sie auf **Weiter**.
4. Auf der Seite **Namen und Ordner auswählen** können Sie einen eindeutigen Namen für die Appliance eingeben und das Datencenter als Speicherort für die Bereitstellung auswählen.

5 Wählen Sie auf der Seite **Computing-Ressource auswählen** den vSAN-Cluster als Computing-Ressource aus.

6 Konfigurieren Sie den Datenspeicher auf der Seite **Speicher auswählen**.

7 Wählen Sie auf der Seite **Netzwerke auswählen** dasselbe Netzwerk wie für das vCenter aus und klicken Sie auf **Weiter**.

8 Geben Sie auf der Seite **Vorlage anpassen** das Root-Kennwort für die Appliance-VM ein und wählen Sie das vCenter aus, auf dem die Appliance bereitgestellt werden soll. Geben Sie im Feld **vCenter Server-Zertifikat** den Zertifikattext ein.

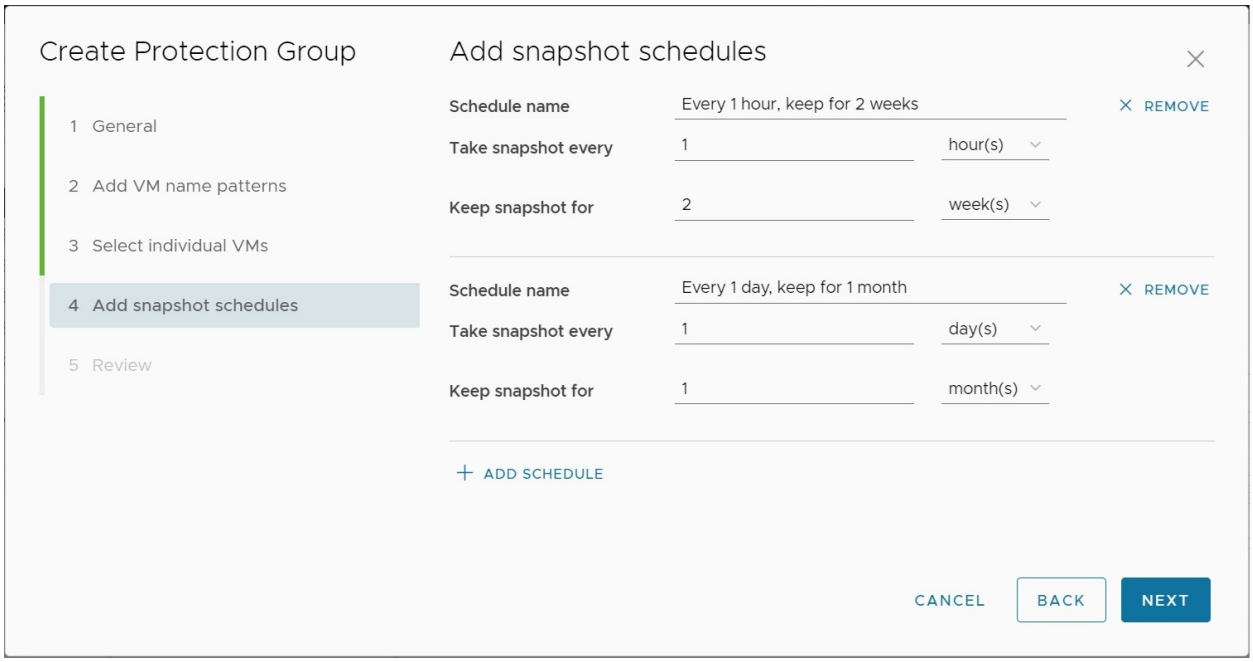
Ergebnisse

Der VMware Snapshot Service wird im angegebenen vCenter bereitgestellt, und vSAN Data Protection-Seiten sind im vSphere Client verfügbar.

Erstellen einer vSAN Data Protection-Gruppe

Platzieren Sie VMs in einer Datenschutzgruppe, um Snapshots für alle VM-Mitglieder der Gruppe konsistent zu planen und zu verwalten.

Mit Schutzgruppen können Sie vSAN-Snapshots für eine oder mehrere VMs planen und verwalten. Sie können verknüpfte Klon-VMs oder VMs mit vSphere-Snapshots nicht zu einer vSAN Data Protection-Gruppe hinzufügen.



Voraussetzungen

Stellen Sie sicher, dass Ihr vSAN-Cluster die folgenden Anforderungen erfüllt:

- vSAN Express Storage Architecture
- vSAN 8.0 Update 3 oder höher

- Auf vCenter bereitgestellte VMware Snapshot Service-Appliance

Verfahren

1. Navigieren Sie zu einem vSAN-Cluster im vSphere Client.
2. Klicken Sie auf die Registerkarte „Konfigurieren“ und wählen Sie **vSAN > Datenschutz** aus.
3. Wählen Sie „Schutzgruppen“ aus und klicken Sie auf **Schutzgruppe erstellen**, um den Assistenten zu öffnen.
   a. Geben Sie auf der Seite „Allgemein“ einen Namen für die Schutzgruppe ein und legen Sie fest, wie die VM-Mitgliedschaft definiert werden soll.

      Hinweis Aktivieren Sie den Unveränderlichkeitsmodus, um schreibgeschützte Snapshots zu erstellen, die selbst von einem Angreifer mit Administratorrechten nicht geändert oder gelöscht werden können. Sobald der Unveränderlichkeitsmodus aktiviert ist, kann dieser nicht mehr von einem Administrator deaktiviert werden.

   b. (Optional) Geben Sie auf der Seite **VM-Namensmuster hinzufügen** mindestens ein passendes VM-Namensmuster ein.

      Alle VMs im Cluster mit einem dem Muster entsprechenden Namen werden der Schutzgruppe hinzugefügt. Verwenden Sie Sonderzeichen, um jedes VM-Namensmuster zu definieren.

      - Verwenden Sie *, um null oder mehr Zeichen abzugleichen. So stimmen die VM-Namensmuster *database** und *prod-*-x* beispielsweise mit den VMs namens „databaseSQL“, „prod-1-x“ und „prod-23-x“ überein.
      - Verwenden Sie ?, um genau ein Zeichen abzubilden. Beispiel: VM-Namensmuster *prod-?* entspricht VMs mit dem Namen „prod-1“, aber nicht mit dem Namen „prod-23“

   c. (Optional) Wählen Sie auf der Seite **Einzelne VMs auswählen** in der Liste VMs aus, die Sie als Mitglieder der Schutzgruppe hinzufügen möchten.

   d. Definieren Sie auf der Seite **Snapshot-Zeitpläne hinzufügen** die Snapshot-Zeitpläne und Aufbewahrungsintervalle.

      Sie können maximal 10 Snapshot-Zeitpläne hinzufügen. Geben Sie den Namen des Zeitplans ein und wählen Sie die Häufigkeit aus, mit der VM-Snapshots von vSAN in der Schutzgruppe erstellt werden. Geben Sie an, wie lange die geplanten Snapshots gespeichert werden sollen.

   e. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl und klicken Sie auf **Erstellen**.

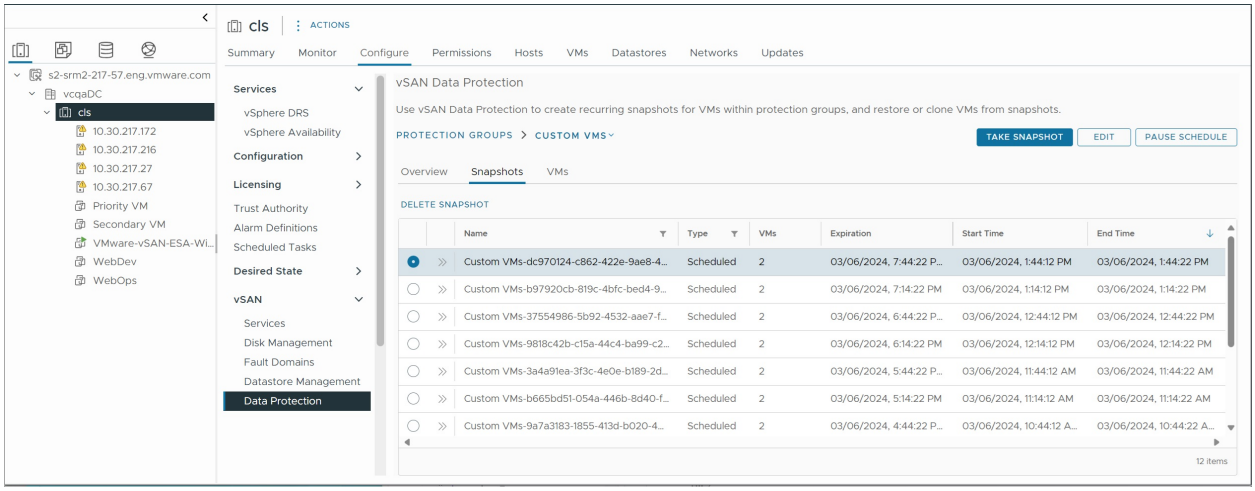
Nächste Schritte

Sie können die Einstellungen der Schutzgruppe bearbeiten. Sie können einen manuellen Snapshot erstellen, um den aktuellen Status der VMs in der Schutzgruppe zu erfassen.

Löschen von vSAN-Snapshots

Verwenden Sie den vSphere Client, um vSAN-Snapshots aus einer Schutzgruppe zu löschen.

Wählen Sie vSAN-Snapshots in einer Schutzgruppe aus und löschen Sie die Snapshots aus der Gruppe.



Verfahren

1. Navigieren Sie zum vSAN-Cluster im vSphere Client und wählen Sie **Konfigurieren > vSAN > Datenschutz** aus.
2. Klicken Sie auf der Registerkarte **Schutzgruppen** auf eine Schutzgruppe und wählen Sie die Registerkarte „Snapshots“ aus.
3. Wählen Sie einen Snapshot aus und klicken Sie auf **Snapshot löschen**.
4. Klicken Sie auf **Löschen**.

Wiederherstellen einer VM aus einem vSAN-Snapshot

Mithilfe eines vSAN-Snapshots können Sie eine VM auf ihren vorherigen im Snapshot beibehaltenen Zustand zurücksetzen.

Wenn Sie eine VM aus einem vSAN-Snapshot wiederherstellen, ersetzt vSAN die aktuelle VM durch die Snapshot-VM. Sie können eine gelöschte VM wiederherstellen, für die Snapshots zur Verfügung stehen.

Verfahren

1. Klicken Sie im vSphere Client mit der rechten Maustaste auf eine VM und wählen Sie das Menü **Snapshots > vSAN Data Protection > Snapshot-Verwaltung** aus.

   Für die Suche nach Snapshots für eine entfernte oder gelöschte VM navigieren Sie zur Seite „Konfigurieren“ > „vSAN“ > „Datenschutz“, klicken auf die Registerkarte **VMs** und dann auf **Entfernte VMs**.
2. Wählen Sie ein Snapshot in der Liste aus und klicken Sie auf **VM wiederherstellen**.

3 Klicken Sie im Dialogfeld „Wiederherstellen“ auf **Wiederherstellen**, um den Vorgang durchzuführen.

   Die VM ist ausgeschaltet, und ein neuer Snapshot wird zum Erfassen des aktuellen Zustands der VM erstellt, der bei Bedarf wiederhergestellt werden kann.

Ergebnisse

Die VM wird in dem vom Snapshot angegebenen vorherigen Zustand wiederhergestellt.

Klonen einer VM aus einem vSAN-Snapshot

Sie können einen vSAN-Snapshot verwenden, um eine verknüpfte Klon-VM zu erstellen, die dem Zustand der ursprünglichen VM entspricht.

Wenn Sie eine VM aus einem vSAN-Snapshot klonen, müssen Sie den Speicherort und die Computing-Ressource für den Klon angeben.

Verfahren

1 Klicken Sie im vSphere Client mit der rechten Maustaste auf eine VM und wählen Sie das Menü **Snapshots > vSAN Data Protection > Snapshot-Verwaltung** aus.

2 Wählen Sie einen Snapshot in der Liste aus und klicken Sie auf **VM klonen**, um das gleichnamige Dialogfeld zu öffnen.

3 Geben Sie einen Namen für den Klon ein, wählen Sie einen Speicherort aus und klicken Sie auf **Weiter**.

4 Wählen Sie eine Computing-Ressource für den Klon aus und klicken Sie auf **Weiter**.

5 Überprüfen Sie die Informationen und klicken Sie auf **Klonen**.

Ergebnisse

Der verknüpfte VM-Klon wird erstellt und steht im vCenter zur Verfügung.

Verwenden des vSAN-iSCSI-Zieldiensts

Mit dem iSCSI-Zieldienst können Sie Hosts und physische Arbeitslasten aktivieren, die außerhalb des vSAN-Clusters liegen, um auf den vSAN-Datenspeicher zuzugreifen.

Diese Funktion aktiviert einen iSCSI-Initiator auf einem Remotehost, um Blockebenendaten an ein iSCSI-Ziel auf einem Speichergerät im vSAN-Cluster zu übertragen. vSAN 6.7 und neuere Versionen unterstützen Windows Server Failover Clustering (WSFC), damit WSFC-Knoten auf vSAN-iSCSI-Ziele zugreifen können.

Nachdem Sie den vSAN-iSCSI-Zieldienst konfiguriert haben, können Sie die vSAN-iSCSI-Ziele über einen ortsfernen Host ermitteln. Um vSAN-iSCSI-Ziele zu ermitteln, verwenden Sie die IP-Adresse eines beliebigen Hosts im vSAN-Cluster und den TCP-Port des iSCSI-Ziels. Um Hochverfügbarkeit des vSAN-iSCSI-Ziels sicherzustellen, konfigurieren Sie die MultiPath-Unterstützung für Ihre iSCSI-Anwendung. Sie können die IP-Adressen von zwei oder mehreren Hosts verwenden, um den MultiPath zu konfigurieren.

Hinweis Der vSAN iSCSI-Zieldienst unterstützt keine anderen vSphere- oder ESXi-Clients oder -Initiatoren, Hypervisoren von Drittanbietern oder Migrationen mit RDMs (Raw Device Mapping).

Der vSAN-iSCSI-Zieldienst unterstützt die folgenden CHAP-Authentifizierungsmethoden:

CHAP

Bei der CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel.

Beiderseitiges CHAP

Bei der beidseitigen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels.

Weitere Informationen zur Verwendung des vSAN-iSCSI-Zieldiensts finden Sie im *Handbuch zur Verwendung von iSCSI-Zielen* https://core.vmware.com/resource/vsan-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 vSAN-iSCSI-Zieldiensts

Bevor Sie iSCSI-Ziele und -LUNs erstellen und iSCSI-Initiatorgruppen definieren können, müssen Sie den iSCSI-Zieldienst auf dem vSAN-Cluster aktivieren.

Verfahren

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

   Der Assistent „vSAN-iSCSI-Zieldienst bearbeiten“ wird geöffnet.
3. Die Konfiguration des vSAN iSCSI-Zieldienstes bearbeiten.

   Sie können gegenwärtig das Standardnetzwerk, den TCP-Port und die Authentifizierungsmethode auswählen. Sie können auch eine vSAN-Speicherrichtlinie auswählen.
4. Klicken Sie auf den Schieberegler **vSAN-iSCSI-Zieldienst aktivieren** um ihn einzuschalten, und klicken Sie dann auf **ÜBERNEHMEN**.

Ergebnisse

Der vSAN iSCSI-Zieldienst ist aktiviert.

Nächste Schritte

Nach dem Aktivieren des iSCSI-Zieldiensts können Sie iSCSI-Ziele und -LUNs erstellen und iSCSI-Initiatorgruppen definieren.

Erstellen eines vSAN-iSCSI-Ziels

Sie können ein iSCSI-Ziel und die zugehörige LUN erstellen oder bearbeiten.

Voraussetzungen

Vergewissern Sie sich, dass der vSAN-iSCSI-Zieldienst aktiviert ist.

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
   a. Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.
   b. Klicken Sie auf die Registerkarte „iSCSI-Ziele“.
   c. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neues iSCSI-Ziel** wird angezeigt. Wenn Sie das Feld „Ziel-IQN“ leer lassen, wird der IQN automatisch generiert.
   d. Geben Sie einen Ziel-**Alias** ein.

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

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

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

3 Klicken Sie auf **OK**.

Ergebnisse

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

Nächste Schritte

Definieren Sie eine Liste von iSCSI-Initiatoren, die auf dieses Ziel zugreifen können.

Hinzufügen einer LUN zu einem vSAN-iSCSI-Ziel

Sie können einem vSAN-iSCSI-Ziel eine oder mehrere LUNs hinzufügen oder eine vorhandene LUN bearbeiten.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

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

d Geben Sie die Größe der LUN ein. Die für den iSCSI-Zieldienst konfigurierte vSAN-Speicherrichtlinie wird automatisch zugewiesen. Sie können jeder LUN eine andere Richtlinie zuweisen.

3 Klicken Sie auf **Hinzufügen**.

Ändern der Größe einer LUN auf einem vSAN-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 vSAN-iSCSI-Initiatorgruppe

Sie können eine vSAN-iSCSI-Initiatorgruppe erstellen, um Zugriffssteuerung für vSAN-iSCSI-Ziele bereitzustellen.

Nur iSCSI-Initiatoren, die Mitglieder der Initiatorgruppe sind, können auf die vSAN-iSCSI-Ziele zugreifen.

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

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
   a. Klicken Sie unter vSAN auf **iSCSI-Zieldienst**.
   b. Klicken Sie auf die Registerkarte „Initiatorgruppe“ und dann auf **Hinzufügen**. Das Dialogfeld **Neue Initiatorgruppe** wird angezeigt.

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

d (Optional) Geben Sie zum Hinzufügen von Mitgliedern zu der Initiatorgruppe den IQN jedes Mitglieds ein. Verwenden Sie für die Eingabe des IQN der Mitglieder folgendes Format:

iqn.YYYY-MM.domain:name

Dabei gilt:

- YYYY = Jahr, z. B. 2016
- MM = Monat, z. B. 09
- domain = Domäne, in der sich der Initiator befindet
- name = Name des Mitglieds (optional)

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

Nächste Schritte

Fügen Sie der iSCSI-Initiatorgruppe die Mitglieder hinzu.

Zuweisen eines Ziels zu einer vSAN-iSCSI-Initiatorgruppe

Sie können einer vSAN-iSCSI-Initiatorgruppe ein iSCSI-Ziel zuweisen.

Nur Initiatoren, die Mitglieder der Initiatorgruppe sind, können auf die zugewiesenen Ziele zugreifen.

Voraussetzungen

Vergewissern Sie sich, dass eine iSCSI-Initiatorgruppe vorhanden ist.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

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

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

3 Klicken Sie auf **Hinzufügen**.

Abschalten des vSAN-iSCSI-Zieldienstes

Sie können den vSAN iSCSI-Zieldienst abschalten.

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

Voraussetzungen

Arbeitslasten, die auf iSCSI-LUNs ausgeführt werden, werden beendet, wenn Sie den iSCSI-Zieldienst abschalten. Vergewissern Sie sich vor dem Abschalten, dass keine Arbeitslasten auf iSCSI-LUNs ausgeführt werden.

Verfahren

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

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

Ergebnisse

Der vSAN iSCSI-Zieldienst ist nicht aktiviert.

Nächste Schritte

Überwachen des vSAN-iSCSI-Zieldiensts

Sie können den iSCSI-Zieldienst überwachen, um die physische Platzierung von iSCSI-Zielkomponenten anzuzeigen und nach fehlgeschlagenen Komponenten zu suchen.

Sie können auch den Integritätsstatus des iSCSI-Zieldienstes überwachen.

Voraussetzungen

Stellen Sie sicher, dass Sie den vSAN-iSCSI-Zieldienst aktiviert und Ziele sowie LUNs erstellt haben.

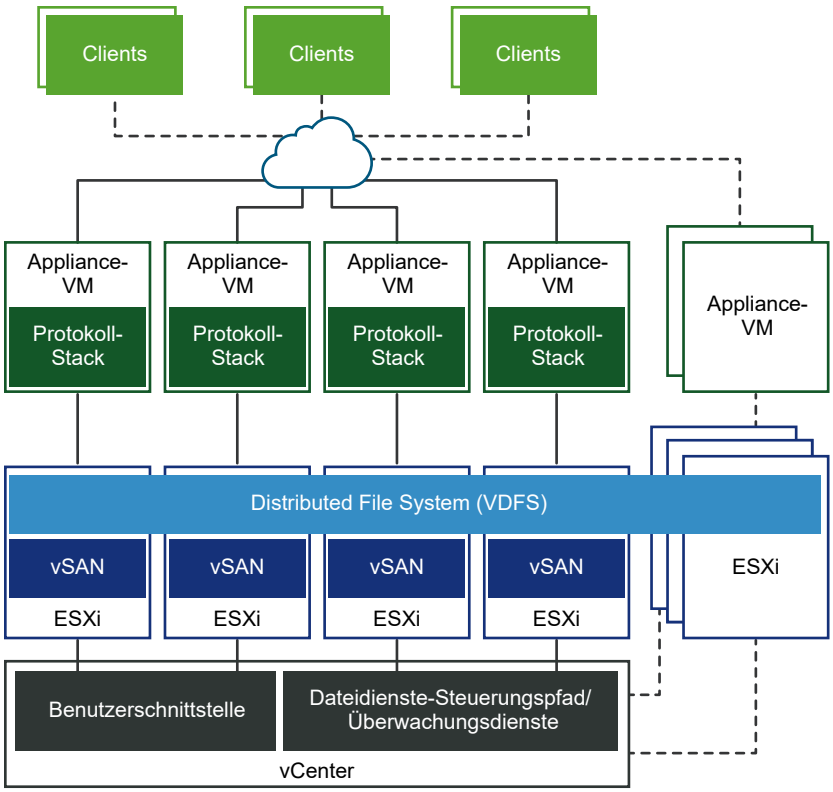
Verfahren

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

vSAN-Dateidienst

Nutzen Sie den vSAN-Dateidienst, um im vSAN-Datenspeicher Dateifreigaben zu erstellen, auf die Client-Arbeitsplätze oder VMs zugreifen können.

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



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

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

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

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

Einschränkungen und Überlegungen zum vSAN-Dateidienst

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

- vSAN 8.0 unterstützt Konfigurationen mit zwei Knoten und Stretched Cluster.
- vSAN 8.0 unterstützt 64 Dateiserver in einer 64-Host-Konfiguration.
- vSAN 8.0 unterstützt 100 Dateifreigaben.
- vSAN 8.0 Update 2 unterstützt den Dateidienst in Express Storage Architecture (ESA).
- Ab vSAN 8.0 Update 3 unterstützen ESA-Cluster 250 Dateifreigaben. Diese 250 Dateifreigaben können maximal 100 SMB-Dateifreigaben enthalten. Wenn Sie beispielsweise 100 SMB-Dateifreigaben erstellen, kann der Cluster lediglich 150 weitere NFS-Dateifreigaben unterstützen.
- vSAN-Dateidienste unterstützen Folgendes nicht:
  - Schreibgeschützte Domänencontroller (RODC) zum Beitritt zu Domänen, da der RODC keine Computerkonten erstellen kann. Als Best Practice für die Sicherheit sollte vorab eine dedizierte Organisationseinheit im Active Directory erstellt werden, und der hier erwähnte Benutzername sollte diese Organisation kontrollieren.
  - Namespace-Verknüpfung entfernen.
  - Umgebungen mit mehreren Domänen und einer einzelnen Active Directory Forest-Struktur.
- Wenn ein Host in den Wartungsmodus wechselt, wird der Dateiserver in eine andere FSVM verschoben. Die FSVM auf dem Host, der in den Wartungsmodus gewechselt ist, wird ausgeschaltet. Nachdem der Host den Wartungsmodus verlassen hat, wird die FSVM eingeschaltet.

- Das interne Docker-Netzwerk der vSAN-Dateidienst-VM kann sich ohne Warnung oder Neukonfiguration mit dem Kundennetzwerk überschneiden.

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

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

Aktivieren des vSAN-Dateidienstes

Sie können vSAN-Dateidienste auf einem vSAN OSA-Cluster (Original Storage Architecture) oder einem vSAN ESA-Cluster (Express Storage Architecture) aktivieren.

Voraussetzungen

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

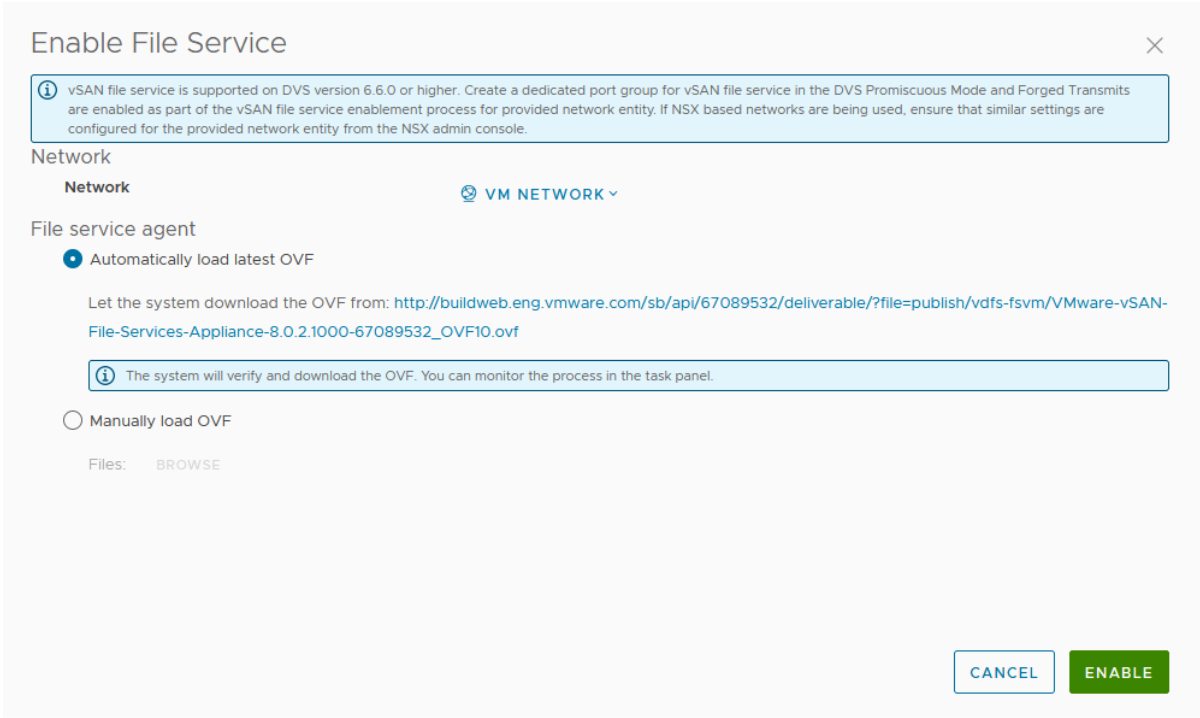
- Der vSAN-Cluster muss ein regulärer vSAN-Cluster, ein vSAN Stretched Cluster oder ein vSAN ROBO-Cluster sein.
- Alle ESXi-Hosts im vSAN-Cluster müssen folgende Mindestanforderungen an die Hardware erfüllen:
  - CPU mit 4 Kernen
  - 16 GB physischer Arbeitsspeicher
- Sie müssen sicherstellen, dass das Netzwerk als vSAN-Dateidienstnetzwerk vorbereitet wird:
  - Bei Verwendung eines auf Standard-Switches basierenden Netzwerks werden der promiskuitive Modus und gefälschte Übertragungen im Rahmen des Aktivierungsvorgangs der vSAN-Dateidienste aktiviert.
  - Bei Verwendung eines DVS-basierten Netzwerks werden vSAN-Dateidienste auf DVS-Version 6.6.0 oder höher unterstützt. Erstellen Sie eine dedizierte Portgruppe für vSAN-Dateidienste im DVS. MacLearning und gefälschte Übertragungen werden im Rahmen der Aktivierung der vSAN-Dateidienste für eine angegebene DVS-Portgruppe aktiviert.
  - **Wichtig** Stellen Sie bei Verwendung eines NSX-basierten Netzwerks sicher, dass MacLearning für die bereitgestellte Netzwerkentität in der NSX-Administrationskonsole aktiviert ist und alle Hosts und Dateidienstknoten mit dem gewünschten NSX-T-Netzwerk verbunden sind.

Verfahren

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

2 Klicken Sie in der Zeile „Dateidienst“ auf **Aktivieren**.

Der Assistent zum Aktivieren des Dateidienstes wird geöffnet.



3 Wählen Sie im Dropdown-Menü **Auswählen** ein Netzwerk aus.

4 Wählen Sie im Dateidienst-Agenten eine der folgenden Optionen aus, um die OVF-Datei herunterzuladen.

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

5 Klicken Sie auf **Aktivieren**.

Ergebnisse

- Die OVF-Datei wird heruntergeladen und bereitgestellt.
- Die vSAN-Dateidienste sind aktiviert.

- Auf jedem Host wird eine Dateidienste-VM (FSVM) platziert.

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

Konfigurieren des vSAN-Dateidiensts

Sie können den Dateidienst konfigurieren, mit dem Sie Dateifreigaben in Ihrem vSAN-Datenspeicher erstellen können.

Voraussetzungen

Stellen Sie Folgendes sicher, bevor Sie den vSAN-Dateidienst konfigurieren:

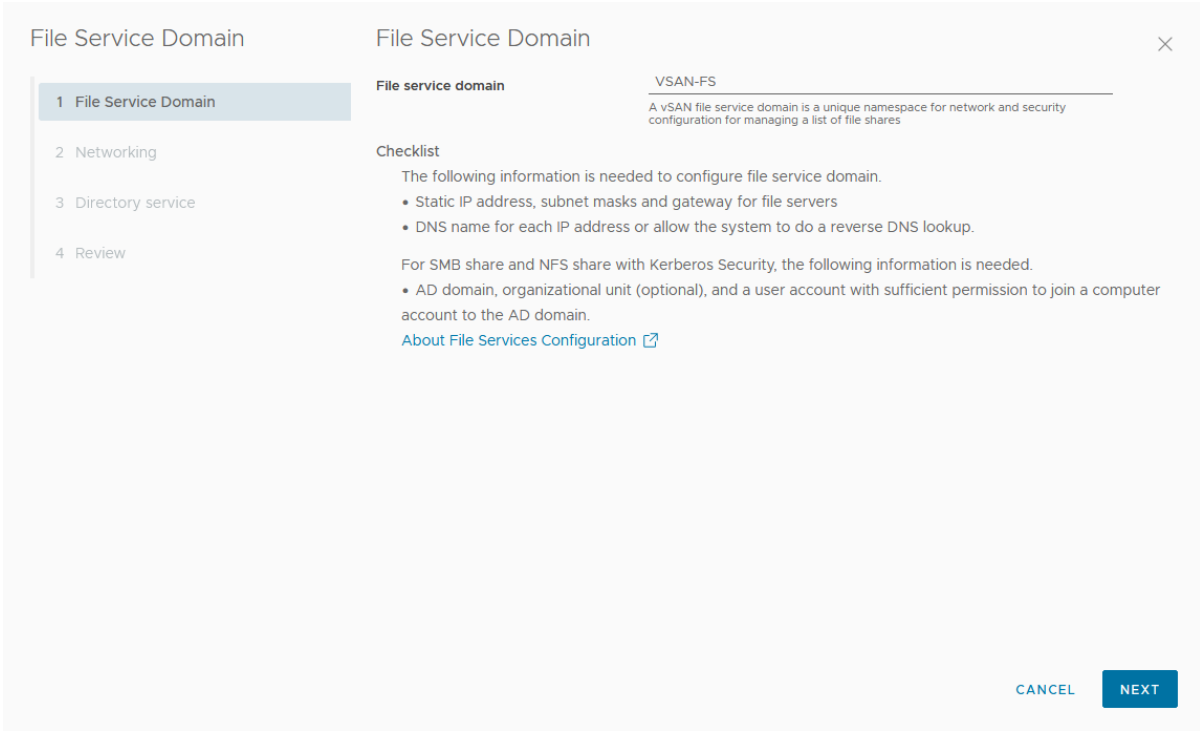
- Aktivieren Sie den vSAN-Dateidienst.
- Weisen Sie statische IP-Adressen als Dateiserver-IPs über das vSAN-Dateidienstnetzwerk zu, wobei mit jeder IP zentral auf vSAN-Dateifreigaben zugegriffen werden kann.
  - Für optimale Leistung muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.
  - Alle statischen IP-Adressen müssen aus demselben Subnetz stammen.
  - Jede statische IP-Adresse verfügt über einen zugehörigen FQDN, der Teil der Forward- und Reverse-Lookup-Zonen im DNS-Server sein sollte.
- Wenn Sie eine Kerberos-basierte SMB- oder NFS-Dateifreigabe erstellen möchten, benötigen Sie Folgendes:
  - AD-Domäne (Microsoft Active Directory) zum Bereitstellen von Authentifizierung bei der Erstellung einer SMB- oder NFS-Dateifreigabe mit Kerberos-Sicherheit.
  - (Optional) Active Directory-Organisationseinheit zum Erstellen aller Computerobjekte des Dateiservers.
  - Ein Domänenbenutzer im Verzeichnisdienst mit ausreichenden Berechtigungen zum Erstellen und Löschen von Computerobjekten.

Verfahren

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

2 Klicken Sie in der Zeile „Dateidienst“ auf **Domäne konfigurieren**.

Der Assistent für die Dateidienstdomäne wird geöffnet.



3 Geben Sie auf der Seite „Dateidienstdomäne“ den eindeutigen Namespace ein und klicken Sie auf **Weiter**. Der Domänenname muss mindestens zwei Zeichen lang sein. Das erste Zeichen muss ein Buchstabe oder eine Zahl sein. Die übrigen Zeichen können Buchstaben, Zahlen, Unterstriche (_), Punkte (.) und Bindestriche (-) sein.

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

- **Protokoll**: Sie können IPv4 oder IPv6 auswählen. Der vSAN-Dateidienst unterstützt nur IPv4- oder IPv6-Stacks. Die Neukonfiguration zwischen IPv4 und IPv6 wird nicht unterstützt.
- **DNS-Server**: Geben Sie einen gültigen DNS-Server ein, um die ordnungsgemäße Konfiguration des Dateidiensts sicherzustellen.
- **DNS-Suffixe**: Geben Sie das DNS-Suffix an, das mit dem Dateidienst verwendet wird. Alle anderen DNS-Suffixe, von denen aus die Clients auf diese Dateiserver zugreifen können, müssen ebenfalls enthalten sein. Der Dateidienst unterstützt keine DNS-Domäne mit einer einzelnen Bezeichnung wie „app“, „wiz“, „com“ usw. Ein Domänenname, der dem Dateidienst zugeordnet ist, sollte das Format „thisdomain.registerdrootdnsname“ aufweisen. DNS-Name und Suffix müssen den Best Practices entsprechen, die unter https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain ausführlich erläutert sind.

- **Subnetzmaske**: Geben Sie eine gültige Subnetzmaske ein. Dieses Textfeld wird bei Auswahl von IPv4 angezeigt.
- **Präfixlänge**: Geben Sie eine Zahl zwischen 1 und 128 ein. Dieses Textfeld wird bei Auswahl von IPv6 angezeigt.
- **Gateway**: Geben Sie ein gültiges Gateway ein.
- **IP-Pool**: Geben Sie die primäre IP-Adresse und den DNS-Namen ein.

Ab vSAN 8.0 Update 3 unterstützen vSAN ESA-Cluster 250 Dateifreigaben. Diese 250 Dateifreigaben können maximal 100 SMB-Dateifreigaben enthalten. Wenn Sie beispielsweise 100 SMB-Dateifreigaben erstellen, kann der Cluster lediglich 150 weitere NFS-Dateifreigaben unterstützen.

Jeder Dateiserver in einem vSAN ESA-Cluster kann maximal 25 Dateifreigaben unterstützen und benötigt mindestens 10 IPs, um die maximale Anzahl von 250 Freigaben zu erreichen. Durch die Zunahme der Dateiserver oder Dateifreigaben pro Host kann es zu Auswirkungen auf die Leistung des vSAN-Dateidiensts kommen. Für eine optimale Leistung muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.

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

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

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

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

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

- Um eine ordnungsgemäße Konfiguration des Dateidiensts zu gewährleisten, muss es sich bei den IP-Adressen, die Sie auf der Seite „Netzwerk“ eingeben, um statische Adressen handeln, und der DNS-Server muss über Datensätze für diese IP-Adressen verfügen. Um eine optimale Leistung zu erzielen, muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.
- Es können maximal 64 Hosts im Cluster vorhanden sein. Wenn die Unterstützung für umfangreiche Cluster konfiguriert ist, können Sie bis zu 64 IP-Adressen eingeben.

- Sie können die folgenden Optionen nutzen, um die Textfelder für die IP-Adresse und den Namen des DNS-Servers automatisch auszufüllen:

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

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

  Hinweis

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

  Die FQDNs werden nur unter den folgenden Bedingungen automatisch abgerufen:

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

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

Option	Beschreibung
Verzeichnisdienst	Konfigurieren Sie eine Active Directory-Domäne für den vSAN-Dateidienst zur Authentifizierung. Wenn Sie planen, eine SMB-Dateifreigabe oder eine NFSv4.1-Dateifreigabe mit Kerberos-Authentifizierung zu erstellen, müssen Sie eine AD-Domäne für den vSAN-Dateidienst konfigurieren.
AD-Domäne	Der vollqualifizierte Domänenname, der vom Dateiserver verknüpft wurde.
Bevorzugter AD-Server	Geben Sie die IP-Adresse des bevorzugten AD-Servers ein. Bei mehreren IP-Adressen ist darauf zu achten, dass sie durch ein Komma getrennt werden.

Option	Beschreibung
Organisationseinheit (optional)	Enthält das Computerkonto, das vom vSAN-Dateidienst erstellt wird. Erstellen Sie in einer Organisation mit komplexen Hierarchien das Computerkonto in einem angegebenen Container, indem Sie einen Schrägstrich verwenden, um Hierarchien zu bezeichnen (z. B. organizational_unit/inner_organizational_unit). **Hinweis** Standardmäßig erstellt der vSAN-Dateidienst das Computerkonto im Computer-Container.
AD-Benutzername	Der Benutzername, der zum Verbinden und Konfigurieren des Active Directory-Diensts verwendet werden soll. Mit diesem Benutzernamen wird Active Directory in der Domäne authentifiziert. Ein Domänenbenutzer authentifiziert den Domänencontroller und erstellt vSAN-Dateidienst-Computerkonten, zugehörige SPN-Einträge und DNS-Einträge (bei Verwendung von Microsoft DNS). Als Best Practice wird empfohlen, ein dediziertes Dienstkonto für den Dateidienst zu erstellen. Ein Domänenbenutzer im Verzeichnisdienst mit den folgenden ausreichenden Berechtigungen zum Erstellen und Löschen von Computerobjekten: ■ (Optional) Hinzufügen/Aktualisieren von DNS-Einträgen
Kennwort	Kennwort für den Benutzernamen des Active Directory in der Domäne. Der vSAN-Dateidienst verwenden das Kennwort, um sich bei AD zu authentifizieren und das Computerkonto für die vSAN-Dateidienste zu erstellen.

Hinweis

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

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

Ergebnisse

Die Dateidienstdomäne ist konfiguriert. Dateiserver werden mit den IP-Adressen gestartet, die während der Konfiguration des vSAN-Dateidiensts zugewiesen wurden.

Bearbeiten des vSAN-Dateidiensts

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

Voraussetzungen

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

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

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

Verfahren

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

   Der Assistent für die Dateidienstdomäne wird geöffnet.
3. Bearbeiten Sie auf der Seite „Dateidienstdomäne“ den Domänennamen des Dateidiensts und klicken Sie auf **Weiter**.
4. Nehmen Sie auf der Seite „Netzwerk“ die entsprechenden Konfigurationsänderungen vor und klicken Sie auf **Weiter**. Sie können die primären IP-Adressen, statischen IP-Adressen und DNS-Namen bearbeiten. Sie können die primären IP-Adressen oder statischen IP-Adressen hinzufügen oder entfernen. Sie können den DNS-Namen nicht ändern, ohne die IP-Adresse zu ändern.

   Hinweis Das Ändern von Domäneninformationen ist eine Aktion, die Unterbrechungen nach sich zieht. Möglicherweise müssen dadurch alle Clients neue URLs verwenden, um erneut eine Verbindung mit den Dateifreigaben herzustellen.
5. Nehmen Sie auf der Seite „Verzeichnisdienst“ die entsprechenden verzeichnisbezogenen Änderungen vor und klicken Sie auf **Weiter**.

   Hinweis Sie können die AD-Domäne, die Organisationseinheit und den Benutzernamen nicht ändern, nachdem Sie vSAN-Dateidienste konfiguriert haben.
6. Klicken Sie auf der Seite „Überprüfen“ auf **Fertigstellen**, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

Ergebnisse

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

Erstellen einer vSAN-Dateifreigabe

Sofern der vSAN-Dateidienst aktiviert ist, können Sie im vSAN-Datenspeicher eine oder mehrere Dateifreigaben erstellen.

Der vSAN-Dateidienst bietet keine Unterstützung für die Verwendung von NFS-Dateifreigaben auf ESXi.

Voraussetzungen

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

Überlegungen zum Namen und zur Nutzung von Freigaben

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

Verfahren

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

   Ab vSAN 8.0 Update 3 unterstützen vSAN ESA-Cluster 250 Dateifreigaben. Diese 250 Dateifreigaben können maximal 100 SMB-Dateifreigaben enthalten. Wenn Sie beispielsweise 100 SMB-Dateifreigaben erstellen, kann der Cluster lediglich 150 weitere NFS-Dateifreigaben unterstützen.

   Jeder Dateiserver in einem vSAN ESA-Cluster kann maximal 25 Dateifreigaben unterstützen und benötigt mindestens 10 IPs, um die maximale Anzahl von 250 Freigaben zu erreichen. Durch die Zunahme der Dateiserver oder Dateifreigaben pro Host kann es zu Auswirkungen auf die Leistung des vSAN-Dateidiensts kommen. Für eine optimale Leistung muss die Anzahl der IP-Adressen mit der Anzahl der Hosts im vSAN-Cluster übereinstimmen.

2 Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen von Dateifreigaben wird geöffnet.

3 Geben Sie auf der Seite „Allgemein“ die folgenden allgemeinen Informationen ein und klicken Sie auf **Weiter**.

   - **Name:** Geben Sie einen Namen für die Dateifreigabe ein.
   - **Protokoll**: Wählen Sie ein geeignetes Protokoll aus. Der vSAN-Dateidienst unterstützt die Dateisystemprotokolle „SMB“ und „NFS“.

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

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

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

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

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

- **Kein Zugriff**: Wählen Sie diese Option aus, um den Zugriff auf die Dateifreigabe von allen IP-Adressen zu verhindern.

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

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

Im vSAN-Datenspeicher wird eine neue Dateifreigabe erstellt.

Anzeigen von vSAN-Dateifreigaben

Sie können die Liste der vSAN-Dateifreigaben anzeigen.

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

Eine Liste der vSAN-Dateifreigaben wird angezeigt. Für jede Dateifreigabe werden Informationen wie Speicherrichtlinie, harte Kontingentgrenze, Nutzung über Kontingent, tatsächliche Nutzung und so weiter angezeigt. Im vSAN ESA-Cluster werden die Anzahl der vorhandenen Dateifreigaben und der maximal zulässige Grenzwert für Dateifreigaben in einem Cluster angezeigt.

Zugreifen auf vSAN-Dateifreigaben

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

Zugreifen auf eine NFS-Dateifreigabe

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

Befehl „mount“ verwenden, um eine vSAN-Dateifreigabe für den Client zu mounten. Beispiel: Mounten Sie `-t nfs vers=3 <nfsv3_access_point> <localmount_point>`.

Beispiel

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

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

Zugreifen auf eine NFS Kerberos-Dateifreigabe

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

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

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

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

Ändern der Zuständigkeit für eine NFS Kerberos-Freigabe

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

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

Zugreifen auf eine SMB-Dateifreigabe

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

Voraussetzungen

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

Verfahren

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

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

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

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

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

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

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

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

Bearbeiten einer vSAN-Dateifreigabe

Sie können die Einstellungen einer vSAN-Dateifreigabe bearbeiten.

Verfahren

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

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

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

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

Ergebnisse

Die Einstellungen der Dateifreigabe werden aktualisiert.

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

Verwalten der SMB-Dateifreigabe in einem vSAN-Cluster

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

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

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

Verfahren

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

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

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

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

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

   Der MMC-Befehlsspeicher wird in Ihre Zwischenablage kopiert.

2 Melden Sie sich beim Windows-Client als Dateidienst-Admin-Benutzer an. Der Dateidienst-Admin-Benutzer wird beim Erstellen der Dateidienstdomäne konfiguriert. Ein Dateidienst-Admin-Benutzer verfügt über alle Berechtigungen auf dem Dateiserver.

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

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

Löschen einer vSAN-Dateifreigabe

Wenn Sie eine Dateifreigabe nicht länger benötigen, können Sie sie löschen.

Wenn Sie eine Dateifreigabe löschen, werden auch alle mit dieser Dateifreigabe verknüpften Snapshots gelöscht.

Verfahren

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

   Eine Liste aller vSAN-Dateifreigaben wird angezeigt.

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

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

vSAN-Snapshot des verteilten Dateisystems

Ein Snapshot bietet eine platzsparende und zeitbezogene Archivierung der Daten.

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

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

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

Überlegungen zum Snapshot des Dateisystems

- Verwenden Sie „Standard“ als Snapshot-Namen, um Daten abzurufen.
- Der Snapshot-Name darf maximal 100 Zeichen umfassen und kann mit Ausnahme der folgenden Zeichen englische Zeichen, Zahlen und Sonderzeichen enthalten:
  - " (ASCII 34)
  - $ (ASCII 36)
  - % (ASCII 37)
  - & (ASCII 38)
  - * (ASCII 42)
  - / (ASCII 47)
  - : (ASCII 58)
  - < (ASCII 60)
  - > (ASCII 62)
  - ? (ASCII 63)
  - \ (ASCII 92)
  - ^ (ASCII 94)
  - | (ASCII 124)
  - ~ (ASCII 126)

Einen Snapshot erstellen

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

Voraussetzungen

Sie sollten eine vSAN-Dateifreigabe erstellt haben.

Verfahren

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

   Eine Liste der vSAN-Dateifreigaben wird angezeigt.

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

   Das Dialogfeld zum Erstellen eines neuen Snapshots wird angezeigt.

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

Ergebnisse

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

Einen Snapshot anzeigen

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

Verfahren

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

   Eine Liste der vSAN-Dateifreigaben wird angezeigt.

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

Ergebnisse

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

Löschen eines Snapshots

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

Verfahren

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

   Eine Liste der vSAN-Dateifreigaben wird angezeigt.

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

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

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

Neuverteilen der Arbeitslast auf vSAN-Dateidiensthosts

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

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

Voraussetzungen

Verfahren

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

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

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

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

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

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

Ergebnisse

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

Rückfordern von Speicherplatz mit Unmap in vSAN Distributed File System

Mithilfe von UNMAP-Befehlen können Sie Speicherplatz zurückfordern, der gelöschten Dateien im vSAN Distributed File System (VDFS) zugeordnet ist, das vom Gast im vSAN-Objekt erstellt wurde.

vSAN 6.7 Update 2 und höher unterstützt UNMAP-Befehle. Durch Löschen oder Entfernen von Dateien und Snapshots wird Speicherplatz im Dateisystem freigegeben. Dieser freie Speicherplatz wird einem Speichergerät zugewiesen, bis er vom Dateisystem freigegeben oder die Zuordnung aufgehoben wird. vSAN unterstützt die Rückforderung von freiem Speicherplatz, die auch als Aufhebung der Zuordnung bezeichnet wird. Sie können Speicherplatz im VDFS freigeben, wenn Sie Dateifreigaben und Snapshots löschen, Dateifreigaben und Snapshots konsolidieren usw. Sie können die Zuordnung von Speicherplatz aufheben, wenn Sie Dateien oder Snapshots löschen.

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

```
vsan.unmap_support –enable
```

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

Upgrade des vSAN-Dateidiensts

Ein Upgrade des Dateidienstes wird rollierend durchgeführt.

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

Voraussetzungen

Stellen Sie sicher, dass für Folgendes ein Upgrade erfolgt:

- ESXi-Hosts
- vCenter Server
- vSAN-Datenträgerformat

Verfahren

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

3 Wählen Sie im Dialogfeld „Upgrade des Dateidiensts“ eine der folgenden Bereitstellungsoptionen aus und klicken Sie auf **UPGRADE**.

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

Überwachen der Leistung des vSAN-Dateidiensts

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

Voraussetzungen

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

Verfahren

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

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

3 Wählen Sie eine der folgenden Optionen aus:

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

4 Klicken Sie auf **ERGEBNISSE ANZEIGEN**.

Ergebnisse

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

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

Überwachen der Kapazität der vSAN-Dateifreigabe

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

Verfahren

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

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

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

Ergebnisse

Die Kapazitätsinformationen für die Dateifreigabe werden angezeigt.

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

Überwachen des vSAN-Dateidiensts und der Integrität der Dateifreigabe

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

Anzeigen der Integrität des vSAN-Dateidienstes

Sie können den Zustand des vSAN-Dateidienstes überwachen.

Voraussetzungen

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

Verfahren

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

2 Erweitern Sie im Abschnitt „Skyline-Integrität“ **Dateidienst**.

3 Klicken Sie auf die folgenden Parameter für die Dateidienstintegrität, um den Status anzuzeigen.

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

Überwachen der Integrität von vSAN-Dateifreigabeobjekten

Sie können den Zustand von Dateifreigabeobjekten überwachen.

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

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

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

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

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

Hinweis Führen Sie die Schritte aus, um einen hybriden vSAN-Cluster zu SSD (Solid State Drive), einen hybriden vSAN-Cluster zu NVMe oder ein SSD zu NVMe zu migrieren.

Voraussetzungen

- Stellen Sie sicher, dass alle vom Cluster verwendeten vSAN-Richtlinien **Keine Einstellung** für Verschlüsselungsdienste, Speicherplatzeffizienz und Speicherebene angeben.

- Sie müssen RAID-1 (Spiegelung) für **Zu tolerierende Fehler** verwenden, bis alle Datenträgergruppen in „All-Flash“ konvertiert sind.

  Diese Voraussetzungen sind nicht anwendbar, wenn Sie einen Cluster von SSD zu NVMe oder NVMe zu SSD migrieren.

Verfahren

1 Entfernen Sie die hybriden Datenträgergruppen vom Host.

   a Navigieren Sie im vSphere Client zum vSAN-Cluster und klicken Sie auf die Registerkarte **Konfigurieren**.

   b Klicken Sie unter vSAN auf **Datenträgerverwaltung**.

   c Wählen Sie unter „Datenträgergruppen“ die zu entfernende Datenträgergruppe aus. Klicken Sie auf **...** und dann auf **Entfernen**.

   Wählen Sie **Vollständige Datenmigration** als Migrationsmodus aus und klicken Sie auf **Ja**.

   Hinweis Migrieren Sie die Datenträgergruppen auf jedem Host im vSAN-Cluster.

2 Entfernen Sie die physischen Magnetdatenträger vom Host.

3 Fügen Sie die Flash-Geräte zum Host hinzu.

   Stellen Sie sicher, dass keine Partitionen auf den Flash-Geräten vorhanden sind.

4 Erstellen Sie die All-Flash-Datenträgergruppen auf dem Host.

5 Wiederholen Sie die Schritte 1 bis 4 auf jedem Host, bis alle hybriden Datenträgergruppen in die All-Flash-Datenträgergruppen konvertiert wurden.

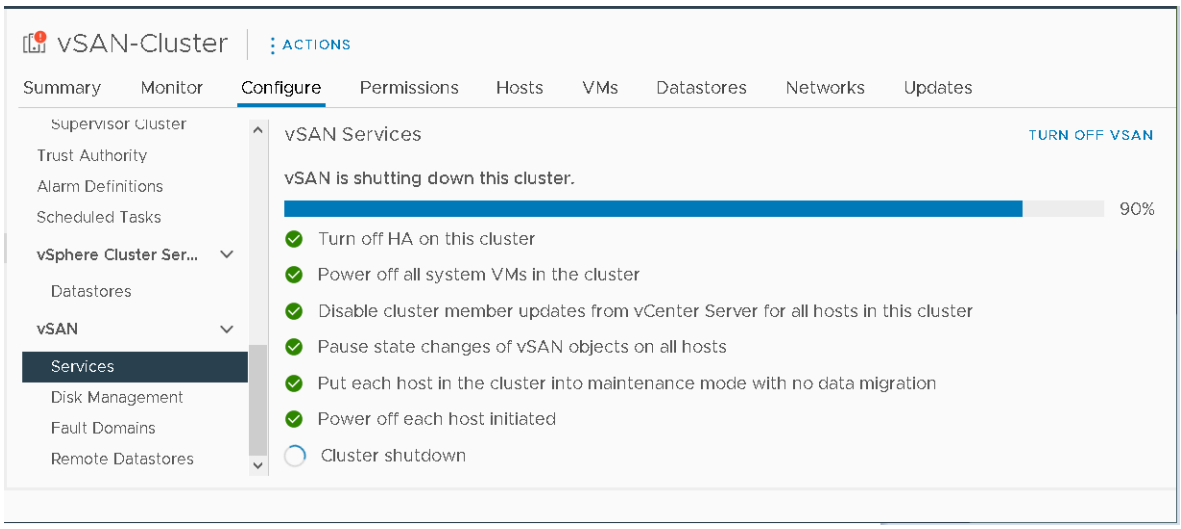
   Hinweis Wenn Sie kein Hot-Plugging von Datenträgern auf dem Host ausführen können, versetzen Sie den Host in den Wartungsmodus, bevor Sie Datenträger im vSphere-Client entfernen. Fahren Sie den Host herunter, um die Datenträger durch Flash-Geräte zu ersetzen. Schalten Sie dann den Host ein, beenden Sie den Wartungsmodus und erstellen Sie neue Datenträgergruppen.

Herunterfahren und Neustarten des vSAN-Clusters

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

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

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



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

Verwenden Sie den Assistenten zum Herunterfahren von Clustern, um den vSAN-Cluster zu Wartungszwecken oder zur Fehlerbehebung ordnungsgemäß herunterzufahren.

Der Assistent zum Herunterfahren von Clustern ist mit vSAN 7.0 Update 3 und höheren Versionen verfügbar.

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

Verfahren

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

   a Überprüfen Sie vSAN Skyline Health, um zu bestätigen, dass der Cluster fehlerfrei ist.

   b Schalten Sie alle virtuellen Maschinen (VMs) aus, die im vSAN-Cluster gespeichert sind, mit Ausnahme von vCenter Server-VMs, vCLS-VMs und Dateidienst-VMs. Wenn vCenter Server auf dem vSAN-Cluster gehostet wird, schalten Sie die vCenter Server-VM oder die von vCenter Server verwendeten VM-Dienst-VMs (z. B. DNS, Active Directory) nicht aus.

c Wenn es sich um einen HCI Mesh-Servercluster handelt, schalten Sie alle auf dem Cluster gespeicherten Client-VMs aus. Wenn die vCenter Server-VM des Client-Clusters in diesem Cluster gespeichert ist, migrieren Sie die VM oder schalten Sie sie aus. Nach dem Herunterfahren des Serverclusters können Clients nicht mehr auf den zugehörigen freigegebenen Datenspeicher zugreifen.

d Vergewissern Sie sich, dass alle Neusynchronisierungsaufgaben abgeschlossen sind.

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

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

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

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

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

Wenn die vCenter Server-Appliance auf dem vSAN-Cluster bereitgestellt wird, zeigt der Assistent zum Herunterfahren des Clusters den Hinweis auf vCenter Server an. Notieren Sie sich die IP-Adresse des Orchestrierungshosts, falls Sie sie während des Neustarts des Clusters benötigen. Wenn vCenter Server Dienst-VMs wie DNS oder Active Directory verwendet, notieren Sie diese als Ausnahme-VMs im Assistenten zum Herunterfahren des Clusters.

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

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

5 Überwachen Sie den Vorgang zum Herunterfahren.

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

Nächste Schritte

Starten Sie den vSAN-Cluster neu. Siehe Neustart des vSAN-Clusters.

Neustart des vSAN-Clusters

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

Verfahren

1 Schalten Sie die Cluster-Hosts ein.

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

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

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

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

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

4 Nachdem der Cluster neu gestartet wurde, überprüfen Sie vSAN Skyline Health und beheben Sie alle ausstehenden Probleme.

Manuelles Herunterfahren und Neustarten des vSAN-Clusters

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

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

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

Verfahren

1 Fahren Sie den vSAN-Cluster herunter.

   a Überprüfen Sie vSAN Skyline Health, 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 oder die von vCenter Server verwendeten Dienst-VMs (z. B. DNS, Active Directory) nicht aus.

   c Wenn der vSAN-Dateidienst im vSAN-Cluster aktiviert ist, müssen Sie den Dateidienst deaktivieren. Durch Deaktivierung des vSAN-Dateidiensts wird die leere Dateidienstdomäne entfernt. Wenn Sie die leere Dateidienstdomäne nach dem Neustart des vSAN-Clusters beibehalten möchten, müssen Sie eine NFS- oder SMB-Dateifreigabe erstellen, bevor Sie den vSAN-Dateidienst deaktivieren.

d 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.

e Vergewissern Sie sich, dass alle Neusynchronisierungsaufgaben abgeschlossen sind.

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

f 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.

g 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
```

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

i 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.

j 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.

k 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 vSAN Skyline Health und beheben Sie alle ausstehenden Probleme.

k (Optional) Aktivieren Sie den vSAN-Dateidienst.

l (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. Wenn vCenter Server Dienst-VMs wie DNS oder Active Directory verwendet, notieren Sie diese als Ausnahme-VMs im Assistenten zum Herunterfahren des Clusters.

Versuchen Sie, die obigen Befehle erst dann erneut zu verwenden, wenn vSAN Skyline Health 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
```

Nächste Schritte

Starten Sie den vSAN-Cluster neu. Siehe Neustart des vSAN-Clusters.

Geräteverwaltung in einem vSAN-Cluster

9

Sie können verschiedene Geräteverwaltungsaufgaben in einem vSAN-Cluster durchführen.

Sie können Hybrid- oder All-Flash-Datenträgergruppen erstellen, vSAN für die Beanspruchung von Geräten für Kapazität und Cache aktivieren, LED-Indikatoren ein- oder ausschalten, Geräte als Flash-Geräte markieren, Remotegeräte als lokal markieren usw.

Hinweis Das Markieren von Geräten als Flash-Gerät und das Markieren von Remotegeräten als lokal werden in einem vSAN Express Storage Architecture-Cluster nicht unterstützt.

Lesen Sie als Nächstes die folgenden Themen:

- Verwalten von Speichergeräten in einem vSAN-Cluster
- Arbeiten mit einzelnen Geräten in einem vSAN-Cluster

Verwalten von Speichergeräten in einem vSAN-Cluster

Wenn Sie vSAN auf einem Cluster konfigurieren, beanspruchen Sie Speichergeräte auf jedem Host, um den vSAN-Datenspeicher zu erstellen.

Der vSAN-Cluster enthält zunächst einen einzelnen vSAN-Datenspeicher. Wenn Sie Datenträger für Datenträgergruppen oder Speicherpools auf jedem Host beanspruchen, nimmt die Größe des Datenspeichers entsprechend der durch diese Geräte hinzugefügten physischen Kapazität zu.

vSAN weist einen einheitlichen Workflow für die Beanspruchung von Datenträgern in allen Szenarien auf. Sie können alle verfügbaren Datenträger nach Modell und Größe oder nach Host auflisten.

Hinzufügen einer Datenträgergruppe (vSAN Original Storage Architecture)

Wenn Sie eine Datenträgergruppe hinzufügen, müssen Sie den Host und die zu beanspruchenden Geräte angeben. Jede Datenträgergruppe enthält ein Flash-Cache- und mindestens ein Kapazitätsgerät. Sie können mehrere Datenträgergruppen auf jedem Host erstellen und ein Cache-Gerät für jede Datenträgergruppe beanspruchen.

Beachten Sie beim Hinzufügen einer Datenträgergruppe 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).

Hinweis Wenn einem vSAN-Cluster ein neuer ESXi-Host hinzugefügt wird, wird der lokale Speicher dieses Hosts nicht automatisch dem vSAN-Datenspeicher hinzugefügt. Sie müssen eine Datenträgergruppe hinzufügen, um den Speicher des neuen Hosts verwenden zu können.

Hinzufügen eines Speicherpools (vSAN Express Storage Architecture)

Jeder Host, der Speicher bereitstellt, enthält einen einzelnen Speicherpool mit Flash-Geräten. Jedes Flash-Gerät stellt dem Cluster Zwischenspeicher und Kapazität zur Verfügung.
Sie können einen Speicherpool mit allen kompatiblen Geräten hinzufügen. vSAN erstellt unabhängig von der Anzahl der Speicherdatenträger, an die der Host angehängt ist, nur einen Speicherpool pro Host.

Datenträger für vSAN Direct beanspruchen

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

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

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

Hinweis Wenn vSAN Express Storage Architecture für den Cluster aktiviert ist, können Sie keine Datenträger für vSAN Direct beanspruchen.

Erstellen einer Datenträgergruppe oder eines Speicherpools in einem vSAN-Cluster

Je nach verwendeter Speicherarchitektur in Ihrem Cluster können Sie eine Datenträgergruppe oder einen Speicherpool erstellen.

Erstellen einer Datenträgergruppe auf einem Host (vSAN Original Storage Architecture)

Sie können Zwischenspeicher- und Kapazitätsgeräte beanspruchen, um Datenträgergruppen auf einem vSAN-Host zu definieren. Wählen Sie ein Zwischenspeichergerät und ein oder mehrere Kapazitätsgeräte aus, um die Datenträgergruppe zu erstellen.

1 Navigieren Sie zum vSAN-Cluster.

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

3 Klicken Sie unter vSAN auf **Datenträgerverwaltung**, wählen Sie einen Host aus der Tabelle aus und klicken Sie dann auf **DATENTRÄGER ANZEIGEN**.

4 Klicken Sie auf **DATENTRÄGERGRUPPE ERSTELLEN**.

5 Wählen Sie die zu beanspruchenden Datenträger aus.

a Wählen Sie das für die Cacheebene zu verwendende Flash-Gerät aus.

b Wählen Sie die für die Kapazitätsebene zu verwendenden Datenträger aus.

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

Hinweis Die neue Datenträgergruppe wird in der Liste angezeigt.

Erstellen eines Speicherpools auf einem Host (vSAN Express Storage Architecture)

Sie können Datenträgergruppe beanspruchen, um einen Speicherpool auf einem vSAN-Host zu definieren. Jeder Host, der Speicher bereitstellt, enthält einen einzelnen Speicherpool mit Flash-Geräten. Jedes Flash-Gerät stellt dem Cluster Zwischenspeicher und Kapazität zur Verfügung. Sie können einen Speicherpool mit allen Geräten erstellen, die für ESA kompatibel sind. vSAN erstellt nur einen Speicherpool pro Host.

In einem Speicherpool stellt jedes Gerät sowohl Cache als auch Kapazität in einer einzigen Ebene bereit. Dies unterscheidet sich von einer Datenträgergruppe, die über dedizierte Geräte in verschiedenen Ebenen von Cache und Kapazität verfügt.

Verwenden Sie die von vSAN verwaltete Datenträgerbeanspruchung, um automatisch alle kompatiblen Datenträger auf den Cluster-Hosts zu beanspruchen. Wenn Sie neue Hosts hinzufügen, beanspruchen vSAN auch kompatible Datenträger auf diesen Hosts. Alle manuell hinzugefügten Datenträger sind von dieser Einstellung nicht betroffen. Sie können solche Datenträger manuell zum Speicherpool hinzufügen.

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

Hinweis Sie können den Datenträgerbeanspruchungsmodus ändern, um **von vSAN beanspruchte verwaltete Datenträger** zu verwenden. vSAN beansprucht automatisch alle kompatiblen Geräte auf Clusterhosts.

5 Gruppieren Sie nach Host.

6 Wählen Sie die kompatiblen Datenträger aus, die beansprucht werden sollen.

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

Hinweis Die Seite „Datenträgerverwaltung“ wird mit den aufgelisteten Hosts angezeigt. In der Spalte „Verwendete Datenträger“ wird angezeigt, dass auf den Hosts Datenträger beansprucht werden, wobei die aktualisierte Anzahl der Datenträger pro Host angegeben wird. Um die beanspruchten Datenträger für den Host anzuzeigen, klicken Sie auf die Schaltfläche „Datenträger anzeigen“.

Beanspruchen von Speichergeräten für Cluster der vSAN Original Storage Architecture

Sie können eine Gruppe von Cache- und Kapazitätsgeräten auswählen. Diese werden dann von vSAN in Standarddatenträgergruppen eingeteilt.

Bei dieser Methode wählen Sie Geräte aus, um Datenträgergruppen für den vSAN-Cluster zu erstellen. Sie benötigen für jede Datenträgergruppe ein Cache-Gerät und mindestens ein Kapazitätsgerät.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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

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

- Bei Hybrid-Datenträgergruppen muss jeder Host, der Speicher bereitstellt, ein Flash-Cache-Gerät und ein oder mehrere Geräte mit Datenträgerkapazität beisteuern. Pro Datenträgergruppe 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 eine oder mehrere HDD-Datenträgergruppe aus, die als Kapazitätsgerät verwendet werden sollen, und klicken Sie für jeden Datenträger auf **Für Kapazitätsschicht beanspruchen**.
  - Klicken Sie auf **Erstellen** oder **OK**.
- Bei All-Flash-Datenträgergruppen muss jeder Host, der Speicher bereitstellt, ein Flash-Cache-Gerät und ein oder mehrere Geräte mit Flash-Kapazität beisteuern. Pro Datenträgergruppe kann nur ein Cache-Gerät hinzugefügt werden.
  - Wählen Sie ein oder mehrere Flash-Geräte aus, die als Cache-Gerät eingesetzt werden sollen, und klicken Sie für jedes dieser Geräte 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**.

vSAN beansprucht die von Ihnen ausgewählten Geräte und ordnet sie in standardmäßigen Datenträgergruppen, die zum vSAN-Datenspeicher beitragen.

Um die Rolle jedes Geräts, das der All-Flash-Datenträgergruppe hinzugefügt wurde, zu überprüfen, navigieren Sie auf der Seite „Datenträgerverwaltung“ zur Spalte „Beansprucht als“ für einen bestimmten Host. Die Tabelle zeigt eine Liste der Geräte und ihrem jeweiligen Zweck in einer Datenträgergruppe an. Bei All-Flash- und Hybrid-Datenträgergruppen wird der Cache-Datenträger immer als erste im Datenträgergruppenraster angezeigt.

Beanspruchen von Speichergeräten für Cluster der vSANExpress Storage Architecture

Sie können eine Gruppe von Geräten auf einem Host auswählen, die von vSAN in Speicherpools organisiert werden.

Nachdem vSAN ESA aktiviert wurde, können Sie Festplatten entweder manuell oder automatisch beanspruchen. Bei der manuellen Methode können Sie eine Gruppe von Speichergeräten auswählen, die beansprucht werden sollen.

Bei der automatischen Festplattenbeanspruchung wählt vSAN automatisch alle kompatiblen Festplatten von den Hosts aus. Wenn dem Cluster neue Hosts hinzugefügt werden, beansprucht vSAN automatisch die kompatiblen Festplatten, die auf diesen Hosts verfügbar sind, und fügt den Speicher dem vSAN-Datenspeicher hinzu.

Sie können Geräte auswählen, die nicht als für vSAN ESA zertifiziert gemeldet sind, und diese Geräte werden im Speicherpool berücksichtigt. Eine solche Konfiguration wird jedoch nicht empfohlen und kann die Leistung beeinträchtigen.

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter vSAN auf **Festplattenverwaltung**.
4. Um Festplatten manuell zu beanspruchen, klicken Sie auf **Ungenutzte Festplatten beanspruchen**.
   a. Wählen Sie die Geräte aus, die Sie beanspruchen möchten.
   b. Klicken Sie auf **Erstellen**.
5. Um Festplatten automatisch zu beanspruchen, klicken Sie auf **FESTPLATTENBEANSPRUCHUNGSMODUS ÄNDERN** und klicken Sie auf die Umschaltfläche **Von vSAN beanspruchte verwaltete Festplatte**.

   Hinweis Wenn Sie sich bei der Konfiguration des Clusters für die Verwendung von vSAN zur Beanspruchung verwalteter Festplatten entschieden haben, ist die Umschaltfläche bereits aktiviert.

vSAN beansprucht die von Ihnen ausgewählten Geräte und ordnet sie in Speicherpools zur Unterstützung des vSAN-Datenspeichers an. Standardmäßig erstellt vSAN einen Speicherpool für jeden ESXi-Host, der dem Cluster Speicher bereitstellt. Wenn die ausgewählten Geräte nicht für vSAN ESA zertifiziert sind, werden diese Geräte nicht für die Erstellung von Speicherpools berücksichtigt.

Festplatten für vSAN Direct beanspruchen

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

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

Verfahren

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

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

Ergebnisse

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

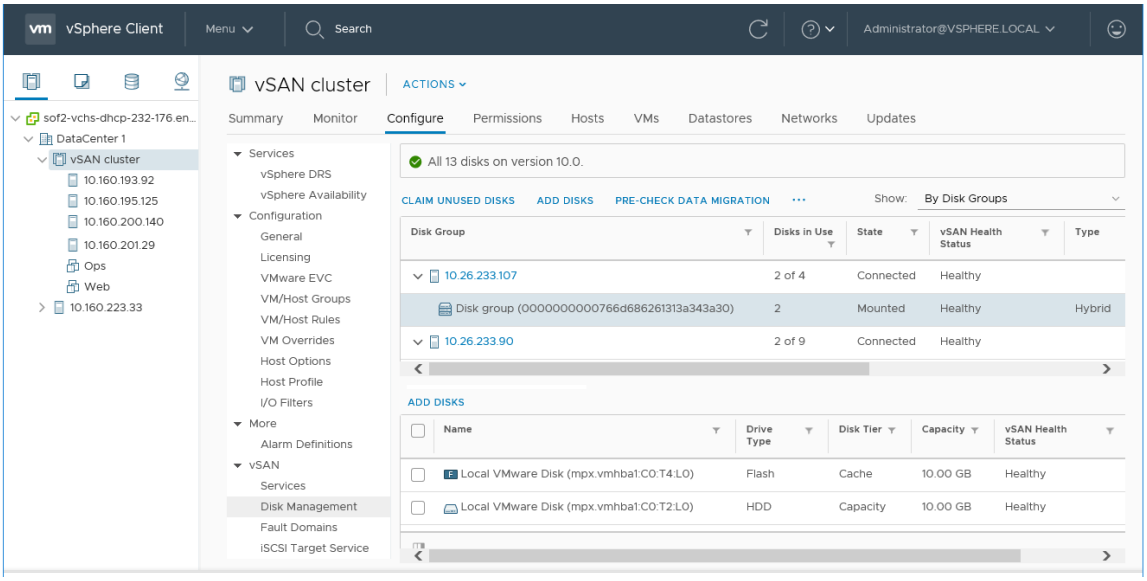
Nächste Schritte

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

Arbeiten mit einzelnen Geräten in einem vSAN-Cluster

Sie können verschiedene Geräteverwaltungsaufgaben im vSAN-Cluster durchführen.

Sie können Geräte zu einer Datenträgergruppe hinzufügen, Geräte aus einer Datenträgergruppe entfernen, Locator-LEDs aktivieren oder deaktivieren und Geräte kennzeichnen. Sie können auch Datenträger hinzufügen oder entfernen, die mit vSAN Direct beansprucht werden.



Hinzufügen von Geräten zu einer Datenträgergruppe im vSAN-Cluster

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

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

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 Datenträgergruppe aus und klicken Sie auf **Datenträger 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 von 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.

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 automatische Neuverteilung außerhalb der Spitzenzeiten durch. Weitere Informationen finden Sie unter „Konfigurieren der automatischen Neuverteilung in vSAN-Clustern“ in *vSAN-Überwachung und -Fehlerbehebung*.

Überprüfen der Datenmigrationsfunktionen eines Datenträgers oder einer Datenträgergruppe im vSAN-Cluster

Verwenden Sie die Vorabprüfung der Datenmigration, um die Auswirkungen von Migrationsoptionen zu ermitteln, wenn Sie einen Datenträger oder Datenträgergruppen unmounten oder aus dem vSAN-Cluster entfernen.

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

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte „Überwachen“.
3. Klicken Sie unter vSAN auf **Vorabprüfung der Datenmigration**.
4. Wählen Sie einen Datenträger oder eine Datenträgergruppe aus, wählen Sie eine Datenmigrationsoption aus und klicken Sie auf **Vorabprüfung**.

   vSAN führt die Tests für die Vorabprüfung der Datenmigration aus.
5. Zeigen Sie die Testergebnisse an.

   Die Ergebnisse der Vorabprüfung zeigen, ob Sie den Datenträger oder die Datenträgergruppe sicher unmounten oder entfernen können.

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

Nächste Schritte

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

Entfernen von Datenträgergruppen oder Geräten aus vSAN

Sie können die ausgewählten Geräte aus einer Datenträgergruppe oder eine komplette Datenträgergruppe aus einem vSAN OSA-Cluster 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 Datenträgergruppen vermeiden sollten.

In der Regel löschen Sie Geräte oder Datenträgergruppen 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 Datenträgergruppe werden die Datenträgermitgliedschaft und die auf den Geräten gespeicherten Daten endgültig gelöscht.

Hinweis Durch das Entfernen eines einzelnen Flash-Cache-Geräts oder aller Kapazitätsgeräte aus einer Datenträgergruppe wird die gesamte Datenträgergruppe entfernt.

Hinweis Wenn der Cluster Deduplizierung und Komprimierung verwendet, können Sie keinen einzelnen Datenträger aus der Datenträgergruppe entfernen. Sie müssen die gesamte Datenträgergruppe entfernen.

Das Evakuieren der Daten aus Geräten oder Datenträgergruppen kann zur vorübergehenden Nichtübereinstimmung mit VM-Speicherrichtlinien führen.

Voraussetzungen

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

Verfahren

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

4 Entfernen Sie eine Datenträgergruppe oder ausgewählte Geräte.

Option	Beschreibung
Datenträgergruppe entfernen	a Wählen Sie unter „Datenträgergruppen“ die zu entfernende Datenträgergruppe aus, klicken Sie auf **...** und dann auf **Entfernen**. b Wählen Sie einen Datenevakuierungsmodus aus.
Ausgewählte Datenträgergruppe entfernen	a Wählen Sie unter „Datenträgergruppen“ die Datenträgergruppe aus, die das zu entfernende Gerät enthält. b Wählen Sie unter „Datenträger“ das zu entfernende Gerät aus und klicken Sie auf das Symbol **Datenträger entfernen**. c Wählen Sie einen Datenevakuierungsmodus aus.

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

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

Erneutes Erstellen einer Datenträgergruppe in einem vSAN-Cluster

Wenn Sie eine Datenträgergruppe im vSAN-Cluster neu erstellen, werden die vorhandenen Datenträger aus der Datenträgergruppe entfernt und die Datenträgergruppe wird gelöscht.

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

Verfahren

1 Navigieren Sie im vSphere Client zum vSAN-Cluster.

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

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

4 Wählen Sie unter „Datenträger“ die Datenträgergruppe aus, die Sie neu erstellen möchten.

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

Das Dialogfeld „Datenträgergruppe neu erstellen“ wird angezeigt.

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

Ergebnisse

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

Verwenden von Locator-LEDs in vSAN

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.

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 führen Sie die gewünschte Aktion für die Locator-LEDs aus.

Option	Aktion
LED einschalten	Schaltet die Locator-LED auf dem ausgewählten Speichergerät ein. Sie können auch die Registerkarte **Verwalten** verwenden und auf **Speicher > Speichergeräte** klicken.
LED ausschalten	Schaltet die Locator-LED auf dem ausgewählten Speichergerät aus. Sie können auch die Registerkarte **Verwalten** verwenden und auf **Speicher > Speichergeräte** klicken.

Markieren von Geräten als Flash-Geräte in vSAN

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 **Datenträgerverwaltung**.

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-Datenträger 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 in vSAN

Wenn lokale Magnetdatenträger von ESXi-Hosts nicht automatisch als HDD-Geräte erkannt werden, können Sie sie manuell als lokale HDD-Geräte markieren.

Wenn Sie ein Magnetdatenträger als Flash-Gerät markiert haben, können Sie den Datenträgertyp des Geräts ändern, indem Sie es als Magnetdatenträger markieren.

Voraussetzungen

- Vergewissern Sie sich, dass der Magnetdatenträger für Ihren Host lokal ist.
- Vergewissern Sie sich, dass der Magnetdatenträger 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 **Datenträgerverwaltung**.
4. Wählen Sie den Host aus, um die Liste der verfügbaren Magnetdatenträger anzuzeigen.
5. Wählen Sie im Dropdown-Menü **Anzeigen** unten auf der Seite die Option **Nicht in Gebrauch** aus.
6. Wählen Sie eine oder mehrere Magnetdatenträger in der Liste aus und klicken Sie auf das Symbol **Als HDD-Datenträger markieren**.
7. Klicken Sie zum Speichern auf **Ja**.

   Als Datenträgertyp des ausgewählten Magnetdatenträgers wird „HDD“ angezeigt.

Markieren von Geräten als lokale Geräte in vSAN

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 **Datenträgerverwaltung**.
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 lokalen Datenträger markieren**.

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

Markieren von Geräten als Remotegeräte in vSAN

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 Datenträgergruppen nicht beansprucht. In vSAN können Sie keine freigegebenen Geräte zu einer Datenträgergruppe hinzufügen.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

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 zur vSAN-Datenträgergruppe

Sie können einer vorhandenen vSAN-Datenträgergruppe ein Kapazitätsgerät hinzufügen.

Sie können ein gemeinsam genutztes Gerät nicht einer Datenträgergruppe 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 Datenträgergruppe aus.

5 Klicken Sie unten auf der Seite auf **Datenträger hinzufügen**.

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

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

Das Gerät wird zur Datenträgergruppe hinzugefügt.

Entfernen der Partition von Geräten

Sie können Partitionsinformationen von einem Gerät entfernen, sodass vSAN das Gerät zur Verwendung beanspruchen kann.

Wenn Sie ein Gerät hinzugefügt haben, das verbleibende Daten oder Partitionsinformationen enthält, müssen Sie alle bereits vorhandenen Partitionsinformationen vom Gerät entfernen, bevor Sie es zur Verwendung durch vSAN beanspruchen können. VMware empfiehlt das Hinzufügen von bereinigten Geräten zu Festplattengruppen.

Wenn Sie Partitionsinformationen von einem Gerät entfernen, löscht vSAN die primäre Partition, die Informationen zum Festplattenformat und logische Partitionen vom Gerät enthält.

Voraussetzungen

Vergewissern Sie sich, dass das Gerät nicht von ESXi als Startfestplatte, VMFS-Datenspeicher oder vSAN verwendet wird.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

4 Wählen Sie einen Host aus, um die Liste der verfügbaren Geräte anzuzeigen.

5 Wählen Sie im Dropdown-Menü **Anzeigen** die Option **Nicht geeignet** aus.

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

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

Das Gerät ist bereinigt und enthält keine Partitionsinformationen mehr.

Erhöhen der Speichereffizienz in einem vSAN-Cluster

10

Mit den Speichereffizienztechniken können Sie den Speicherplatz zum Speichern von Daten verringern.

Diese Techniken reduzieren den zum Erfüllen Ihrer Anforderungen benötigten Gesamtspeicherplatz.

Lesen Sie als Nächstes die folgenden Themen:

- Speichereffizienzfunktionen von vSAN
- Rückfordern von Speicherplatz in vSAN mit SCSI Unmap
- Verwenden von Deduplizierung und Komprimierung in einem vSAN-Cluster
- Verwenden von RAID 5- oder RAID 6-Erasure Coding in einem vSAN-Cluster
- Technische Erwägungen für RAID 5 oder RAID 6 in einem vSAN-Cluster

Speichereffizienzfunktionen von vSAN

Mit den Speichereffizienztechniken können Sie den Speicherplatz zum Speichern von Daten verringern.

Diese Techniken reduzieren die zum Erfüllen Ihrer Anforderungen benötigte Gesamtspeicherkapazität. vSAN 6.7 Update 1 und höher unterstützt Befehle zur Aufhebung der SCSI-Zuordnung (SCSI Unmap), mit denen Sie den Speicherplatz zurückgewinnen können, der einem gelöschten vSAN-Objekt zugeordnet ist.

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

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

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

Rückfordern von Speicherplatz in vSAN mit SCSI Unmap

Mithilfe von SCSI UNMAP-Befehlen können Sie Speicherplatz zurückfordern, der gelöschten Dateien in dem Dateisystem zugeordnet ist, das vom Gast im vSAN-Objekt erstellt wurde.

vSAN 6.7 Update 1 und höher unterstützt SCSI UNMAP. 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.

Die Funktion zum Aufheben der Zuordnung (Unmap) ist standardmäßig nicht aktiviert. Aktivieren Sie **Gast anpassen/Zuordnung von Gast aufheben** auf der Registerkarte „Erweiterte Optionen“ der vSAN-Dienste. 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.

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

Verwenden von Deduplizierung und Komprimierung in einem vSAN-Cluster

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 in jeder Datenträgergruppe oder jedem Speicherpool reduziert. Bei der Deduplizierung werden redundante Datenblöcke entfernt, wohingegen bei der Komprimierung zusätzliche redundante in allen Datenblöcken entfernt werden. Diese Techniken arbeiten zusammen, um den zum Speichern der Daten erforderlichen Speicherplatz zu reduzieren. vSAN wendet Deduplizierung und Komprimierung beim Verschieben von Daten aus der Cache-Schicht in die Kapazitätsschicht an. Verwenden Sie vSAN nur mit Komprimierung für Arbeitslasten, die nicht von der Deduplizierung profitieren, wie z. B. die Online-Transaktionsverwaltung.

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

Bei der vSAN Original Storage Architecture sind Deduplizierung und Komprimierung als clusterweite Einstellung aktiviert, die Anwendung findet jedoch auf Datenträgergruppenbasis statt. Darüber hinaus können Sie die Komprimierung auf bestimmten Arbeitslasten nicht aktivieren, da die Einstellungen nicht über vSAN-Richtlinien geändert werden können. Wenn Sie Deduplizierung und Komprimierung auf einem vSAN-Cluster aktivieren, werden redundante Daten innerhalb jeder Datenträgergruppe auf eine einzelne Kopie reduziert.

Hinweis vSAN nur mit Komprimierung wird auf Datenträgerebene angewendet.

Bei der vSAN Express Storage Architecture ist die Komprimierung auf dem Cluster standardmäßig aktiviert. Wenn Sie die Komprimierung für einige Ihrer VM-Arbeitslasten nicht aktivieren möchten, können Sie dazu eine angepasste Speicherrichtlinie erstellen und die Richtlinie auf die virtuellen Maschinen anwenden. Außerdem ist die Komprimierung für die vSAN Express Storage Architecture nur für neue Schreibvorgänge vorgesehen. Alte Blöcke bleiben unkomprimiert, auch wenn die Komprimierung für ein Objekt aktiviert ist.

Sie können Deduplizierung und Komprimierung beim Erstellen eines vSAN-All-Flash-Clusters oder beim Bearbeiten eines vorhandenen vSAN-All-Flash-Clusters aktivieren. Weitere Informationen finden Sie unter Aktivieren von Deduplizierung und Komprimierung auf einem vorhandenen vSAN-Cluster.

Wenn Sie Deduplizierung und Komprimierung aktivieren oder deaktivieren, führt vSAN eine rollende Neuformatierung aller Datenträgergruppen oder Speicherpools 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 Datenträgern in einem Cluster mit Deduplizierung und Komprimierung

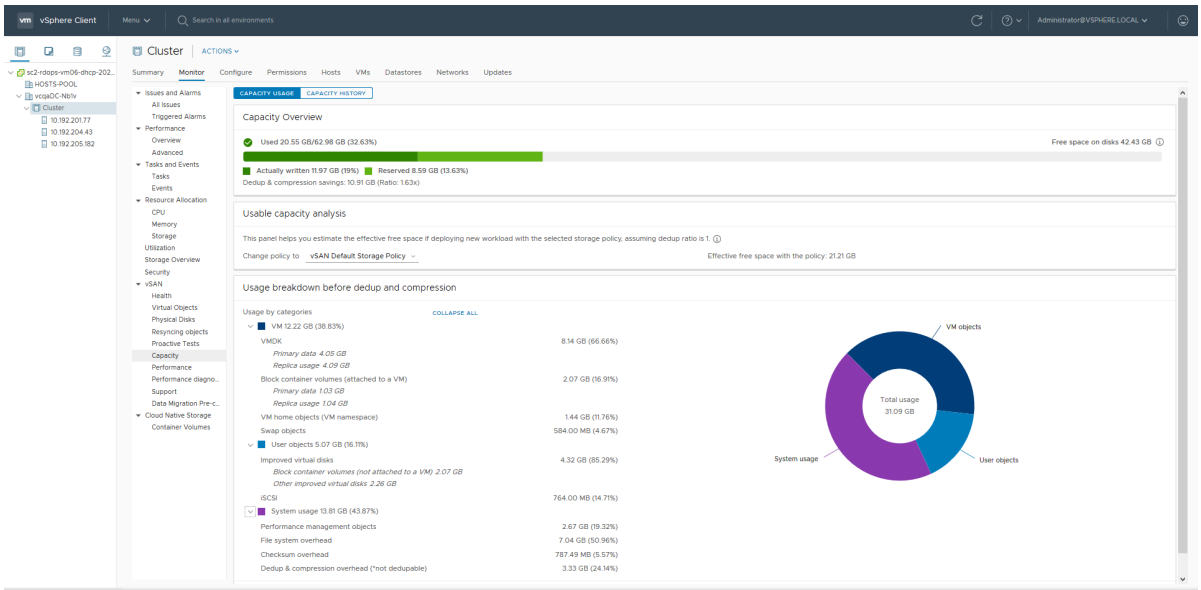
Hinweis Dieses Thema gilt nur für vSAN Original Storage Architecture-Cluster.

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

- Fügen Sie einer Datenträgergruppe keine Datenträger hinzu. Fügen Sie für effizientere Deduplizierung und Komprimierung eine Datenträgergruppe hinzu, um die Speicherkapazität des Clusters zu erhöhen.
- Wenn Sie eine Datenträgergruppe manuell hinzufügen, fügen Sie alle Kapazitätsdatenträger gleichzeitig hinzu.
- Sie können einen einzelnen Datenträger nicht aus einer Datenträgergruppe entfernen. Sie müssen die gesamte Datenträgergruppe entfernen, um Änderungen vorzunehmen.
- Der Ausfall eines einzelnen Datenträgers führt dazu, dass die gesamte Datenträgergruppe 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 Datenträgergruppen 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 Datenträgerspeicher in Anspruch genommen und neu zugeteilt wird.

Technische Erwägungen für Deduplizierung und Komprimierung in einem vSAN-Cluster

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

- Deduplizierung und Komprimierung sind nur auf All-Flash-Datenträgergruppen verfügbar.
- Datenträgerformat 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 Datenträgergruppen über die Deduplizierung und Komprimierung von der Reduzierung von Daten betroffen.
- vSAN kann doppelte Datenblöcke innerhalb jeder einzelnen Datenträgergruppe entfernen, aber nicht über Datenträgergruppen hinweg (gilt nur für vSAN Original Storage Architecture).
- Der Kapazitäts-Overhead für Deduplizierung und Komprimierung beträgt ungefähr fünf Prozent der gesamten Rohkapazität.
- Richtlinien müssen entweder 0 % oder 100 % reservierten Objektspeicherplatz aufweisen. Richtlinien mit 100 % reserviertem Objektspeicherplatz werden immer berücksichtigt. Dies kann jedoch dazu führen, dass Deduplizierung und Komprimierung weniger effizient sind.

Aktivieren von Deduplizierung und Komprimierung auf einem neuen vSAN-Cluster

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

Verfahren

1 Navigieren Sie zu einem neuen All-Flash-vSAN-Cluster.

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

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

   a Klicken Sie unter **Datendienste** auf **BEARBEITEN**.

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

   c Aktivieren Sie unter **Verschlüsselung** die Verschlüsselung ruhender Daten mithilfe der Umschaltfläche.

   Hinweis Wenn Sie vSAN Express Storage Architecture-Cluster verwenden, können Sie diese Einstellung nach dem Beanspruchen von Festplatten nicht mehr ändern.

   d (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 einen vSAN-Cluster.

4 Schließen Sie die Clusterkonfiguration ab.

Aktivieren von Deduplizierung und Komprimierung auf einem vorhandenen vSAN-Cluster

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

So aktivieren Sie sie auf einem vSAN Original Storage Architecture-Cluster:

1 Navigieren Sie zum vSAN-Cluster.

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

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

   a Klicken Sie, um die Speichereffizienz zu bearbeiten.

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

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

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

So aktivieren Sie sie auf einem vSAN Express Storage Architecture-Cluster:

1 Navigieren Sie zum Cluster.

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

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

4 Klicken Sie unter „Datendienste“ auf **BEARBEITEN**.

a Aktivieren Sie unter **Verschlüsselung** die Verschlüsselung ruhender Daten mithilfe der Umschaltfläche.

Hinweis Sie können diese Einstellung nach dem Beanspruchen von Festplatten nicht mehr ändern.

b Aktivieren Sie die Verschlüsselung in Übertragung begriffener Daten, indem Sie die Umschaltfläche „Verschlüsselung in Übertragung begriffener Daten“ verwenden, und geben Sie das Intervall für die erneute Schlüsselerstellung an.

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 einen vSAN-Cluster.

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

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 in einem vSAN-Cluster

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

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

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

   b Klicken Sie auf **Bearbeiten**.

   c Deaktivieren Sie die Deduplizierung und Komprimierung.

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

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

Ergebnisse

Während des Deaktivierens der Deduplizierung und Komprimierung ändert sich das Datenträgerformat für vSAN in jeder Datenträgergruppe des Clusters. vSAN evakuiert die Daten aus der Datenträgergruppe, entfernt die Datenträgergruppe 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 einen 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 Datenträgergruppen notwendig. Zur Ausführung dieser Änderung evakuiert vSAN die Daten aus der Datenträgergruppe, entfernt die Datenträgergruppe 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 Datenträgergruppe 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 Datenträgern mit aktivierter Deduplizierung und Komprimierung

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

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

Verwenden von RAID 5- oder RAID 6-Erasure Coding in einem vSAN-Cluster

Sie können RAID 5- oder RAID 6-Erasure Coding für den Schutz vor Datenverlust und zum Erhöhen der Speichereffizienz verwenden.

Mit Erasure Coding kann derselbe Datenschutz wie bei der Spiegelung (RAID 1) erzielt werden, es wird jedoch weniger Speicherkapazität benötigt. Mit RAID 5- oder RAID 6-Erasure Coding kann vSAN einen Ausfall von bis zu zwei Kapazitätsgeräten im Datenspeicher tolerieren. Sie können RAID 5 auf All-Flash-Clustern mit mindestens vier Fault Domains konfigurieren. Sie können RAID 5 oder RAID 6 auf All-Flash-Clustern mit mindestens sechs Fault Domains konfigurieren.

Im Vergleich zur RAID-1-Spiegelung benötigt RAID 5- oder RAID 6-Erasure Coding weniger zusätzliche Speicherkapazität für den Schutz Ihrer Daten. Beispiel: Eine VM mit RAID 1, die durch die Festlegung von **Zu tolerierende Fehler** auf den Wert 1 geschützt ist, benötigt die zweifache virtuelle Datenträgergröße. 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 10-1. Zum Speichern und Schützen von Daten auf verschiedenen RAID-Ebenen erforderliche Kapazität

RAID-Konfiguration	Zu tolerierende Fehler	Datengröße	Benötigte Kapazität
RAID 1 (Spiegelung)	1	100 GB	200 GB
RAID 5 oder RAID 6 (Erasure Coding) mit vier Fault Domains	1	100 GB	133 GB
RAID 1 (Spiegelung)	2	100 GB	300 GB
RAID 5 oder RAID 6 (Erasure Coding) mit sechs Fault Domains	2	100 GB	150 GB

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

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

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

Hinweis Bei einem vSAN Express Storage Architecture-Cluster variiert je nach Anzahl der verwendeten Fehlerdomänen die Anzahl der Komponenten, die unter **RAID 5** (**Überwachen** > **vSAN**> **Virtuelle Objekte**> testVM > **Platzierungsdetails anzeigen**) aufgeführt sind. Wenn sechs oder mehr Fehlerdomänen im Cluster verfügbar sind, werden fünf Komponenten unter **RAID 5** aufgelistet. Wenn fünf oder weniger Fehlerdomänen verfügbar sind, werden drei Komponenten aufgelistet.

Weitere Informationen zum Konfigurieren von Richtlinien finden Sie unter Kapitel 7 Verwenden von vSAN-Speicherrichtlinien.

Technische Erwägungen für RAID 5 oder RAID 6 in einem vSAN-Cluster

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-Datenträgergruppen verfügbar.
- Datenträgerformat Version 3.0 oder höher ist für die Unterstützung von RAID 5 oder RAID 6 erforderlich.
- Sie müssen über eine gültige Lizenz verfügen, um RAID 5/6 auf einem Cluster zu aktivieren.
- Sie können weitere Speichereinsparungen vornehmen, wenn Sie Deduplizierung und Komprimierung auf dem vSAN-Cluster aktivieren.

Verwenden der Verschlüsselung in einem vSAN-Cluster

11

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

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

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

Lesen Sie als Nächstes die folgenden Themen:

- Verschlüsselung in Übertragung begriffener vSAN-Daten
- Verschlüsselung ruhender vSAN-Daten

Verschlüsselung in Übertragung begriffener vSAN-Daten

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

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

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

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

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

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

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

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

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

Verfahren

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

Ergebnisse

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

Verschlüsselung ruhender vSAN-Daten

vSAN kann ruhende Daten in Ihrem vSAN-Datenspeicher verschlüsseln.

Wenn Sie die Verschlüsselung ruhender Daten aktivieren, verschlüsselt vSAN die Daten, nachdem alle anderen Verarbeitungen durchgeführt wurden, wie z. B. Deduplizierung. Die Verschlüsselung ruhender Daten schützt Daten auf Speichergeräten, wenn ein Gerät aus dem Cluster entfernt wird.

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

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

Sie können einen externen Schlüsselverwaltungsserver (Key Management Server, KMS), das vCenter Server-System und Ihre ESXi-Hosts verwenden, um Daten in Ihrem vSAN-Cluster zu verschlüsseln. vCenter Server fordert Verschlüsselungsschlüssel von einem externen KMS an. Der KMS generiert und speichert die Schlüssel und vCenter Server erhält die Schlüssel-IDs vom KMS und verteilt sie auf den ESXi-Hosts.

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

Funktionsweise der Verschlüsselung ruhender Daten in vSAN

Wenn Sie die Verschlüsselung ruhender Daten aktivieren, verschlüsselt vSAN alles, was sich im vSAN-Datenspeicher befindet.

Alle Dateien werden verschlüsselt, sodass alle virtuellen Maschinen und ihre entsprechenden Daten geschützt sind. Nur Administratoren mit Verschlüsselungsberechtigungen können Verschlüsselungs- und Entschlüsselungsaufgaben durchführen. vSAN verwendet Verschlüsselungsschlüssel wie folgt:

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

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

Verschlüsselungsschlüsselpersistenz

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

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

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

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

```
esxcli system security keypersistence enable
```

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

Verwenden von vSphere Native Key Provider

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

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

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

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

Design-Überlegungen für die Verschlüsselung ruhender Daten in vSAN

Halten Sie sich beim Arbeiten mit der Verschlüsselung ruhender Daten an die folgenden Richtlinien.

- Stellen Sie Ihren KMS-Server nicht im selben vSAN-Datenspeicher bereit, den Sie verschlüsseln möchten.

- Die Verschlüsselung ist CPU-intensiv. Mit AES-NI wird die Verschlüsselungsleistung deutlich gesteigert. Aktivieren Sie AES-NI im BIOS.
- Der Zeugenhost in einem vSAN Stretched Cluster nimmt nicht an der vSAN-Verschlüsselung teil. Der Zeugenhost speichert keine Kundendaten, sondern nur Metadaten wie Größe und UUID des vSAN-Objekts und der Komponenten.

  Hinweis Wenn der Zeugenhost eine Appliance ist, die auf einem anderen Cluster ausgeführt wird, können Sie die darauf gespeicherten Metadaten verschlüsseln. Aktivieren Sie die Verschlüsselung ruhender Daten (Data-at-Rest) auf dem Cluster, der den Zeugenhost enthält.

- Erstellen Sie eine Richtlinie bezüglich Core-Dumps. Core-Dumps sind verschlüsselt, da sie vertrauliche Informationen enthalten können. Gehen Sie sorgfältig mit den vertraulichen Daten um, wenn Sie einen Core-Dump entschlüsseln. ESXi-Core-Dumps können Schlüssel für den ESXi-Host und die sich darauf befindlichen Daten enthalten.
  - Verwenden Sie immer ein Kennwort, wenn Sie ein `vm-support`-Paket erfassen. Sie können das Kennwort angeben, wenn Sie das Support-Paket vom vSphere Client generieren oder den `vm-support`-Befehl verwenden.

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

Einrichten des Standard-Schlüsselanbieters

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

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

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

Hinzufügen eines KMS zu vCenter Server

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

vCenter Server erstellt einen Standard-Schlüsselanbieter, wenn Sie die erste KMS-Instanz hinzufügen. Stellen Sie sicher, dass Sie denselben Schlüsselanbieternamen verwenden, wenn Sie den Schlüsselanbieter auf zwei oder mehreren vCenter Servern konfigurieren.

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

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

Voraussetzungen

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

Verfahren

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

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

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

Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten

Nach dem Hinzufügen des Standardschlüsselanbieters zum vCenter Server-System können Sie eine vertrauenswürdige Verbindung herstellen.

Der spezifische Prozess hängt von den Zertifikaten, die der Schlüsselanbieter akzeptiert, sowie von der Unternehmensrichtlinie ab.

Voraussetzungen

Fügen Sie den Standardschlüsselanbieter hinzu.

Verfahren

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

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

Option	Siehe
CA-Root-Zertifikat von vCenter Server	Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
vCenter Server-Zertifikat	Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Zertifikat und privaten Schlüssel hochladen	Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Neue Zertifikatssignieranforderung	Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.

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

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das Root-CA-Zertifikat auf den KMS hochladen.

Alle von Ihrer Root-Zertifizierungsstelle signierten Zertifikate werden dann von diesem KMS als vertrauensvoll angesehen. Das von der vSphere VM-Verschlüsselung verwendete Root-CA-Zertifikat ist ein selbst signiertes Zertifikat, das in einem separaten Speicher im VECS (VMware Endpoint Certificate Store) auf dem vCenter Server-System gespeichert wird.

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

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

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

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

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

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

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

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

Nächste Schritte

Schließen Sie den Zertifikatsaustausch ab. Siehe Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das vCenter Server-Zertifikat auf den KMS hochladen.

Nach dem Upload akzeptiert der KMS den Datenverkehr, der von einem System mit diesem Zertifikat stammt. vCenter Server generiert ein Zertifikat, um Verbindungen mit dem KMS zu schützen. Das Zertifikat wird in einem getrennten Keystore im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System gespeichert.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

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

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

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

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

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

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

Nächste Schritte

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

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

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass vCenter Server eine Zertifikatssignieranforderung (CSR) generiert und an den KMS übermittelt.

Der KMS signiert die Zertifikatssignieranforderung 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 **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

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

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

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

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

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

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

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

Nächste Schritte

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

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

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

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

Voraussetzungen

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

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

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

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

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

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

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

Nächste Schritte

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

Festlegen des Standardschlüsselanbieters mithilfe des vSphere Client

Sie können den vSphere Client verwenden, um den Standardschlüsselanbieter auf der vCenter Server-Ebene festzulegen.

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

Voraussetzungen

Als Best Practice stellen Sie sicher, dass der Verbindungsstatus auf der Registerkarte „Schlüsselanbieter“ aktiv und mit einem grünen Häkchen versehen ist.

Verfahren

1 Melden Sie sich mithilfe von vSphere Client an.

2 Navigieren Sie zum vCenter Server.

3 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

4 Wählen Sie den Schlüsselanbieter aus.

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

Ein Bestätigungsdialogfeld wird angezeigt.

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

Der Schlüsselanbieter wird als aktueller Standardschlüsselanbieter angezeigt.

Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter

Sofern Sie im Dialogfeld **Standardschlüsselanbieter hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS herzustellen, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikatsaustausch explizit einrichten.

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

- Legen Sie das Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** explizit als vertrauenswürdig fest.
- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat in vCenter Server hoch, indem Sie die Option **vCenter für KMS vertrauenswürdig machen** verwenden.

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

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie den KMS aus.
5. Wählen Sie eine der folgenden Optionen im Dropdown-Menü **Vertrauensstellung herstellen** aus.

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

Aktivieren der Verschlüsselung ruhender Daten auf einem neuen vSAN-Cluster

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

Voraussetzungen

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

Verfahren

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

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

Ergebnisse

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

Generieren neuer Verschlüsselungsschlüssel zur Verschlüsselung ruhender Daten

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

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

- Wenn Sie einen neuen KEK generieren, erhalten alle Hosts im vSAN-Cluster den neuen KEK vom KMS. Der DEK eines jeden Hosts wird mit dem neuen KEK neu verschlüsselt.

- Wenn Sie eine tiefe erneute Schlüsselerstellung durchführen möchten und alle Daten mit neuen Schlüsseln neu verschlüsseln, werden ein neuer KEK und neue DEKs generiert. Eine rollierende Neuformatierung der Datenträger ist erforderlich, um die Daten neu zu verschlüsseln.

Voraussetzungen

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

Verfahren

1. Navigieren Sie zum vSAN-Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter „vSAN“ die Option **Dienste** aus.
4. Klicken Sie auf **Neue Verschlüsselungsschlüssel generieren**.
5. Klicken Sie auf **Übernehmen**, um einen neuen KEK zu generieren. Die DEKs werden mit dem neuen KEK neu verschlüsselt.
   - Um einen neuen KEK und neue DEKs zu generieren und alle Daten im vSAN-Cluster neu zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Auch alle Daten auf dem Speicher mit neuen Schlüsseln neu verschlüsseln**.
   - Wenn der vSAN-Cluster über beschränkte Ressourcen verfügt, aktivieren Sie das Kontrollkästchen **Verringerte Redundanz zulassen**. Wenn Sie verringerte Redundanz zulassen, sind Ihre Daten bei der Neuformatierung des Datenträgers möglicherweise gefährdet.

Aktivieren der Verschlüsselung ruhender Daten auf einem vorhandenen vSAN-Cluster

Sie können die Verschlüsselung ruhender Daten auf vorhandenen vSAN OSA- und vSAN ESA-Clustern aktivieren.

Voraussetzungen

- Erforderliche Rechte:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**

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

Verfahren

1. Navigieren Sie zum vSAN-Host-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Wählen Sie unter vSAN die Option **Dienste** aus.
4. Klicken Sie unter „Verschlüsselung“ auf die Schaltfläche **Bearbeiten**.
5. Aktivieren Sie im Dialogfeld „vSAN-Dienste“ die Option **Verschlüsselung** und wählen Sie einen KMS-Cluster oder Schlüsselanbieter aus.
6. (Optional) Wenn die Speichergeräte in Ihrem Cluster sensible Daten enthalten, aktivieren Sie die Option **Restdaten löschen**.

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

Ergebnisse

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

Nächste Schritte

Sie können die Verschlüsselung im Cluster jederzeit deaktivieren. Eine Neuformatierung des Datenträgers ist erforderlich, da vSAN alle Daten im Datenspeicher entschlüsselt.

vSAN-Verschlüsselung und Core-Dumps

Wenn Ihr vSAN-Cluster die Verschlüsselung ruhender Daten verwendet und auf dem ESXi-Host ein Fehler auftritt, ist der dadurch entstandene Core-Dump aus Datenschutzgründen verschlüsselt.

Auch die Core-Dumps im `vm-support`-Paket sind verschlüsselt.

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

Core-Dumps auf ESXi-Hosts

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

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

Core-Dumps und vm-support-Pakete

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

Core-Dumps auf vCenter Server-Systemen

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

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

Falls auf einem vSAN-Cluster die Verschlüsselung ruhender Daten aktiviert ist, sind die Core-Dumps im `vm-support`-Paket verschlüsselt.

Sie können das Paket erfassen und ein Kennwort angeben, falls Sie davon ausgehen, dass der Core-Dump zu einem späteren Zeitpunkt entschlüsselt werden muss. Das `vm-support` Paket enthält u. a. Protokolldateien und Core-Dump-Dateien.

Voraussetzungen

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

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie die Sicherheits- und Datenschutzrichtlinien Ihrer Organisation, um vertrauliche Informationen wie beispielsweise den Host-Schlüssel zu schützen.

Verfahren

1. Melden Sie sich bei vCenter Server mithilfe von vSphere Client an.
2. Klicken Sie auf **Hosts und Cluster** und klicken Sie dann mit der rechten Maustaste auf den ESXi-Host.
3. Wählen Sie **Systemprotokolle exportieren** aus.
4. Wählen Sie im Dialogfeld **Kennwort für verschlüsselte Core-Dumps** aus, geben Sie ein Kennwort an und bestätigen Sie es.
5. Behalten Sie die Standardeinstellungen für die anderen Optionen bei oder nehmen Sie Änderungen vor, wenn dies vom technischen Support von VMware angefordert wird, und klicken Sie dann auf **Beenden**.
6. Geben Sie einen Speicherort für die Datei an.
7. Falls der Supportmitarbeiter Sie dazu aufgefordert hat, den Core-Dump im `vm-support`-Paket zu entschlüsseln, melden Sie sich bei einem ESXi-Host an und führen Sie die folgenden Schritte aus.
   a. Melden Sie sich beim ESXi-Host an und stellen Sie eine Verbindung zu dem Verzeichnis her, in dem sich das `vm-support`-Paket befindet.

      Der Dateiname richtet sich nach folgendem Muster: **`esx.Datum_und_Uhrzeit.tgz`**.

   b. Stellen Sie sicher, dass das Verzeichnis ausreichend Speicherplatz für das Paket, das dekomprimierte Paket und das erneut komprimierte Paket enthält, oder verschieben Sie das Paket.

   c. Extrahieren Sie das Paket in das lokale Verzeichnis.

      ```
      vm-support -x *.tgz .
      ```

      Die daraus resultierende Dateihierarchie enthält möglicherweise Core-Dump-Dateien für den ESXi-Host (üblicherweise im Verzeichnis `/var/core`) und mehrere Core-Dump-Dateien für virtuelle Maschinen.

d Entschlüsseln Sie jede verschlüsselte Core-Dump-Datei separat.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file ist die Schlüsseldatei des Vorfalls. Sie befindet sich auf der obersten Ebene im Verzeichnis.

encryptedZdump ist der Name der verschlüsselten Core-Dump-Datei.

decryptedZdump ist der von dem Befehl generierte Name der Datei. Legen Sie einen Namen fest, der *encryptedZdump* ähnelt.

e Geben Sie das Kennwort an, das Sie beim Erstellen des `vm-support`-Pakets angegeben haben.

f Entfernen Sie die verschlüsselten Core-Dumps und komprimieren Sie das Paket erneut.

```
vm-support --reconstruct
```

8 Entfernen Sie alle Dateien, die vertrauliche Informationen enthalten.

Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump auf einem ESXi-Host

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 nicht aktiviert ist, müssen Sie möglicherweise zuerst den Zugriff aktivieren.

2 Ermitteln Sie, ob der Core-Dump verschlüsselt ist.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope describe vmmcores.ve`
zdump-Datei	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Entschlüsseln Sie den Core-Dump, je nach Typ.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump-Datei	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

Upgrade des vSAN-Clusters

12

Das Upgrade von vSAN ist ein Prozess mit verschiedenen Phasen, in dem die jeweiligen Vorgänge in der hier beschriebenen Reihenfolge ausgeführt werden müssen.

Hinweis Sie können kein Upgrade eines vSAN Original Architecture-Clusters auf einen vSAN Express Storage Architecture-Cluster mithilfe des vSphere-Clients oder Ruby vSphere Console (RVC) durchführen.

Stellen Sie vor dem Aktualisieren sicher, dass Sie den kompletten Upgradevorgang verstehen, um den Vorgang ohne Probleme und Unterbrechungen durchführen zu können. Wenn Sie mit dem allgemeinen Upgrade-Vorgang für vSphere nicht vertraut sind, sollten Sie zuerst die Dokumentation zum *vSphere Upgrade* lesen.

Hinweis Wenn die hier beschriebene Reihenfolge der Upgrade-Aufgaben nicht befolgt wird, führt dies zu Datenverlust und Ausfall des Clusters.

Das Upgrade des vSAN-Clusters wird in der folgenden Reihenfolge der Aufgaben ausgeführt.

1. Aktualisieren Sie den vCenter Server. Weitere Informationen finden Sie in der *vSphere-Upgrade*-Dokumentation.
2. Aktualisieren Sie die ESXi-Hosts. Siehe Aktualisieren der ESXi-Hosts. Informationen zum Migrieren und Vorbereiten der ESXi-Hosts für das Upgrade finden Sie in der *vSphere Upgrade*-Dokumentation.
3. Führen Sie ein Upgrade des vSAN-Festplattenformats durch. Das Upgrade des Festplattenformats ist optional. Um jedoch optimale Ergebnisse zu erzielen, sollten Sie ein Upgrade der zu verwendenden Objekte auf die aktuelle Version durchführen. Mit dem Festplattenformat wird Ihre Umgebung dem kompletten Funktionssatz von vSAN ausgesetzt. Siehe Upgrade des vSAN-Festplattenformats mit RVC.

Lesen Sie als Nächstes die folgenden Themen:

- Vor dem Upgrade von vSAN
- Aktualisieren von vCenter Server
- Aktualisieren der ESXi-Hosts
- Informationen zum vSAN-Datenträgerformat
- Informationen zum vSAN-Objektformat

- Überprüfen des vSAN-Cluster-Upgrades
- Verwenden der RVC-Upgrade-Befehlsoptionen während des vSAN-Cluster-Upgrades
- vSAN-Build-Empfehlungen für vSphere Lifecycle Manager

Vor dem Upgrade von vSAN

Planen und entwerfen Sie ein ausfallsicheres Upgrade.

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

Voraussetzungen für das Upgrade

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

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

Tabelle 12-1. Voraussetzungen für das Upgrade

Voraussetzungen für das Upgrade	Beschreibung
Software, Hardware, Treiber, Firmware und Speicher-E/A-Controller	Vergewissern Sie sich, dass die neue Version von vSAN die Software- und Hardwarekomponenten, Treiber, Firmware und Speicher-E/A-Controller unterstützt, die Sie verwenden möchten. Die unterstützten Elemente sind auf der Website des VMware-Kompatibilitätshandbuchs unter http://www.vmware.com/resources/compatibility/search.php aufgelistet.
vSAN-Version	Stellen Sie sicher, dass Sie die neueste Version von vSAN verwenden. Sie können kein Upgrade von einer Beta-Version auf die neue vSAN-Version vornehmen. Wenn Sie ein Upgrade von einer Beta-Version durchführen, müssen Sie eine neue Bereitstellung von vSAN ausführen.
Datenträgerspeicher	Stellen Sie sicher, dass ausreichend Speicherplatz verfügbar ist, um das Upgrade der Softwareversion fertig zu stellen. Die Menge des benötigten Datenträgerspeichers für die vCenter Server-Installation hängt von Ihrer vCenter Server-Konfiguration ab. Richtlinien zum erforderlichen Datenträgerspeicher für ein vSphere-Upgrade finden Sie in der Dokumentation zum *vSphere-Upgrade*.
vSAN-Datenträgerformat	Beim vSAN-Datenträgerformat handelt es sich um ein Metadaten-Upgrade, bei dem Daten weder evakuiert noch neu erstellt werden müssen.

Tabelle 12-1. 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 Lifecycle Manager verwenden, um den Upgradevorgang zu automatisieren und zu testen. Wenn Sie allerdings den vSphere Lifecycle Manager zum Aktualisieren von vSAN verwenden, lautet der Standardevakuierungsmodus **Datenzugriff sicherstellen**. Bei Verwendung des Modus **Datenzugriff sicherstellen** sind Ihre Daten nicht geschützt. Falls während des Upgrades von vSAN ein Fehler auftritt, kann dies einen unerwarteten Datenverlust zur Folge haben. Der Modus **Datenzugriff sicherstellen** ist jedoch schneller als der Modus **Alle Daten evakuieren**, weil nicht alle Daten auf einen anderen Host im Cluster verschoben werden müssen. Informationen zu verschiedenen Evakuierungsmodi finden Sie in der Dokumentation *Verwalten von VMware vSAN*.
Virtuelle Maschinen	Vergewissern Sie sich, dass Sie Ihre virtuellen Maschinen gesichert haben.

Empfehlungen

Berücksichtigen Sie die folgenden Empfehlungen beim Bereitstellen von ESXi-Hosts zur Verwendung mit vSAN:

- Wenn ESXi-Hosts mit einer Arbeitsspeicherkapazität von 512 GB oder weniger konfiguriert sind, verwenden Sie SATADOM-, SD-, USB- oder Festplattengeräte als Installationsmedium.
- Wenn ESXi-Hosts mit einer Arbeitsspeicherkapazität von mehr als 512 GB konfiguriert sind, verwenden Sie eine separate Magnetdatenträger oder ein eigenes Flash-Gerät als Installationsgerät. Wenn Sie ein separates Gerät verwenden, stellen Sie sicher, dass vSAN das Gerät nicht beansprucht.
- Wenn Sie einen vSAN-Host von einem SATADOM-Gerät aus starten, müssen Sie ein SLC-Gerät (Single-Level Cell) verwenden und die Größe des Startgeräts muss mindestens 16 GB betragen.
- Informationen dazu, ob Ihre Hardware die Anforderungen für vSAN erfüllt, finden Sie unter *vSAN-Planung und -Bereitstellung*.

vSAN 6.5 und neuere Versionen ermöglichen Ihnen, die Anforderungen der Boot-Größe für einen ESXi-Host in einem vSAN-Cluster anzupassen.

Aktualisieren des Zeugenhosts in einem Cluster mit zwei Hosts oder einem vSAN Stretched Cluster

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

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

Die Verwendung von vSphere Lifecycle Manager zur gleichzeitigen Aktualisierung von Hosts kann unter Umständen dazu führen, dass der Zeugenhost gleichzeitig mit einem der Datenhosts aktualisiert wird. Um diese Probleme bei der Aktualisierung zu vermeiden, konfigurieren Sie vSphere Lifecycle Manager so, dass er den Witness-Server nicht parallel mit den Datenhosts aktualisiert.

Aktualisieren von vCenter Server

Bei dieser ersten Aufgabe im Rahmen des vSAN-Upgrades handelt es sich um ein allgemeines vSphere-Upgrade, das das Upgrade der vCenter Server- und ESXi-Hosts umfasst.

VMware unterstützt In-Place-Upgrades auf 64-Bit-Systemen von vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x und vCenter Server 5.5 auf vCenter Server 6.0 und höher. Das Upgrade von vCenter Server umfasst ein Upgrade des Datenbankschemas sowie ein Upgrade von vCenter Server.

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

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

Aktualisieren der ESXi-Hosts

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

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

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

- Esxcli-Befehl: Sie können Komponenten, Basis-Images und Add-ons als neue Softwareleistung verwenden, um ESXi 7.0-Hosts mithilfe des manuellen Upgrades zu aktualisieren oder zu patchen.

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

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

Nächste Schritte

1. (Optional) Führen Sie ein Upgrade des vSAN-Datenträgerformats durch. Siehe Upgrade des vSAN-Festplattenformats mit RVC.
2. Prüfen Sie die Hostlizenz. In den meisten Fällen müssen Sie Ihre Hostlizenz neu anwenden. Weitere Informationen zum Anwenden von Hostlizenzen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.
3. (Optional) Aktualisieren Sie die virtuellen Maschinen auf den Hosts mithilfe von vSphere Client oder vSphere Lifecycle Manager.

Informationen zum vSAN-Datenträgerformat

Nach Abschluss des ESXi-Updates aktualisieren Sie das vSAN-Datenträgerformat, um auf den vollständigen Funktionssatz von vSAN zuzugreifen.

Jede vSAN-Version unterstützt das Datenträgerformat vorheriger Versionen. Alle Hosts im Cluster müssen dieselbe Version des Datenträgerformats aufweisen. Da bestimmte Funktionen an die Version des Datenträgerformats gebunden sind, sollten Sie ein Upgrade des vSAN-Datenträgerformats auf die höchste Version durchzuführen, die von der ESXi-Version unterstützt wird. Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/2148493.

Version 3 und höher des vSAN-Datenträgerformats benötigt lediglich ein Metadaten-Upgrade, das einige Minuten in Anspruch nimmt. Während des Upgrades des Datenträgerformats wird keine Evakuierung oder Neukonfiguration durchgeführt.

Führen Sie vor dem Upgrade des vSAN-Datenträgerformats das **Upgrade der Vorabprüfung** aus, um ein reibungsloses Upgrade zu gewährleisten. Bei der Vorabprüfung werden potenzielle Probleme erkannt, die ein erfolgreiches Upgrade verhindern könnten, wie z. B. fehlgeschlagene Datenträger oder fehlerhafte Objekte.

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

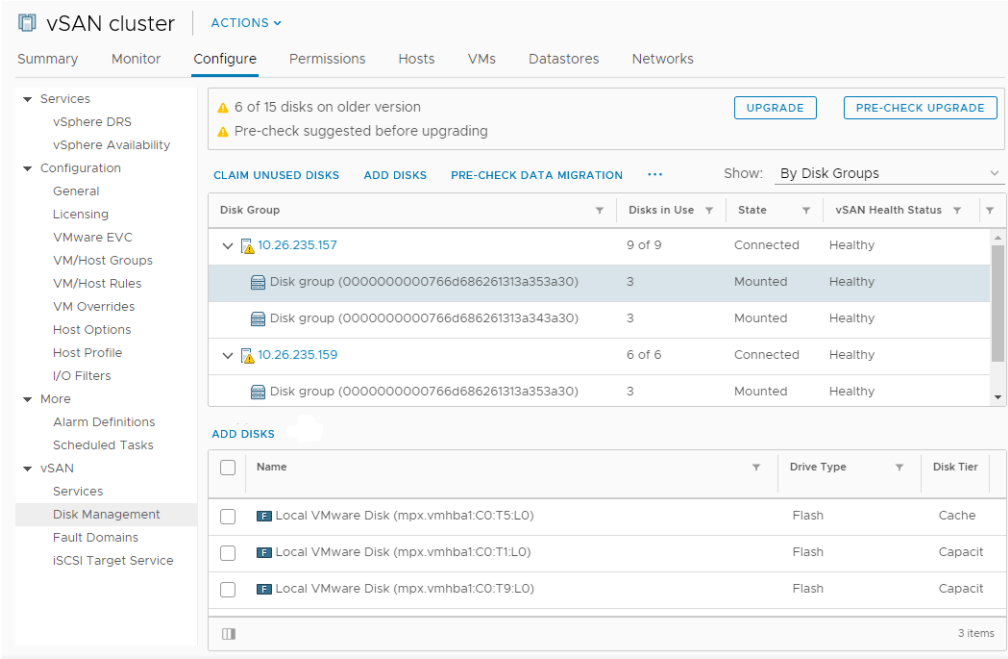
Upgrade des vSAN-Datenträgerformats über den vSphere Client

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

Hinweis Wenn Sie die Verschlüsselung oder die Deduplizierung und Komprimierung auf einem vorhandenen vSAN-Cluster aktivieren, wird das Datenträgerformat 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 Datenträger einen ordnungsgemäßen Status aufweisen. Navigieren Sie zur Seite „Datenträgerverwaltung“, 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 Datenträgerformats 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 Datenträgerformats 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 **Datenträgerverwaltung** 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 Datenträgerstatus, der Netzwerkstatus und der Objektstatus. Upgradeprobleme werden im Textfeld **Status der Datenträgervorabprüfung** angezeigt.

5 Klicken Sie auf **Upgrade durchführen**.

6 Klicken Sie im Dialogfeld „Upgrade“ auf **Ja**, um das Upgrade des Datenträgerformats durchzuführen.

Ergebnisse

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

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

Upgrade des vSAN-Festplattenformats mit RVC

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

Voraussetzungen

- Stellen Sie sicher, dass Sie die aktualisierte Version von vCenter Server verwenden.
- Stellen Sie sicher, dass auf den ESXi-Hosts im vSAN-Cluster Version 6.5 oder höher ausgeführt wird.
- Stellen Sie sicher, dass die Datenträger auf der Seite „Datenträgerverwaltung“ einen ordnungsgemäßen Status aufweisen. Sie können auch den RVC-Befehl `vsan.disks_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 Datenträgerstatus 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 Datenträgerformat durchgeführt wurde: `vsan.obj_status_report`

Überprüfen des Upgrade des vSAN-Festplattenformats

Nachdem Sie das Upgrade des Festplattenformats abgeschlossen haben, müssen Sie überprüfen, ob der vSAN-Cluster das neue Festplattenformat verwendet.

Verfahren

1 Navigieren Sie zum vSAN-Cluster.

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

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

Das aktuelle Festplattenformat wird in der Spalte „Version des Festplattenformats“ angezeigt.

Informationen zum vSAN-Objektformat

Der Arbeitsspeicherplatz, den vSAN zum Durchführen der Richtlinienänderung oder anderer derartiger Vorgänge für ein Objekt, das von vSAN 7.0 oder früher erstellt wurde, benötigt, ist der vom größten Objekt im Cluster verwendete Speicherplatz.

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

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

Überprüfen des vSAN-Cluster-Upgrades

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

Verfahren

1. Navigieren Sie zum vSAN-Cluster.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und stellen Sie sicher, dass vSAN aufgelistet ist.
   - Sie können auch zu Ihrem ESXi-Host navigieren und **Übersicht** > **Konfiguration** auswählen, um sicherzustellen, dass Sie die neueste Version des ESXi-Hosts verwenden.

Verwenden der RVC-Upgrade-Befehlsoptionen während des vSAN-Cluster-Upgrades

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 12-2. 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 Datenträgerformats.
`--allow-reduced-redundancy, -a`	Mit dieser Option entfernen Sie die Anforderung, dass die Menge an freiem Speicherplatz während des Datenträger-Upgrades der Größe einer Datenträgergruppe entsprechen muss. Mit dieser Option werden virtuelle Maschinen während des Upgrades in einem Modus mit reduzierter Redundanz betrieben. Das bedeutet, dass bestimmte virtuelle Maschinen möglicherweise vorübergehend keine Fehler tolerieren und dass ein Ausfall zu Datenverlust führen kann. vSAN stellt die vollständige Übereinstimmung und Redundanz nach Abschluss des Upgrades wieder her.
`--force, -f`	Verwenden Sie diese Option, um „force-proceed“ zu aktivieren und alle Bestätigungsanfragen automatisch zu beantworten.
`--help, -h`	Hiermit werden die Hilfeoptionen angezeigt.

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

vSAN-Build-Empfehlungen für vSphere Lifecycle Manager

vSAN generiert System-Baselines und Baseline-Gruppen, die Sie mit vSphere Lifecycle Manager verwenden können.

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

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

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

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

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

vSAN-System-Baselines

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

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

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

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

vSAN-Versionskatalog

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

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

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

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

Arbeiten mit vSAN-Build-Empfehlungen

vSphere Lifecycle Manager überprüft die installierten ESXi-Versionen anhand der Informationen in der Hardwarekompatibilitätsliste (HCL) im VMware-Kompatibilitätshandbuch. Er bestimmt den richtigen Upgrade-Pfad für jeden vSAN-Cluster basierend auf dem aktuellen vSAN-Versionskatalog. vSAN enthält auch die erforderlichen Treiber und Patch-Updates für die empfohlene Version in der System-Baseline.

vSAN-Build-Empfehlungen stellen sicher, dass für jeden vSAN-Cluster der aktuelle Hardwarekompatibilitätsstatus erhalten bleibt oder verbessert wird. Wenn Hardware im vSAN-Cluster nicht in der HCL enthalten ist, kann vSAN ein Upgrade auf die neueste Version empfehlen, da sie nicht schlechter als der aktuelle Status ist.

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

Die folgenden Beispiele beschreiben die Logik der vSAN-Build-Empfehlungen.

Beispiel 1

Ein vSAN-Cluster führt Version 6.0 Update 2 aus, und die Hardware ist in der HCL für 6.0 Update 2 enthalten. Die HCL gibt an, dass die Hardware bis zu Version 6.0 Update 3, aber nicht für 6.5 und höher unterstützt wird. vSAN empfiehlt ein Upgrade auf Version 6.0 Update 3, einschließlich der erforderlichen kritischen Patches für die Version.

Beispiel 2

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

Beispiel 3

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

Beispiel 4

Ein vSAN-Cluster führt Version 6.7 Update 2 aus, und die Hardware ist in der HCL für 6.7 Update 2 enthalten. Die Hardware wird auch in der HCL für Version 7.0 Update 3 unterstützt,

wobei die ausgewählte Baseline-Einstellung nur für Patches gilt. vSAN empfiehlt ein Upgrade auf Version 7.0 Update 3, einschließlich der erforderlichen kritischen Patches für die Version.

Die Engine für die Empfehlungen wird in regelmäßigen Abständen (einmal täglich) oder bei Eintreten der folgenden Ereignisse ausgeführt.

- Änderungen an Cluster-Mitgliedschaften. Beispiele hierfür sind das Hinzufügen oder Entfernen eines Hosts.
- Der vSAN Management Service wird neu gestartet.
- Ein Benutzer meldet sich über einen Webbrowser oder RVC bei VMware Customer Connect an.
- Das VMware-Kompatibilitätshandbuch oder der vSAN-Versionskatalog wird aktualisiert.

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

Systemanforderungen

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

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

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

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