vSAN-Netzwerkdesign

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 vSAN-Netzwerkdesign

1

Im *vSAN-Netzwerkdesign*-Handbuch werden die Netzwerkanforderungen, das Netzwerkdesign und die Konfigurationsmethoden für die Bereitstellung eines hoch verfügbaren und skalierbaren vSAN-Clusters beschrieben.

vSAN ist eine verteilte Speicherlösung. Wie bei jeder verteilten Lösung ist das Netzwerk eine wichtige Komponente des Designs. Um optimale Ergebnisse zu erzielen, müssen Sie die in diesem Dokument bereitgestellten Anleitungen beachten, da ungeeignete Netzwerkhardware und -designs zu unvorteilhaften Ergebnissen führen können.

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

Dieses Handbuch richtet sich an alle Benutzer, die einen vSAN-Cluster konzipieren, bereitstellen und verwalten. Die Informationen in diesem Handbuch sind für erfahrene Netzwerkadministratoren bestimmt, die mit dem Netzwerkdesign und der Konfiguration, der Verwaltung virtueller Maschinen und den Vorgängen des virtuellen Datencenters vertraut sind. In diesem Handbuch wird zudem davon ausgegangen, dass Sie mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Client vertraut sind.

Zugehörige Dokumente

Zusätzlich zu diesem Handbuch finden Sie in den folgenden Handbüchern weitere Informationen zu vSAN-Netzwerken:

- *vSAN-Planungs- und Bereitstellungshandbuch* mit weiteren Informationen zum Erstellen von vSAN-Clustern
- *Verwalten von VMware vSAN* zum Konfigurieren eines vSAN-Clusters und mit weiteren Informationen zu vSAN-Funktionen
- *vSAN-Überwachungs- und Fehlerbehebungshandbuch* für Überwachung und Fehlerbehebung von vSAN-Clustern

Was ist ein vSAN-Netzwerk?

2

Sie können vSAN verwenden, um den freigegebenen Speicher innerhalb von vSphere bereitzustellen. vSAN fasst lokale oder direkt angeschlossene Speichergeräte eines Hostclusters zusammen und erstellt einen einzelnen Speicherpool, der von allen Hosts im vSAN-Cluster verwendet wird.

vSAN ist eine verteilte und gemeinsam genutzte Speicherlösung, die von einem hoch verfügbaren, ordnungsgemäß konfigurierten Netzwerk für vSAN-Speicherdatenverkehr abhängig ist. Ein leistungsfähiges und verfügbares Netzwerk ist entscheidend für eine erfolgreiche vSAN-Bereitstellung. Dieses Handbuch enthält Empfehlungen zum Konzipieren und Konfigurieren eines vSAN-Netzwerks.

vSAN verfügt über eine verteilte Architektur, die auf einem leistungsstarken, skalierbaren und stabilen Netzwerk basiert. Alle Hostknoten innerhalb eines vSAN-Clusters kommunizieren über das IP-Netzwerk. Alle Hosts müssen die IP-Unicast-Konnektivität beibehalten, damit sie über ein Schicht-2-oder Schicht-3-Netzwerk kommunizieren können. Weitere Informationen zur Unicast-Kommunikation finden Sie unter Kapitel 4 Verwenden von Unicast in einem vSAN-Netzwerk.

vSAN-Begriffe und -Definitionen

vSAN führt bestimmte Begriffe und Definitionen ein, die Sie unbedingt verstehen müssen. Bevor Sie mit der Konzeption Ihres vSAN-Netzwerks beginnen, sehen Sie sich die wichtigen vSAN-Begriffe und -Definitionen an.

Begriffe	Definitionen
CLOM	Der Objektmanager auf Cluster-Ebene (CLOM) ist dafür verantwortlich, sicherzustellen, dass die Konfiguration eines Objekts mit der zugehörigen Speicherrichtlinie übereinstimmt. Der CLOM prüft, ob genügend Fehlerdomänen verfügbar sind, um diese Richtlinie zu erfüllen. Er entscheidet, wo Komponenten und Zeugen in einem Cluster platziert werden.
CMMDS	Der Clusterüberwachungs, Mitgliedschafts- und Verzeichnisdienst (CMMDS) sind für die Wiederherstellung und Wartung eines Clusters mit Netzwerkknotenmitgliedern verantwortlich. Er verwaltet den Bestand von Elementen wie Hostknoten, Geräten und Netzwerken. Außerdem werden Metadateninformationen wie Richtlinien und RAID-Konfiguration für vSAN-Objekte gespeichert.
DOM	Der Manager für verteilte Objekte (DOM) ist für die Erstellung der Komponenten und deren Verteilung auf dem Cluster verantwortlich. Nach dem Erstellen eines DOM-Objekts wird einer der Knoten (Host) als DOM-Besitzer für dieses Objekt nominiert. Dieser Host verarbeitet alle IOPS für dieses DOM-Objekt, indem er die entsprechenden untergeordneten Komponenten im Cluster lokalisiert und die E/A-Vorgänge auf die entsprechenden Komponenten über das vSAN-Netzwerk umleitet. DOM-Objekte umfassen vdisk, Snapshot, vmnamespace, vmswap, vmem usw.
LSOM	Der Log-Structured Object Manager (LSOM) ist verantwortlich für die lokale Speicherung der Daten auf dem vSAN-Dateisystem als vSAN-Komponente oder LSOM-Objekt (Datenkomponente oder Zeugenkomponente).
NIC-Gruppierung	Die Gruppierung der Netzwerkschnittstellenkarte (NIC) kann als zwei oder mehr Netzwerkadapter (NICs) definiert werden, die als „Gruppe“ für Hochverfügbarkeit und Lastausgleich eingerichtet sind.
NIOC	Mit Network I/O Control (NIOC) wird die Bandbreite unterschiedlicher Typen von Netzwerkdatenverkehr auf einem bestimmten vSphere Distributed Switch definiert. Die Bandbreitenverteilung ist ein vom Benutzer konfigurierbarer Parameter. Wenn NIOC aktiviert ist, wird der Distributed Switch-Datenverkehr in vordefinierte Netzwerkressourcenpools aufgeteilt: Fault Tolerance-Datenverkehr, iSCSI-Datenverkehr, vMotion-Datenverkehr, Management-Datenverkehr, vSphere Replication-Datenverkehr, NFS-Datenverkehr und Datenverkehr virtueller Maschinen.

Begriffe	Definitionen
Objekte und Komponenten	Jedes Objekt besteht aus einem Satz von Komponenten, die durch die in der VM-Speicherrichtlinie verwendeten Funktionen bestimmt werden. Ein vSAN-Datenspeicher enthält mehrere Objekttypen: ■ **VM Home-Namespace** – Der VM-Home-Namespace ist ein Startverzeichnis der virtuellen Maschine, in dem alle Konfigurationsdateien der virtuellen Maschine gespeichert werden. Dazu gehören Dateien wie .vmx, Protokolldateien, vmdks und Snapshot-Delta-Beschreibungsdateien. ■ **VMDK** – VMDK ist eine Datenträgerdatei für eine virtuelle Maschine oder .vmdk zur Speicherung der Inhalte eines Festplattenlaufwerks einer virtuellen Maschine. ■ **VM-Auslagerungsobjekt** – VM-Auslagerungsobjekte werden beim Einschalten einer virtuellen Maschine erstellt. ■ **Snapshot Delta-VMDKs** – Snapshot-Delta-VMDKs werden beim Erstellen von VM-Snapshots angelegt. ■ **Arbeitsspeicherobjekt** – Arbeitsspeicherobjekte werden beim Erstellen oder Anhalten einer virtuellen Maschine erstellt, wenn die Arbeitsspeicher-Snapshot-Option aktiviert ist.
RDT	Das RDT-Protokoll wird für die Kommunikation zwischen Hosts über die vSAN-VMkernel-Ports verwendet. Es verwendet TCP auf der Transportschicht und ist dafür verantwortlich, TCP-Verbindungen (Sockets) nach Bedarf zu erstellen und zu löschen. Es ist für das Senden großer Dateien optimiert.
SPBM	Die speicherrichtlinienbasierte Verwaltung (Storage Policy Based Management, SPBM) stellt ein Speicherrichtlinien-Framework bereit, das als einzelne einheitliche Steuerzentrale für ein breites Spektrum von Datendiensten und Speicherlösungen dient. Dieses Framework unterstützt Sie bei der Anpassung des Speichers an den Anwendungsanforderungen der virtuellen Maschinen.
VASA	Die vSphere-Speiche-APIs für Speicherbewusstsein (VASA) ist ein Satz mit Anwendungsprogrammschnittstellen (APIs), mit dem vCenter Server die Funktionen von Speicher-Arrays erkennen kann. VASA-Anbieter kommunizieren mit vCenter Server, um die Speichertopologie, die Funktion und die Statusinformationen zu ermitteln, die die richtlinienbasierte Verwaltung, die Betriebsverwaltung und die DRS-Funktionalität unterstützen.

Begriffe	Definitionen
VLAN	Mit einem VLAN kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten.
Zeugenkomponente	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 belegt etwa 2 MB Speicherplatz für Metadaten im vSAN-Datenspeicher bei Verwendung des Datenträgerformats der Version 1.0 bzw. 4 MB für das Datenträgerformat der Version 2.0 und höher.

Grundlegendes zum vSAN-Netzwerk

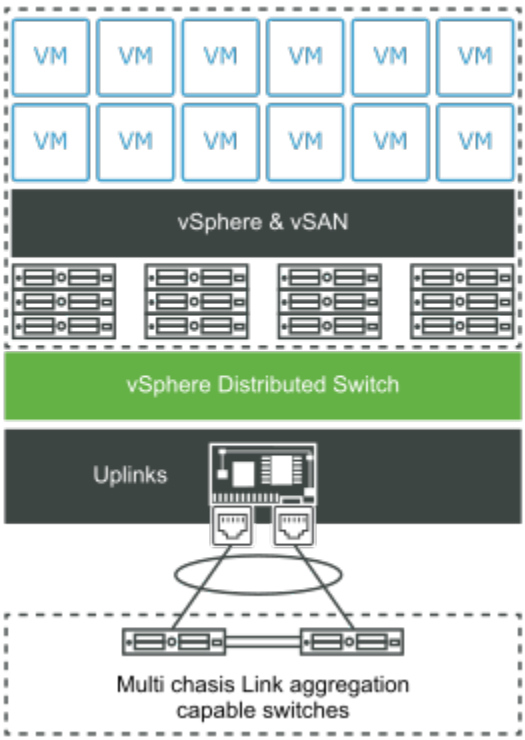
3

Ein vSAN-Netzwerk erleichtert die Kommunikation zwischen Cluster-Hosts und muss eine schnelle Leistung, Hochverfügbarkeit und hohe Bandbreite garantieren.

vSAN verwendet das Netzwerk für die Kommunikation zwischen den ESXi-Hosts und für die Festplatten-E/A der virtuellen Maschine.

Virtuelle Maschinen (VMs) auf vSAN-Datenspeichern bestehen aus einem Satz mit Objekten, und jedes Objekt kann aus einer oder mehreren Komponenten bestehen. Diese Komponenten werden auf mehrere Hosts verteilt, um Ausfallsicherheit für Laufwerk- und Host-Ausfälle zu bieten. vSAN verwaltet und aktualisiert diese Komponenten über das vSAN-Netzwerk.

Das folgende Diagramm bietet eine allgemeine Übersicht über das vSAN-Netzwerk:



Lesen Sie als Nächstes die folgenden Themen:

- vSAN-Netzwerkmerkmale
- Arten des Datenverkehrs von ESXi

vSAN-Netzwerkmerkmale

vSAN ist netzwerkabhängig. Das Verständnis und die Konfiguration der richtigen vSAN-Netzwerkeinstellungen ist der Schlüssel zur Vermeidung von Leistungs- und Stabilitätsproblemen.

Ein zuverlässiges und stabiles vSAN-Netzwerk weist die folgenden Merkmale auf:

Unicast

vSAN 6.6 und höhere Versionen unterstützen die Unicast-Kommunikation. Der Unicast-Datenverkehr ist eine Eins-zu-Eins-Übertragung von IP-Paketen von einem Punkt im Netzwerk zu einem anderen Punkt. Unicast überträgt das vom primären Host gesendete Taktsignal einmal pro Sekunde an alle anderen Hosts. Dadurch wird sichergestellt, dass die Hosts aktiv sind. Zudem wird somit die Teilnahme von Hosts im vSAN-Cluster angezeigt. Sie können für vSAN ein einfaches Unicast-Netzwerk entwerfen. Weitere Informationen zur Unicast-Kommunikation finden Sie unter Kapitel 4 Verwenden von Unicast in einem vSAN-Netzwerk.

Hinweis Verwenden Sie möglichst immer die neueste Version von vSAN.

Schicht-2- und Schicht-3-Netzwerk

Alle Hosts im vSAN-Cluster müssen über ein Netzwerk der Schicht 2 oder Schicht 3 verbunden sein. vSAN-Versionen vor vSAN 6.0 unterstützen nur das Schicht-2-Netzwerk, wohingegen die nachfolgenden Versionen sowohl Schicht-2- als auch Schicht-3-Protokolle unterstützen. Verwenden Sie ein Schicht-2- oder Schicht-3-Netzwerk, um die Kommunikation zwischen den Daten-Sites und der Zeugen-Site bereitzustellen. Weitere Informationen zu Topologien von Schicht-2- und Schicht-3-Netzwerken finden Sie unter Standardbereitstellungen.

VMkernel-Netzwerk

Jeder ESXi-Host in einem vSAN-Cluster muss über einen Netzwerkadapter für die vSAN-Kommunikation verfügen. Die gesamte Intra-Cluster-Knotenkommunikation erfolgt über den vSAN-VMkernel-Port. VMkernel-Ports stellen Schicht-2- und Schicht-3-Dienste für jeden vSAN-Host und gehostete virtuelle Maschinen bereit.

vSAN-Netzwerkdatenverkehr

Im vSAN-Netzwerk sind verschiedene Datenverkehrstypen verfügbar, z. B. der Speicherdatenverkehr und der Unicast-Datenverkehr. Die Berechnung und die Speicherung einer virtuellen Maschine können auf demselben Host oder auf unterschiedlichen Hosts im Cluster erfolgen. Eine VM, die nicht zur Tolerierung eines Fehlers konfiguriert ist, wird möglicherweise auf einem Host ausgeführt und greift auf ein VM-Objekt oder eine Komponente zu, die sich auf einem anderen Host befindet. Dies bedeutet, dass alle E/A-Vorgänge von der VM durch das Netzwerk geleitet werden. Der Speicherdatenverkehr stellt den größten Teil des Datenverkehrs in einem vSAN-Cluster dar.

Die Cluster-bezogene Kommunikation zwischen allen ESXi-Hosts erzeugt den Datenverkehr im vSAN-Cluster. Dieser Unicast-Datenverkehr trägt auch zum vSAN-Netzwerkdatenverkehr bei.

Virtueller Switch

vSAN unterstützt die folgenden Typen virtueller Switches:

- Der virtuelle Standard-Switch stellt die Konnektivität von VMs und VMkernel-Ports zu externen Netzwerken bereit. Dieser Switch ist für jeden ESXi-Host lokal.
- Ein vSphere Distributed Switch bietet eine zentrale Steuerung der Verwaltung des virtuellen Switches über mehrere ESXi-Hosts hinweg. Ein Distributed Switch bietet auch Netzwerkfunktionen wie Network I/O Control (NIOC), die Ihnen bei der Festlegung von QoS-Ebenen (Dienstqualität) in vSphere oder im virtuellen Netzwerk helfen können. vSAN Beinhaltet vSphere Distributed Switch unabhängig von der vCenter Server-Version.

Bandbreite

Der von vSAN generierte Datenverkehr kann physische Netzwerkadapter gemeinsam mit anderem Systemdatenverkehr nutzen, der beispielsweise durch vSphere vMotion, vSphere HA und VMs generiert wird. Er bietet auch mehr Bandbreite für gemeinsam genutzte Netzwerkkonfigurationen, bei denen sich vSAN, vSphere-Verwaltung, vSphere vMotion-Datenverkehr usw. im selben physischen Netzwerk befinden. Die erforderliche Bandbreite für vSAN gewährleisten Sie mithilfe von vSphere Network I/O Control im Distributed Switch.

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

- Nehmen Sie eine Reservierung vor, damit Network I/O Control auf dem physischen Adapter die Mindestbandbreite für vSAN garantiert.
- Legen Sie den Anteilswert auf 100 fest, damit bei einer Sättigung des für vSAN zugewiesenen physischen Adapters eine bestimmte Bandbreite für vSAN verfügbar ist. Beispielsweise könnte der physische Adapter gesättigt sein, wenn ein anderer physischer Adapter im Team fehlschlägt und der gesamte Datenverkehr in der Portgruppe an die anderen Adapter im Team übertragen wird.

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

Arten des Datenverkehrs von ESXi

ESXi-Hosts verwenden unterschiedliche Netzwerkdatenverkehrstypen für die vSAN-Unterstützung.

Im Folgenden finden Sie die unterschiedlichen Arten des Datenverkehrs, die Sie für vSAN einrichten müssen.

Tabelle 3-1. Arten des Datenverkehrs von Netzwerken

Arten des Datenverkehrs	Beschreibung
Verwaltungsnetzwerk	Das Verwaltungsnetzwerk ist die primäre Netzwerkschnittstelle, die einen VMkernel-TCP/IP-Stack verwendet, um die Hostkonnektivität und -verwaltung zu vereinfachen. Es kann auch den Systemdatenverkehr wie vMotion, iSCSI, Netzwerkdateisystem (NFS) (NFS), Fiber Channel over Ethernet (FCoE) und Fault Tolerance verarbeiten.
Netzwerk mit virtuellen Maschinen	Mit virtuellen Netzwerken können Sie virtuelle Maschinen vernetzen und komplexe Netzwerke innerhalb eines einzelnen ESXi-Hosts oder auf mehreren ESXi-Hosts erstellen.
vMotion-Netzwerk	Art des Datenverkehrs, der die VM-Migration von einem Host zu einem anderen erleichtert. Die Migration mit vMotion setzt ordnungsgemäß konfigurierte Netzwerkschnittstellen auf den Quell- und Zielhosts voraus. Stellen Sie sicher, dass sich das vMotion-Netzwerk vom vSAN-Netzwerk unterscheidet.
vSAN-Netzwerk	Ein vSAN-Cluster benötigt das VMkernel-Netzwerk für den Austausch von Daten. Jeder ESXi-Host im vSAN-Cluster muss über einen VMkernel-Netzwerkadapter für den vSAN-Datenverkehr verfügen. Weitere Informationen finden Sie unter „Manuelles Aktivieren von vSAN“ in *vSAN-Planung und -Bereitstellung*.

Netzwerkanforderungen für vSAN

vSAN ist eine verteilte Speicherlösung, die vom Netzwerk für die Kommunikation zwischen Hosts abhängt. Stellen Sie vor der Bereitstellung sicher, dass Ihre vSAN-Umgebung über alle Netzwerkanforderungen verfügt.

Anforderungen an die physische Netzwerkkarte

Netzwerkschnittstellenkarten (NICs), die in vSAN-Hosts verwendet werden, müssen bestimmte Anforderungen erfüllen. vSAN funktioniert in Netzwerken mit 10 Gbit/s, 25 Gbit/s, 40 Gbit/s, 50 Gbit/s und 100 Gbit/s.

Stellen Sie sicher, dass Ihre Hosts die minimalen Anforderungen an die Netzwerkkarte für vSAN Original Storage Architecture (OSA) oder vSAN Express Storage Architecture (ESA) erfüllen.

Tabelle 3-2. vSAN OSA – Mindestanforderungen und Empfehlungen für die Netzwerkkarte (NIC)

Topologie- oder Bereitstellungsmodus	Architektur	Unterstützung von 1-GbE-Netzwerkkarten	Unterstützung von 10-GbE-Netzwerkkarten	Unterstützung von Netzwerkkarten mit mehr als 10 GbE	Latenz zwischen Knoten	Link-Bandbreite oder Latenz zwischen den Sites	Latenz zwischen Knoten und vSAN-Zeugenhosts	Bandbreite zwischen Knoten und vSAN-Zeugenhosts
vSAN-Cluster mit einer Site	Hybrid-Cluster	Ja (Minimum)	Ja (empfohlen)	Ja	Weniger als 1 ms RTT.	NA	NA	NA
	All-Flash-Cluster	Nein	Ja	Ja (empfohlen)				
Stretched vSAN-Cluster	Hybrid- oder All-Flash-Cluster	Nein	Ja (Minimum)	Ja	Weniger als 1 ms RTT innerhalb jeder Site.	Empfohlen werden 10 GbE (arbeitslastabhängig) und 5 ms RTT oder weniger.	Weniger als 200 ms RTT. Bis zu 10 Hosts pro Site.	2 Mbit/s pro 1000 Komponenten (maximal 100 Mbit/s mit 45.000 Komponenten).
							Weniger als 100 ms RTT. 11–15 Hosts pro Site.	
vSAN-Cluster mit zwei Knoten	Hybrid-Cluster	Ja (bis zu 10 VMs)	Ja (empfohlen)	Ja	Weniger als 1 ms RTT innerhalb derselben Site.	Empfohlen werden 10 GbE und 5 ms RTT oder weniger.	Weniger als 500 ms RTT.	2 Mbit/s pro 1000 Komponenten (maximal 1,5 Mbit/s).
	All-Flash-Cluster	Nein	Ja (Minimum)					

Tabelle 3-3. vSAN ESA – Mindestanforderungen und Empfehlungen für die Netzwerkkarte (NIC)

Bereitstellungstyp	Unterstützung von 1-GbE-Netzwerkkarten	Unterstützung von 10-GbE-Netzwerkkarten	Unterstützung von Netzwerkkarten mit mehr als 10 GbE	Latenz zwischen Knoten	Link-Bandbreite oder Latenz zwischen den Sites	Latenz zwischen Knoten und vSAN-Zeugenhosts	Bandbreite zwischen Knoten und vSAN-Zeugenhosts
vSAN-Cluster mit einer Site	Nein	Ja	Ja	Weniger als 1 ms RTT.	NA	NA	NA
Stretched vSAN-Cluster	Nein	Ja	Ja	Weniger als 1 ms RTT innerhalb jeder Site.	Mindestens 10 GbE (arbeitslastabhängig) und 5 ms RTT.	Weniger als 200 ms RTT. Bis zu 10 Hosts pro Site.	2 Mbit/s pro 1000 Komponenten (maximal 100 Mbit/s mit

Tabelle 3-3. vSAN ESA – Mindestanforderungen und Empfehlungen für die Netzwerkkarte (NIC) (Fortsetzung)

Bereitstellungstyp	Unterstützung von 1-GbE-Netzwerkkarten	Unterstützung von 10-GbE-Netzwerkkarten	Unterstützung von Netzwerkkarten mit mehr als 10 GbE	Latenz zwischen Knoten	Link-Bandbreite oder Latenz zwischen den Sites	Latenz zwischen Knoten und vSAN-Zeugenhosts	Bandbreite zwischen Knoten und vSAN-Zeugenhosts
						Weniger als 100 ms RTT. 11–15 Hosts pro Site.	45.000 Komponenten).
vSAN-Cluster mit zwei Knoten	Nein	Ja	Ja	Weniger als 1 ms RTT innerhalb derselben Site.	Empfohlen werden 25 GbE und 5 ms RTT oder weniger.	Weniger als 500 ms RTT.	2 Mbit/s pro 1000 Komponenten (maximal 1,5 Mbit/s).

Hinweis Diese NIC-Anforderungen gehen davon aus, dass der Paketverlust in den hyperkonvergierten Umgebungen nicht mehr als 0,0001 % beträgt. Es kann zu drastischen Auswirkungen auf die vSAN-Leistung führen, wenn eine dieser Anforderungen überschritten wird.

Weitere Informationen zu den Netzwerkkartenanforderungen für vSAN Stretched Cluster finden Sie im *vSAN Stretched Cluster-Handbuch*.

Anforderungen an Bandbreite und Latenz

Um eine hohe Leistung und Verfügbarkeit zu gewährleisten, müssen vSAN-Cluster bestimmte Anforderungen an die Bandbreite und Netzwerklatenz erfüllen.

Die Bandbreitenanforderungen zwischen den primären und sekundären Sites für einen vSAN Stretched Cluster hängen von der vSAN-Arbeitslast, der Datenmenge und der Art und Weise ab, wie Sie Fehler behandeln möchten. Weitere Informationen finden Sie im *Handbuch für VMware vSAN Design und Dimensionierung*.

Tabelle 3-4. Anforderungen an Bandbreite und Latenz

Site-Kommunikation	Bandbreite	Latenz
Site zu Site	vSAN OSA: mindestens 10 GBit/s vSAN ESA: mindestens 10 GBit/s	Weniger als 5 ms Latenz RTT.
Site zum Zeugen	2 Mbit/s pro 1000 vSAN-Komponenten	■ Weniger als 500 ms Latenz RTT für 1 Host pro Site. ■ Weniger als 200 ms Latenz RTT für bis zu 10 Hosts pro Site. ■ Weniger als 100 ms Latenz-RTT für 11–15 Hosts pro Site.

Unterstützung von Schicht 2 und Schicht 3

VMware empfiehlt die Schicht-2-Konnektivität zwischen allen vSAN-Hosts, die das Subnetz gemeinsam nutzen.

vSAN unterstützt auch Bereitstellungen mit gerouteter Schicht-3-Konnektivität zwischen vSAN-Hosts. Sie müssen die Anzahl Hops und die zusätzliche Latenz berücksichtigen, die während des Routings des Datenverkehrs auftreten.

Tabelle 3-5. Unterstützung von Schicht 2 und Schicht 3

Clustertyp	S2 unterstützt	S3 unterstützt	Überlegungen
Hybrid-Cluster	Ja	Ja	S2 wird empfohlen und S3 wird unterstützt.
All-Flash-Cluster	Ja	Ja	S2 wird empfohlen und S3 wird unterstützt.
vSAN Stretched Cluster-Daten	Ja	Ja	Sowohl S2 als auch S3 zwischen Daten-Sites werden unterstützt.
vSAN Stretched Cluster-Zeuge	Nein	Ja	S3 wird unterstützt. S2 zwischen Daten und Zeugen-Sites wird nicht unterstützt.
vSAN-Cluster mit zwei Knoten	Ja	Ja	Sowohl S2 als auch S3 zwischen Daten-Sites werden unterstützt.

Routing- und Switching-Anforderungen

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

Im Folgenden finden Sie die vSAN Stretched Cluster-Routing-Anforderungen:

Tabelle 3-6. Routing-Anforderungen

Site-Kommunikation	Bereitstellungsmodell	Schicht	Routing
Site zu Site	Standard	Schicht 2	Nicht erforderlich
Site zu Site	Standard	Schicht 3	Verwenden Sie statische Routen oder Gateway-Überschreibung.
Site zum Zeugen	Standard	Schicht 3	Verwenden Sie statische Routen oder Gateway-Überschreibung.

Tabelle 3-6. Routing-Anforderungen (Fortsetzung)

Site-Kommunikation	Bereitstellungsmodell	Schicht	Routing
Site zum Zeugen	Trennung des Zeugen-Datenverkehrs	Schicht 3	Verwenden Sie statische Routen oder Gateway-Überschreibung, wenn Sie eine andere Schnittstelle als die Verwaltungsschnittstelle (vmk0) verwenden.
Site zum Zeugen	Trennung des Zeugen-Datenverkehrs	Schicht 2 für zwei-Host-Cluster	Statische Routen sind nicht erforderlich.

Anforderungen an virtuelle Switches

Sie können ein vSAN-Netzwerk mit vSphere Standard-Switch oder vSphere Distributed Switch erstellen. Verwenden Sie einen Distributed Switch, um die Bandbreite für vSAN-Datenverkehr zu priorisieren. vSAN verwendet einen Distributed Switch mit allen vCenter Server-Versionen.

In der folgenden Tabelle werden die Vorteile und Annehmlichkeiten eines Distributed Switches gegenüber einem Standard-Switch verglichen:

Tabelle 3-7. Virtuelle Switch-Typen

Design-Anforderung	Option 1 – vSphere Distributed Switch	Option 2 – vSphere Standard-Switch	Beschreibung
Verfügbarkeit	Keine Auswirkung	Keine Auswirkung	Sie können eine der folgenden Optionen verwenden
Verwaltbarkeit	Positive Auswirkungen	Negative Auswirkungen	Der Distributed Switch wird zentral auf allen Hosts verwaltet. Dies steht im Gegensatz zum Standard-Switch, der auf jedem Host einzeln verwaltet wird.
Leistung	Positive Auswirkungen	Negative Auswirkungen	Der Distributed Switch verfügt über zusätzliche Steuerelemente wie Network I/O Control, mit denen Sie die Leistung für vSAN-Datenverkehr gewährleisten können.

Tabelle 3-7. Virtuelle Switch-Typen (Fortsetzung)

Design-Anforderung	Option 1 – vSphere Distributed Switch	Option 2 – vSphere Standard-Switch	Beschreibung
Wiederherstellbarkeit	Positive Auswirkungen	Negative Auswirkungen	Die Distributed Switch-Konfiguration kann gesichert und wiederhergestellt werden. Der Standard-Switch verfügt nicht über diese Funktionalität.
Sicherheit	Positive Auswirkungen	Negative Auswirkungen	Der Distributed Switch verfügt über integrierte Sicherheitskontrollen, um den Datenverkehr zu schützen.

Anforderungen an den vSAN-Netzwerkport

Für vSAN-Bereitstellungen sind bestimmte Netzwerkports und -einstellungen erforderlich, um Zugriff und Dienste bereitzustellen.

vSAN sendet Meldungen an bestimmte Ports auf jedem Host im Cluster. Stellen Sie sicher, dass die Firewalls der Hosts Datenverkehr über diese Ports zulassen. Eine Liste aller unterstützten vSAN-Ports und Protokolle finden Sie im Portal „VMware Ports and Protocols“ unter https://ports.vmware.com/.

Überlegungen zur Firewall

Wenn Sie vSAN auf einem Cluster aktivieren, werden alle erforderlichen Ports zu ESXi-Firewallregeln hinzugefügt und automatisch konfiguriert. Ein Administrator muss keine Firewall-Ports öffnen oder keine Firewall-Dienste manuell aktivieren.

Sie können offene Ports für eingehende und ausgehende Verbindungen anzeigen. Wählen Sie den ESXi-Host aus und klicken Sie auf **Konfigurieren > Sicherheitsprofil**.

Netzwerkfirewall-Anforderungen

Wenn Sie die Netzwerkfirewall konfigurieren, berücksichtigen Sie, welche Version von vSAN Sie bereitstellen.

Wenn Sie vSAN auf einem Cluster aktivieren, werden alle erforderlichen Ports zu ESXi-Firewallregeln hinzugefügt und automatisch konfiguriert. Sie müssen keine Firewall-Ports öffnen oder keine Firewall-Dienste manuell aktivieren. Sie können offene Ports für eingehende und ausgehende Verbindungen im ESXi-Hostsicherheitsprofil (**Konfigurieren > Sicherheitsprofil**) anzeigen.

vsanEncryption-Firewallregel

Wenn Ihr Cluster die vSAN-Verschlüsselung verwendet, sollten Sie die Kommunikation zwischen Hosts und dem KMS-Server berücksichtigen.

Für die vSAN-Verschlüsselung ist ein externer Schlüsselverwaltungsserver (KMS) erforderlich. vCenter Server ruft Schlüssel-IDs vom KMS ab und verteilt diese an die ESXi-Hosts. KMS-Server und ESXi-Hosts kommunizieren direkt miteinander. KMS-Server verwenden möglicherweise unterschiedliche Portnummern, sodass Sie mit der vsanEncryption-Firewallregel die Kommunikation zwischen den einzelnen vSAN-Hosts und dem KMS-Server vereinfachen können. Auf diese Weise kann ein vSAN-Host direkt mit einem beliebigen Port auf einem KMS-Server kommunizieren (TCP-Port 0 bis 65535).

Wenn ein Host die Kommunikation mit einem KMS-Server herstellt, treten die folgenden Vorgänge auf.

- Die KMS-Server-IP wird der vsanEncryption-Regel hinzugefügt, und die Firewallregel wird aktiviert.
- Die Kommunikation zwischen dem vSAN-Knoten und dem KMS-Server wird während des Austauschs eingerichtet.
- Nachdem die Kommunikation zwischen dem vSAN-Knoten und dem KMS-Server beendet ist, wird die IP-Adresse aus der Regel vsanEncryption entfernt und die Firewallregel wird wieder deaktiviert .

vSAN-Hosts können mit mehreren KMS-Hosts mit derselben Regel kommunizieren.

Verwenden von Unicast in einem vSAN-Netzwerk

4

Der Unicast-Datenverkehr bezieht sich auf eine Eins-zu-Eins-Übertragung von einem Punkt im Netzwerk zu einem anderen. vSAN-Version 6.6 und höher verwendet Unicast, um das Netzwerkdesign und die Bereitstellung zu vereinfachen.

Alle ESXi-Hosts verwenden den Unicast-Datenverkehr, und der vCenter Server wird zur Quelle für die Cluster-Mitgliedschaft. Die vSAN-Knoten werden automatisch mit der neuesten Host-Mitgliedschaftsliste aktualisiert, die von vCenter bereitgestellt wird. vSAN kommuniziert mithilfe von Unicast für CMMDS-Updates.

Versionen vor vSAN 6.6 vertrauen auf Multicast, um Taktsignale zu aktivieren und Metadaten zwischen Hosts im Cluster auszutauschen. Wenn auf einigen Hosts in Ihrem vSAN-Cluster frühere Softwareversionen ausgeführt werden, ist dennoch ein Multicast-Netzwerk erforderlich. Der Wechsel zum Unicast-Netzwerk von Multicast bietet eine bessere Leistung und Netzwerkunterstützung. Weitere Informationen zu Multicast finden Sie unter Kapitel 13 Verwenden von Multicast in einem vSAN-Netzwerk.

Lesen Sie als Nächstes die folgenden Themen:

- Verhalten der Festplattengruppe vor Version 5
- Verhalten der Festplattengruppe der Version 5
- DHCP-Unterstützung für Unicast-Netzwerk
- IPv6-Unterstützung für Unicast-Netzwerk
- Unicast-Abfrage mit ESXCLI
- Intra-Cluster-Datenverkehr

Verhalten der Festplattengruppe vor Version 5

Die Verfügbarkeit einer einzelnen Festplattengruppe der Version 5 in einer vSAN-Festplattengruppe der Version 6.6 führt dazu, dass der Cluster dauerhaft im Unicast-Modus kommuniziert.

vSAN-Cluster der Version 6.6 werden in den folgenden Situationen automatisch auf die Multicast-Kommunikation zurückgesetzt:

- Auf allen Cluster-Hosts wird vSAN-Version 6.5 oder niedriger ausgeführt.

- Alle Festplattengruppen verwenden Festplattenversion 3 oder früher.
- Ein nicht-vSAN-6.6-Host wie z. B. vSAN 6.2 oder vSAN 6.5 wird dem Cluster hinzugefügt.

Wenn beispielsweise ein Host, auf dem vSAN 6.5 oder früher ausgeführt wird, einem vorhandenen vSAN 6.6-Cluster hinzugefügt wird, kehrt der Cluster in den Multicast-Modus zurück und enthält den 6.5-Host als gültigen Knoten. Um dieses Verhalten zu vermeiden, verwenden Sie die neueste Version sowohl für ESXi-Hosts als auch für das Festplattenformat. Um sicherzustellen, dass der vSAN-Cluster weiterhin im Unicast-Modus kommuniziert und nicht auf Multicast zurückgesetzt wird, führen Sie ein Upgrade der Festplattengruppen auf den vSAN 6.6-Hosts auf die Festplattenversion 5.0 durch.

Hinweis Vermeiden Sie die Verwendung eines Clusters im gemischten Modus, auf dem vSAN-Version 6.5 oder früher im selben Cluster zusammen mit vSAN-Version 6.6 oder höher verfügbar ist.

Verhalten der Festplattengruppe der Version 5

Das Vorhandensein einer einzelnen Festplattengruppe der Version 5 in einem vSAN-Cluster der Version 6.6 führt dazu, dass der Cluster dauerhaft im Unicast-Modus kommuniziert.

In einer Umgebung, in der ein vSAN 6.6-Cluster bereits eine Festplattenversion 5 verwendet und dem Cluster ein vSAN 6.5-Knoten hinzugefügt wird, treten die folgenden Ereignisse auf:

- Der vSAN 6.5-Knoten bildet eine eigene Netzwerkpartition.
- Der vSAN 6.5-Knoten kommuniziert weiterhin im Multicast-Modus, kann aber nicht mit vSAN 6.6-Knoten kommunizieren, da sie den Unicast-Modus verwenden.

Eine zusammenfassende Cluster-Warnung wird im Festplattenformat mit dem Hinweis angezeigt, dass ein Knoten eine frühere Version aufweist. Sie können den Knoten auf die neueste Version aktualisieren. Ein Upgrade der Festplatten-Formatversionen ist nicht möglich, wenn sich ein Cluster im gemischten Modus befindet.

DHCP-Unterstützung für Unicast-Netzwerk

In vCenter Server können bei einer Bereitstellung auf einem vSAN 6.6-Cluster IP-Adressen vom Dynamic Host Configuration Protocol (DHCP) ohne Reservierungen verwendet werden.

Sie können DHCP mit Reservierungen verwenden, da die zugewiesenen IP-Adressen an die MAC-Adressen der VMkernel-Ports gebunden sind.

IPv6-Unterstützung für Unicast-Netzwerk

vSAN 6.6 unterstützt IPv6 mit Unicast-Kommunikation.

Bei IPv6 wird die verbindungslokale Adresse automatisch auf einer Schnittstelle mit dem verbindungslokalen Präfix konfiguriert. Standardmäßig fügt vSAN die verbindungslokale Adresse eines Knotens nicht zu anderen benachbarten Clusterknoten hinzu. Daher unterstützt vSAN 6.6 keine verbindungslokalen IPv6-Adressen für Unicast-Kommunikation.

Unicast-Abfrage mit ESXCLI

Sie können ESXCLI-Befehle ausführen, um die Unicast-Konfiguration zu bestimmen.

Anzeigen der Kommunikationsmodi

Mithilfe des Befehls `esxcli vsan cluster get` können Sie den CMMDS-Modus (Unicast oder Multicast) des vSAN-Clusterknotens anzeigen lassen.

Verfahren

- Führen Sie den Befehl `esxcli vsan cluster get` aus.

Ergebnisse

```
Cluster Information
   Enabled: true
   Current Local Time: 2020-04-09T18:19:52Z
   Local Node UUID: 5e8e3dc3-43ab-5452-795b-a03d6f88f022
   Local Node Type: NORMAL
   Local Node State: AGENT
   Local Node Health State: HEALTHY
   Sub-Cluster Master UUID: 5e8e3d3f-3015-9075-49b6-a03d6f88d426
   Sub-Cluster Backup UUID: 5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a
   Sub-Cluster UUID: 5282f9f3-d892-3748-de48-e2408dc34f72
   Sub-Cluster Membership Entry Revision: 11
   Sub_cluster Member Count: 5
   Sub-Cluster Member UUIDs: 5e8e3d3f-3015-9075-49b6-a03d6f88d426, 5e8e3daf-e5e0-ddb6-a523-
a03d6f88dd4a,
   5e8e3d73-6d1c-0b81-1305-a03d6f888d22, 5e8e3d33-5825-ee5c-013c-a03d6f88ea4c,
5e8e3dc3-43ab-5452-795b-a03d6f88f022
   Sub-Cluster Member HostNames: testbed-1.vmware.com, testbed2.vmware.com,
   testbed3.vmware.com, testbed4.vmware.com, testbed5.vmware.com
   Sub-Cluster Membership UUID: 0f438e5e-d400-1bb2-f4d1-a03d6f88d426
   Unicast-Modus aktiviert: true
   Maintenance Mode State: OFF
   Config Generation: ed845022-5c08-48d0-aa1d-6b62c0022222 7 2020-04-08T22:44:14.889
```

Überprüfen der vSAN-Cluster-Hosts

Verwenden Sie den Befehl `esxcli vsan cluster unicastagent list`, um zu überprüfen, ob die vSAN-Cluster-Hosts im Unicast-Modus betrieben werden.

Verfahren

- Führen Sie den Befehl `esxcli vsan cluster unicastagent list` aus.

Ergebnisse

```
NodeUuid                                IsWitness Supports Unicast IP Address  Port  Iface Name
Cert Thumbprint  SubClusterUuid
------------------------------------ --------- ---------------- ----------  ----- ----------
5e8e3d73-6d1c-0b81-1305-a03d6f888d22         0      true
10.198.95.10    12321
43:80:B7:A1:3F:D1:64:07:8C:58:01:2B:CE:A2:F5:DE:D6:B1:41:AB
5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a         0      true
10.198.94.240   12321
FE:39:D7:A5:EF:80:D6:41:CD:13:70:BD:88:2D:38:6C:A0:1D:36:69
5e8e3d3f-3015-9075-49b6-a03d6f88d426         0      true
10.198.94.244   12321
72:A3:80:36:F7:5D:8F:CE:B0:26:02:96:00:23:7D:8E:C5:8C:0B:E1
5e8e3d33-5825-ee5c-013c-a03d6f88ea4c         0      true
10.198.95.11    12321
5A:55:74:E8:5F:40:2F:2B:09:B5:42:29:FF:1C:95:41:AB:28:E0:57
```

Die Ausgabe enthält die vSAN-Knoten-UUID, die IPv4-Adresse, die IPv6-Adresse, den UDP-Port, mit dem der vSAN-Knoten kommuniziert, und Informationen dazu, ob es sich bei dem Knoten um einen Datenhost (0) oder um einen Zeugenhost (1) handelt. Sie können diese Ausgabe verwenden, um die vSAN-Clusterknoten zu identifizieren, die im Unicast-Modus betrieben werden und um die anderen Hosts im Cluster anzuzeigen. vCenter Server verwaltet die Ausgabeliste.

Anzeigen der vSAN-Netzwerkinformationen

Verwenden Sie den Befehl `esxcli vsan network list`, um die vSAN-Netzwerkinformationen anzuzeigen, beispielsweise die VMkernel-Schnittstelle, die vSAN für die Kommunikation verwendet, den Unicast-Port (12321) und den Datenverkehrstyp (vSAN oder Zeuge), der der vSAN-Schnittstelle zugeordnet ist.

Verfahren

- Führen Sie den Befehl `esxcli vsan network list` aus.

Ergebnisse

```
Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: e290be58-15fe-61e5-1043-246e962c24d0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

Diese Ausgabe zeigt auch die Multicast-Informationen an.

Intra-Cluster-Datenverkehr

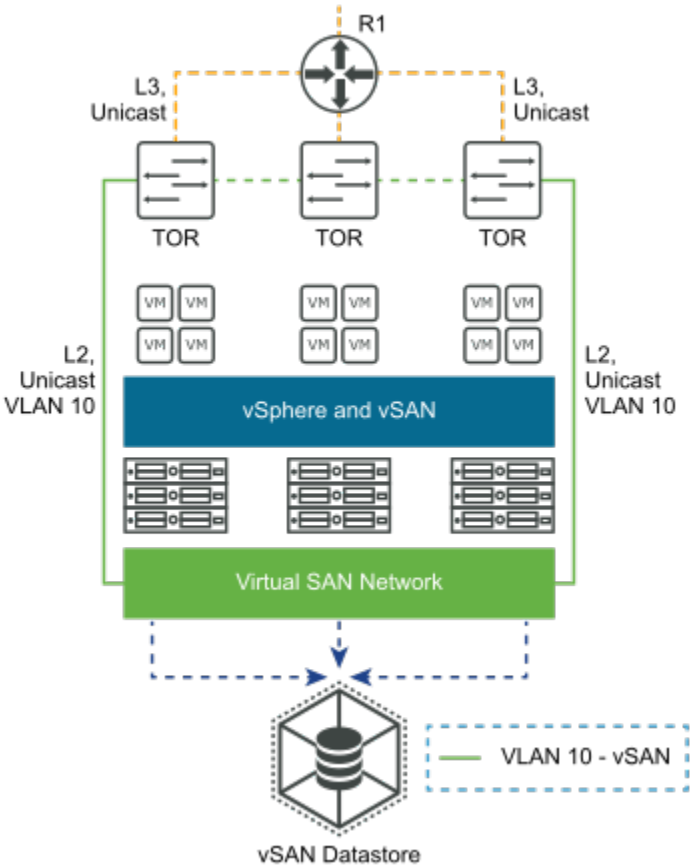
Im Unicast-Modus adressiert der primäre Knoten alle Clusterknoten, da er dieselbe Meldung an alle vSAN-Knoten in einem Cluster sendet.

Wenn z. B. N die Anzahl vSAN Knoten ist, sendet der primäre Knoten die Meldungen N-mal. Dies führt zu einem leichten Anstieg des vSAN-CMMDS-Datenverkehrs. Möglicherweise bemerken Sie diesen leichten Anstieg des Datenverkehrs bei normalen, stabilen Vorgängen nicht.

Intra-Cluster-Datenverkehr in einem einzelnen Rack

Wenn alle Knoten in einem vSAN-Cluster mit demselben TOR-Switch verbunden sind, erfolgt die Gesamtzunahme des Datenverkehrs nur zwischen dem primären Knoten und dem Switch.

Wenn ein vSAN-Cluster mehrere TOR-Switches umfasst, wird der Datenverkehr zwischen dem Switch erweitert. Wenn sich ein Cluster über viele Racks erstreckt, bilden mehrere TORs Fehlerdomänen (FD) für die Rack-Erkennung. Der primäre Knoten sendet N Meldungen an die Racks oder Fehlerdomänen, wobei N die Anzahl Hosts in den einzelnen Fehlerdomänen ist.

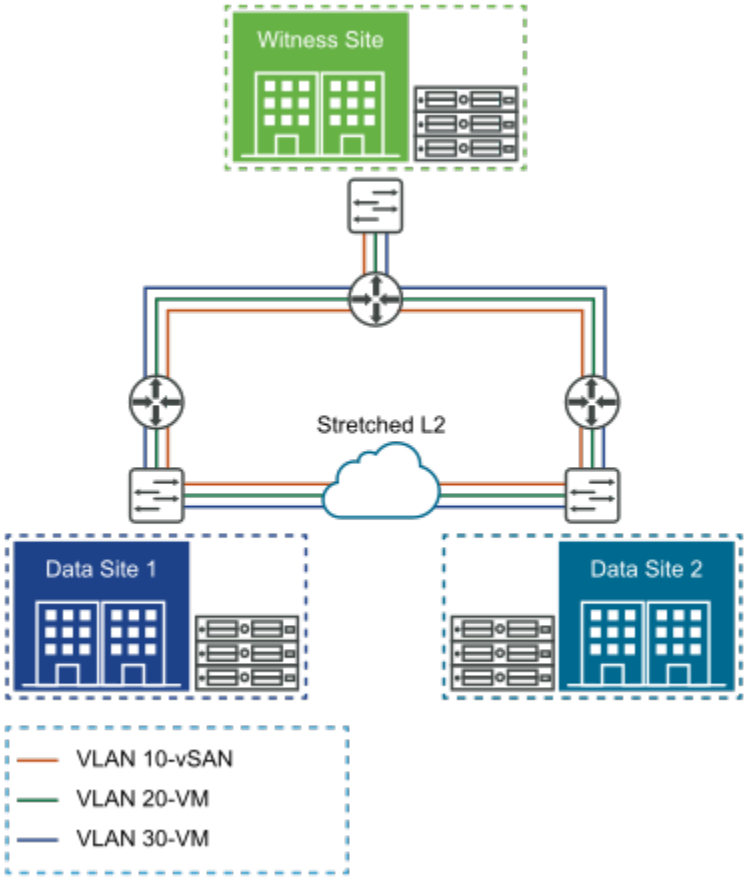


Intra-Cluster-Datenverkehr in einem vSAN Stretched Cluster

In einem vSAN Stretched Cluster befindet sich der primäre Knoten auf der bevorzugten Site.

In einer Fehlerdomäne müssen CMMDS-Daten von der sekundären Site an die bevorzugte Site übermittelt werden. Zur Berechnung des Datenverkehrs in einem vSAN Stretched Cluster müssen Sie die Anzahl der Knoten auf einer sekundären Site mit der Größe des CMMDS-Knotens (in MB) und der Anzahl der Knoten auf der sekundären Site multiplizieren.

Datenverkehr in einem vSAN Stretched Cluster = Anzahl der Knoten auf der sekundären Site * CMMDS-Knotengröße (in MB) * Anzahl der Knoten auf der sekundären Site.



Beim Unicast-Datenverkehr gibt es keine Änderungen an den Anforderungen für den Datenverkehr der Zeugen-Site.

Konfigurieren des IP-Netzwerktransports

5

Transportprotokolle stellen Kommunikationsdienste über das Netzwerk bereit. Diese Dienste beinhalten den TCP/IP-Stack und die Flusssteuerung.

Lesen Sie als Nächstes die folgenden Themen:

- vSphere TCP/IP-Stacks
- Object Missing
- IPv6-Unterstützung
- Statische Routen
- Jumbo-Frames

vSphere TCP/IP-Stacks

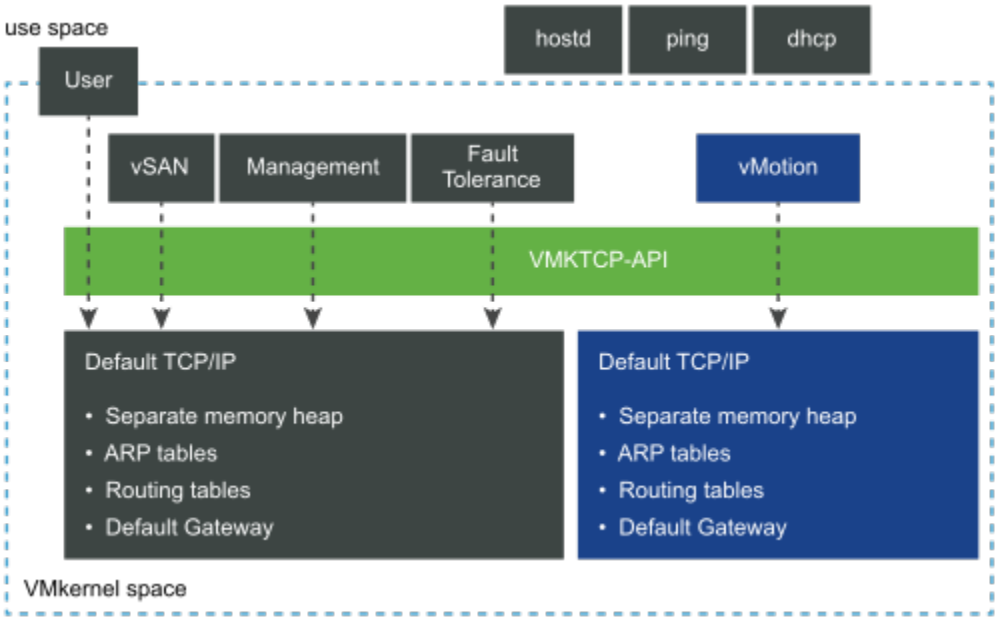
vSphere enthält keinen dedizierten TCP/IP-Stack für den vSAN-Datenverkehrsdienst. Sie können die vSAN VMkernel-Netzwerkschnittstelle dem Standard-TCP/IP-Stack hinzufügen und statische Routen für alle Hosts im vSAN-Cluster definieren.

vSphere unterstützt nicht die Erstellung eines benutzerdefinierten vSAN TCP/IP-Stacks. Sie können sicherstellen, dass vSAN-Datenverkehr in Schicht-3-Netzwerktopologien über die vSAN VMkernel-Netzwerkschnittstelle verbleibt. Fügen Sie die vSAN VMkernel-Netzwerkschnittstelle dem Standard-TCP/IP-Stack hinzu, und definieren Sie statische Routen für alle Hosts im vSAN-Cluster.

Hinweis vSAN verfügt über keinen eigenen TCP/IP-Stack. Verwenden Sie statische Routen, um vSAN-Datenverkehr über L3-Netzwerke zu leiten.

Mit vSphere 6.0 wurde eine neue TCP/IP-Stack-Architektur eingeführt, die mehrere TPC/IP-Stacks verwenden kann, um verschiedene VMkernel-Netzwerkschnittstellen zu verwalten. Mit dieser Architektur können Sie Datenverkehrsdienste wie vMotion, Management und Fault Tolerance auf isolierten TCP/IP-Stacks konfigurieren, die mehrere Standard-Gateways verwenden können.

Stellen Sie für die Isolierung des Netzwerkdatenverkehrs und die Sicherheitsanforderungen die verschiedenen Datenverkehrsdienste auf verschiedenen Netzwerksegmenten oder VLANs bereit. Dadurch wird verhindert, dass die unterschiedlichen Datenverkehrsdienste über dasselbe Standard-Gateway durchlaufen werden.



Wenn Sie die Datenverkehrsdienste auf getrennten TCP/IP-Stacks konfigurieren, stellen Sie jeden Datenverkehrsdiensttyp auf seinem eigenen Netzwerksegment bereit. Der Zugriff auf die Netzwerksegmente erfolgt über einen physischen Netzwerkadapter mit VLAN-Segmentierung. Ordnen Sie jedes Segment verschiedenen VMkernel-Netzwerkschnittstellen zu, wobei die entsprechenden Datenverkehrsdienste aktiviert sind.

In vSphere verfügbare TCP/IP-Stacks

vSphere stellt TCP/IP-Stacks bereit, die vSAN-Datenverkehrsanforderungen unterstützen.

- **Standard-TCP/IP-Stack**. Verwalten Sie die Host-bezogenen Datenverkehrsdienste. Dieser Stack teilt ein einzelnes Standard-Gateway zwischen allen konfigurierten Netzwerkdiensten.
- **vMotion TCP/IP-Stack**. Isoliert den vMotion-Datenverkehr auf einem eigenen Stack. Durch die Verwendung dieses Stacks wird der vMotion-Datenverkehr vom Standard-TCP/IP-Stack vollständig entfernt oder deaktiviert.
- **Bereitstellen von TCP/IP-Stacks**. Isoliert einige Vorgänge für virtuelle Maschinen, z. B. Cold-Migrationen, Klonen, Snapshots oder NFC-Datenverkehr.
- **Spiegeln von TCP/IP-Stacks**. Trennt den Portspiegelungsdatenverkehr vom Verwaltungsdatenverkehr. Ohne diesen Stack ist der Spiegelungsdatenverkehr an den Standard-TCP/IP-Stack gebunden.
- **OPS-TCP/IP-Stack**. Bietet Unterstützung für die Erfassung von Flow-Daten im vSphere-Netzwerk.

Sie können während der Erstellung einer VMkernel-Schnittstelle einen anderen TCP/IP-Stack auswählen.

Umgebungen mit isolierten Netzwerkanforderungen für die vSphere-Datenverkehrsdienste können nicht dasselbe Standard-Gateway für die Weiterleitung des Datenverkehrs verwenden. Die Verwendung unterschiedlicher TCP/IP-Stacks vereinfacht die Verwaltung für die Datenverkehrsisolierung, da Sie verschiedene Standard-Gateways verwenden und das Hinzufügen statischer Routen vermeiden können. Verwenden Sie diese Technik, wenn Sie vSAN-Datenverkehr an ein anderes Netzwerk weiterleiten müssen, auf das über das Standard-Gateway nicht zugegriffen werden kann.

Object Missing

This object is not available in the repository.

IPv6-Unterstützung

vSAN 6.2 und höher unterstützt IPv6.

vSAN unterstützt die folgenden IP-Versionen.

- IPv4
- IPv6 (vSAN 6.2 und höher)
- Gemischtes IPv4/IPv6 (vSAN 6.2 und höher)

In Versionen vor vSAN 6.2 wird nur IPv4 unterstützt. Verwenden Sie den gemischten Modus beim Migrieren Ihres vSAN-Clusters von IPv4 zu IPv6.

IPv6-Multicast wird ebenfalls unterstützt.

Weitere Informationen zur Verwendung von IPv6 erhalten Sie von Ihrem Netzwerkanbieter.

Statische Routen

Sie können statische Routen verwenden, um vSAN-Netzwerkschnittstellen von Hosts in einem Subnetz zuzulassen, um die Hosts in einem anderen Netzwerk zu erreichen.

Die meisten Organisationen trennen das vSAN-Netzwerk vom Verwaltungsnetzwerk, sodass das vSAN-Netzwerk über kein Standard-Gateway verfügt. In einer Schicht-3-Bereitstellung können sich Hosts, die sich in unterschiedlichen Subnetzen oder unterschiedlichen Schicht-2-Segmenten befinden, nicht über das Standard-Gateway erreichen, das normalerweise dem Verwaltungsnetzwerk zugeordnet ist.

Verwende Sie *statische Routen*, damit die vSAN-Netzwerkschnittstellen von Hosts in einem Subnetz die vSAN-Netzwerke auf Hosts im anderen Netzwerk erreichen können. Statische Routen weisen einen Host an, wie ein bestimmtes Netzwerk über eine Schnittstelle erreicht werden soll, anstatt das Standard-Gateway zu verwenden.

Das folgende Beispiel zeigt, wie einem ESXi-Host eine statische IPv4-Route hinzugefügt wird. Geben Sie das Gateway (-g) und das Netzwerk (-n) an, das Sie über dieses Gateway erreichen möchten:

```
esxcli network ip route ipv4 add –g 172.16.10.253 -n 192.168.10.0/24
```

Wenn die statischen Routen hinzugefügt wurden, ist die vSAN-Datenverkehrskonnektivität in allen Netzwerken verfügbar, sofern die physische Infrastruktur dies zulässt. Führen Sie den Befehl `vmkping` aus, um die Kommunikation zwischen den verschiedenen Netzwerken zu testen und zu bestätigen, indem Sie einen Ping-Vorgang für die IP-Adresse oder das Standard-Gateway des Remote-Netzwerks ausführen. Sie können auch verschiedene Paketgrößen (-s) überprüfen und eine Fragmentierung (-d) des Pakets verhindern.

```
vmkping –I vmk3 192.168.10.253
```

Jumbo-Frames

vSAN unterstützt bietet vollständige Unterstützung für Jumbo-Frames im vSAN-Netzwerk.

Jumbo-Frames sind Ethernet-Frames mit mehr als 1500 Byte Nutzlast. Jumbo-Frames tragen in der Regel bis zu 9000 Byte der Nutzlast, dieser Wert variiert jedoch.

Die Verwendung von Jumbo-Frames kann die CPU-Nutzung verringern und den Durchsatz verbessern.

Hinweis Aktivieren Sie die Unterstützung von Jumbo-Frames für vSAN Max-Bereitstellungen zur Leistungssteigerung.

Sie müssen entscheiden, ob diese Gewinne den Overhead bei der Implementierung von Jumbo-Frames im gesamten Netzwerk überwiegen. In Datencentern, in denen Jumbo-Frames bereits in der Netzwerkinfrastruktur aktiviert sind, können Sie sie für vSAN verwenden. Die Betriebskosten für die Konfiguration von Jumbo-Frames im gesamten Netzwerk können die begrenzten CPU- und Leistungsvorteile überwiegen.

Verwenden von VMware NSX mit vSAN

6

vSAN und VMware NSX können in derselben vSphere-Infrastruktur bereitgestellt werden und nebeneinander bestehen.

NSX unterstützt die Konfiguration des vSAN-Datennetzwerks über ein NSX-verwaltetes VXLAN- oder Geneve-Overlay nicht.

vSAN und NSX sind kompatibel. vSAN und NSX sind nicht voneinander abhängig, um ihre Funktionalitäten, Ressourcen und Dienste bereitzustellen.

Sie können den vSAN-Netzwerkdatenverkehr jedoch nicht auf einem NSX-verwalteten VxLAN/Geneve-Overlay positionieren. NSX unterstützt nicht die Konfiguration des vSAN-Datennetzwerk-Datenverkehrs über ein NSX-verwaltetes VxLAN/Geneve-Overlay.

Ein Grund dafür, dass der VMkernel-Datenverkehr über das von NSX verwaltete VxLAN-Overlay nicht unterstützt wird, besteht darin, eine zirkuläre Abhängigkeit zwischen den VMkernel-Netzwerken und dem von ihnen unterstützten VxLAN-Overlay zu vermeiden. Die mit dem NSX-verwalteten VxLAN-Overlay bereitgestellten logischen Netzwerke werden von virtuellen Maschinen verwendet, die Netzwerkmobilität und Flexibilität erfordern.

Wenn Sie LACP/LAG in NSX implementieren, definiert eine Cisco Nexus-Umgebung die LAGs als virtuelle Portkanäle (vPCs).

Verwenden der Überlastungs- und Flusssteuerung

7

Mithilfe der Flusssteuerung können Sie die Rate der Datenübertragung zwischen Absendern und Empfängern im vSAN-Netzwerk verwalten. Die Überlastungssteuerung behandelt Überlastungen im Netzwerk.

Flusssteuerung

Mithilfe der Flusssteuerung können Sie die Datenübertragungsrate zwischen zwei Geräten verwalten.

Die Flusssteuerung wird konfiguriert, wenn zwei physisch verbundene Geräte eine automatische Aushandlung durchführen.

Ein überlasteter Netzwerkknoten sendet möglicherweise einen Pause-Frame, um die Übertragung des Absenders für einen bestimmten Zeitraum zu stoppen. Ein Frame mit einer Multicast-Zieladresse, die an einen Switch gesendet wird, wird über alle anderen Ports des Switches weitergeleitet. Pause-Frames haben eine spezielle Multicast-Zieladresse, die sie von anderweitigem Multicast-Datenverkehr unterscheidet. Ein kompatibler Switch leitet keinen Pause-Frame weiter. An diesen Bereich gesendete Frames sollen nur innerhalb des Switches behandelt werden. Pause-Frames haben eine begrenzte Dauer und laufen nach einem Zeitintervall ab. Zwei Computer, die über einen Switch verbunden sind, senden sich niemals Pause-Frames, sondern können Pause-Frames an einen Switch senden.

Ein Grund für die Verwendung von Pause-Frames ist die Unterstützung von Netzwerkschnittstellen-Controllern (NICs), die nicht über genügend Puffer verfügen, um den Empfang mit voller Geschwindigkeit zu verarbeiten. Dieses Problem ist bei fortschreitenden Bus-Geschwindigkeiten und Arbeitsspeichergrößen selten.

Überlastungssteuerung

Die Überlastungssteuerung hilft Ihnen, den Datenverkehr im Netzwerk zu steuern.

Die Überlastungssteuerung wird hauptsächlich auf Paket-Switching-Netzwerke angewendet. Eine Netzwerküberlastung innerhalb eines Switches kann durch überlastete Inter-Switch-Links verursacht werden. Wenn Inter-Switch-Links die Funktion auf der physischen Ebene überlasten, leitet der Switch Pause-Frames ein, um sich selbst zu schützen.

Prioritätsbasierte Flusssteuerung

Die prioritätsbasierte Flusssteuerung (PFC) hilft Ihnen, den Frame-Verlust aufgrund von Überlastung zu eliminieren.

Die prioritätsbasierte Flusssteuerung (IEEE 802.1Qbb) wird durch einen Mechanismus erreicht, der zwar Pause-Frames ähnelt, aber mit individuellen Prioritäten arbeitet. PFC wird auch als klassenbasierte Flussteuerung (CBFC) oder Per Priority Pause (PPP) bezeichnet.

Fluss- und Überlastungssteuerung

Die Flusssteuerung ist ein End-to-End-Mechanismus, der den Datenverkehr zwischen einem Absender und einem Empfänger steuert. Die Flusssteuerung erfolgt in der Datenverknüpfungs- und Transportebene.

Die Überlastungssteuerung wird von einem Netzwerk verwendet, um Überlastungen im Netzwerk zu steuern. Dieses Problem tritt in modernen Netzwerken mit fortschreitenden Bus-Geschwindigkeiten und Arbeitsspeichergrößen nicht so häufig auf. Ein wahrscheinlicheres Szenario ist eine Netzwerküberlastung innerhalb eines Switches. Die Überlastungssteuerung wird von der Netzwerk- und der Transportebene verarbeitet.

Überlegungen zum Design der Flusssteuerung

Standardmäßig ist die Flusssteuerung auf allen Netzwerkschnittstellen in ESXi-Hosts aktiviert.

Die Konfiguration der Flusssteuerung auf einer Netzwerkkarte wird vom Treiber durchgeführt. Wenn eine Netzwerkkarte durch den Netzwerkdatenverkehr überlastet ist, sendet sie Pause-Frames.

Flusssteuerungsmechanismen wie Pause-Frames können zu einer Gesamtlatenz in der VM-Gast-E/A aufgrund einer erhöhten Latenz in der vSAN-Netzwerkebene führen. Einige Netzwerktreiber stellen Moduloptionen bereit, mit deren Hilfe die Flusssteuerungsfunktionalität innerhalb des Treibers konfiguriert wird. Einige Netzwerktreiber ermöglichen es Ihnen, die Konfigurationsoptionen mithilfe des Befehlszeilendienstprogramms `ethtool` in der Konsole des ESXi-Hosts zu ändern. Verwenden Sie in Abhängigkeit von den Implementierungsdetails eines bestimmten Treibers Moduloptionen oder `ethtool`.

Informationen zum Konfigurieren der Flusssteuerung auf ESXi-Hosts finden Sie im VMware Knowledgebase-Artikel 1013413.

Bei Bereitstellungen mit 1 GBit/s lassen Sie die Flusssteuerung auf den ESXi-Netzwerkschnittstellen aktiviert (Standardeinstellung). Wenn Pause-Frames ein Problem darstellen, planen Sie die Deaktivierung der Flusssteuerung zusammen mit dem Support des Hardwareherstellers oder den VMware Global Support Services sorgfältig ein.

Informationen dazu, wie Sie das Vorhandensein von Pause-Frames erkennen können, die von einem Empfänger an einen ESXi-Host gesendet werden, finden Sie unter Kapitel 12 Fehlerbehebung für das vSAN-Netzwerk. Eine hohe Anzahl Pause-Frames in einer Umgebung weist in der Regel auf ein zugrunde liegendes Netzwerk- oder Transportproblem hin, das es zu untersuchen gilt.

Grundlegende NIC-Gruppierung, Failover und Lastausgleich

8

Für viele vSAN-Umgebungen ist ein gewisser Grad an Netzwerkredundanz erforderlich.

Sie können die NIC-Gruppierung verwenden, um Netzwerkredundanz zu erreichen. Sie können zwei oder mehr Netzwerkadapter (NICs) als Gruppe für Hochverfügbarkeit und Lastausgleich konfigurieren. Die grundlegende NIC-Gruppierung ist für vSphere-Netzwerke verfügbar, und diese Techniken können sich auf vSAN-Design und -Architektur auswirken.

Es sind mehrere NIC-Gruppierungsoptionen verfügbar. Vermeiden Sie NIC-Gruppierungsrichtlinien, die physische Switch-Konfigurationen oder die ein Verständnis von Netzwerkkonzepten wie z. B. der Link Linkaggregation erfordern. Die besten Ergebnisse werden mit einer grundlegenden, einfachen und zuverlässigen Einrichtung erzielt.

Wenn Sie sich bezüglich der NIC-Gruppierungsoptionen nicht sicher sind, verwenden Sie eine Aktiv/Standby-Konfiguration mit expliziten Failover.

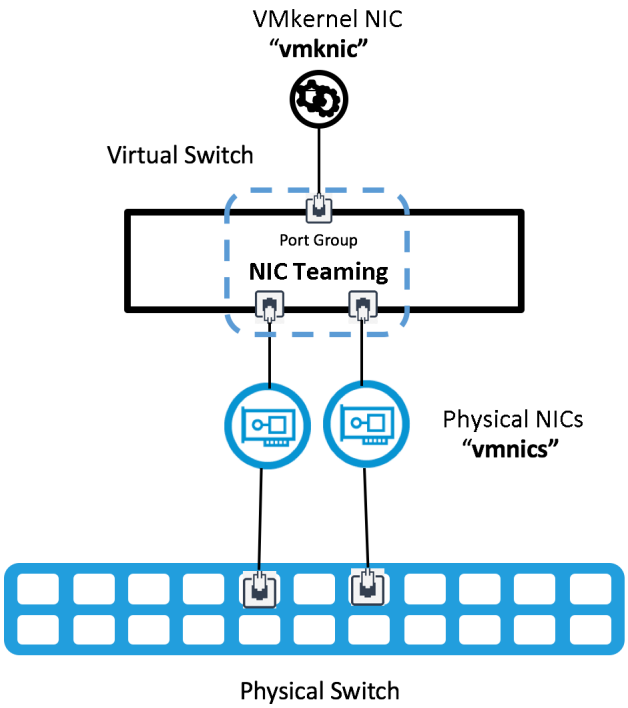
Lesen Sie als Nächstes die folgenden Themen:

- Einfache NIC-Gruppierung

Einfache NIC-Gruppierung

Die grundlegende NIC-Gruppierung verwendet mehrere physische Uplinks, eine vmknic und einen einzelnen Switch.

Bei der vSphere-NIC-Gruppierung kommen mehrere Uplink-Adapter, sogenannte vmnics, zum Einsatz. Sie sind mit einem einzelnen virtuellen Switch verknüpft, um so eine Gruppe zu bilden. Dies ist die einfachste Option und Sie können sie mit einem vSphere Standard-Switch oder einem vSphere Distributed Switch konfigurieren.



Failover und Redundanz

vSAN kann die von vSphere bereitgestellte einfache NIC-Gruppierung und Failover-Richtlinie verwenden.

Die NIC-Gruppierung auf einem vSwitch kann mehrere aktive Uplinks oder eine Aktiv/Standby-Uplink-Konfiguration aufweisen. Die einfache NIC-Gruppierung erfordert keine spezielle Konfiguration auf der physischen Switch-Ebene.

Hinweis vSAN verwendet die NIC-Gruppierung nicht für den Lastausgleich.

Eine typische NIC-Gruppierungskonfiguration weist die folgenden Einstellungen auf. Bearbeiten Sie bei der Arbeit an verteilten Switches die Einstellungen der verteilten Portgruppe, die für den vSAN-Datenverkehr verwendet wird.

- Lastausgleich: Anhand des ursprünglichen virtuellen Ports routen
- Netzwerkfehlererkennung: nur Linkstatus
- Switches benachrichtigen: Ja
- Failback: Ja

Lastausgleich für den vSAN-Datenverkehr.

- Lastausgleich: Anhand des ursprünglichen virtuellen Ports routen
- Netzwerkfehlererkennung: nur Linkstatus
- Switches benachrichtigen: Ja
- Failback: Ja

Konfigurieren des Lastausgleichs für NIC-Gruppen

Für die NIC-Gruppierung stehen mehrere Lastausgleichstechniken zur Verfügung und jede Technik verfügt über Vor- und Nachteile.

Anhand des ursprünglichen virtuellen Ports routen

Verwenden Sie in Aktiv/Aktiv- oder Aktiv/Passiv-Konfigurationen **Anhand des ursprünglichen virtuellen Ports routen** für die grundlegende NIC-Gruppierung. Wenn diese Richtlinie aktiv ist, wird pro VMkernel-Port nur eine physische Netzwerkkarte verwendet.

Vorteile

- Dies ist die einfachste NIC-Gruppierungsmethode, die eine minimale Konfiguration des physischen Switches erfordert.
- Diese Methode erfordert nur einen einzelnen Port für vSAN-Datenverkehr, was die Fehlerbehebung vereinfacht.

Nachteile

- Eine einzelne VMkernel-Schnittstelle ist auf die Bandbreite einer einzelnen physischen Netzwerkkarte beschränkt. Da typische vSAN-Umgebungen einen VMkernel-Adapter verwenden, wird nur eine physische Netzwerkkarte in der Gruppe verwendet.

Anhand der physischen Netzwerkkartenauslastung routen

Anhand der physischen Netzwerkkartenauslastung routen basiert auf **Anhand des ursprünglichen virtuellen Ports routen**, wobei der virtuelle Switch die effektive Auslastung der Uplinks prüft und die entsprechenden Schritte zum Verringern der Last auf überlasteten Uplinks ausführt. Diese Lastausgleichsmethode ist nur für einen vSphere Distributed Switch und nicht für vSphere Standard-Switches verfügbar.

Der Distributed Switch berechnet Uplinks für jeden VMkernel-Port mithilfe der Port-ID und der Anzahl Uplinks in der Netzwerkkartengruppe. Der Distributed Switch testet die Uplinks aller 30 Sekunden. Wenn die Auslastung 75 Prozent übersteigt, wird die Port-ID des VMkernel-Ports mit der höchsten E/A zu einem anderen Uplink verschoben.

Vorteile

- Es ist keine Konfiguration des physischen Switches erforderlich.
- Obwohl vSAN über einen VMkernel-Port verfügt, können dieselben Uplinks von anderen VMkernel-Ports oder Netzwerkdiensten gemeinsam genutzt werden. vSAN können durch die Verwendung unterschiedlicher Uplinks von anderen konkurrierenden Diensten wie vMotion oder Management profitieren.

Nachteile

- Da für vSAN in der Regel nur ein VMkernel-Port konfiguriert ist, ist die Effektivität begrenzt.
- Der ESXi VMkernel wertet die Datenverkehrslast nach jedem Zeitintervall erneut aus, was zu einem Overhead bei der Verarbeitung führen kann.

Einstellungen: Netzwerkfehlererkennung

Verwenden Sie die Standardeinstellung: **Nur Verbindungsstatus**. Verwenden Sie keine Signalprüfung für die Erkennung von Verbindungsfehlern. Für die Signalprüfung sind mindestens drei physische Netzwerkkarten erforderlich, um Split-Brain-Szenarien zu vermeiden. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 1005577.

Einstellungen: Switches benachrichtigen

Verwenden Sie die Standardeinstellung: **Ja**. Physische Switches verfügen über Weiterleitungstabellen für die MAC-Adressen, um jede MAC-Adresse einem physischen Switch-Port zuzuordnen. Wenn ein Frame eingeht, bestimmt der Switch die MAC-Zieladresse in der Tabelle und entscheidet über den korrekten physischen Port.

Wenn ein NIC-Failover auftritt, muss der ESXi-Host die Netzwerk-Switches darüber benachrichtigen, dass sich etwas geändert hat oder der physische Switch verwendet möglicherweise weiterhin die alten Informationen und sendet die Frames an den falschen Port.

Wenn Sie „Switches benachrichtigen“ auf **Ja** festlegen und für eine physische Netzwerkkarte ein Fehler auftritt und der Datenverkehr zu einer anderen physischen Netzwerkkarte in der Gruppe umgeleitet wird, sendet der virtuelle Switch Benachrichtigungen über das Netzwerk, um die Suchtabellen der physischen Switches zu aktualisieren.

Diese Einstellung erfasst keine VLAN-Fehlkonfigurationen oder Uplink-Verluste, die zuvor im Netzwerk auftreten. Die Integritätsprüfung der vSAN-Netzwerkpartitionen kann diese Probleme erkennen.

Einstellungen: Failback

Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Ein Failover-Ereignis löst das Verschieben des Netzwerkdatenverkehrs von einer Netzwerkkarte zu einer anderen aus. Wenn auf der ursprünglichen Netzwerkkarte der Status **Verbindung aktiv** erkannt wird, wird der Datenverkehr automatisch auf den ursprünglichen Netzwerkadapter zurückgesetzt, sofern das Failback auf **Ja** festgelegt ist. Wenn das Failback auf **Nein** festgelegt ist, ist ein manuelles Failback erforderlich.

Die Failback-Festlegung auf **Nein** kann in einigen Situationen nützlich sein. Beispielsweise kann nach dem Wiederherstellen eines physischen Switch-Ports nach einem Fehler der Port aktiv sein, es kann aber einige Sekunden dauern, bis der Datenverkehr weitergeleitet wird. Das automatische Failback hat bekanntermaßen Probleme in bestimmten Umgebungen verursacht, die das Spanning Tree-Protokoll verwenden. Weitere Informationen zum Spanning Tree-Protocol (STP) finden Sie im VMware Knowledgebase-Artikel 1003804.

Festlegen der Failover-Reihenfolge

Die Failover-Reihenfolge legt fest, welche Links während des normalen Betriebs aktiv sind und welche Links im Falle eines Failovers aktiv sind. Für das vSAN-Netzwerk sind unterschiedliche unterstützte Konfigurationen möglich.

Aktiv/Standby-Uplinks: Wenn ein Fehler bei einer Aktiv/Standby-Einrichtung auftritt, benachrichtigt der NIC-Treiber vSphere über ein Link-Down-Ereignis für Uplink 1. Der Standby-Uplink 2 wird aktiv, und der Datenverkehr wird über Uplink 2 fortgesetzt.

Aktiv/Aktiv-Uplinks: Wenn Sie die Failover-Reihenfolge auf „Aktiv/Aktiv“ festlegen, kann der vom vSAN-Datenverkehr verwendete virtuelle Port nicht beide physischen Ports gleichzeitig verwenden.

Wenn Ihre NIC-Gruppierungskonfiguration für Uplink 1 und Uplink 2 aktiv ist, muss der Standby-Uplink nicht aktiv werden.

Hinweis Stellen Sie bei Verwendung einer Aktiv/Aktiv-Konfiguration sicher, dass das Failback auf **Nein** festgelegt ist. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 2072928.

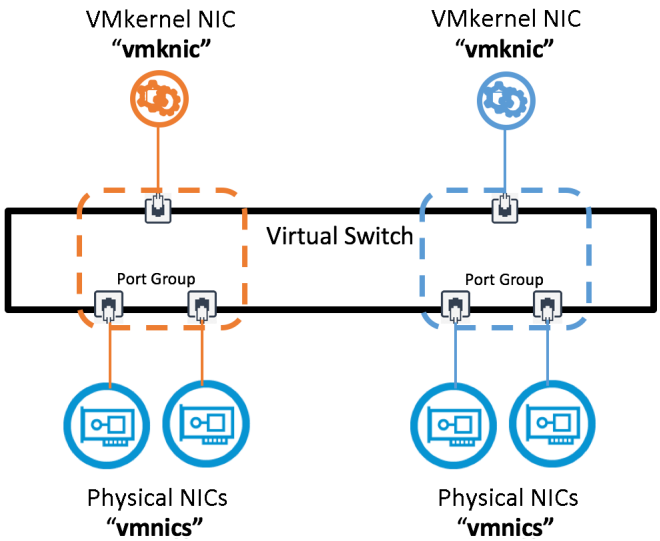
Erweiterte NIC-Gruppierung

9

Sie können erweiterte NIC-Gruppierungsmethoden mit mehreren VMkernel-Adaptern verwenden, um das vSAN-Netzwerk zu konfigurieren. Wenn Sie das Link-Aggregationsprotokoll (LAG/LACP) verwenden, kann das vSAN-Netzwerk mit einem einzelnen VMkernel-Adapter konfiguriert werden.

Sie können die erweiterte NIC-Gruppierung verwenden, um eine Air Gap zu implementieren. Dadurch hat ein Fehler, der in einem Netzwerkpfad auftritt, keinen Einfluss auf den anderen Netzwerkpfad. Wenn ein Teil eines Netzwerkpfads ausfällt, kann der andere Netzwerkpfad den Datenverkehr übertragen. Konfigurieren Sie mehrere VMkernel-Netzwerkkarten für vSAN in unterschiedlichen Subnetzen, z. B. in einem anderen VLAN oder einer separaten physischen Netzwerk-Fabric.

Mehrere VMkernel-Adapter (vmknics) im selben Subnetz werden von vSphere und vSAN nicht unterstützt. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 2010877.



Lesen Sie als Nächstes die folgenden Themen:

- Übersicht über die Link-Aggregationsgruppe
- Grundlegendes zu Air-Gaps im Netzwerk

- Vor- und Nachteile von Air-Gap-Netzwerkkonfigurationen mit vSAN
- Konfigurationsbeispiele für die NIC-Gruppierung

Übersicht über die Link-Aggregationsgruppe

Mithilfe des LACP-Protokolls kann ein Netzwerkgerät eine automatische Bündelung von Links aushandeln, indem LACP-Pakete an einen Peer gesendet werden.

Eine Link-Aggregationsgruppe (LAG) wird durch den Standard IEEE 802.1AX-2008 definiert, der besagt, dass ein oder mehrere Links zusammengefasst werden können, um eine Link-Aggregationsgruppe zu bilden.

LAG kann entweder statisch (manuell) oder dynamisch konfiguriert werden, indem LACP zum Aushandeln der LAG-Formation verwendet wird. LACP kann wie folgt konfiguriert werden:

Aktiv

Geräte senden LACP-Meldungen sofort, wenn der Port aktiv wird. Endgeräte mit aktiviertem LACP (z. B. ESXi-Hosts und physische Switches) senden und empfangen Frames, die als LACP-Meldungen bezeichnet werden, um die Erstellung einer LAG auszuhandeln.

Passiv

Geräte versetzen einen Port in einen passiven Aushandlungszustand, in dem der Port nur auf empfangene LACP-Meldungen reagiert, aber keine Aushandlung initiiert.

Hinweis Wenn sich der Host und der Switch im passiven Modus befinden, wird die LAG nicht initialisiert, da ein aktiver Teil zum Auslösen der Verknüpfung erforderlich ist. Mindestens einer muss aktiv sein.

In vSphere 5.5 und neueren Versionen wird diese Funktionalität als **Erweitertes LACP** bezeichnet. Diese Funktionalität wird nur auf vSphere Distributed Switch Version 5.5 oder höher unterstützt.

Weitere Informationen zur LACP-Unterstützung auf einem vSphere Distributed Switch finden Sie in der Dokumentation zum vSphere 6-Netzwerk.

Hinweis Die Anzahl verwendbarer LAGs hängt von der Funktion der zugrunde liegenden physischen Umgebung sowie der Topologie des virtuellen Netzwerks ab.

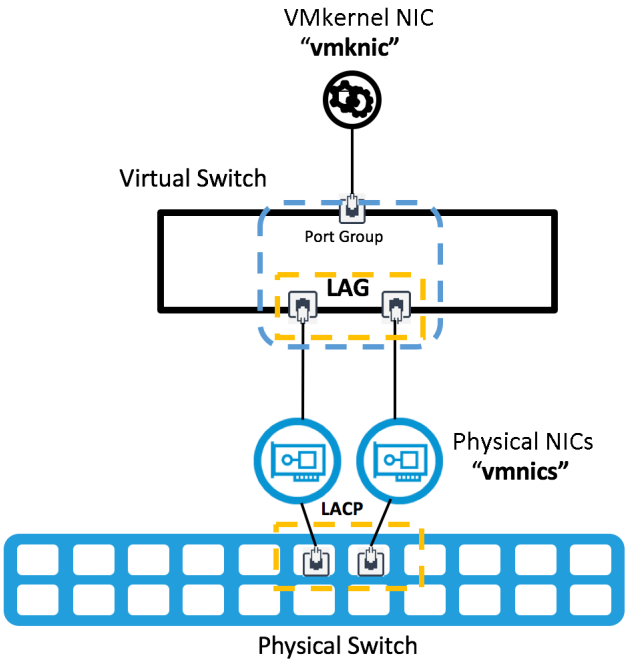
Weitere Informationen zu den verschiedenen Lastausgleichsoptionen finden Sie im Knowledgebase-Artikel 2051826.

Statische und dynamische Linkaggregation

Sie können LACP verwenden, um mehrere Netzwerkverbindungen zu kombinieren und zu aggregieren.

Wenn sich LACP im **aktiven** oder **dynamischen** Modus befindet, sendet ein physischer Switch LACP-Meldungen an Netzwerkgeräte wie ESXi-Hosts, um die Erstellung einer Link-Aggregationsgruppe (LAG) auszuhandeln.

Wenn Sie die Link-Aggregation auf Hosts konfigurieren möchten, die vSphere Standard-Switches verwenden (und vor 5.5 vSphere Distributed Switches), konfigurieren Sie eine statische Kanalgruppe auf dem physischen Switch. Weitere Informationen finden Sie in der Herstellerdokumentation.



Vor- und Nachteile der dynamischen Link-Aggregation

Ziehen Sie die folgenden Kompromisse bei der Verwendung der dynamischen Link-Aggregation in Erwägung.

Vorteile

Verbessert die Leistung und Bandbreite. Ein vSAN-Host oder VMkernel-Port kann mithilfe von vielen unterschiedlichen Lastausgleichsoptionen mit vielen anderen vSAN-Hosts kommunizieren.

Stellt Netzwerkadapterredundanz bereit. Wenn eine Netzwerkkarte ausfällt und der Verbindungsstatus fehlschlägt, leiten die verbleibenden Netzwerkkarten in der Gruppierung weiterhin den Datenverkehr weiter.

Verbessert den Datenverkehrsausgleich. Das Ausgleichen des Datenverkehrs nach einem Ausfall erfolgt schnell und automatisch.

Nachteile

Weniger flexibel. Für die Konfiguration des physischen Switches müssen physische Switch-Ports in einer Portkanalkonfiguration konfiguriert werden.

Komplexer. Die Verwendung mehrerer Switches zur Erzeugung einer vollständigen physischen Redundanzkonfiguration ist komplex. Herstellerspezifische Implementierungen erhöhen die Komplexität noch weiter.

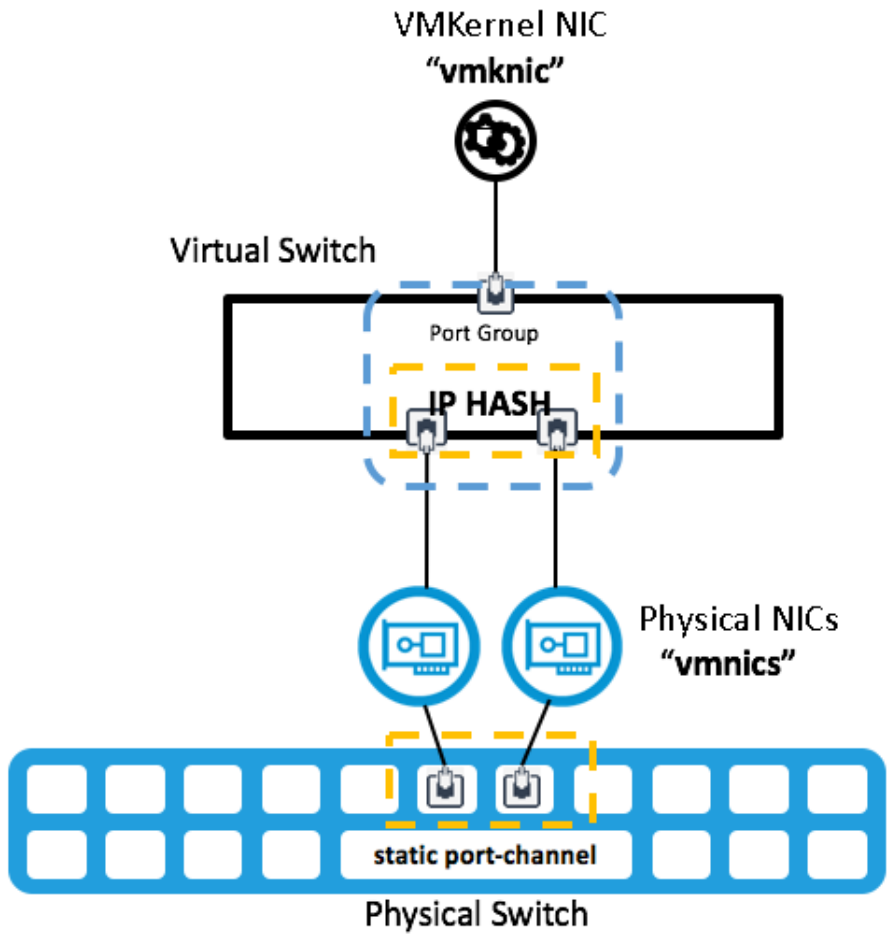
Statische LACP mit „Anhand des IP-Hashs routen“

Sie können einen vSAN 6.6-Cluster mit statischer LACP mit einer IP-Hash-Richtlinie erstellen. Der Schwerpunkt dieses Abschnitts liegt auf vSphere Standard-Switches, Sie können aber auch vSphere Distributed Switches verwenden.

Sie können die Lastausgleichsrichtlinie „Anhand des IP-Hashs routen“ verwenden.

Wählen Sie die Lastausgleichsrichtlinie **Anhand des IP-Hashs routen** auf einer vSwitch- oder Portgruppenebene aus. Legen Sie auf Ebene des virtuellen Switches oder der Portgruppe alle Uplinks, die der statischen Kanalgruppe zugewiesen sind, auf die Uplink-Position „Aktiv“ in den Gruppenbildungs- und Failover-Richtlinien fest.

Wenn der IP-Hash auf einer vSphere-Portgruppe konfiguriert ist, verwendet die Portgruppe die Richtlinie **Anhand des IP-Hashs routen**. Die Anzahl Ports im Portkanal muss gleich der Anzahl Uplinks in der Gruppierung sein.



Vor- und Nachteile von statischem LACP mit IP-Hash

Berücksichtigen Sie die Kompromisse bei der Verwendung von statischem LACP mit IP-Hash.

Vorteile

- **Verbessert die Leistung und Bandbreite**. Ein vSAN-Host oder VMkernel-Port kann mithilfe des IP-Hash-Algorithmus mit vielen anderen vSAN-Hosts kommunizieren.
- **Stellt Netzwerkadapterredundanz bereit**. Wenn eine Netzwerkkarte ausfällt und der Verbindungsstatus fehlschlägt, leiten die verbleibenden Netzwerkkarten in der Gruppierung weiterhin den Datenverkehr weiter.
- **Mehr Flexibilität**. Sie können den IP-Hash sowohl mit vSphere Standard-Switches als auch mit vSphere Distributed Switches verwenden.

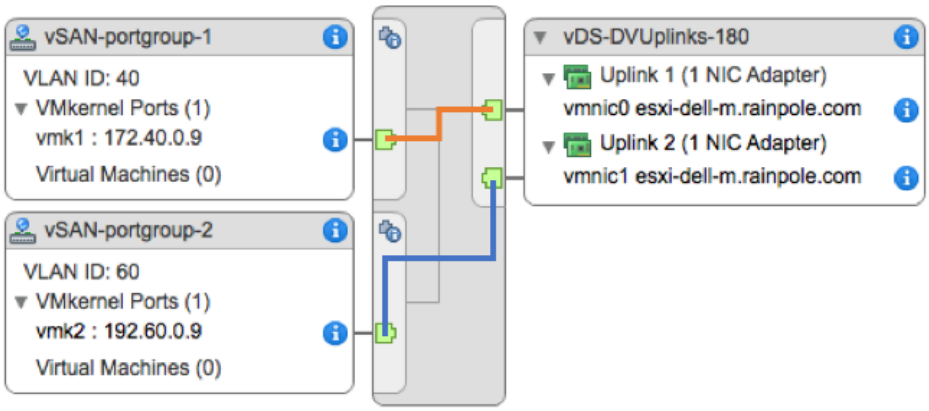
Nachteile

- **Die Konfiguration des physischen Switches ist weniger flexibel**. Physische Switch-Ports müssen in einer statischen Portkanalkonfiguration konfiguriert werden.
- **Erhöhte Wahrscheinlichkeit einer Fehlkonfiguration**. Für statische Portkanäle erfolgt an beiden Enden keine Überprüfung (im Gegensatz zu zum dynamischen LACP-Portkanal).
- **Komplexer**. Durch die Einführung der Konfiguration einer vollständigen physischen Redundanz wird die Komplexität erhöht, wenn mehrere Switches verwendet werden. Implementierungen können sehr herstellerspezifisch werden.
- **Begrenzter Lastausgleich**. Wenn Ihre Umgebung nur wenige IP-Adressen aufweist, leitet der virtuelle Switch den Datenverkehr möglicherweise immer über denselben Uplink in der Gruppierung. Dies kann besonders für kleine vSAN-Cluster der Fall sein.

Grundlegendes zu Air-Gaps im Netzwerk

Sie können erweiterte NIC-Gruppierungsmethoden verwenden, um eine Air-Gap-Speicher-Fabric zu erstellen. Zwei Speichernetzwerke werden verwendet, um eine redundante Speichernetzwerktopologie zu erstellen, wobei die einzelnen Speichernetzwerke per Air-Gap physisch und logisch voneinander isoliert werden.

Sie können einen Netzwerk-Air-Gap für vSAN in einer vSphere-Umgebung konfigurieren. Konfigurieren Sie mehrere -VMkernel-Ports pro vSAN-Host. Verknüpfen Sie jeden VMkernel-Port mit dedizierten physischen Uplinks, indem Sie entweder einen einzelnen vSwitch oder mehrere virtuelle Switches verwenden, z. B. vSphere Standard-Switch oder vSphere Distributed Switch .



In der Regel muss jeder Uplink mit einer vollständig redundanten physischen Infrastruktur verbunden sein.

Diese Topologie ist nicht ideal. Der Ausfall von-Komponenten wie Netzwerkkarten auf verschiedenen Hosts, die sich im selben Netzwerk befinden, kann zu einer Unterbrechung der Speicher-E/A führen. Um dieses Problem zu vermeiden, implementieren Sie die Redundanz der physischen Netzwerkkarte auf allen Hosts und allen Netzwerksegmenten. Im Konfigurationsbeispiel 2 wird diese Topologie ausführlich behandelt.

Diese Konfigurationen gelten sowohl für Schicht-2- als auch für Schicht-3-Topologien mit Unicast- und Multicast-Konfigurationen.

Vor- und Nachteile von Air-Gap-Netzwerkkonfigurationen mit vSAN

Air-Gaps in Netzwerken können nützlich sein, um vSAN-Datenverkehr zu trennen und zu isolieren. Gehen Sie beim Konfigurieren dieser Topologie vorsichtig vor.

Vorteile

- Physische und logische Trennung von vSAN-Datenverkehr.

Nachteile

- Mehrere VMkernel-Adapter (vmknics) im selben Subnetz werden von vSAN nicht unterstützt. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 2010877.
- Die Einrichtung ist komplex und fehleranfällig, daher ist die Fehlerbehebung komplexer.
- Die Netzwerkverfügbarkeit wird mit mehreren vmknics bei einigen asymmetrischen Fehlern nicht garantiert, z. B. mit einem NIC-Fehler auf einem Host und einem anderen NIC-Fehler auf einem anderen Host.
- Der vSAN-Datenverkehr mit Lastausgleich über physische Netzwerkkarten hinweg ist nicht garantiert.

- Die Kosten für vSAN-Hosts steigen, da Sie möglicherweise mehrere VMkernel-Adapter (vmknics) benötigen, um mehrere physische Netzwerkkarten (vmnics) zu schützen. Beispielsweise können 2 x 2 vmnics erforderlich sein, um Redundanz für zwei vSAN vmknics bereitzustellen.
- Erforderliche logische Ressourcen werden verdoppelt, z. B. VMkernel-Ports, IP-Adressen und VLANs.
- vSAN implementiert keine Port-Bindung. Dies bedeutet, dass Techniken wie Multi-Pathing nicht verfügbar sind.
- Schicht-3-Topologien eignen sich nicht für vSAN-Datenverkehr mit mehreren vmknics. Diese Topologien funktionieren möglicherweise nicht wie erwartet.
- Die Befehlszeilen-Hostkonfiguration ist möglicherweise erforderlich, um vSAN Multicast-Adressen zu ändern.

Dynamisches LACP kombiniert oder aggregiert mehrere Netzwerkverbindungen parallel, um den Durchsatz zu erhöhen und Redundanz bereitzustellen. Wenn die NIC-Gruppierung mit LACP konfiguriert ist, erfolgt der Lastausgleich des vSAN-Netzwerks über mehrere Uplinks hinweg. Dieser Lastausgleich erfolgt auf der Netzwerkschicht und wird nicht über vSAN durchgeführt.

Hinweis Andere Begriffe, die manchmal zur Beschreibung der Link-Aggregation verwendet werden, umfassen Port Trunking, Link-Bündelung, Ethernet/Netzwerk/NIC-Bonding, EtherChannel.

Der Schwerpunkt dieses Abschnitts liegt auf dem Aggregationssteuerungsprotokoll (LACP). Der IEEE-Standard ist 802.3ad, aber einige Anbieter verfügen über proprietäre LACP-Funktionen, wie z. B. PAgP (Portaggregationsprotokoll). Befolgen Sie die Best Practices, die von Ihrem Anbieter empfohlen werden.

Hinweis Die in vSphere Distributed Switch 5.1 eingeführte LACP-Unterstützung unterstützt nur den IP-Hash-Lastausgleich. vSphere Distributed Switch 5.5 und höher unterstützen LACP vollständig.

LACP ist ein Industriestandard, der Portkanäle verwendet. Es sind viele Hash-Algorithmen verfügbar. Die vSwitch-Portgruppenrichtlinie und die Portkanalkonfiguration müssen zusammenpassen und übereinstimmen.

Konfigurationsbeispiele für die NIC-Gruppierung

Die folgenden NIC-Gruppierungskonfigurationen veranschaulichen typische vSAN-Netzwerkszenarien.

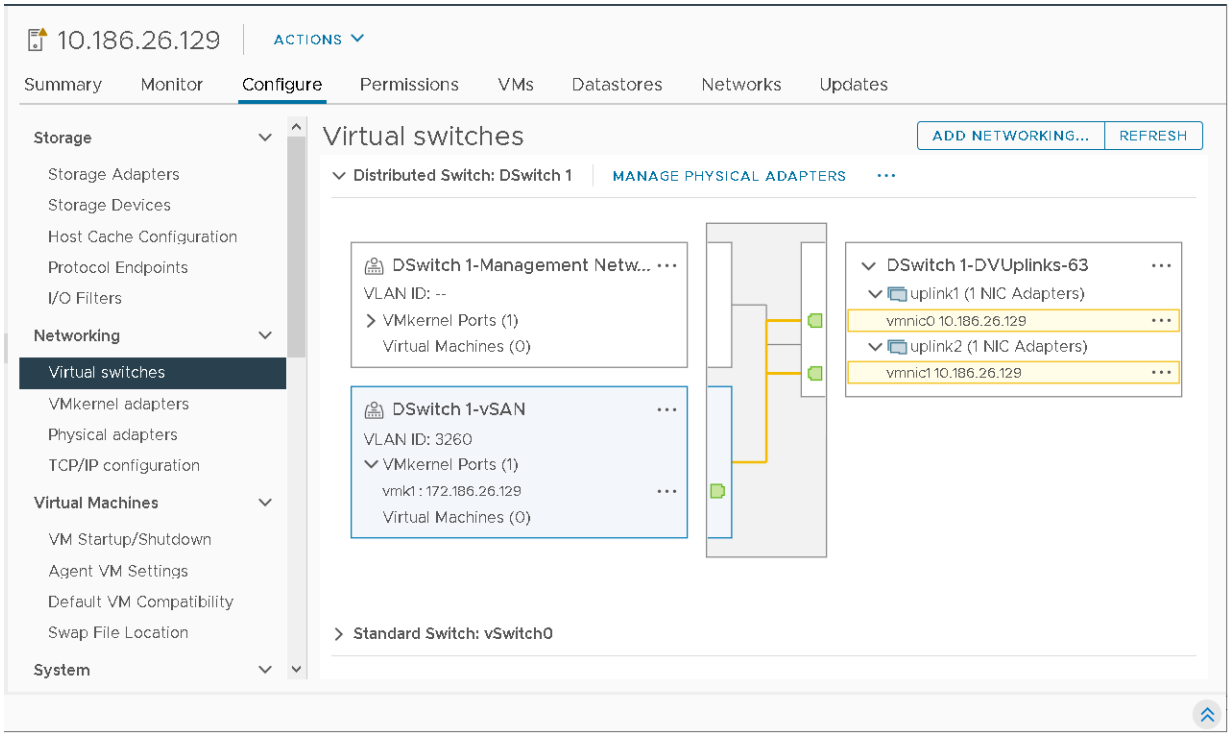
Konfiguration 1: Einzelne vmknic, Anhand der physischen Netzwerkkartenauslastung routen

Sie können die grundlegende Aktiv/Aktiv-NIC-Gruppierung mit der Richtlinie **Anhand der physischen Netzwerkkartenauslastung routen** für vSAN-Hosts konfigurieren. Verwenden Sie einen vSphere Distributed Switch (vDS).

Für dieses Beispiel muss der vDS über zwei Uplinks verfügen, die für jeden Host konfiguriert sind. Eine verteilte Portgruppe ist für vSAN-Datenverkehr vorgesehen und für ein bestimmtes VLAN isoliert. Jumbo-Frames sind bereits auf dem vDS mit einem MTU-Wert von 9000 aktiviert.

Konfigurieren Sie Gruppierung und Failover für die verteilte Portgruppe für vSAN-Datenverkehr wie folgt:

- Die Lastausgleichsrichtlinie wird auf **Anhand der physischen Netzwerkkartenauslastung routen** festgelegt.
- Die Netzwerkfehlererkennung wird auf **Nur Verbindungsstatus** festgelegt.
- „Switches benachrichtigen“ wird auf **Ja** festgelegt.
- Failback wird auf **Nein** festgelegt. Sie können das Failback auf **Ja** festlegen, jedoch nicht in diesem Beispiel.
- Stellen Sie sicher, dass sich beide Uplinks in der Position **Aktive Uplinks** befinden.



Netzwerk-Uplink-Redundanz verloren

Wenn der Link-Down-Status erkannt wird, wechselt die Arbeitslast von einem Uplink zu einem anderen. Es gibt keine spürbaren Auswirkungen auf den vSAN-Cluster und die VM-Arbeitslast.

Wiederherstellung und Failback

Wenn Sie **Failback** auf **Nein** festlegen, wird der Datenverkehr nicht wieder auf die ursprüngliche Vmnic heraufgestuft. Wenn **Failback** auf **Ja** festgelegt ist, wird der Datenverkehr bei der Wiederherstellung wieder auf den ursprünglichen vmnic heraufgestuft.

Lastausgleich

Da es sich hierbei um eine einzelne VMkernel-Netzwerkkarte handelt, gibt es keinen Leistungsvorteil für die Verwendung von **Anhand der physischen Last routen**.

Es wird jeweils nur eine physische Netzwerkkarte verwendet. Die andere physische Netzwerkkarte befindet sich im Leerlauf.

Konfiguration 2: Mehrere vmknics, Anhand der ursprünglichen ID des Ports routen

Sie können zwei nicht routingfähige VLANs verwenden, die logisch und physisch getrennt sind, um eine Air-Gap-Topologie zu erstellen.

In diesem Beispiel werden Konfigurationsschritte für einen vSphere Distributed Switch bereitgestellt, aber Sie können auch vSphere Standard-Switches verwenden. Es werden zwei physische Netzwerkkarten mit 10 GB verwendet und logisch auf der vSphere-Netzwerkschicht geteilt.

Erstellen Sie zwei verteilte Portgruppen für jede vSAN VMkernel-vmknic. Jede Portgruppe verfügt über ein separates VLAN-Tag. Für die vSAN VMkernel-Konfiguration sind zwei IP-Adressen in beiden VLANs für den vSAN-Datenverkehr erforderlich.

Hinweis Bei praktischen Implementierungen werden üblicherweise vier physische Uplinks für die vollständige Redundanz verwendet.

Für jede Portgruppe werden hinsichtlich der Gruppierungs- und Failover-Richtlinien die Standardeinstellungen verwendet.

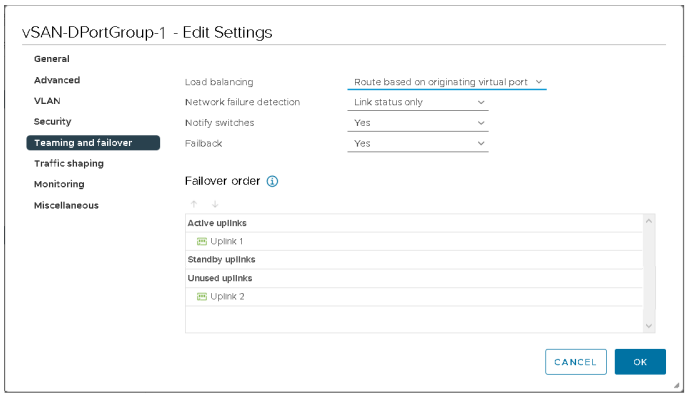
- Lastausgleich festgelegt auf **Anhand der ursprünglichen ID des Ports routen**
- Netzwerkfehlererkennung festgelegt auf **Nur Verbindungsstatus**
- „Switches benachrichtigen“ festgelegt auf den Standardwert **Ja**
- Failback festgelegt auf den Standardwert **Ja**
- Die Uplink-Konfiguration verfügt über einen Uplink in der Position **Aktiv** Position und einen Uplink in der Position **Nicht verwendet**.

Ein Netzwerk ist vollständig vom anderen Netzwerk isoliert.

vSAN-Portgruppe 1

In diesem Beispiel wird eine verteilte Portgruppe mit dem Namen **vSAN-DPortGroup-1** verwendet. **VLAN 3266** ist für diese Portgruppe mit der folgenden Gruppierungs- und Failover-Richtlinie gekennzeichnet:

- Datenverkehr auf der Portgruppe mit dem Tag VLAN 3266
- Lastausgleich festgelegt auf **Anhand der ursprünglichen ID des Ports routen**
- Netzwerkfehlererkennung festgelegt auf **Nur Verbindungsstatus**
- „Switches benachrichtigen“ festgelegt auf den Standardwert **Ja**
- Failback festgelegt auf den Standardwert **Ja**
- In der Uplink-Konfiguration ist **Uplink 1** in der Position **Aktiv** und **Uplink 2** in der Position **Nicht verwendet**.



vSAN-Portgruppe 2

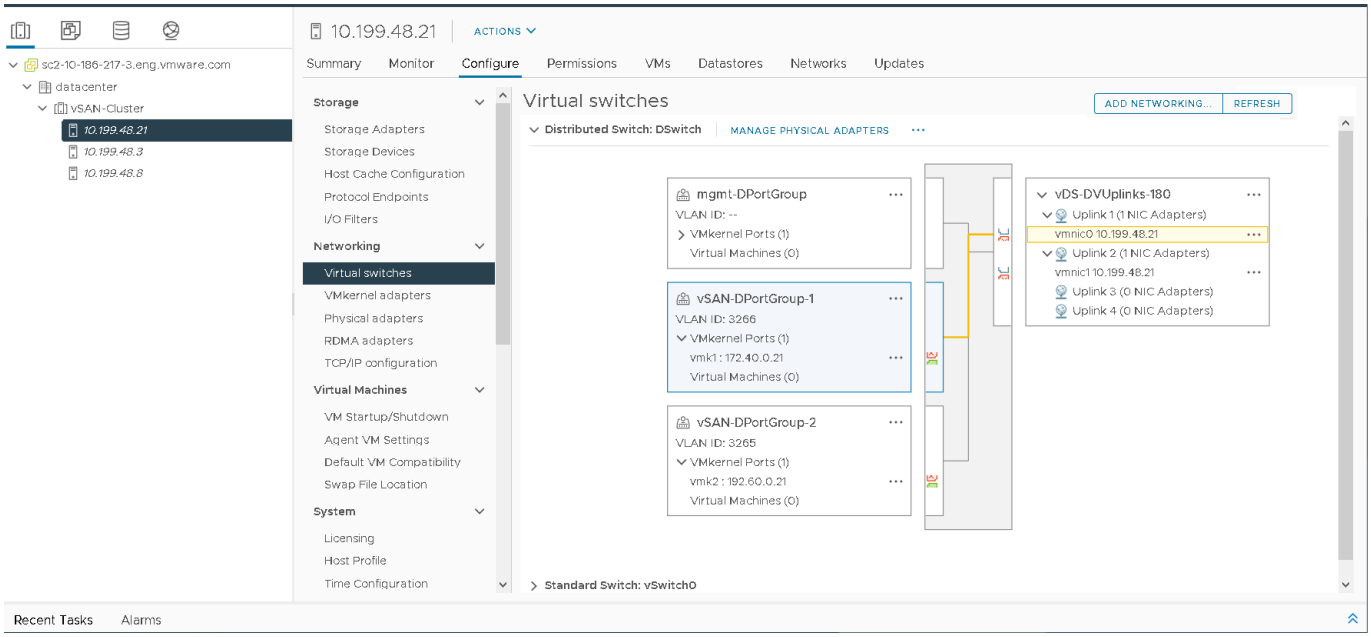
Konfigurieren Sie zur Ergänzung von vSAN-Portgruppe 1 eine zweite verteilte Portgruppe mit dem Namen **vSAN-portgroup-2** mit den folgenden Unterschieden:

- Datenverkehr auf der Portgruppe mit dem Tag VLAN 3265
- In der Uplink-Konfiguration ist **Uplink 2** in der Position **Aktiv** und **Uplink 1** in der Position **Nicht verwendet**.

vSAN VMkernel-Portkonfiguration

Erstellen Sie zwei vSAN-VMkernel-Schnittstellen auf beiden Portgruppen. In diesem Beispiel werden die Portgruppen **vmk1** und **vmk2** benannt.

- **vmk1** ist mit VLAN 3266 (172.40.0.xx) verknüpft und demzufolge die Portgruppe **vSAN-DPortGroup-1**.
- **vmk2** ist mit VLAN 3265 (192.60.0.xx) verknüpft und demzufolge die Portgruppe **vSAN-DPortGroup-2**.



Lastausgleich

vSAN verfügt über keinen Lastausgleichsmechanismus, um zwischen mehreren vmknics zu unterscheiden, sodass der ausgewählte E/A-Pfad für vSAN nicht über physische Netzwerkkarten hinweg deterministisch ist. Die vSphere-Leistungsdiagramme zeigen, dass eine physische Netzwerkkarte häufig stärker ausgelastet ist als die andere. Ein einfacher E/A-Test, der in unseren Labors durchgeführt wurde mit 120 VMs mit einem Lese-/Schreibverhältnis von 70:30 und einer Blockgröße von 64 KB auf einem vSAN-All-Flash-Cluster mit vier Hosts ergab eine unausgeglichene Last der Netzwerkkarten.

vSphere-Leistungsdiagramme zeigen eine nicht ausgeglichene Last für die verschiedenen Netzwerkkarten.

Netzwerk-Uplink-Redundanz verloren

Berücksichtigen Sie einen Netzwerkfehler, der in dieser Konfiguration eingeführt wurde. vmnic1 ist auf einem bestimmten vSAN-Host nicht aktiviert. Dadurch wird Port **vmk2** beeinträchtigt. Eine fehlerhafte Netzwerkkarte löst sowohl Netzwerkkonnektivitätsalarme als auch Redundanzalarme aus.

Für vSAN wird dieser Failover-Vorgang nach ungefähr **10 Sekunden** ausgelöst, sobald CMMDS (Clusterüberwachung, Mitgliedschaft und Verzeichnisdienste) einen Fehler erkannt hat. Während des Failovers und der Wiederherstellung stoppt vSAN alle aktiven Verbindungen für das fehlerhafte Netzwerk ab und versucht, Verbindungen im noch funktionstüchtigen Netzwerk wiederherzustellen.

Da zwei getrennte vSAN VMkernel-Ports in isolierten VLANs kommunizieren, können vSAN-Systemzustandsprüfungsfehler ausgelöst werden. Dies wird erwartet, da **vmk2** nicht mehr mit seinen Peers über VLAN 3265 kommunizieren kann.

Die Leistungsdiagramme zeigen, dass die betroffene Arbeitslast auf vmnic0 neu gestartet wurde, da vmnic1 einen Fehler aufweist. Dieser Test veranschaulicht einen wichtigen Unterschied zwischen der vSphere NIC-Gruppierung und dieser Topologie. vSAN versucht, Verbindungen im verbleibenden Netzwerk erneut herzustellen oder neu zu starten.

In einigen Fehlerszenarien kann die Wiederherstellung der betroffenen Verbindungen jedoch aufgrund des ESXi TCP-Verbindungszeitüberschreitung bis zu **90 Sekunden** dauern. Nachfolgende Verbindungsversuche schlagen möglicherweise fehl, aber für die Verbindungsversuche tritt bei 5 Sekunden eine Zeitüberschreitung ein, und die Versuche durchlaufen alle möglichen IP-Adressen. Dieses Verhalten kann sich auf die Gast-E/A der virtuellen Maschine auswirken. Folglich müssen die E/A-Vorgänge für Anwendungen und virtuelle Maschinen möglicherweise erneut versucht werden.

Auf Windows Server 2012-VMs werden möglicherweise während des Failover- und Wiederherstellungsvorgangs die Ereignis-IDs 153 (Gerät zurücksetzen) und 129 (Wiederholungsereignisse) protokolliert. In dem Beispiel wurde die Ereignis-ID 129 für ca. 90 Sekunden protokolliert, bis die E/A wiederhergestellt wurde.

Möglicherweise müssen Sie die Zeitüberschreitungseinstellungen für Datenträger einiger Gastbetriebssysteme ändern, um sicherzustellen, dass sie nicht schwerwiegend beeinträchtigt werden. Datenträger-Zeitüberschreitungswerte können variieren. Dies ist von den vorhandenen VMware Tools und dem jeweiligen Typ und der jeweiligen Version des Gastbetriebssystems abhängig. Weitere Informationen zum Ändern der Werte für die Datenträger-Zeitüberschreitung des Gastbetriebssystems finden Sie im VMware-Knowledgebase-Artikel 1009465.

Wiederherstellung und Failback

Beim Reparieren des Netzwerks werden Arbeitslasten nicht automatisch neu verteilt, es sei denn, die Arbeitslast wird aufgrund eines anderen Fehlers nicht erzwungen. Sobald das betroffene Netzwerk wiederhergestellt wurde, ist es für neue TCP-Verbindungen verfügbar.

Konfiguration 3: dynamisches LACP

Sie können einen LACP-Portkanal mit zwei Ports auf einem Switch und eine Link-Aggregationsgruppe mit zwei Uplinks auf einem vSphere Distributed Switch konfigurieren.

Verwenden Sie in diesem Beispiel ein 10-GB-Netzwerk mit zwei physischen Uplinks pro Server.

Hinweis vSAN über RDMA unterstützt diese Konfiguration nicht.

Konfigurieren des Netzwerk-Switches

Konfigurieren Sie den vSphere Distributed Switch mit den folgenden Einstellungen.

- Identifizieren Sie die fraglichen Ports, mit denen der vSAN-Host eine Verbindung herstellt.
- Erstellen Sie einen Portkanal.
- Wenn Sie VLANs verwenden, führen Sie ein Trunking des korrekten VLANs auf dem Portkanal durch.

- Konfigurieren Sie die gewünschten Verteilungs- oder Lastausgleichsoptionen (Hash).
- Der LACP-Modus wird auf aktiv/dynamisch festgelegt.
- Überprüfen Sie die MTU-Konfiguration.

Konfigurieren von vSphere

Konfigurieren Sie das vSphere-Netzwerk mit den folgenden Einstellungen.

- Konfigurieren Sie vDS mit der richtigen MTU.
- Fügen Sie vDS Hosts hinzu.
- Erstellen Sie eine LAG mit der korrekten Anzahl Uplinks und übereinstimmenden Attributen mit dem Portkanal.
- Weisen Sie der LAG physische Uplinks zu.
- Erstellen Sie eine verteilte Portgruppe für vSAN-Datenverkehr, und weisen Sie das richtige VLAN zu.
- Konfigurieren Sie VMkernel-Ports für vSAN mit der richtigen MTU.

Einrichten des physischen Switches

Konfigurieren Sie den physischen Switch mit den folgenden Einstellungen. Eine Anleitung zum Einrichten dieser Konfiguration auf Dell-Servern finden Sie unter: http://www.dell.com/Support/Article/de/de/19/HOW10364.

Konfigurieren Sie LAG mit zwei Uplinks:

- Verwenden Sie die Switch-Ports 36 und 18.
- Diese Konfiguration verwendet VLAN-Trunking, daher befindet sich der Portkanal im VLAN-Trunk-Modus mit den entsprechenden Trunked-VLANs.
- Verwenden Sie die folgende Methode für den Lastausgleich oder die Lastverteilung: **Quell- und Ziel-IP-Adressen, TCP/UDP-Port und VLAN**.
- Stellen Sie sicher, dass der LACP-Modus **Aktiv** (Dynamisch) lautet.

Verwenden Sie die folgenden Befehle, um einen einzelnen Portkanal auf einem Dell-Switch zu konfigurieren:

- Erstellen Sie einen Portkanal.

```
#interface port-channel 1
```

- Legen Sie den Portkanal auf VLAN-Trunk-Modus fest.

```
#switchport mode trunk
```

- Lassen Sie den Zugriff für VLAN zu.

```
#switchport trunk allowed vlan 3262
```

- Konfigurieren Sie die Lastausgleichsoption.

```
#hashing-mode 6
```

- Weisen Sie dem Portkanal die korrekten Ports zu, und legen Sie den Modus auf „Aktiv“ fest.
- Stellen Sie sicher, dass der Portkanal konfiguriert ist.

```
#show interfaces port-channel 1


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ---------------------------- -------- --------- --------- ----------

Po1 Active: Te1/0/36, Te1/0/18 Dynamic 6 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
#interface range Te1/0/36, Te1/0/18

#channel-group 1 mode active
```

Vollständige Konfiguration:

```
#interface port-channel 1

#switchport mode trunk

#switchport trunk allowed vlan 3262

#hashing-mode 6

#exit

#interface range Te1/0/36,Te1/018

#channel-group 1 mode active

#show interfaces port-channel 1
```

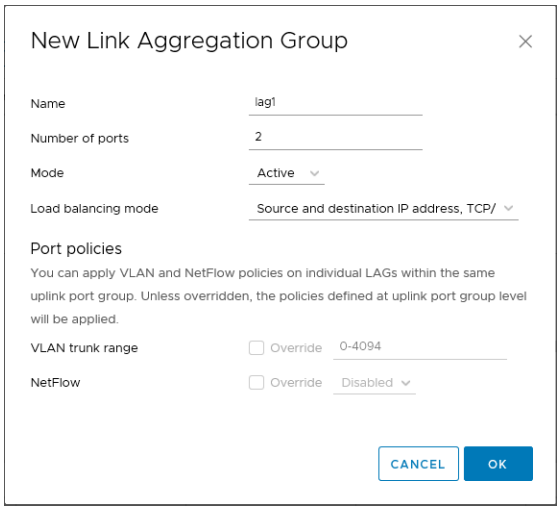
Hinweis Wiederholen Sie diesen Vorgang für alle teilnehmenden Switch-Ports, die mit vSAN-Hosts verbunden sind.

Einrichten von vSphere Distributed Switch

Bevor Sie beginnen, stellen Sie sicher, dass der vDS auf eine Version aktualisiert wird, die LACP unterstützt. Klicken Sie für die Überprüfung mit der rechten Maustaste auf den vDS und überprüfen Sie, ob die Upgrade-Option verfügbar ist. Möglicherweise müssen Sie ein vDS-Upgrade auf eine Version durchführen, die LACP unterstützt.

Erstellen von LAG auf vDS

Wenn Sie eine LAG auf einem Distributed Switch erstellen möchten, wählen Sie den vDS aus, klicken auf die Registerkarte **Konfigurieren**, und wählen Sie **LACP** aus. Fügen Sie eine neue LAG hinzu.



Konfigurieren Sie die LAG mit den folgenden Eigenschaften:

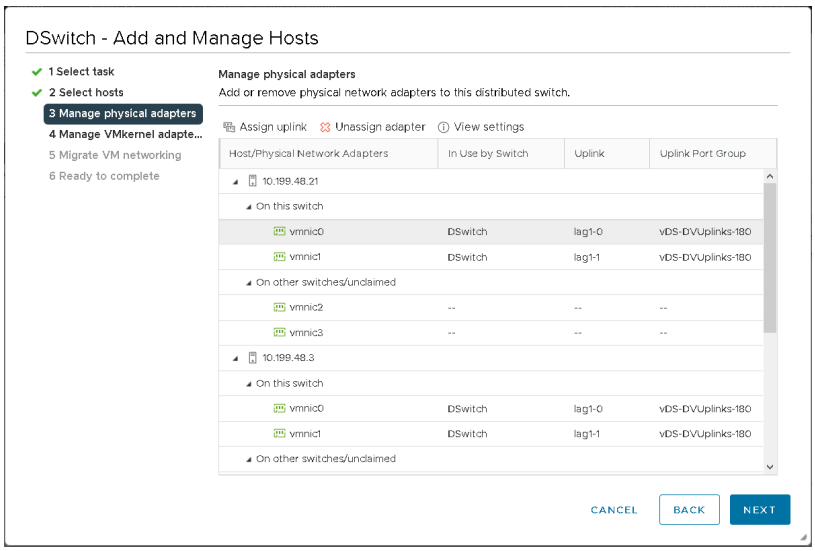
- LAG-Name: **lag1**
- Anzahl Ports: **2** (sollte mit dem Portkanal auf dem Switch übereinstimmen)
- Modus: **Aktiv** (sollte mit dem physischen Switch übereinstimmen).
- Lastausgleichsmodus: **Quell- und Ziel-IP-Adressen, TCP/UDP-Port und VLAN**

Hinzufügen physischer Uplinks zu LAG

vSAN-Hosts wurden dem vDS hinzugefügt. Weisen Sie die einzelnen vmnics den entsprechenden LAG-Ports zu.

- Klicken Sie mit der rechten Maustaste auf den vDS, und wählen Sie **Hosts hinzufügen und verwalten...** aus.
- Wählen Sie **Hostnetzwerk verwalten** aus, und fügen Sie die angehängten Hosts hinzu.
- Wählen Sie unter **Physische Adapter verwalten** die entsprechenden Adapter aus, und weisen Sie sie dem LAG-Port zu.
- Migrieren Sie vmnic0 von der Uplink 1-Position zu dem Port 0 auf LAG1.

Wiederholen Sie den Vorgang für vmnic1 an der zweiten LAG-Portposition, lag1-1.



Konfigurieren der Gruppenbildungs- und Failover-Richtlinie für verteilte Portgruppen

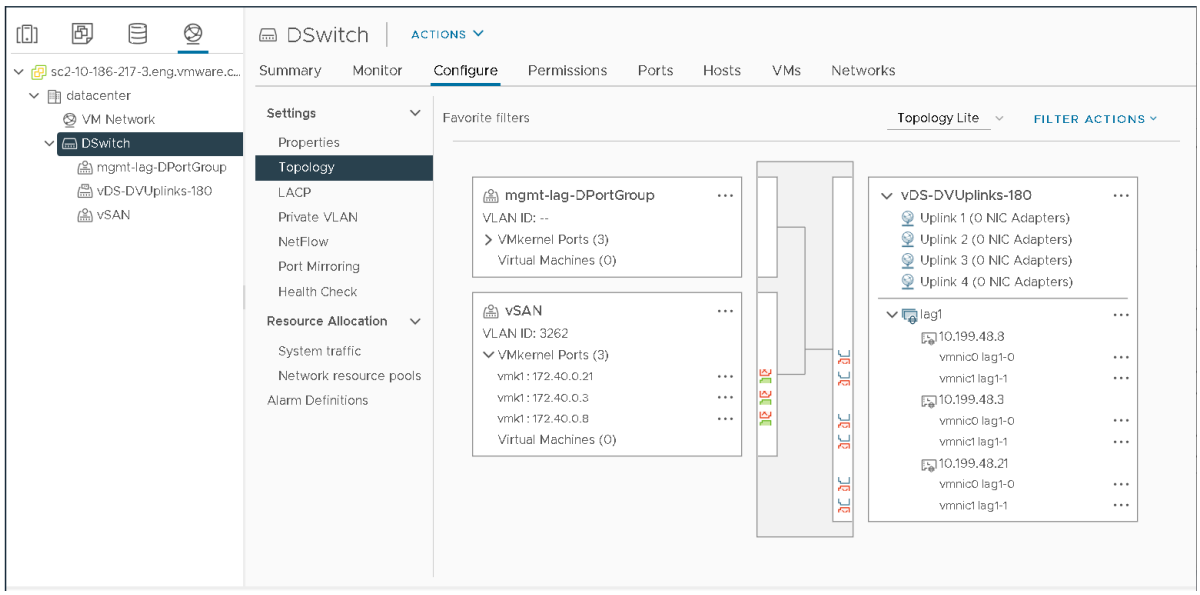
Weisen Sie die LAG-Gruppe als **Aktiven Uplink** für die Gruppenbildungs- und Failover-Richtlinie für verteilte Portgruppen zu. Wählen Sie die angegebene verteilte Portgruppe für vSAN-Datenverkehr aus, oder erstellen Sie sie. Diese Konfiguration verwendet eine vSAN-Portgruppe mit dem Namen **vSAN** mit der markierten VLAN-ID 3262. Bearbeiten Sie die Portgruppe, und konfigurieren Sie die Gruppenbildungs- und Failover-Richtlinie, sodass sie die neue LAG-Konfiguration widerspiegelt.

Stellen Sie sicher, dass sich die LAG-Gruppe **lag1** an der Position der aktiven Uplinks befindet, und stellen Sie sicher, dass sich die verbleibenden Uplinks in der Position **Nicht verwendet** befinden.

Hinweis Wenn eine Link-Aggregationsgruppe (LAG) als einziger aktiver Uplink ausgewählt wird, überschreibt der LAG-Lastausgleichsmodus den Lastausgleichsmodus der Portgruppe. Daher spielt die folgende Richtlinie keine Rolle: **Anhand des ursprünglichen virtuellen Ports routen**.

Erstellen der VMkernel-Schnittstellen

Der letzte Schritt besteht darin, die VMkernel-Schnittstellen für die Verwendung der neuen verteilten Portgruppe zu erstellen, um sicherzustellen, dass sie für vSAN-Datenverkehr gekennzeichnet sind. Beachten Sie, dass jede vSAN vmknic über vmnic0 und vmnic1 in einer LAG-Gruppe kommunizieren kann, um Lastausgleich und Failover bereitzustellen.



Konfigurieren des Lastausgleichs

Aus der Perspektive des Lastausgleichs besteht kein konsistentes Gleichgewicht des Datenverkehrs an allen Hosts auf allen vmnics in dieser LAG-Einrichtung, aber die Konsistenz ist im Vergleich zur Option **Anhand der physischen Netzwerkkartenauslastung routen**, die in der Konfiguration 1 verwendet wird, und der Air-Gap-Methode/Methode mit mehreren vmknics, die in Konfiguration 2 verwendet wird, höher.

Das vSphere-Leistungsdiagramm der einzelnen Hosts zeigt einen verbesserten Lastausgleich.

Netzwerk-Uplink-Redundanz verloren

Wenn vmnic1 auf einem bestimmten vSAN-Host nicht aktiviert ist, wird ein Netzwerkredundanz Alarm ausgelöst.

Es werden keine vSAN-Systemzustandsalarme ausgelöst, und die Auswirkungen auf Gast-E/A sind im Vergleich zur Air-Gap-Konfiguration mit mehreren vmknics minimal. Bei dieser Konfiguration müssen keine TCP-Sitzungen mit konfiguriertem LACP angehalten werden.

Wiederherstellung und Failback

In einem Failback-Szenario unterscheidet sich das Verhalten zwischen lastbasierter Gruppenbildung, mehreren vmknics und LACP in einer vSAN-Umgebung. Nach der Wiederherstellung von vmnic1 wird der Datenverkehr automatisch über beide aktiven Uplinks ausgeglichen. Dieses Verhalten kann für vSAN-Datenverkehr vorteilhaft sein.

Failback auf „Ja“ oder „Nein“ festgelegt?

Eine Richtlinie für den LAG-Lastausgleichsdienst überschreibt die Gruppierungs- und Failover-Richtlinie für verteilte vSphere-Portgruppen. Beachten Sie auch die Anleitung zum Failback-Wert. Labortests zeigen keine erkennbaren Verhaltensunterschiede zwischen der Failbackfestlegung auf **ja** oder **nein** mit LACP. Die LAG-Einstellungen haben Vorrang vor den Portgruppeneinstellungen.

Hinweis Die Werte für die Netzwerkfehlererkennung bleiben auf **Nur Verbindungsstatus** festgelegt, da die Signalprüfung für LACP nicht unterstützt wird. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel Grundlegendes zum IP-Hash-Lastausgleich (2006129).

Konfiguration 4: statische LACP – Anhand des IP-Hashs routen

Sie können einen statischen LACP-Portkanal mit zwei Ports auf einem Switch und zwei aktive Uplinks auf einem vSphere Standard-Switch verwenden.

Verwenden Sie in dieser Konfiguration ein 10-GB-Netzwerk mit zwei physischen Uplinks pro Server. Auf jedem Host ist eine einzelne VMkernel-Schnittstelle (vmknic) für vSAN vorhanden.

Weitere Informationen zu den Hostanforderungen sowie Konfigurationsbeispiele finden Sie in den folgenden VMware-Knowledgebase-Artikeln:

- Hostanforderungen für die Linkaggregation für ESXi und ESX (1001938)
- Beispielkonfiguration von EtherChannel/Link-Aggregationssteuerungsprotokoll (LACP) mit ESXi/ESX und Cisco/HP-Switches (Knowledgebase-Artikel 1004048)

Hinweis vSAN über RDMA unterstützt diese Konfiguration nicht.

Konfigurieren des physischen Switches

Konfigurieren Sie einen statischen Portkanal mit zwei Uplinks wie folgt:

- Switch-Ports 43 und 44
- VLAN-Trunking, sodass sich der Portkanal im VLAN-Trunk-Modus befindet (mit den entsprechenden Trunked-VLANs).
- Geben Sie die Lastausgleichsrichtlinie für die Portkanalgruppe nicht an.

Diese Schritte können verwendet werden, um einen einzelnen Portkanal auf dem Switch zu konfigurieren:

Schritt 1: Erstellen eines Portkanals.

```
#interface port-channel 13
```

Schritt 2: Festlegen des Portkanals auf VLAN-Trunk-Modus.

```
#switchport mode trunk
```

Schritt 3: Zulassen geeigneter VLANs.

```
#switchport trunk allowed vlan 3266
```

Schritt 4: Zuweisen der korrekten Ports zum Portkanal und Festlegen des aktiven Modus.

```
#interface range Te1/0/43, Te1/0/44

#channel-group 1 mode on
```

Schritt 5: Sicherstellen, dass der Portkanal als statischer Portkanal konfiguriert ist.

```
#show interfaces port-channel 13


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ---------------------------- -------- --------- --------- --

Po13 Active: Te1/0/43, Te1/0/44 Static 7 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
```

Konfigurieren des vSphere Standard-Switches

In diesem Beispiel wird davon ausgegangen, dass Sie die Konfiguration und Erstellung von vSphere Standard-Switches verstehen.

In diesem Beispiel wird die folgende Konfiguration verwendet:

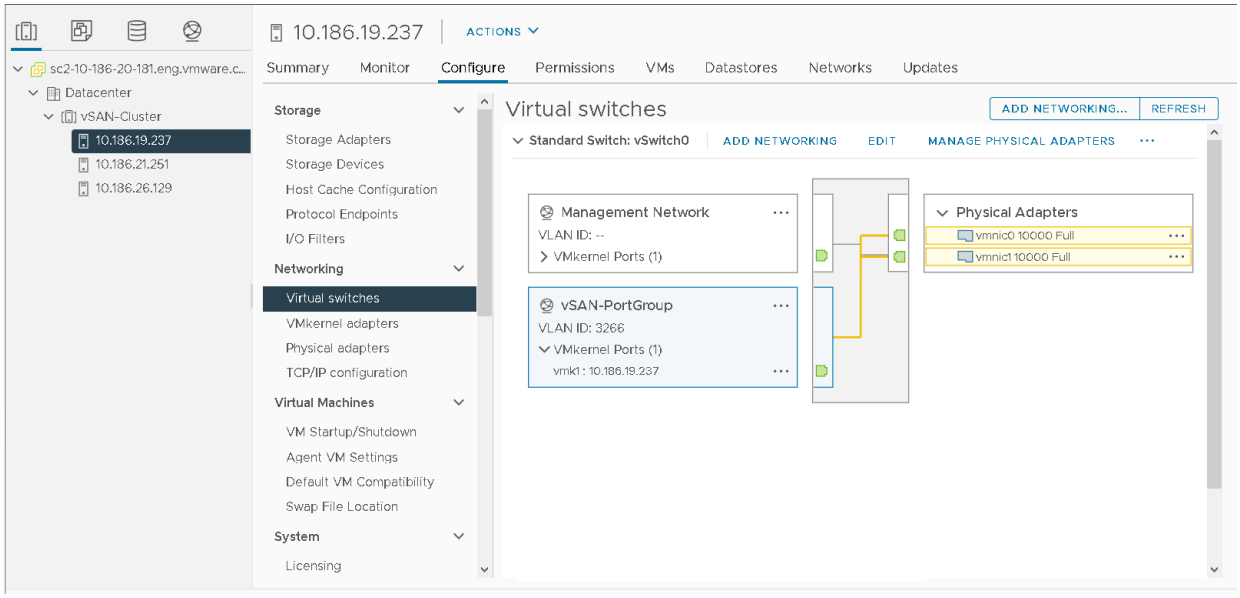
- Identische vSAN-Hosts
- Uplinks mit den Namen vmnic0 und vmnic1
- Trunked-VLAN 3266 zu den Switch-Ports und zum Portkanal
- Jumbo-Frames

Erstellen Sie auf jedem Host einen **vSwitch1**, wobei der MTU-Wert auf 9000 festgelegt ist und dem vSwitch vmnic0 und vmnic1 hinzugefügt wurde. Legen Sie in der Gruppierungs- und Failover-Richtlinie beide Adapter auf die Position **Aktiv** fest. Legen Sie die Lastausgleichsrichtlinie auf **Anhand des IP-Hashs routen** fest.

Konfigurieren Sie Gruppierung und Failover für die verteilte Portgruppe für vSAN-Datenverkehr wie folgt:

- Die Lastausgleichsrichtlinie wird auf **Anhand des IP-Hashs routen** festgelegt.
- Die Netzwerkfehlererkennung wird auf **Nur Verbindungsstatus** festgelegt.
- „Switches benachrichtigen“ wird auf **Ja** festgelegt.
- Failback wird auf **Ja** festgelegt.
- Stellen Sie sicher, dass sich beide Uplinks in der Position **Aktive Uplinks** befinden.

Verwenden Sie Standardeinstellungen für die Netzwerkerkennung, für „Switches benachrichtigen“ und für das Failback. Alle Portgruppen erben die Gruppierungs- und Failover-Richtlinie, die auf vSwitch-Ebene festgelegt wurde. Sie können die einzelnen Gruppierungs- und Failover-Richtlinien für Portgruppen überschreiben, sodass sie sich vom übergeordneten vSwitch unterscheiden. Stellen Sie jedoch sicher, dass Sie denselben Satz mit Uplinks für den IP-Hash-Lastausgleich für alle Portgruppen verwenden.



Konfigurieren des Lastausgleichs

Obwohl beide physischen Uplinks verwendet werden, gibt es kein konsistentes Gleichgewicht des Datenverkehrs über alle physischen vmnics hinweg. Die Abbildung zeigt, dass nur aktiver Datenverkehr vSAN-Datenverkehr ist. Dies waren im Wesentlichen vier vmknics-oder IP-Adressen. Das Verhalten kann durch die geringe Anzahl IP-Adressen und mögliche Hashes verursacht werden. In einigen Situationen kann der virtuelle Switch den Datenverkehr jedoch über einen Uplink in der Gruppe konsistent weiterleiten. Weitere Einzelheiten zum IP-Hash-Algorithmus finden Sie in der offiziellen vSphere-Dokumentation zum Thema *Anhand des IP-Hashs routen*.

Netzwerkredundanz

In diesem Beispiel ist vmnic1 mit einem Port verbunden, der vom Switch deaktiviert wurde, um sich auf das Fehler- und Redundanzverhalten zu konzentrieren. Beachten Sie, dass ein Netzwerk-Uplink-Redundanzalarm ausgelöst wurde.

Es wurden keine vSAN-Systemzustandsalarme ausgelöst. Cluster- und VM-Komponenten sind nicht betroffen, und die Speicher-E/A für den Gast wird durch diesen Fehler nicht unterbrochen.

Wiederherstellung und Failback

Nach der Wiederherstellung von vmnic1 wird der Datenverkehr automatisch über beide aktiven Uplinks ausgeglichen.

Network I/O Control

10

Verwenden Sie vSphere Network I/O Control, um QoS-Ebenen (Dienstqualität) für den Netzwerkdatenverkehr festzulegen.

vSphere Network I/O Control ist eine für vSphere Distributed Switches verfügbare Funktion. Verwenden Sie sie für die QoS-Implementierung (Dienstqualität) für den Netzwerkdatenverkehr. Dies kann für vSAN hilfreich sein, wenn der vSAN-Datenverkehr die physische Netzwerkkarte mit anderen Datenverkehrstypen wie vMotion, Management und virtuellen Maschinen gemeinsam nutzen muss.

Reservierungen, Anteile und Grenzwerte

Sie können eine **Reservierung** festlegen, damit Network I/O Control auf dem physischen Adapter für vSAN die Mindestbandbreite gewährleistet.

Reservierungen können nützlich sein, wenn sich *diskontinuierlicher* Datenverkehr wie vMotion oder die vollständige Host-Evakuierung sich auf vSAN-Datenverkehr auswirken kann. Reservierungen werden nur dann aufgerufen, wenn es Konflikte für die Netzwerkbandbreite gibt. Ein Nachteil bei Reservierungen in Network I/O Control besteht darin, dass die nicht verwendete Reservierungsbandbreite nicht dem Datenverkehr der virtuellen Maschine zugeteilt werden kann. Die Gesamtbandbreite, die für alle Systemdatenverkehrstypen reserviert wird, darf 75 Prozent der Bandbreite des physischen Netzwerkadapters mit der geringsten Kapazität nicht überschreiten.

vSAN Best Practices für Reservierungen. Der für vSAN reservierte Datenverkehr kann nicht dem Datenverkehr der virtuellen Maschine zugeteilt werden kann. Vermeiden Sie daher NIOC-Reservierungen in vSAN-Umgebungen.

Wenn Sie **Anteile** festlegen, ist eine bestimmte Bandbreite für vSAN verfügbar, wenn der für vSAN zugewiesene physische Adapter gesättigt ist. Dadurch wird verhindert, dass vSAN während der Neuerstellungs- und Synchronisierungsvorgänge die gesamte Kapazität des physischen Adapters verbraucht. Beispielsweise könnte der physische Adapter gesättigt sein, wenn ein anderer physischer Adapter in der Gruppe fehlschlägt und der gesamte Datenverkehr in der Portgruppe an die anderen Adapter in der Gruppe übertragen wird. Die Option **Anteile** stellt sicher, dass kein anderer Datenverkehr das vSAN-Netzwerk beeinträchtigt.

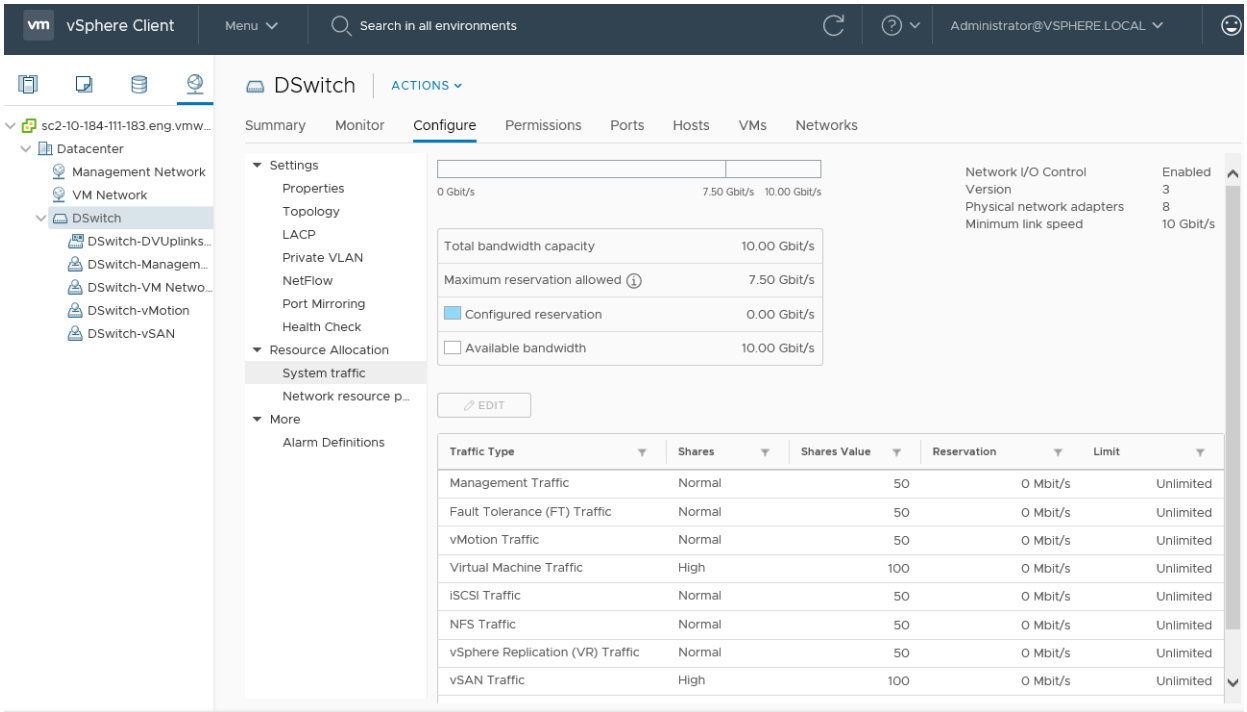
vSAN-Empfehlung für Anteile . Dies ist die fairste Technik der Bandbreitenzuteilung in NIOC und wird für den Einsatz in vSAN-Umgebungen bevorzugt.

Durch das Festlegen von **Grenzwerten** wird die maximale Bandbreite definiert, die ein bestimmter Datenverkehrstyp auf einem Adapter verbrauchen kann. Wenn niemand sonst zusätzliche Bandbreite verwendet, kann der Datenverkehrstyp mit dem Grenzwert sie auch nicht verbrauchen.

vSAN-Empfehlung zu Grenzwerten. Da Datenverkehrstypen mit Grenzwerten keine zusätzliche Bandbreite verbrauchen können, vermeiden Sie die Verwendung von NIOC-Grenzwerten in vSAN-Umgebungen.

Netzwerkressourcenpools

Sie können alle Systemdatenverkehrstypen anzeigen, die mit Network I/O Control gesteuert werden können. Wenn Sie über mehrere Netzwerke virtueller Maschinen verfügen, können Sie dem Datenverkehr der virtuellen Maschine eine bestimmte Bandbreite zuweisen. Verwenden Sie Netzwerkressourcenpools, um Teile dieser Bandbreite basierend auf der Portgruppe der virtuellen Maschine zu verbrauchen.



Aktivieren von Network I/O Control

Sie können Network I/O Control in den Konfigurationseigenschaften des vDS aktivieren. Klicken Sie mit der rechten Maustaste auf den vDS im vSphere Client, und wählen Sie das Menü **Einstellungen > Einstellungen bearbeiten** aus.

Hinweis Network I/O Control ist nur für vSphere Distributed Switches und nicht für Standard-vSwitches verfügbar.

Sie können Network I/O Control verwenden, um Bandbreite für den Netzwerkdatenverkehr basierend auf der Kapazität der physischen Adapter auf einem Host zu reservieren. Wenn z. B. vSAN-Datenverkehr physische Netzwerkadapter mit 10 GbE verwendet und diese Adapter mit anderen Systemdatenverkehrstypen gemeinsam genutzt werden, können Sie vSphere Network I/O Control verwenden, um eine bestimmte Bandbreiten Bandbreite für vSAN zu gewährleisten. Dies kann nützlich sein, wenn Datenverkehr wie vSphere vMotion, vSphere HA und der Datenverkehr der virtuellen Maschine dieselbe physische Netzwerkkarte wie das vSAN-Netzwerk nutzen.

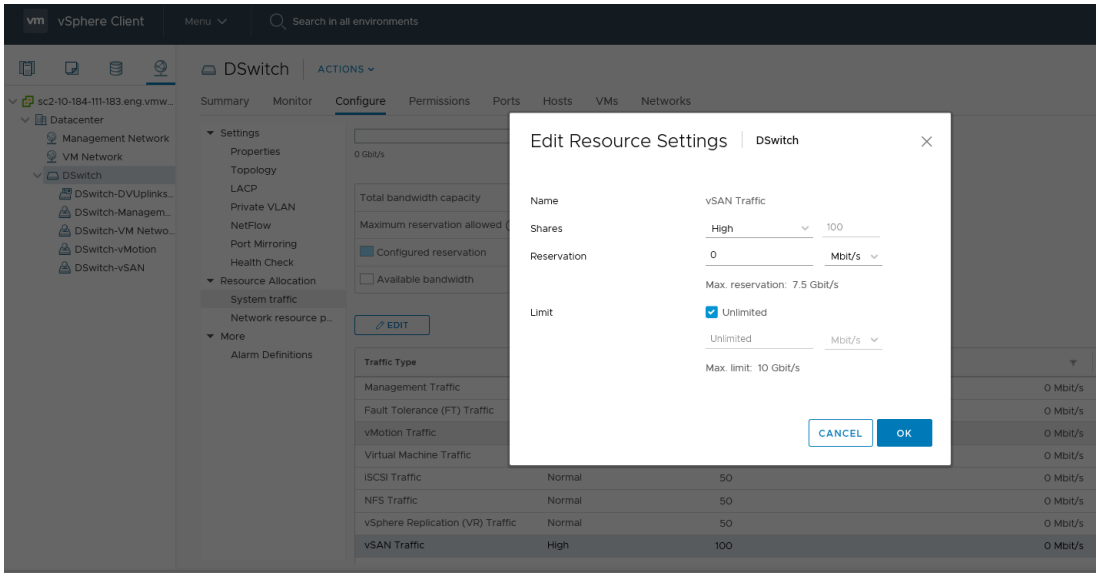
Lesen Sie als Nächstes die folgenden Themen:

- Beispiel für die Network I/O Control-Konfiguration

Beispiel für die Network I/O Control-Konfiguration

Sie können Network I/O Control für einen vSAN-Cluster konfigurieren.

Berücksichtigen Sie einen vSAN-Cluster mit einem einzelnen physischen Adapter mit 10 GbE. Diese Netzwerkkarte verarbeitet Datenverkehr für vSAN, vSphere vMotion und virtuelle Maschinen. Um den Anteilwert für einen Datenverkehrstyp zu ändern, wählen Sie diesen Datenverkehrstyp in der Ansicht „Systemdatenverkehr“ (**VDS > Konfigurieren > Ressourcenzuteilung > Systemdatenverkehr**) aus, und klicken Sie auf **Bearbeiten**. Der Anteilwert für vSAN-Datenverkehr wurde von der Standardeinstellung „Normal/50“ in „Hoch/100“ geändert.



Bearbeiten Sie die anderen Datenverkehrstypen, sodass Sie mit den in der Tabelle angezeigten Anteilwerten übereinstimmen.

Tabelle 10-1. Beispiel für NIOC-Einstellungen

Art des Datenverkehrs	Anteile	Wert
vSAN	Hoch	100

Tabelle 10-1. Beispiel für NIOC-Einstellungen (Fortsetzung)

vSphere vMotion	Niedrig	25
Virtuelle Maschine	Normal	50
iSCSI/NFS	Niedrig	25

Wenn der 10-GbE-Adapter ausgelastet ist, weist Network I/O Control 5 Gbit/s zu vSAN auf dem physischen Adapter, 3,5 Gbit/s für den Datenverkehr der virtuellen Maschine und 1,5 Gbit/s für vMotion zu. Verwenden Sie diese Werte als Ausgangspunkt, um die NIOC-Konfiguration in Ihrem vSAN-Netzwerk zu konfigurieren. Stellen Sie sicher, dass vSAN die höchste Priorität eines beliebigen Protokolls hat.

Weitere Informationen zu den verschiedenen Parametern für die Bandbreitenzuteilung finden Sie in der Dokumentation zum *vSphere-Netzwerk*.

Mit jeder vSphere-Edition für vSAN stellt VMware einen vSphere Distributed Switch als Teil der Edition bereit. Network I/O Control kann mit einer beliebigen vSAN-Edition konfiguriert werden.

Grundlegendes zu vSAN-Netzwerktopologien

11

vSAN-Architektur unterstützt unterschiedliche Netzwerktopologien. Diese Topologien wirken sich auf die gesamte Bereitstellung und Verwaltung von vSAN aus.

Die Einführung der Unicast-Unterstützung in vSAN 6.6 vereinfacht das Netzwerkdesign.

Lesen Sie als Nächstes die folgenden Themen:

- Standardbereitstellungen
- vSAN Stretched Cluster-Bereitstellungen
- vSAN-Bereitstellungen mit zwei Knoten
- Konfigurieren des Netzwerks von Datensites zum Zeugenhost
- Bereitstellungen für seltene Szenarien

Standardbereitstellungen

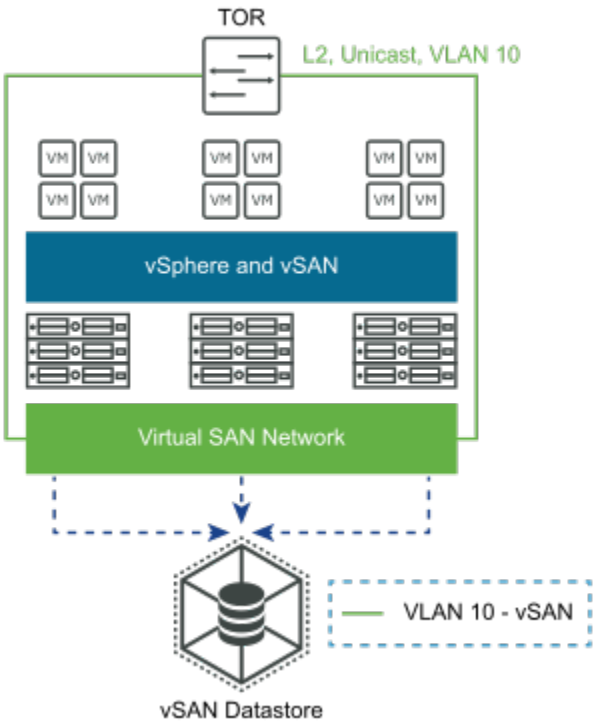
vSAN unterstützt mehrere Bereitstellungstypen für einzelne Sites.

Schicht 2, einzelne Site, einzelnes Rack

Diese Netzwerktopologie ist für die Weiterleitung von Paketen über Zwischengeräte der Schicht 2, z. B. Hosts, Brücken oder Switches, verantwortlich.

Die Schicht-2-Netzwerktopologie bietet die einfachste Implementierung und Verwaltung von vSAN. VMware empfiehlt die Verwendung und Konfiguration von IGMP-Snooping, um zu vermeiden, dass unnötiger Multicast-Datenverkehr im Netzwerk gesendet wird. In diesem ersten Beispiel untersuchen wir eine einzelne Site und möglicherweise sogar ein einzelnes Rack mit Servern, für die vSAN 6.5 oder früher verwendet wird. Diese Version verwendet Multicast, aktivieren Sie also IGMP-Snooping. Da sich alles auf derselben Schicht 2 befindet, müssen Sie das Routing für Multicast-Datenverkehr nicht konfigurieren.

Schicht-2-Implementierungen werden mit vSAN 6.6 und höher noch weiter vereinfacht, wodurch die Unicast-Unterstützung ins Spiel kommt. IGMP-Snooping ist nicht erforderlich.



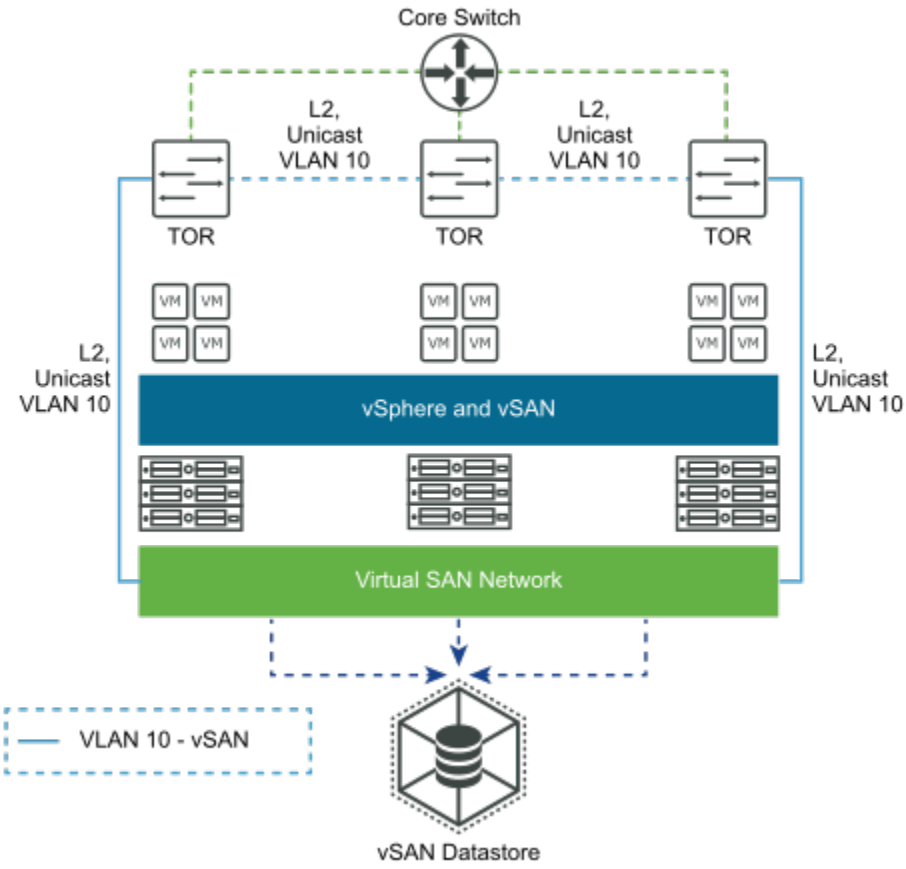
Schicht 2, einzelne Site, mehrere Racks

Diese Netzwerktopologie funktioniert mit der Schicht-2-Implementierung, bei der mehrere Racks und mehrere Top-of-Rack-Switches oder TORs vorhanden sind, die mit einem Core-Switch verbunden sind.

In den folgenden Abbildungen zeigt die blaue gepunktete Linie zwischen den TORs, dass das vSAN-Netzwerk verfügbar und für alle Hosts im vSAN-Cluster zugänglich ist. Die Hosts in den verschiedenen Racks kommunizieren jedoch über Schicht 3 miteinander, was bedeutet, dass Multicast-Datenverkehr zwischen den Hosts mit PIM geroutet werden muss. Die TORs sind nicht physisch miteinander verbunden.

VMware empfiehlt, dass alle TORs für das IGMP-Snooping konfiguriert sind, um unnötigen Multicast-Datenverkehr im Netzwerk zu verhindern. Da kein Routing des Datenverkehrs erfolgt, ist es nicht erforderlich, PIM für die Weiterleitung des Multicast-Datenverkehrs zu konfigurieren.

Diese Implementierung ist in vSAN 6.6 und höher einfacher, da der vSAN-Datenverkehr Unicast ist. Bei Unicast-Datenverkehr ist es nicht erforderlich, IGMP-Snooping auf den Switches zu konfigurieren.



Schicht 3, einzelne Site, mehrere Racks

Diese Netzwerktopologie funktioniert für vSAN-Bereitstellungen, bei denen Schicht 3 für die Weiterleitung von vSAN-Datenverkehr verwendet wird.

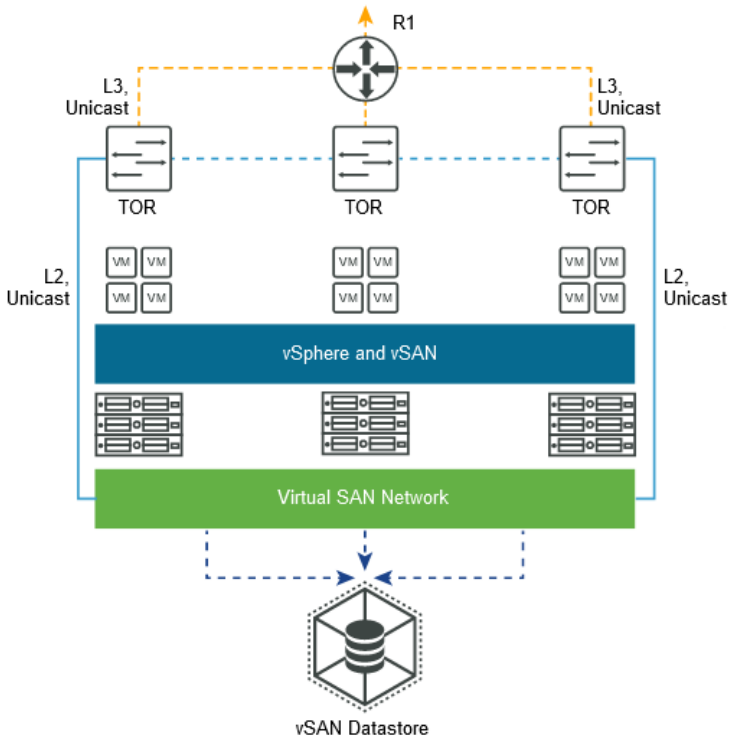
Diese einfache Schicht-3-Netzwerktopologie verwendet mehrere Racks im selben Datencenter, die jeweils über einen eigenen Tor-Switch verfügen. Leiten Sie das vSAN-Netzwerk zwischen den verschiedenen Racks über Schicht 3, damit alle Hosts im vSAN-Cluster kommunizieren können. Platzieren Sie vSAN VMkernel-Ports auf unterschiedlichen Subnetzen oder VLANs und verwenden Sie ein separates Subnetz oder VLAN für jedes Rack.

Diese Netzwerktopologie leitet Pakete über Zwischenschicht-3-fähige Geräte wie Router und Schicht-3-fähige Switches weiter. Wenn Hosts in verschiedenen Schicht-3-Netzwerksegmenten bereitgestellt werden, ist das Ergebnis eine geroutete Netzwerktopologie.

Bei vSAN 6.5 und früher empfiehlt VMware die Verwendung und Konfiguration von IGMP-Snooping, da für diese Bereitstellungen Multicast erforderlich ist. Konfigurieren Sie PIM auf den physischen Switches, um das Routing des Multicast-Datenverkehrs zu vereinfachen.

vSAN 6.6 und höher vereinfacht diese Topologie. Da kein Multicast-Datenverkehr vorhanden ist, muss das IGMP-Snooping nicht konfiguriert werden. Sie müssen PIM nicht so konfigurieren, dass Multicast-Datenverkehr weitergeleitet wird.

Im Folgenden finden Sie eine Übersicht über eine beispielhafte vSAN 6.6-Bereitstellung über Schicht 3. IGMP-Snooping oder PIM ist nicht erforderlich, da kein Multicast-Datenverkehr vorhanden ist.



vSAN Stretched Cluster-Bereitstellungen

vSAN unterstützt Stretched Cluster-Bereitstellungen, die sich über zwei Standorte erstrecken.

In vSAN 6.5 und früher ist der vSAN-Datenverkehr zwischen Daten-Sites **Multicast** für Metadaten und **Unicast** für E/A.

In vSAN 6.6 und höher ist der gesamte Datenverkehr **Unicast**. In allen Versionen von vSAN ist der Zeugen-Datenverkehr zwischen einer Daten-Site und dem Zeugenhost Unicast.

Schicht 2 – Überall

Sie können einen vSAN Stretched Cluster in einem Schicht-2-Netzwerk konfigurieren, diese Konfiguration wird jedoch nicht empfohlen.

Ziehen Sie ein Design in Erwägung, bei dem der vSAN Stretched Cluster in einem großen Schicht-2-Design konfiguriert ist. Auf Daten-Site 1 und Site 2 werden die virtuellen Maschinen bereitgestellt. Site 3 enthält den Zeugenhost.

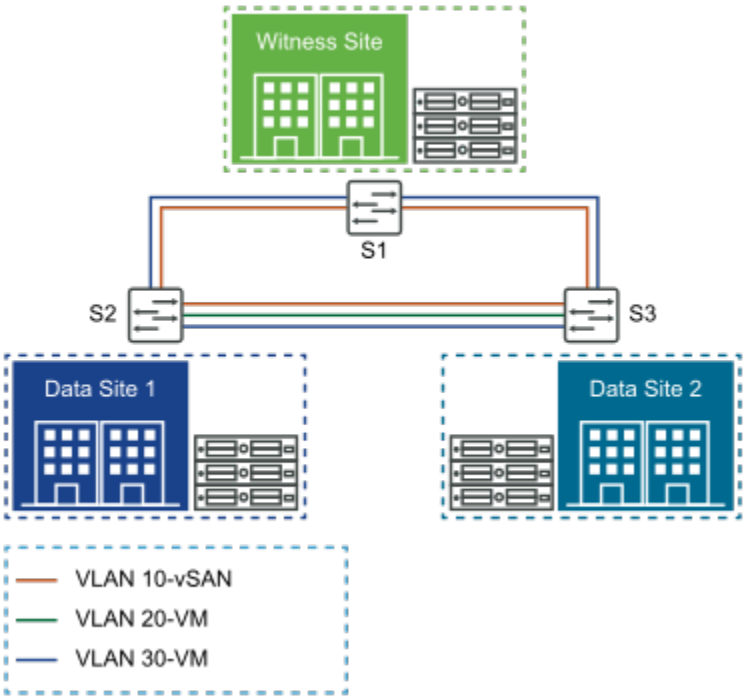
Hinweis Verwenden Sie für optimale Ergebnisse kein gestrecktes Schicht-2-Netzwerk über alle Sites hinweg.

Um Schicht 2 überall möglichst einfach zu demonstrieren, verwenden wir Switches (und keine Router) in den Topologien.

Schicht-2-Netzwerke dürfen keine Schleifen (mehrere Pfade) aufweisen, sodass Funktionen wie das Spanning Tree Protocol (STP) erforderlich sind, um eine der Verbindungen zwischen Site 1 und Site 2 zu blockieren. Ziehen Sie nun eine Situation in Betracht, in der die Verbindung zwischen Site 2 und Site 3 unterbrochen ist (die Verbindung zwischen Site 1 und Site 2). Der Netzwerkdatenverkehr kann jetzt über den Zeugenhost auf Site 3 von Site 1 auf Site 2 umgeschaltet werden. Da VMware eine wesentlich geringere Bandbreite und eine höhere Latenz für den Zeugenhost unterstützt, sehen Sie einen deutlichen Leistungsabfall, wenn der Datennetzwerk-Datenverkehr über eine Zeugen-Site mit einer niedrigeren Spezifikation verläuft.

Wenn das Wechseln des Datenverkehrs zwischen Daten-Sites über die Zeugen-Site die Latenz der Anwendungen nicht beeinträchtigt und die Bandbreite akzeptabel ist, ist eine gestreckte Schicht-2-Konfiguration zwischen den Sites möglich. In den meisten Fällen ist eine solche Konfiguration nicht möglich und die Netzwerkanforderungen werden noch komplexer.

Bei der Software vSAN 6.5 oder früher, bei der Multicast-Datenverkehr verwendet wird, müssen Sie IGMP-Snooping auf den Switches konfigurieren. Dies ist bei vSAN 6.6 und höher nicht erforderlich. PIM ist nicht erforderlich, da kein Routing des Multicast-Datenverkehrs erfolgt.



Unterstützte vSAN Stretched Cluster-Konfigurationen

vSAN unterstützt Stretched Cluster-Konfigurationen.

Die folgende Konfiguration verhindert, dass der Datenverkehr von Site 1 über den Zeugenhost an Site 2 weitergeleitet wird, falls ein Fehler auf einem der Daten-Site-Netzwerke vorliegt. Durch diese Konfiguration werden Leistungsbeeinträchtigungen vermieden. Wenn Sie sicherstellen möchten, dass der Datenverkehr nicht über den Zeugenhost gewechselt wird, verwenden Sie die folgende Netzwerktopologie.

Implementieren Sie zwischen Site 1 und Site 2 eine gestreckte Schicht-2-Konfiguration mit Switch oder eine geroutete Schicht-3-Konfiguration. Beide Konfigurationen werden unterstützt.

Implementieren Sie zwischen Site 1 und dem Zeugenhost eine geroutete Schicht-3-Konfiguration.

Implementieren Sie zwischen Site 2 und dem Zeugenhost eine geroutete Schicht-3-Konfiguration.

Die Beschreibung dieser Konfigurationen (Schicht 2 + Schicht 3 sowie Schicht 3 – überall) umfasst Aspekte für Multicast in vSAN 6.5 und früher und nur für Unicast, welches in vSAN 6.6 verfügbar ist. Durch den Multicast-Datenverkehr ergeben sich zusätzliche Konfigurationsschritte für das IGMP-Snooping und PIM für das Routing von Multicast-Datenverkehr.

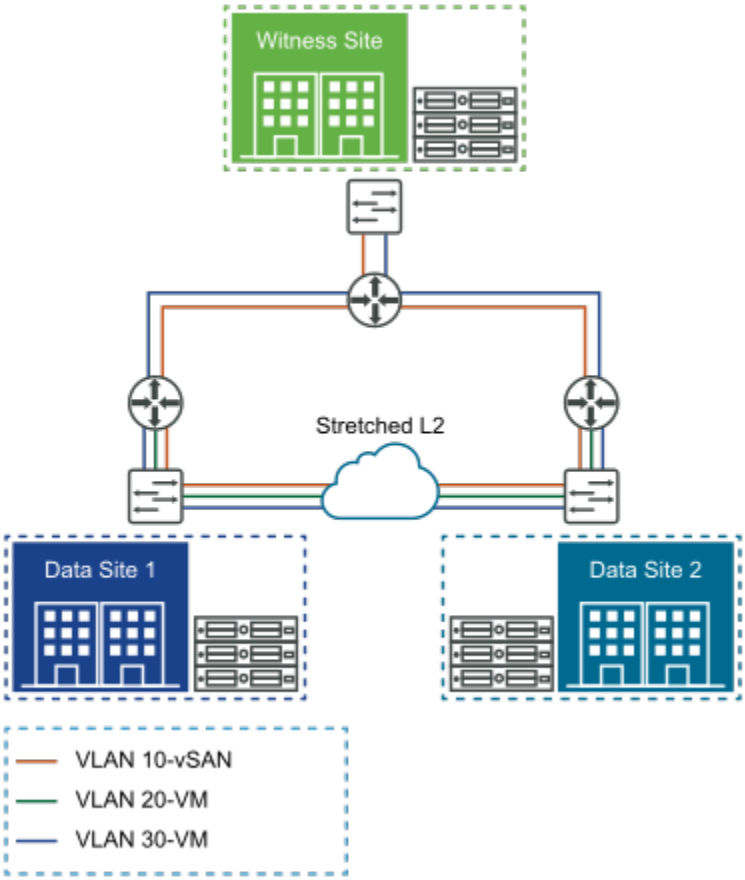
Untersuchen wir ein gestrecktes Schicht-2-Netzwerk zwischen den Daten-Sites und einem gerouteten Schicht-3-Netzwerk zur Zeugen-Site. Um eine Kombination aus Schicht 2 und Schicht 3 möglichst einfach darzustellen, verwenden Sie eine Kombination aus Switches und Routern in den Topologien.

Gestreckte Schicht 2 zwischen Daten-Sites, Schicht 3 zu Zeugenhost

vSAN unterstützt gestreckte Schicht-2-Konfigurationen zwischen Daten-Sites.

Der einzige Datenverkehr, der in diesem Fall geroutet wird, ist der Zeugen-Datenverkehr. Verwenden Sie bei vSAN 6.5 und früher, bei dem Multicast zum Einsatz kommt, IGMP-Snooping für den Multicast-Datenverkehr auf dem ausgeweiteten Schicht-2-vSAN zwischen Daten Sites. Da der Zeugen-Datenverkehr jedoch Unicast ist, muss PIM nicht auf den Schicht-3-Segmenten implementiert werden.

Bei vSAN 6.6 mit Unicast ist es nicht erforderlich, IGMP-Snooping oder PIM zu berücksichtigen.



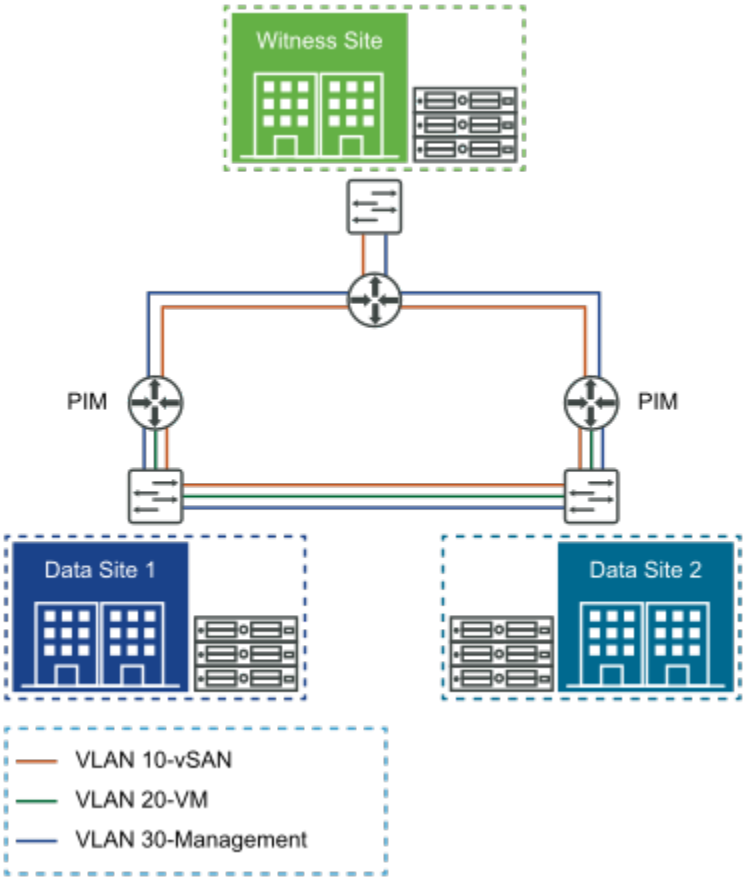
Schicht 3 – Überall

In dieser vSAN Stretched Cluster-Konfiguration wird der Datenverkehr zwischen den Daten-Sites und dem Zeugenhost geroutet.

Um Schicht 3 überall möglichst einfach zu implementieren, verwenden Sie Router oder Routing-Switches in den Topologien.

Beispiel: ziehen Sie eine Umgebung mit vSAN 6.5 oder früher in Erwägung, die Multicast-Datenverkehr verwendet. Konfigurieren Sie in diesem Fall das IGMP-Snooping auf den Daten-Site-Switches, um die Menge des Multicast-Datenverkehrs im Netzwerk zu verwalten. Dies ist auf dem Zeugenhost nicht erforderlich, da der Zeugen-Datenverkehr Unicast ist. Der Multicast-Datenverkehr wird zwischen den Daten-Sites geroutet. Konfigurieren Sie daher PIM, um Multicast-Routing zuzulassen.

Bei vSAN 6.6 und höher sind weder IGMP-Snooping noch PIM erforderlich, da der gesamte geroutete Datenverkehr Unicast ist.



Trennen des Zeugen-Datenverkehrs für vSAN Stretched Cluster

vSAN unterstützt die Trennung des Zeugen-Datenverkehrs auf einem Stretched Cluster.

In vSAN 6.5 und neueren Versionen können Sie den Zeugen-Datenverkehr vom vSAN-Datenverkehr in Konfigurationen mit zwei Knoten trennen. Dies bedeutet, dass die beiden vSAN-Hosts direkt ohne einen 10-GB-Switch verbunden werden können.

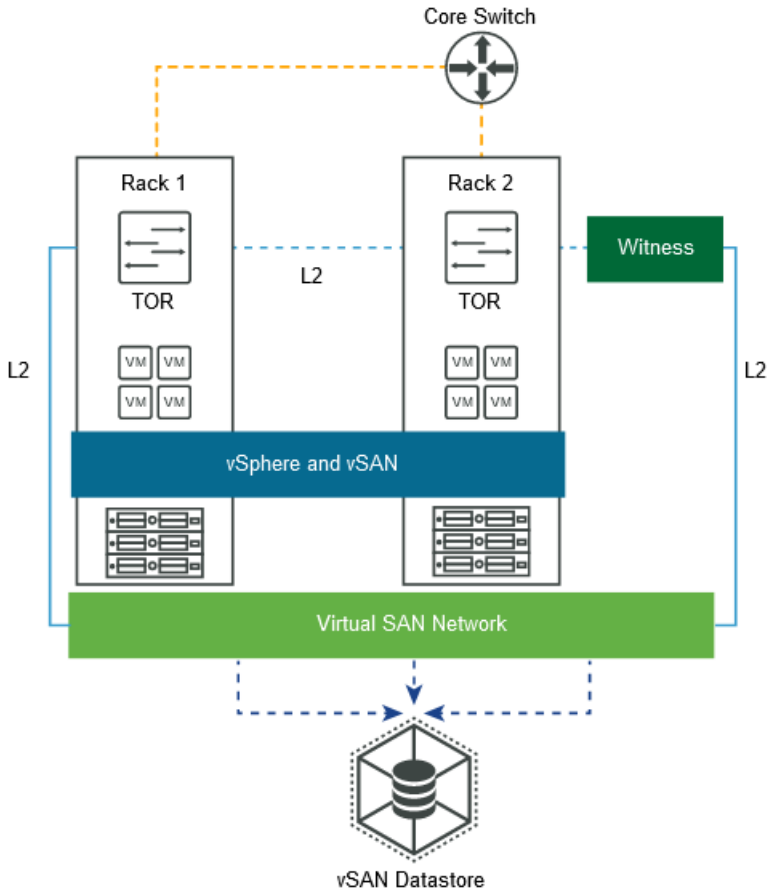
Diese Trennung des Zeugen-Datenverkehrs wird nur in Bereitstellungen mit zwei Knoten in vSAN 6.6 unterstützt. Die Trennung des Zeugen-Datenverkehrs auf einem vSAN Stretched Cluster wird in vSAN 6.7 und höher unterstützt.

Verwenden des vSAN Stretched Clusters zum Erreichen von Rack-Erkennung

Für vSAN Stretched Cluster stellt vSAN Rack-Erkennung auf einer einzelnen Site bereit.

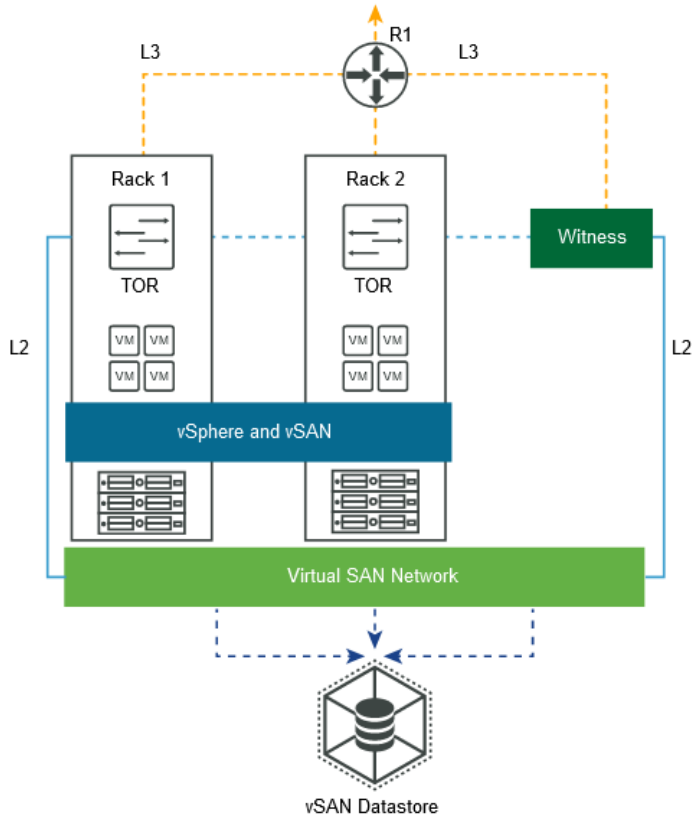
Wenn Sie über zwei Racks mit vSAN-Hosts verfügen, können Sie Ihren vSAN-Cluster nach einem vollständigen Rack-Ausfall weiterhin ausführen. In diesem Fall wird die Verfügbarkeit der VM-Arbeitslasten durch das verbleibende Rack und einen Remote-Zeugenhost bereitgestellt.

Hinweis Damit diese Konfiguration unterstützt wird, platzieren Sie den Zeugenhost nicht innerhalb der beiden Racks der vSAN-Hosts.



Wenn in diesem Beispiel Rack 1 ausfällt, erfolgt die Bereitstellung der VM-Verfügbarkeit über Rack 2 und den Zeugenhost. Bei dieser Konfiguration handelt es sich um eine Umgebung vor vSAN 6.6, für die Multicast im Netzwerk konfiguriert werden muss. Der Zeugenhost muss sich im vSAN-Netzwerk befinden. Der Zeugen-Datenverkehr ist Unicast. In vSAN 6.6 und höher ist der gesamte Datenverkehr Unicast.

Diese Topologie wird auch über Schicht 3 unterstützt. Platzieren Sie vSAN VMkernel-Ports auf unterschiedlichen Subnetzen oder VLANs und verwenden Sie ein separates Subnetz oder VLAN für jedes Rack.



Diese Topologie unterstützt Bereitstellungen mit zwei Racks, um die Rack-Erkennung (Fehlerdomänen) mit einem vSAN Stretched Cluster zu ermöglichen. Diese Lösung verwendet einen Zeugenhost, der sich außerhalb des Clusters befindet.

vSAN-Bereitstellungen mit zwei Knoten

vSAN unterstützt Bereitstellungen mit zwei Knoten. vSAN-Bereitstellungen mit zwei Knoten werden für Remote-Niederlassungen/Niederlassungen (ROBO) verwendet, die eine geringe Anzahl Arbeitslasten aufweisen, aber Hochverfügbarkeit erfordern.

vSAN-Bereitstellungen mit zwei Knoten verwenden einen dritten Zeugenhost, der sich von der Niederlassung entfernt befinden kann. Häufig wird der Zeuge in der Zweigstelle zusammen mit den Verwaltungskomponenten wie vCenter Server verwaltet.

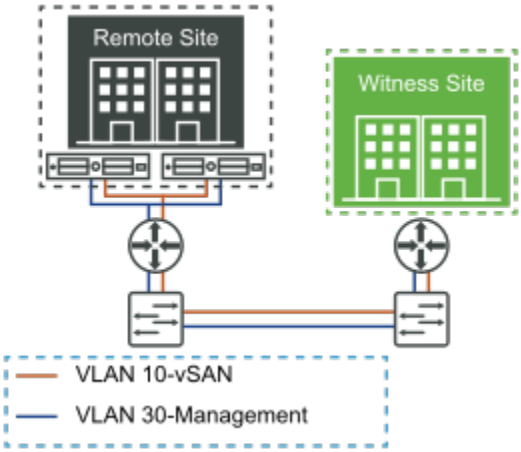
vSAN-Bereitstellungen mit zwei Knoten vor vSAN 6.5

Für vSAN-Versionen vor 6.5, die Bereitstellungen mit zwei Knoten unterstützen, ist ein physischer Switch auf der Remote-Site erforderlich.

Frühe Versionen von vSAN mit zwei Knoten ist ein physischer 10-GB-Switch auf der-Remote-Site erforderlich. Falls die einzigen Server auf dieser Remote-Site die vSAN-Hosts waren, konnte diese Lösung ineffizient sein.

Wenn bei dieser Bereitstellung keine anderen Geräte den 10-GB-Switch verwenden, muss das IGMP-Snooping nicht berücksichtigt werden. Wenn andere Geräte auf der Remote-Site den 10-GB-Switch gemeinsam nutzen, verwenden Sie das IGMP-Snooping, um übermäßigen und unnötigen Multicast-Datenverkehr zu verhindern.

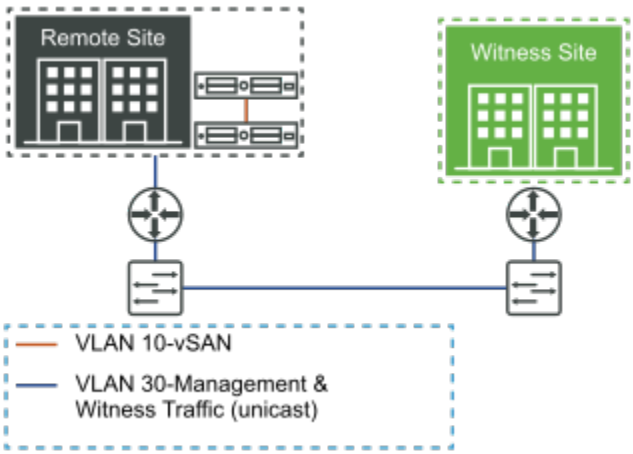
PIM ist nicht erforderlich, da es sich bei dem einzigen gerouteten Datenverkehr um Zeugen-Datenverkehr handelt, der Unicast ist.



Bereitstellungen mit zwei Knoten für vSAN 6.5 und höher

vSAN 6.5 und höher unterstützt Bereitstellungen mit zwei Knoten.

Bei der vSAN-Version 6.5 und höher ist diese vSAN-Implementierung mit zwei Knoten wesentlich einfacher. Bei vSAN 6.5 und höher können die beiden Hosts auf der Daten-Site direkt verbunden werden.

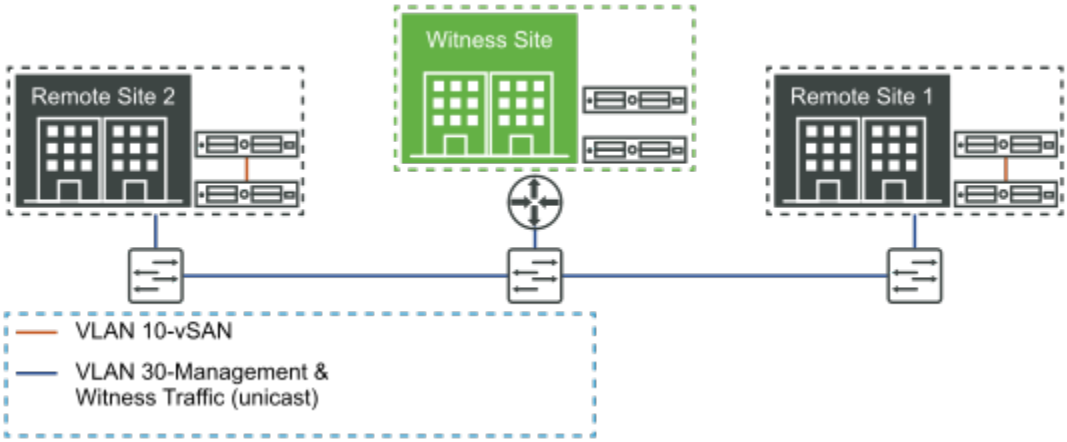


Um diese Funktionalität zu aktivieren, wird der Zeugen-Datenverkehr vollständig vom vSAN-Datenverkehr getrennt. Der vSAN-Datenverkehr kann nun zwischen den beiden Knoten der Direct Connect-Verbindung fließen, während der Zeugen-Datenverkehr über das Verwaltungsnetzwerk an die Zeugen-Site weitergeleitet werden kann.

Die Zeugen-Appliance kann sich außerhalb der Niederlassung befinden. Beispielsweise kann der Zeuge im Hauptdatencenter neben der Verwaltungsinfrastruktur (vCenter Server, vROps, Log Insight usw.) wieder aktiv werden. Eine weitere unterstützte Stelle, an der sich der Zeuge entfernt von der Niederlassung befinden kann, ist in vCloud Air.

In dieser Konfiguration existiert kein Switch auf der Remote-Site. Daher ist es nicht erforderlich, die Unterstützung für Multicast-Datenverkehr auf dem vSAN-Back-to-Back-Netzwerk zu konfigurieren. Sie müssen Multicast im Verwaltungsnetzwerk nicht berücksichtigen, da der Zeugen-Datenverkehr Unicast ist.

vSAN 6.6 und höher verwendet ausschließlich Unicast, sodass es keine Überlegungen zu Multicast gibt. Es werden auch Bereitstellungen mit zwei Knoten in mehreren Remote-Büros/ Zweigstellen unterstützt, solange jeder Knoten über einen eigenen eindeutigen Zeugen verfügt.



Allgemeine Überlegungen für vSAN-Bereitstellungen mit zwei Knoten

vSAN-Bereitstellungen mit zwei Knoten unterstützen weitere Topologien. In diesem Abschnitt werden gängige Konfigurationen beschrieben.

Weitere Informationen zu Konfigurationen mit zwei Knoten und detaillierten Bereitstellungsaspekten außerhalb des Netzwerks finden Sie in der offiziellen vSAN-Dokumentation.

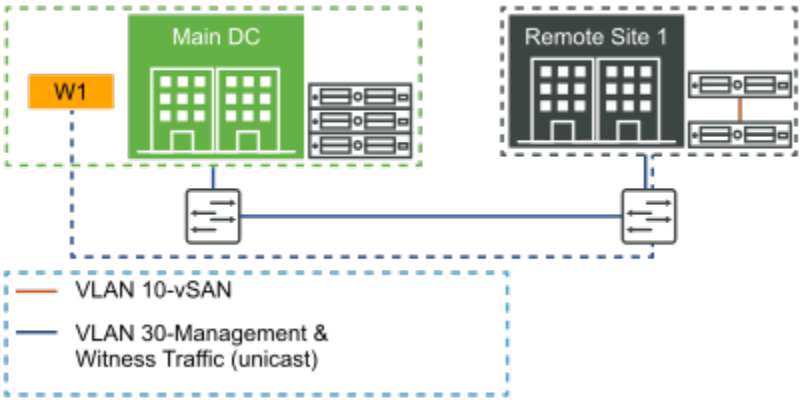
Ausführen des Zeugen auf einem anderen vSAN-Cluster mit zwei Knoten

vSAN unterstützt die Ausführung des Zeugen auf einem anderen Cluster mit zwei Knoten nicht.

Zeuge mit Ausführung in einer anderen vSAN-Standardbereitstellung

vSAN unterstützt Zeugen, die in einer anderen vSAN-Standardbereitstellung ausgeführt werden.

Diese Konfiguration wird unterstützt. Ein Fehler auf dem vSAN mit zwei Knoten auf der Remote-Site hat keine Auswirkungen auf die Verfügbarkeit der vSAN-Standardumgebung im Hauptdatencenter.



Konfigurieren des Netzwerks von Datensites zum Zeugenhost

Die Hostschnittstellen in den Datensites kommunizieren mit dem Zeugenhost über das vSAN-Netzwerk. Es stehen verschiedene Konfigurationsoptionen zur Verfügung.

In diesem Thema wird die Implementierung dieser Konfigurationen behandelt. Es wird beschrieben, wie die Schnittstellen auf den Hosts in den untereinander über das vSAN-Netzwerk kommunizierenden Datensites mit dem Zeugenhost kommunizieren.

Option 1: Physischer ESXi-Zeuge, der über L3 mit statischen Routen verbunden ist

Die Datensites können über ein gestrecktes L2-Netzwerk verbunden werden. Verwenden Sie dieses auch für das Verwaltungsnetzwerk der Datensites, das vSAN-Netzwerk, das vMotion-Netzwerk und das Netzwerk virtueller Maschinen.

Der physische Netzwerkrouter in dieser Netzwerkinfrastruktur überträgt nicht automatisch den Datenverkehr von den Hosts in den Datensites (Site 1 und Site 2) an den Host auf der Zeugen-Site (Site 3). Damit der vSAN-Stretched Cluster erfolgreich konfiguriert werden kann, müssen alle Hosts im Cluster kommunizieren. In dieser Umgebung kann ein vSAN Stretched Cluster bereitgestellt werden.

Die Lösung besteht darin, auf den ESXi-Hosts konfigurierte *statische Routen* zu verwenden, sodass der vSAN-Datenverkehr von Site 1 und Site 2 den Zeugenhost in Site 3 erreichen kann. Fügen Sie im Falle der ESXi-Hosts auf den Datensites eine statische Route zur vSAN-Oberfläche hinzu, die den Datenverkehr an den Zeugenhost auf Site 3 über ein bestimmtes Gateway für dieses Netzwerk umleitet. Im Falle des Zeugenhosts muss auf der vSAN-Oberfläche eine statische

Route hinzugefügt werden, die vSAN-Datenverkehr für die Hosts in den Datensites umleitet. Verwenden Sie den folgenden Befehl, um auf jedem ESXi Host im vSAN Stretched Cluster eine statische Route hinzuzufügen: **`esxcli network ip route ipv4 add -g`** *<gateway>* **`-n`** *<network>*

Hinweis Der vCenter Server muss die ESXi-Hosts sowohl auf den Datensites als auch auf der Zeugensite verwalten können. Solange die direkte Konnektivität zwischen dem Zeugenhost und dem vCenter Server besteht, gibt es keine weiteren Bedenken bezüglich des Verwaltungsnetzwerks.

Es ist nicht notwendig, ein vMotion-Netzwerk oder ein VM-Netzwerk zu konfigurieren oder statische Routen für diese Netzwerke im Zusammenhang mit einem vSAN-Stretched Cluster hinzuzufügen. Virtuelle Maschinen werden nie auf den vSAN-Zeugenhost migriert oder dort bereitgestellt. Er muss nur Zeugenobjekte enthalten und benötigt keines dieser Netzwerke für diese Aufgabe.

Option 2: Virtuelle ESXi-Zeugen-Appliance, die über L3 mit statischen Routen verbunden ist

Da es sich bei dem Zeugenhost um eine virtuelle Maschine handelt, die auf einem physischen ESXi-Host bereitgestellt wird, der nicht Teil des vSAN-Clusters ist, muss der physische ESXi-Host über mindestens ein vorkonfiguriertes VM-Netzwerk verfügen. Dieses VM-Netzwerk muss sowohl das Verwaltungsnetzwerk als auch das vSAN-Netzwerk, das von den ESXi-Hosts auf den Datensites gemeinsam genutzt wird, erreichen.

Hinweis Der Zeugenhost muss kein dedizierter Host sein. Er kann für viele andere VM-Arbeitslasten verwendet werden, während er gleichzeitig den Zeugen hostet.

Eine alternative Option besteht darin, zwei vorkonfigurierte VM-Netzwerke auf dem zugrunde liegenden physischen ESXi-Host zu haben: eines für das Verwaltungsnetzwerk und eines für das vSAN-Netzwerk. Wenn der virtuelle ESXi-Zeuge auf diesem physischen ESXi-Host bereitgestellt wird, muss das Netzwerk entsprechend angehängt und konfiguriert werden.

Nachdem Sie den virtuellen ESXi-Zeugenhost bereitgestellt haben, konfigurieren Sie die statische Route. Gehen Sie davon aus, dass die Datensites über ein ausgeweitetes L2-Netzwerk verbunden sind. Verwenden Sie dieses auch für das Verwaltungsnetzwerk der Datensites, das vSAN-Netzwerk, das vMotion-Netzwerk und das Netzwerk virtueller Maschinen. Der vSAN-Datenverkehr wird von den Hosts in den Datensites (Site 1 und Site 2) nicht zum Host auf der Zeugensite (Site 3) über das Standard-Gateway weitergeleitet. Um den vSAN-Stretched Cluster erfolgreich zu konfigurieren, benötigen alle Hosts im Cluster statische Routen, damit der vSAN-Datenverkehr von Site 1 und Site 2 den Zeugenhost 3 erreichen kann. Verwenden Sie den Befehl **`esxcli network ip route`**, um eine statische Route auf jedem ESXi-Host hinzuzufügen.

Bereitstellungen für seltene Szenarien

vSAN kann in ungewöhnlichen oder seltenen Konfigurationen bereitgestellt werden.

Diese ungewöhnlichen Topologien erfordern besondere Überlegungen.

Drei Speicherorte, kein vSAN Stretched Cluster, verteilte Zeugenhosts

Sie können vSAN für mehrere Räume, Gebäude oder Sites bereitstellen, anstatt eine Stretched Cluster-Konfiguration vorzunehmen.

Diese Konfiguration wird unterstützt. Die einzige Anforderung besteht darin, dass die Latenz zwischen den Sites auf derselben Ebene wie die erwartete Latenz für eine normale vSAN-Bereitstellung im selben Datencenter sein muss. Die Latenz zwischen allen Hosts muss **< 1 ms** sein. Wenn die Latenz größer als dieser Wert ist, sollten Sie einen vSAN Stretched Cluster in Betracht ziehen, der eine Latenz von 5 ms toleriert. Mit vSAN 6.5 oder früher müssen zusätzliche Überlegungen für Multicast angestellt werden.

Behalte Sie für optimale Ergebnisse eine einheitliche Konfiguration für alle Sites in einer solchen Topologie bei. Konfigurieren Sie zur Aufrechterhaltung der VM-Verfügbarkeit Fehlerdomänen, wobei die Hosts in den einzelnen Räumen, Gebäuden oder Sites in derselben Fehlerdomäne platziert werden. Vermeiden Sie asymmetrische Partitionierungen des Clusters, in denen Host A nicht mit Host B, Host B jedoch mit Host A kommunizieren kann.

Bereitstellung mit zwei Knoten als Stretched Cluster vom Typ 1+1+N

Sie können eine Konfiguration mit zwei Knoten als vSAN Stretched Cluster-Konfiguration bereitstellen, indem Sie die einzelnen Hosts in verschiedenen Räumen, Gebäuden oder an verschiedenen Sites platzieren.

Der Versuch, die Anzahl Hosts an den einzelnen Sites zu erhöhen, schlägt mit einem Fehler im Zusammenhang mit der Lizenzierung fehl. Für Cluster, die mehr als zwei Hosts umfassen und für die die dedizierte Zeugen-Appliance/-Host-Funktion (N+N+Zeuge, wobei N > 1) verwendet wird, gilt die Konfiguration als vSAN Stretched Cluster.

Fehlerbehebung für das vSAN-Netzwerk

12

vSAN ermöglicht Ihnen das Untersuchen und Beheben von unterschiedlichen Arten von Problemen, die aus einem falsch konfigurierten vSAN-Netzwerk resultieren.

vSAN-Vorgänge hängen von der Netzwerkkonfiguration, der Zuverlässigkeit und der Leistung ab. Viele Support-Anfragen stammen aus einer falschen Netzwerkkonfiguration oder resultieren aus einem nicht erwartungsgemäß funktionierenden Netzwerk.

Verwenden Sie den vSAN-Integritätsdienst zur Behebung von Netzwerkproblemen. Netzwerkintegritätsprüfungen können Sie in Abhängigkeit von den Ergebnissen der Integritätsprüfung an einen entsprechenden Knowledgebase-Artikel verweisen. Der Knowledgebase-Artikel enthält Anweisungen zur Lösung des Netzwerkproblems.

Netzwerkintegritätsprüfungen

Der Integritätsdienst enthält eine Kategorie für Netzwerkintegritätsprüfungen.

Jede Integritätsprüfung verfügt über den Link **AskVMware**. Wenn eine Integritätsprüfung fehlschlägt, klicken Sie auf **AskVMware**, und lesen Sie den zugehörigen VMware-Knowledgebase-Artikel, um weitere Einzelheiten und Anleitungen zur Behebung des Problems zu erhalten.

Die folgenden Netzwerkintegritätsprüfungen bieten nützliche Informationen zu ihrer vSAN-Umgebung.

- vSAN**: Basis-(Unicast)-Konnektivitätsprüfung**. Diese Prüfung überprüft, ob die IP-Konnektivität für alle ESXi-Hosts im vSAN-Cluster vorhanden ist, indem ein Ping-Vorgang für die einzelnen ESXi-Hosts im vSAN-Netzwerk von jedem anderen ESXi-Host durchgeführt wird.
- **vMotion: vMotion: Basis-(Unicast)-Konnektivitätsprüfung.** Diese Prüfung überprüft, ob die IP-Konnektivität zwischen allen ESXi-Hosts im vSAN-Cluster vorhanden ist, für die vMotion konfiguriert ist. Jeder ESXi-Host im vMotion-Netzwerk führt für alle anderen ESXi-Hosts einen Ping-Vorgang aus.
- **Für alle Hosts ist vSAN-vmknic konfiguriert**. Diese Prüfung stellt sicher, dass jeder ESXi-Host im vSAN-Cluster über eine VMkernel-Netzwerkkarte verfügt, die für vSAN-Datenverkehr konfiguriert ist.
- Alle Hosts weisen dieselben Multicast-Einstellungen auf. Durch diese Überprüfung wird sichergestellt, dass alle Hosts über eine ordnungsgemäß konfigurierte Multicast-Adresse verfügen.

- **Alle Hosts nutzen dieselben Subnetze**. Mit dieser Prüfung wird überprüft, ob alle ESXi-Hosts in einem vSAN-Cluster so konfiguriert wurden, dass sich alle vSAN VMkernel-Netzwerkkarten im selben IP-Subnetz befinden.
- **Von VC getrennte Hosts**. Mit dieser Prüfung wird sichergestellt, dass vCenter Server über eine aktive Verbindung zu allen ESXi-Hosts im vSAN-Cluster verfügt.
- **Hosts mit Konnektivitätsproblemen**. Diese Prüfung bezieht sich auf Situationen, in denen vCenter Server den Host zwar als verbunden auflistet, API-Aufrufe von vCenter zum Host jedoch fehlschlagen. Sie kann Konnektivitätsprobleme zwischen einem Host und vCenter Server hervorheben.
- **Netzwerklatenz**. Diese Prüfung führt eine Netzwerklatenzprüfung für vSAN-Hosts durch. Wenn der Schwellenwert 5 ms überschreitet, wird eine Warnung angezeigt.
- **vMotion: MTU-Prüfung (Ping mit großem Paket)**. Diese Prüfung ergänzt die einfache vMotion-Ping-Konnektivitätsprüfung. Die maximale Übertragungseinheitsgröße wird erhöht, um die Netzwerkleistung zu verbessern. Falsch konfigurierte MTUs werden möglicherweise nicht als Netzwerkkonfigurationsproblem angezeigt, sie können jedoch Leistungsprobleme verursachen.
- **vSAN-Clusterpartition**. Diese Integritätsprüfung untersucht den Cluster, um zu prüfen, wie viele Partitionen vorhanden sind. Es wird ein Fehler angezeigt, wenn es mehrere Partitionen im vSAN-Cluster gibt.
- **Multicast-Überprüfung basierend auf anderen Prüfungen**. Diese Integritätsprüfung aggregiert Daten aus allen Netzwerkintegritätsprüfungen. Wenn diese Prüfung fehlschlägt, bedeutet dies, dass Multicast wahrscheinlich die Hauptursache einer Netzwerkpartition ist.

Befehle zum Überprüfen des Netzwerks

Wenn das vSAN-Netzwerk konfiguriert wurde, überprüfen Sie mit diesen Befehlen seinen Status. Sie können überprüfen, welcher VMkernel-Adapter (vmknic) für vSAN verwendet wird und welche Attribute darin enthalten sind.

Verwenden Sie ESXCLI-und RVC-Befehle, um zu überprüfen, ob das Netzwerk vollständig funktionstüchtig ist und um Netzwerkprobleme mit vSAN zu beheben.

Sie können sicherstellen, dass die für das vSAN-Netzwerk verwendete vmknic einheitlich auf allen Hosts ordnungsgemäß konfiguriert ist, überprüfen, ob Multicast funktionsfähig ist, und sicherstellen, dass die Hosts, die Teil des vSAN-Clusters sind, erfolgreich miteinander kommunizieren können.

esxcli vsan network list

Mit diesem Befehl können Sie die vom vSAN-Netzwerk verwendete VMkernel-Schnittstelle identifizieren.

Die folgende Ausgabe zeigt, dass das vSAN-Netzwerk vmk2 verwendet. Dieser Befehl funktioniert weiterhin, selbst wenn vSAN auf dem Cluster ausgeschaltet wurde und die Hosts nicht mehr Teil von vSAN sind.

Die Agentengruppen-Multicast- und Master-Gruppen-Multicast-Überprüfung ist ebenfalls wichtig.

```
[root@esxi-dell-m:~] esxcli vsan network list
Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: 32efc758-9ca0-57b9-c7e3-246e962c24d0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

Dabei werden nützliche Informationen bereitgestellt, z. B. welche VMkernel-Schnittstelle für vSAN-Datenverkehr verwendet wird. In diesem Fall ist dies **vmk1**. Es werden jedoch auch die Multicast-Adressen angezeigt. Diese Informationen werden möglicherweise auch dann angezeigt, wenn der Cluster im Unicast-Modus ausgeführt wird. Dort gibt es die Multicast-Adresse und den Port der Gruppe. Port 23451 wird für das Taktsignal verwendet, das vom Primären jede Sekunde gesendet wird und auf jedem anderen Host im Cluster sichtbar ist. Port 12345 wird für die CMMDS-Updates zwischen dem Primären und der Sicherung verwendet.

esxcli network ip interface list

Mit diesem Befehl können Sie Elemente wie vSwitch oder Distributed Switch überprüfen.

Verwenden Sie diesen Befehl, um zu überprüfen, mit welchem vSwitch oder Distributed Switch eine Verbindung vorliegt. Zudem können Sie die MTU-Größe überprüfen, was hilfreich sein kann, wenn Jumbo-Frames in der Umgebung konfiguriert wurden. In diesem Fall gilt für MTU der Standardwert 1500.

```
[root@esxi-dell-m:~] esxcli network ip interface list
vmk0
   Name: vmk0
   <<truncated>>
vmk1
   Name: vmk1
   MAC Address: 00:50:56:69:96:f0
   Enabled: true
   Portset: DvsPortset-0
   Portgroup: N/A
   Netstack Instance: defaultTcpipStack
   VDS Name: vDS
   VDS UUID: 50 1e 5b ad e3 b4 af 25-18 f3 1c 4c fa 98 3d bb
```

```
   VDS Port: 16
   VDS Connection: 1123658315
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 9000
   TSO MSS: 65535
   Port ID: 50331814
```

Die maximale Übertragungseinheitsgröße wird als 9000 angezeigt, daher ist dieser VMkernel-Port für Jumbo-Frames konfiguriert, für die ein MTU-Wert von etwa 9.000 erforderlich ist. VMware gibt keine Empfehlung zur Verwendung von Jumbo-Frames. Jumbo-Frames werden jedoch für die Verwendung mit vSAN unterstützt.

esxcli network ip interface ipv4 get –i vmk2

Dieser Befehl zeigt Informationen wie IP-Adresse und Netzmaske der vSAN VMkernel-Schnittstelle an.

Mit diesen Informationen kann ein Administrator nun mit anderen in der Befehlszeile verfügbaren Befehlen überprüfen, ob das vSAN-Netzwerk ordnungsgemäß funktioniert.

```
[root@esxi-dell-m:~] esxcli network ip interface ipv4 get -i vmk1
Name  IPv4 Address  IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway  DHCP DNS
----  ------------  -------------  --------------  ------------  -------  --------
vmk1  172.40.0.9   255.255.255.0   172.40.0.255   STATIC         0.0.0.0 false
```

vmkping

Der `vmkping`-Befehl überprüft, ob alle anderen ESXi-Hosts im Netzwerk auf Ihre Ping-Anforderungen reagieren.

```
~ # vmkping -I vmk2 172.32.0.3 -s 1472 -d
 PING 172.32.0.3 (172.32.0.3): 56 data bytes
 64 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.186 ms
 64 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=2.690 ms
 64 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.139 ms

 --- 172.32.0.3 ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
 round-trip min/avg/max = 0.139/1.005/2.690 ms
```

Obwohl die Multicast-Funktionalität nicht überprüft wird, kann er dabei helfen, einen nicht autorisierten ESXi-Host mit Netzwerkproblemen zu identifizieren. Sie können auch die Antwortzeiten überprüfen, um festzustellen, ob eine abnormale Latenz im vSAN-Netzwerk vorliegt.

Wenn Jumbo-Frames konfiguriert sind, meldet dieser Befehl keine Probleme, falls die Größe der Jumbo-Frame-MTU nicht korrekt ist. Standardmäßig verwendet dieser Befehl eine MTU-Größe von 1500. Wenn überprüft werden muss, ob die Jumbo-Frames End-to-End erfolgreich arbeiten, verwenden Sie vmkping mit einer größeren Paketgrößenoption (-s) wie folgt:

```
~ # vmkping -I vmk2 172.32.0.3 -s 8972 -d
PING 172.32.0.3 (172.32.0.3): 8972 data bytes
9008 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.554 ms
9008 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=0.638 ms
9008 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.533 ms

--- 172.32.0.3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.533/0.575/0.638 ms
~ #
```

Sie sollten dem vmkping-Befehl -d hinzufügen, um zu testen, ob Pakete ohne Fragmentierung gesendet werden können.

esxcli network ip neighbor list

Mit diesem Befehl können Sie überprüfen, ob sich alle vSAN-Hosts im selben Netzwerksegment befinden.

In dieser Konfiguration haben wir einen Cluster mit vier Hosts, und dieser Befehl gibt die ARP-Einträge (Address Resolution Protocol) der anderen drei Hosts zurück, einschließlich ihrer IP-Adressen und deren vmknic (vSAN ist für die Verwendung von vmk1 auf allen Hosts in diesem Cluster konfiguriert).

```
[root@esxi-dell-m:~] esxcli network ip neighbor list -i vmk1
Neighbor     Mac Address        Vmknic   Expiry  State  Type
-----------  -----------------  ------  -------  -----  -------
172.40.0.12  00:50:56:61:ce:22  vmk1    164 sec         Unknown
172.40.0.10  00:50:56:67:1d:b2  vmk1    338 sec         Unknown
172.40.0.11  00:50:56:6c:fe:c5  vmk1    162 sec         Unknown
[root@esxi-dell-m:~]
```

esxcli network diag ping

Mit diesem Befehl erfolgt eine Prüfung auf Duplikate im Netzwerk sowie Roundtrip-Zeiten.

Um noch mehr Details zur vSAN-Netzwerkkonnektivität zwischen den verschiedenen Hosts zu erhalten, stellt ESXCLI einen leistungsstarken Netzwerkdiagnosebefehl bereit. Hier ist ein Beispiel für eine solche Ausgabe, wobei sich die VMkernel-Schnittstelle auf vmk1 befindet und die vSAN Remote-Netzwerk-IP eines anderen Hosts im Netzwerk 172.40.0.10 ist.

```
[root@esxi-dell-m:~] esxcli network diag ping -I vmk1 -H 172.40.0.10
   Trace:
         Received Bytes: 64
         Host: 172.40.0.10
```

```
          ICMP Seq: 0
          TTL: 64
          Round-trip Time: 1864 us
          Dup: false
          Detail:

          Received Bytes: 64
          Host: 172.40.0.10
          ICMP Seq: 1
          TTL: 64
          Round-trip Time: 1834 us
          Dup: false
          Detail:

          Received Bytes: 64
          Host: 172.40.0.10
          ICMP Seq: 2
          TTL: 64
          Round-trip Time: 1824 us
          Dup: false
          Detail:
    Summary:
          Host Addr: 172.40.0.10
          Transmitted: 3
          Recieved: 3
          Duplicated: 0
          Packet Lost: 0
          Round-trip Min: 1824 us
          Round-trip Avg: 1840 us
          Round-trip Max: 1864 us
[root@esxi-dell-m:~]
```

vsan.lldpnetmap

Dieser RVC-Befehl zeigt Uplink-Portinformationen an.

Wenn in der Umgebung nicht-Cisco-Switches mit aktiviertem LLDP (Verbindungsschichterkennungsprotokoll) vorhanden sind, gibt es einen RVC-Befehl zum Anzeigen von Informationen zum Uplink <-> Switch <-> Switch-Port. Weitere Informationen zu RVC finden Sie im RVC-Befehlshandbuch.

Dies hilft Ihnen bei der Ermittlung, welche Hosts an welche Switches angehängt werden, wenn der vSAN-Cluster mehrere Switches umfasst. Es kann dabei helfen, ein Problem auf einen bestimmten Switch zu isolieren, wenn nur eine Teilmenge der Hosts im Cluster betroffen ist.

```
> vsan.lldpnetmap 02013-08-15 19:34:18 -0700: This operation will take
30-60 seconds ...+---------------+---------------------------+| Host          | LLDP
info                 |+---------------+---------------------------+| 10.143.188.54 | w2r13-
vsan-x650-2: vmnic7 ||               | w2r13-vsan-x650-1: vmnic5 |+---------------
+---------------------------+
```

Diese Vorgehensweise ist nur bei Switches verfügbar, die LLDP unterstützen. Melden Sie sich zum Konfigurieren der Funktion bei dem Switch an und führen Sie die folgenden Schritte aus:

```
switch# config t
Switch(Config)# feature lldp
```

So überprüfen Sie, ob LLDP aktiviert ist:

```
switch(config)#do show running-config lldp
```

Hinweis LLDP arbeitet standardmäßig im Sende- und Empfangsmodus. Überprüfen Sie die Einstellungen Ihrer vDS-Eigenschaften, wenn die Informationen zum physischen Switch nicht erkannt werden. Standardmäßig wird vDS mit dem Discovery-Protokoll erstellt, das auf CDP (Cisco Discovery Protocol) festgelegt ist. Um dies zu ändern, legen Sie das Erkennungsprotokoll auf LLDP fest, und legen Sie den Vorgang auf dem vDS auf **beide** fest.

Überprüfen der Multicast-Kommunikation

Multicast-Konfigurationen können Probleme bei der anfänglichen vSAN-Bereitstellung verursachen.

Eine der einfachsten Überprüfungsmöglichkeiten, ob Multicast in Ihrer vSAN-Umgebung ordnungsgemäß funktioniert, ist die Verwendung des Befehls `tcpdump-uw`. Dieser Befehl ist über die Befehlszeile der ESXi-Hosts verfügbar.

Dieser Befehl `tcpdump-uw` zeigt an, ob der Primäre Multicast-Pakete ordnungsgemäß sendet (Port- und IP-Informationen) und ob alle anderen Hosts im Cluster diese empfangen.

Auf dem Primären zeigt dieser Befehl die Pakete an, die an die Multicast-Adresse gesendet werden. Auf allen anderen Hosts sind dieselben Pakete sichtbar (vom Primären bis zur Multicast-Adresse). Wenn Sie nicht angezeigt werden, funktioniert Multicast nicht ordnungsgemäß. Führen Sie den hier angezeigten Befehl `tcpdump-uw` auf einem beliebigen Host im Cluster aus. Daraufhin werden die Taktsignale des Primären angezeigt. In diesem Fall befindet sich der Primäre unter IP-Adresse 172.32.0.2. Das **-v-** für die Ausführlichkeit ist optional.

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 96 bytes
11:04:21.800575 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 34917, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:22.252369 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15011, offset 0,
flags [none], proto UDP (17), length 316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:22.262099 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3359, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:04:22.324496 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 20914, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:04:22.800782 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 35010, offset 0,
```

```
flags [none], proto UDP (17), length 228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:23.252390 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15083, offset 0,
flags [none], proto UDP (17), length 316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:23.262141 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3442, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
```

Diese Ausgabe scheint etwas verwirrend zu sein. Sie besagt jedoch lediglich, dass die hier gezeigte Ausgabe angibt, dass die vier Hosts im Cluster ein Taktsignal vom Primären erhalten. Dieser Befehl **`tcpdump-uw`** muss auf jedem Host ausgeführt werden, um sicherzustellen, dass alle das Taktsignal empfangen. Dadurch wird sichergestellt, dass der Primäre die Taktsignale sendet und alle anderen Hosts im Cluster sie empfangen, was darauf hinweist, dass Multicast funktioniert.

Wenn einige der vSAN-Hosts nicht in der Lage sind, die Ein-Sekunden-Taktsignale vom Primären abzurufen, muss der Netzwerkadministrator die Multicast-Konfiguration der Switches überprüfen.

Um die lästige Meldung **`IP abgeschnitten – 146 Byte fehlen!`** zu vermeiden, verwenden Sie die Option **`-s0`** für denselben Befehl, um das Abschneiden der Pakete zu beenden:

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v -s0
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 65535 bytes
11:18:29.823622 IP (tos 0x0, ttl 5, id 56621, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:18:30.251078 IP (tos 0x0, ttl 5, id 52095, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:18:30.267177 IP (tos 0x0, ttl 5, id 8228, offset 0, flags [none], proto UDP (17), length
316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:18:30.336480 IP (tos 0x0, ttl 5, id 28606, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:18:30.823669 IP (tos 0x0, ttl 5, id 56679, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
```

Der Befehl **`tcpdump`** steht im Zusammenhang mit der IGMP-Mitgliedschaft (Internet-Gruppenverwaltungsprotokoll). Hosts (und Netzwerkgeräte) verwenden IGMP zum Einrichten der Multicast-Gruppenmitgliedschaft.

Jeder ESXi-Host im vSAN-Cluster sendet reguläre IGMP-Mitgliedschaftsberichte (Beitritt).

Der Befehl **`tcpdump`** zeigt IGMP-Mitgliederberichte von einem Host an:

```
[root@esxi-dell-m:~] tcpdump-uw -i vmk1 igmp
tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmk1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:49:23.134458 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
15:50:22.994461 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
```

In der Ausgabe werden IGMP v3-Berichte angezeigt, die darauf hinweisen, dass der ESXi-Host regelmäßig seine Mitgliedschaft aktualisiert. Wenn ein Netzwerkadministrator Zweifel daran hat, ob vSAN ESXi-Hosts IGMP korrekt ausführen, kann zur Überprüfung dieser Befehl auf jedem ESXi-Host im Cluster ausgeführt und diese Nachverfolgung angezeigt werden.

Wenn Sie per Multicast kommunizieren, verwenden Sie IGMP v3.

In der Tat kann der folgende Befehl verwendet werden, um den Multicast- und IGMP-Datenverkehr gleichzeitig zu betrachten:

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast or igmp -v -s0
```

Ein häufiges Problem ist, dass der vSAN-Cluster über mehrere physische Switches hinweg konfiguriert ist und Multicast zwar auf einem Switch, aber nicht Switch-übergreifend aktiviert wurde. In diesem Fall ist der Cluster mit zwei ESXi-Hosts in einer Partition und einem anderen ESXi-Host (verbunden mit dem anderen Switch) nicht in der Lage, diesem Cluster beizutreten. Stattdessen bildet er einen eigenen vSAN-Cluster in einer anderen Partition. Der zuvor gezeigte Befehl `vsan.lldpnetmap` kann bei der Ermittlung der Netzwerkkonfiguration und der mit den einzelnen Switches verbundenen Hosts helfen.

Während sich ein vSAN-Cluster bildet, gibt es Indikatoren, die darauf hindeuten, dass Multicast ein Problem sein kann.

Gehen wir davon aus, dass die Checkliste für Subnetz, VLAN, MTU befolgt wurde und jeder Host im Cluster für jeden anderen Host im Cluster einen `vmkping`-Vorgang ausführen kann.

Wenn beim Erstellen des Clusters ein Multicast-Problem auftritt, ist ein häufig auftretendes Symptom, dass jeder ESXi-Host seinen eigenen vSAN-Cluster mit sich selbst als Primärer bildet. Wenn jeder Host über eine eindeutige Netzwerkpartitions-ID verfügt, schlägt dieses Symptom vor, dass zwischen den Hosts kein Multicast vorhanden ist.

Wenn jedoch eine Teilmenge der ESXi-Hosts einen Cluster bildet und eine andere Teilmenge einen anderen Cluster bildet und beide Teilmengen jeweils über eindeutige Partitionen mit eigenem Primären, eigener Sicherung und möglicherweise sogar eigenen Agent-Hosts verfügen, ist Multicast zwar für den Switch aktiviert, jedoch nicht Switch-übergreifend. vSAN zeigt Hosts auf dem ersten physischen Switch an, die eine eigene Cluster-Partition bilden, und Hosts auf dem zweiten physischen Switch, die eine eigene Cluster-Partition mit jeweils einem eigenen Primären bilden. Wenn Sie überprüfen können, mit welchen Switches die Hosts im Cluster eine Verbindung herstellen und Hosts in einem Cluster mit demselben Switch verbunden sind, ist dies wahrscheinlich das Problem.

Überprüfen der vSAN-Netzwerkleistung

Stellen Sie sicher, dass eine ausreichende Bandbreite zwischen ihren ESXi-Hosts vorhanden ist. Dieses Tool kann Sie dabei unterstützen, zu testen, ob Ihr vSAN-Netzwerk optimal funktioniert.

Um die Leistung des vSAN-Netzwerks zu überprüfen, können Sie das `iperf`-Tool verwenden, um die maximale TCP-Bandbreite und-Latenz zu messen. Es befindet sich unter `/usr/lib/vmware/vsan/bin/iperf.copy`.. Führen Sie es mit `--help` aus, um die verschiedenen Optionen anzuzeigen. Verwenden Sie dieses Tool, um die Netzwerkbandbreite und Latenz zwischen ESXi-Hosts zu überprüfen, die an einem vSAN-Cluster beteiligt sind.

Im VMware Knowledgebase-Artikel 2001003 finden Sie Informationen zum Einrichten und Testen.

Dies ist besonders nützlich, wenn ein vSAN-Cluster in Betrieb genommen wird. Die Ausführung von **iperf**-Tests für das vSAN-Netzwerk, wenn sich der Cluster bereits in der Produktion befindet, kann die Leistung der auf dem Cluster ausgeführten virtuellen Maschinen beeinträchtigen.

Überprüfen der vSAN-Netzwerkgrenzwerte

Mithilfe des Befehls **`vsan.check.limits`** wird sichergestellt, dass keiner der vSAN-Schwellenwerte verletzt wird.

```
> ls
0 /
1 vcsa-04.rainpole.com/
> cd 1
/vcsa-04.rainpole.com> ls
0 Datacenter (datacenter)
/vcsa-04.rainpole.com> cd 0
/vcsa-04.rainpole.com/Datacenter> ls
0 storage/
1 computers [host]/
2 networks [network]/
3 datastores [datastore]/
4 vms [vm]/
/vcsa-04.rainpole.com/Datacenter> cd 1
/vcsa-04.rainpole.com/Datacenter/computers> ls
0 Cluster (cluster): cpu 155 GHz, memory 400 GB
1 esxi-dell-e.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
2 esxi-dell-f.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
3 esxi-dell-g.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
4 esxi-dell-h.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
/vcsa-04.rainpole.com/Datacenter/computers> vsan.check_limits 0
2017-03-14 16:09:32 +0000: Querying limit stats from all hosts ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-m.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-n.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-o.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-p.rainpole.com (may take a
moment) ...
2017-03-14 16:09:39 +0000: Done fetching vSAN disk infos
+--------------------------+--------------------
+-------------------------------------------------------------------+
| Host                     | RDT
| Disks                                                             |
```

```
+--------------------------+--------------------
+-----------------------------------------------------------------+
| esxi-dell-m.rainpole.com |
Assocs: 1309/45000 | Components: 485/9000                                                  |
|                          | Sockets:
89/10000  | naa.500a075113019b33: 0% Components: 0/0                          |
|                          | Clients:
136       | naa.500a075113019b37: 40% Components: 81/47661                    |
|                          | Owners:
138        | t10.ATA_____Micron_P420m2DMTFDGAR1T4MAX_____ 0% Components: 0/0 |
|                          |                     |
naa.500a075113019b41: 37% Components: 80/47661                   |
|                          |                     |
naa.500a07511301a1eb: 38% Components: 81/47661                   |
|                          |                     |
naa.500a075113019b39: 39% Components: 79/47661                   |
|                          |                     |
naa.500a07511301a1ec: 41% Components: 79/47661                   |
<<truncated>>
```

Aus Sicht des Netzwerks sind die RDT-Zuordnungen (Assocs) und die Socket-Anzahl wichtig. Es gibt 45.000 Zuordnungen pro Host in vSAN 6.0 und höher. Eine RDT-Zuordnung wird verwendet, um den Peer-to-Peer-Netzwerkstatus innerhalb von vSAN zu verfolgen. vSAN wird so dimensioniert, dass die RDT-Zuordnungen nie erschöpft sind. vSAN schränkt auch die Anzahl der zu verwendenden TCP-Sockets ein, und vSAN wird so dimensioniert, dass die Zuteilung von TCP-Sockets nie erschöpft. Es gilt ein Grenzwert von 10.000 Sockets pro Host.

Ein vSAN-**Client** stellt den Zugriff des Objekts im vSAN-Cluster dar. Der Client stellt in der Regel eine virtuelle Maschine dar, die auf einem Host ausgeführt wird. Der Client und das Objekt befinden sich möglicherweise nicht auf demselben Host. Es gibt keinen fest definierten Grenzwert, aber diese Metrik wird angezeigt, um zu verstehen, wie Clients auf Hosts verteilt sind.

Es gibt nur einen vSAN-**Besitzer** für ein bestimmtes vSAN-Objekt, das in der Regel mit dem vSAN-Client zusammen vorliegt, der auf dieses Objekt zugreift. vSAN-Besitzer koordinieren den gesamten Zugriff auf das vSAN-Objekt und implementieren Funktionalitäten wie Spiegelung und Striping. Es gibt keinen fest definierten Grenzwert, aber diese Metrik wird angezeigt, um zu verstehen, wie Besitzer auf Hosts verteilt sind.

Verwenden von Multicast in einem vSAN-Netzwerk

13

Multicast ist eine Netzwerk-Kommunikationstechnik, die Informationspakete an eine Gruppe von Zielen über ein IP-Netzwerk sendet.

Versionen vor vSAN-Version 6.6 unterstützen IP-Multicast und verwenden IP-Multicast-Kommunikation als Erkennungsprotokoll, um die Knoten zu identifizieren, die versuchen, einem vSAN-Cluster beizutreten. Versionen vor vSAN-Version 6.6 hängen von der IP-Multicast-Kommunikation ab, während sie den Clustergruppen beitreten und diese verlassen, sowie bei anderen Intra-Cluster-Kommunikationsvorgängen. Stellen Sie sicher, dass Sie den IP-Multicast in den IP-Netzwerksegmenten aktivieren und konfigurieren, um den vSAN-Datenverkehrsdienst zu übertragen.

Eine IP-Multicast-Adresse wird als Multicast-Gruppe (MG) bezeichnet. IP-Multicast sendet Quellpakete an mehrere Empfänger als Gruppenübertragung. IP-Multicast basiert auf Kommunikationsprotokollen, die von Hosts, Clients und Netzwerkgeräten zur Teilnahme an der Multicast-basierten Kommunikation verwendet werden. Kommunikationsprotokolle wie Internet-Gruppenverwaltungsprotokolle (IGMP) und protokollunabhängiges Multicast (PIM) sind die Hauptkomponenten und Abhängigkeiten für die Verwendung der IP-Multicast-Kommunikation.

Beim Erstellen eines vSAN-Clusters wird jedem vSAN-Cluster eine Multicast-Standardadresse zugewiesen. Der vSAN-Datenverkehrsdienst weist jedem Host automatisch die Einstellungen der Multicast-Standardadresse zu. Diese Multicast-Adresse sendet Frames an eine Multicast-Standardgruppe und einen Multicast-Gruppenagent.

Wenn sich mehrere vSAN-Cluster im selben Schicht-2-Netzwerk befinden, empfiehlt VMware die Änderung der Multicast-Standardadresse innerhalb der zusätzlichen vSAN-Cluster. Dadurch wird verhindert, dass mehrere Cluster alle Multicast-Streams empfangen. Weitere Informationen zum Ändern der vSAN Multicast-Standardadresse finden Sie im VMware Knowledgebase-Artikel2075451.

Lesen Sie als Nächstes die folgenden Themen:

- Internet-Gruppenverwaltungsprotokoll
- Protokollunabhängiges Multicast

Internet-Gruppenverwaltungsprotokoll

Mithilfe des Internet-Gruppenverwaltungsprotokolls (IGMP) können Sie der IP-Multicast-Gruppenmitgliedschaft innerhalb der Schicht-2-Domänen Empfänger hinzufügen.

Mit IGMP können Empfänger Anforderungen an die Multicast-Gruppen senden, denen sie beitreten möchten. Wenn sie Mitglied einer Multicast-Gruppe werden, können Router den Datenverkehr für die Multicast-Gruppen auf dem Schicht-3-Segment weiterleiten, in dem der Empfänger mit dem Switch-Port verbunden ist.

Sie können das IGMP-Snooping verwenden, um die an der Multicast-Gruppe beteiligten physischen Switch-Ports auf vSAN VMkernel-Port-Uplinks zu begrenzen. Das IGMP-Snooping ist mit einem IGMP-Snooping-Abfrager konfiguriert. Die Notwendigkeit, einen IGMP-Snooping-Abfrager zur Unterstützung von IGMP-Snooping zu konfigurieren, variiert je nach Switch-Anbieter. Wenden Sie sich an Ihren spezifischen Switch-Anbieter für die IGMP-Snooping-Konfiguration.

vSAN unterstützt sowohl IGMP-Version 2 als auch IGMP-Version 3. Wenn Sie die vSAN-Bereitstellung über Schicht-3-Netzwerksegmente hinweg durchführen, können Sie ein Schicht-3-fähiges Gerät konfigurieren, z. B. einen Router oder einen Switch mit einer Verbindung und Zugriff auf dieselben Schicht-3-Netzwerksegmente.

Alle VMkernel-Ports im vSAN-Netzwerk abonnieren eine Multicast-Gruppe mithilfe von IGMP, um zu vermeiden, dass Multicast alle Netzwerkports überflutet.

Hinweis Sie können das IGMP-Snooping deaktivieren, wenn sich vSAN auf einem nicht gerouteten oder Trunking-VLAN befindet, das Sie auf die vSAN-Ports aller Hosts im Cluster erweitern können.

Protokollunabhängiges Multicast

Das protokollunabhängige Multicast (PIM) besteht aus Schicht-3-Multicast-Routingprotokollen.

Es bietet unterschiedliche Kommunikationstechniken für IP-Multicast-Datenverkehr, um Empfänger zu erreichen, die sich in unterschiedlichen Schicht-3-Segmenten aus den Multicast-Gruppenquellen befinden. Für frühere vSAN-Cluster der Version 6.6 müssen Sie PIM verwenden, damit der Multicast-Datenverkehr über verschiedene Subnetze fließen kann. Wenden Sie sich bei der PIM-Implementierung an Ihren Netzwerkanbieter.

Netzwerküberlegungen für vSAN-Dateidienst

14

Der vSAN-Dateidienst ist eine Schicht über vSAN, die dazu dient, Dateifreigaben bereitzustellen. Momentan werden SMB-, NFS v3- und NFS v4.1-Dateifreigaben unterstützt.

Im Folgenden sind die Netzwerküberlegungen für den vSAN-Dateidienst aufgeführt:

- Sie müssen statische IP-Adressen als Dateiserver-IPs aus dem vSAN-Dateidienstnetzwerk zuteilen, 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.
- 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.

    Hinweis 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.
- Für SMB- und NFS-Freigaben mit Kerberos-Sicherheit müssen Sie Informationen über Ihre AD-Domäne und Organisationseinheit (optional) angeben. Darüber hinaus ist ein Benutzerkonto mit ausreichenden Berechtigungen zum Erstellen und Löschen von Objekten erforderlich.
- Stellen Sie sicher, dass der Dateiserver auf den AD-Server und den DNS-Server zugreifen kann. Der Dateiserver muss in der Lage sein, auf alle für den AD-Dienst erforderlichen Ports zuzugreifen.

Im Folgenden finden Sie die Ports, die der vSAN-Dateidienst für die Netzwerkkonnektivität verwendet. Stellen Sie sicher, dass diese Ports nicht durch die Firewall blockiert werden.

Dienst	Portnummer	Element	Konnektivitätsanforderungen
Server Message Block (SMB)	TCP-Port 445	Dateiserver	Externes Netzwerk zu Dateiservern
Kontingente für einen Benutzer eines lokalen Dateisystems (RQUOTA)	TCP-Port 875	Dateiserver	Externes Netzwerk zu Dateiservern
Netzwerkdateisystem (NFS)	TCP- und UDP-Port 2049	Dateiserver	Externes Netzwerk zu Dateiservern. NFSv3 kann sowohl TCP- als auch UDP-Ports verwenden, NFSv4.1 verwendet jedoch nur TCP.
Mounten von NFS	TCP- und UDP-Port 20048	Dateiserver	Externes Netzwerk zu Dateiservern
Server-Daemon Netzwerkstatusmonitor (Network Status Monitor, NSM)	TCP- und UDP-Port 27689	Dateiserver	Externes Netzwerk zu Dateiservern. Sowohl die eingehende als auch die ausgehende Kommunikation muss zulässig sein.
Netzwerksperrungs-Manager (Network Lock Manager, NLM)	TCP- und UDP-Port 32803	Dateiserver	Externes Netzwerk zu Dateiservern. Ermöglicht die vom Dateiserver initiierte Verbindung zum Client. Eingehende und ausgehende Verbindungen müssen in der Firewall zulässig sein. Der Standardport ist UDP.
Sun-Remoteprozeduraufruf (sunrpc)	TCP- und UDP-Port 111	Dateiserver	Externes Netzwerk zu Dateiservern
LDAP	TCP-Port 389	Active Directory (AD)-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
LDAP zu globalen Katalog	TCP-Port 3268	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
Kerberos	TCP-Port 88	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
Kerberos-Kennwort ändern	TCP-Port 464	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern

Dienst	Portnummer	Element	Konnektivitätsanforderungen
Domain Name Server (DNS)	TCP- und UDP-Port 53	DNS-Server	Dateiserver zu DNS-Servern
vSAN Distributed File System (VDFS)-Server	TCP-Port 1564	ESXi-Hosts	Innerhalb des vSAN-Netzwerks
Remoteprozeduraufruf	TCP-Port 135	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
NetBIOS-Sitzungsdienst	TCP-Port 139	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
DNS	UDP-Port 53	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
LDAP, DC-Locator und Netzanmeldung	UDP-Port 389	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern
Zufällig zugeteilte hohe TCP-Ports	TCP 49152 – 65535	AD-Server (wenn AD-Domäne konfiguriert ist)	Dateiserver zu AD-Servern

Netzwerküberlegungen für iSCSI auf vSAN

15

Mit dem iSCSI-Zieldienst von vSAN können Hosts und physische Arbeitslasten, die sich außerhalb des vSAN-Clusters befinden, auf den vSAN-Datenspeicher zugreifen. Diese Funktion aktiviert einen iSCSI-Initiator auf einem Remotehost, um Blockebenendaten an ein iSCSI-Ziel auf einem Speichergerät im vSAN-Cluster zu übertragen.

Die iSCSI-Ziele auf vSAN werden mithilfe der speicherrichtlinienbasierten Verwaltung (SPBM) ähnlich wie andere vSAN-Objekte verwaltet. Für die iSCSI-LUNs spart dieser Speicherplatz durch Deduplizierung und Komprimierung und bietet Sicherheit durch Verschlüsselung. Für eine verbesserte Sicherheit verwendet der vSAN iSCSI-Zieldienst das Challenge Handshake Authentication Protocol (CHAP) und die beiderseitige CHAP-Authentifizierung.

vSAN identifiziert jedes iSCSI-Ziel durch einen eindeutigen qualifizierten iSCSI-Namen (IQN). Das iSCSI-Ziel wird einem Remote-iSCSI-Initiator mithilfe des IQN angezeigt, sodass der Initiator auf die LUN des Ziels zugreifen kann. Der vSAN iSCSI-Zieldienst ermöglicht das Erstellen von iSCSI-Initiatorgruppen. Die iSCSI-Initiatorgruppe beschränkt den Zugriff nur auf solche Initiatoren, die auch Mitglieder der Gruppe sind.

Lesen Sie als Nächstes die folgenden Themen:

- Merkmale des vSAN-iSCSI-Netzwerks

Merkmale des vSAN-iSCSI-Netzwerks

Nachstehend finden Sie die Merkmale eines vSAN-iSCSI-Netzwerks:

- iSCSI-Routing – iSCSI-Initiatoren können geroutete Verbindungen zu vSAN iSCSI-Zielen über ein L3-Netzwerk herstellen.
- IPv4 und IPv6 – vSAN iSCSI-Netzwerke unterstützen sowohl IPv4 als auch IPv6.
- IP-Sicherheit – IPSec im vSAN iSCSI-Netzwerk bietet mehr Sicherheit.

  Hinweis ESXi-Hosts unterstützen nur IPsec mit IPv6.

- Jumbo-Frames – Jumbo-Frames werden im vSAN iSCSI-Netzwerk unterstützt.
- NIC-Gruppierung – Alle NIC-Gruppierungskonfigurationen werden im vSAN iSCSI-Netzwerk unterstützt.

- Mehrere Verbindungen pro Sitzung (MCS) – Die vSAN iSCSI-Implementierung unterstützt MCS nicht.

Migrieren von Standard zu Distributed vSwitch

16

Sie können eine Migration von einem vSphere Standard-Switch zu einem vSphere Distributed Switch vornehmen und Network I/O Control verwenden. Auf diese Weise können Sie die QoS (Servicequalität) für vSAN-Datenverkehr priorisieren.

Warnung Eine Zugriffsmöglichkeit auf die ESXi-Hosts ist optimal, obwohl sie den Zugriff möglicherweise nicht benötigen. Wenn etwas schiefgeht, können Sie auf die Konsole der ESXi-Hosts zugreifen.

Notieren Sie sich die ursprüngliche vSwitch-Einrichtung. Notieren Sie sich insbesondere die Einstellungen für den Lastausgleich und die NIC-Gruppierung für die Quelle. Stellen Sie sicher, dass die Zielkonfiguration mit der Quelle übereinstimmt.

Erstellen eines Distributed Switches

Erstellen Sie den verteilten vSwitch, und benennen Sie ihn.

1 Klicken Sie in der Ansicht „vSphere Client-Host und -Cluster“ mit der rechten Maustaste auf ein Datencenter, und wählen Sie das Menü **Neuer Distributed Switch** aus.

2 Geben Sie einen Namen ein.

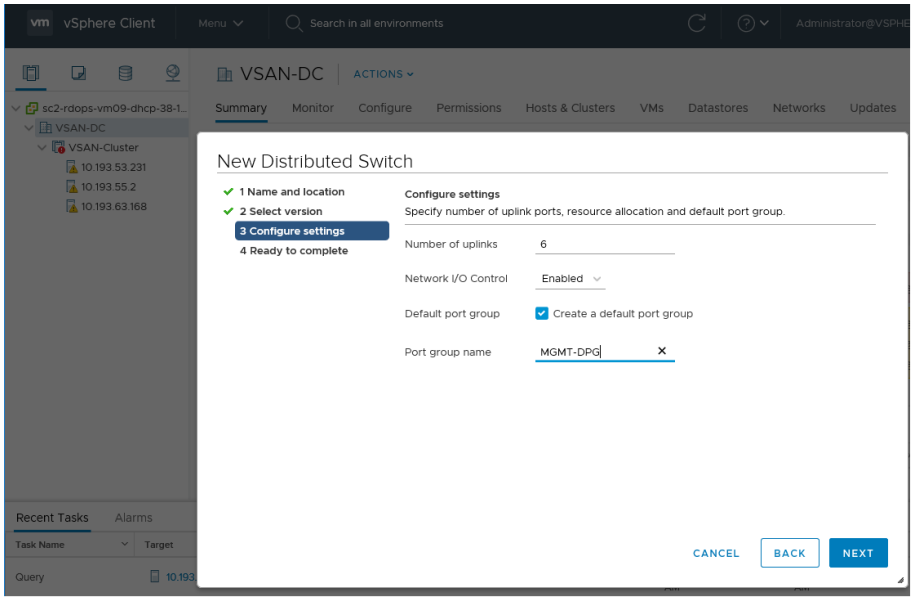
3 Wählen Sie die vSphere Distributed Switch-Version aus. In diesem Beispiel wird Version 6.6.0 für die Migration verwendet.

4 Fügen Sie die Einstellungen hinzu. Legen Sie fest, wie viele Uplinks Sie aktuell für das Netzwerk verwenden. Dieses Beispiel umfasst sechs: Management, vMotion, virtuelle Maschinen und drei für vSAN (eine LAG-Konfiguration). Geben Sie 6 für die Anzahl Uplinks ein. Ihre Umgebung ist möglicherweise anders, Sie können sie aber später bearbeiten.

   Sie können an dieser Stelle eine Standard-Portgruppe erstellen, aber es sind zusätzliche Portgruppen erforderlich.

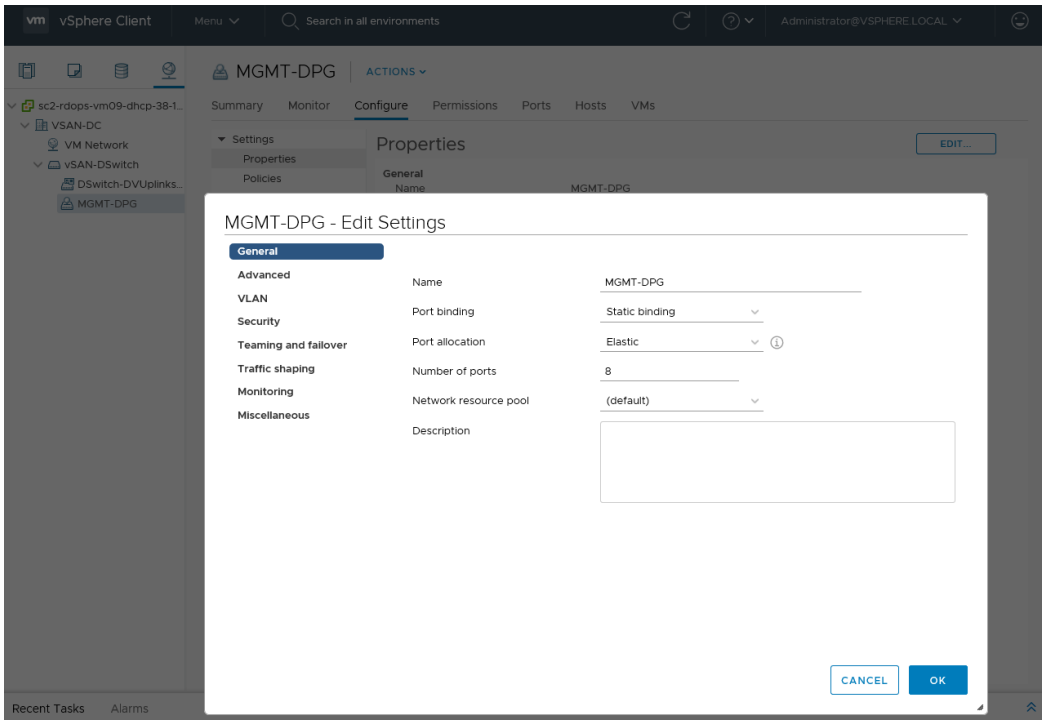
5 Beenden Sie die Konfiguration des verteilten vSwitch.

Der nächste Schritt besteht darin, die zusätzlichen Portgruppen zu konfigurieren und zu erstellen.



Erstellen von Portgruppen

Für das Verwaltungsnetzwerk wurde eine einzelne Standard-Portgruppe erstellt. Bearbeiten Sie diese Portgruppe, um sicherzustellen, dass sie über alle Merkmale der Verwaltungsportgruppe auf dem Standard-vSwitch verfügt, z. B. VLAN und NIC-Gruppierung und Failover-Einstellungen.



Konfigurieren Sie die Verwaltungsportgruppe.

1 Wählen Sie in der Ansicht „vSphere Client-Netzwerk“ die verteilte Portgruppe aus, und klicken Sie auf **Bearbeiten**.

2 Für einige Portgruppen müssen Sie das VLAN ändern. Da VLAN 51 das Verwaltungs-VLAN ist, kennzeichnen Sie die verteilte Portgruppe entsprechend.

3 Klicken Sie auf **OK**.

Erstellen Sie verteilte Portgruppen für vMotion, Netzwerke virtueller Maschinen und vSAN-Netzwerk.

1 Klicken Sie mit der rechten Maustaste auf den vSphere Distributed Switch, und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

2 Erstellen Sie für dieses Beispiel eine Portgruppe für das vMotion-Netzwerk.

Erstellen Sie alle verteilten Portgruppen auf dem verteilten vSwitch. Migrieren Sie dann die Uplinks, das VMkernel-Netzwerk und das VM-Netzwerk auf den verteilten vSwitch und die zugehörigen verteilten Portgruppen.

Warnung Migrieren Sie die Uplinks und Netzwerke schrittweise, um reibungslos und vorsichtig fortzufahren.

Migrieren des Verwaltungsnetzwerks

Migrieren Sie das Verwaltungsnetzwerk (vmk0) und den zugehörigen Uplink (vmnic0) vom Standard-vSwitch zum verteilten vSwitch (vDS).

1 Fügen Sie dem vDS Hosts hinzu.

   a Klicken Sie mit der rechten Maustaste auf den vDS, und wählen Sie das Menü **Hosts hinzufügen und verwalten** aus.

   b Fügen Sie dem vDS Hosts hinzu. Klicken Sie auf das grüne Symbol „Hinzufügen“ (+), und fügen Sie alle Hosts aus dem Cluster hinzu.

2 Konfigurieren Sie die physischen Adapter und VMkernel-Adapter.

   a Klicken Sie auf **Physische Adapter verwalten**, um die physischen Adapter und VMkernel-Adapter, vmnic0 und vmk0, auf den vDS zu migrieren.

   b Wählen Sie einen entsprechenden Uplink auf dem vDS für den physischen Adapter vmnic0 aus. Verwenden Sie für dieses Beispiel Uplink1. Der physische Adapter ist ausgewählt, und ein Uplink wird ausgewählt.

3 Migrieren Sie das Verwaltungsnetzwerk auf vmk0 vom Standard-vSwitch zum verteilten vSwitch. Führen Sie diese Schritte auf jedem Host durch.

   a Wählen Sie vmk0 aus, und klicken Sie auf **Portgruppe zuweisen**.

   b Weisen Sie die verteilte Portgruppe zu, die zuvor für das Verwaltungsnetzwerk erstellt wurde.

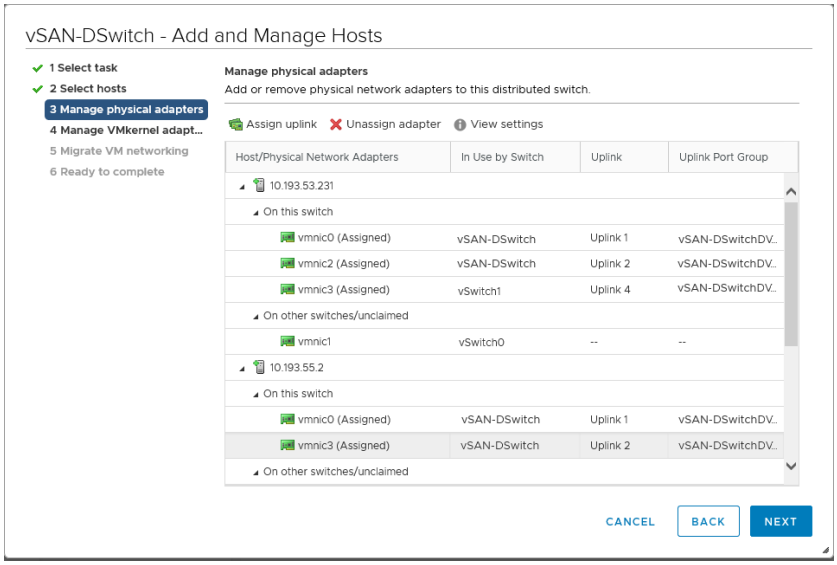
4 Stellen Sie die Konfiguration fertig.

   a Überprüfen Sie die Änderungen, um sicherzustellen, dass Sie vier Hosts, vier Uplinks (vmnic0 von jedem Host) und vier VMkernel-Adapter (vmk0 von jedem Host) hinzufügen.

b Klicken Sie auf **Beenden**.

Wenn Sie die Netzwerkkonfiguration jedes Hosts untersuchen, überprüfen Sie die Switch-Einstellungen mit einem Uplink (vmnic0) und dem vmk0-Verwaltungsport auf jedem Host.

Wiederholen Sie diesen Vorgang für die anderen Netzwerke.



Migrieren von vMotion

Führen Sie zum Migrieren des vMotion-Netzwerks dieselben Schritte aus wie für das Verwaltungsnetzwerk.

Bevor Sie beginnen, stellen Sie sicher, dass die verteilte Portgruppe für das vMotion-Netzwerk über dieselben Attribute wie die Portgruppe auf dem Standard-vSwitch verfügt. Migrieren Sie dann den Uplink, der für vMotion (vmnic1) verwendet wird, mit dem VMkernel-Adapter (vmk1).

Migrieren des vSAN-Netzwerks

Wenn Sie über einen einzelnen Uplink für das vSAN-Netzwerk verfügen, verwenden Sie denselben Vorgang wie zuvor. Wenn Sie jedoch mehrere Uplinks verwenden, gibt es zusätzliche Schritte.

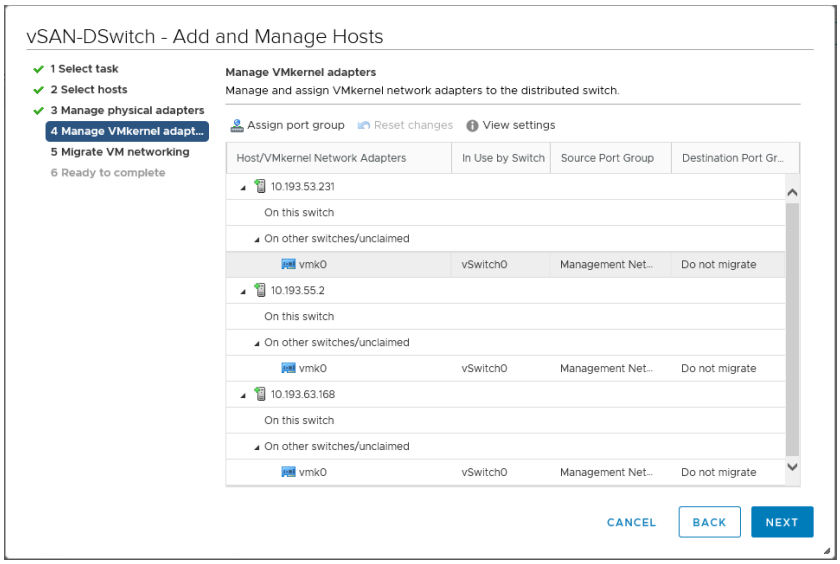
Wenn das vSAN-Netzwerk die Linkaggregation (LACP) verwendet oder sich in einem anderen VLAN zu den anderen VMkernel-Netzwerken befindet, versetzen Sie einige der Uplinks für bestimmte VMkernel-Adapter in einen nicht verwendeten Status.

Beispielsweise wird VMkernel-Adapter vmk2 für vSAN verwendet. Die Uplinks vmnic3, 4 und 5 werden jedoch für vSAN verwendet und sind in einer LACP-Konfiguration enthalten. Daher müssen für vmk2 alle anderen vmnics (0, 1 und 2) in einen nicht verwendeten Zustand versetzt werden. Ebenso sollten Sie für den Verwaltungsadapter (vmk0) und den vMotion-Adapter (vmk0) die vSAN-Uplinks/vmnics in einen nicht verwendeten Zustand.

Ändern Sie die Einstellungen der verteilten Portgruppe, und ändern Sie die Pfadrichtlinie und die Failover-Einstellungen. Führen Sie auf der Seite **Physischen Netzwerkadapter verwalten** die Schritte für mehrere Adapter aus.

Weisen Sie der verteilten Portgruppe für vSAN den vSAN-VMkernel-Adapter (vmk2) zu.

Hinweis Wenn Sie jetzt nur die Uplinks für das vSAN-Netzwerk migrieren, können Sie die Einstellungen der verteilten Portgruppe möglicherweise erst nach der Migration ändern. Während dieser Zeit können für vSAN möglicherweise Kommunikationsprobleme auftreten. Wechseln Sie nach der Migration zu den Einstellungen der verteilten Portgruppe, nehmen Sie Richtlinienänderungen vor, und markieren Sie die Uplinks, die nicht verwendet werden sollen. Das vSAN-Netzwerk wird dann wieder normal, wenn diese Aufgabe abgeschlossen ist. Verwenden Sie den vSAN-Integritätsdienst, um zu überprüfen, ob alles funktioniert.



Migrieren des VM-Netzwerks

Die letzte Aufgabe, die für die Migration des Netzwerks von einem Standard-vSwitch zu einem verteilten vSwitch erforderlich ist, besteht darin, das VM-Netzwerk zu migrieren.

Verwalten Sie das Hostnetzwerk.

1 Klicken Sie mit der rechten Maustaste auf den vDS, und wählen Sie das Menü **Hosts hinzufügen und verwalten** aus.

2 Wählen Sie alle Hosts im Cluster aus, um das Netzwerk virtueller Maschinen für alle Hosts auf den verteilten vSwitch zu migrieren.

   Verschieben Sie keine Uplinks. Wenn das VM-Netzwerk auf Ihren Hosts jedoch einen anderen Uplink verwendet, migrieren Sie den Uplink vom Standard-vSwitch.

3 Wählen Sie die VMs aus, die von einem Netzwerk der virtuellen Maschine auf dem Standard-vSwitch auf die verteilte Portgruppe der virtuellen Maschine des verteilten vSwitches migriert werden sollen. Klicken Sie auf **Portgruppe zuweisen**, und wählen Sie die verteilte Portgruppe aus.

4 Überprüfen Sie die Änderungen, und klicken Sie auf **Beenden**. In diesem Beispiel wechseln Sie zu VMs. Vorlagen, die das ursprüngliche Standard-vSwitch-VM-Netzwerk verwenden, müssen in virtuelle Maschinen konvertiert und bearbeitet werden. Die neue verteilte Portgruppe für virtuelle Maschinen muss als Netzwerk ausgewählt werden. Dieser Schritt kann nicht über den Migrationsassistenten realisiert werden.

Da der Standard-vSwitch keine Uplinks oder Portgruppen mehr aufweist, kann er sicher entfernt werden.

Damit ist die Migration von einem vSphere Standard-Switch zu einem vSphere Distributed Switch abgeschlossen.

Checklisten-Zusammenfassung für vSAN-Netzwerke

17

Verwenden Sie die Checklisten-Zusammenfassung, um Ihre vSAN-Netzwerkanforderungen zu überprüfen.

- Überprüfen Sie, ob Sie eine freigegebene Netzwerkkarte mit 10 GB oder eine dedizierte Netzwerkkarte mit 1 GB verwenden. Für All-Flash-Cluster sind Netzwerkkarten mit 10 GB erforderlich.
- Stellen Sie sicher, dass redundante NIC-Gruppierungsverbindungen konfiguriert sind.
- Stellen Sie sicher, dass die Flusssteuerung auf den Netzwerkkarten des ESXi-Hosts aktiviert ist.
- Stellen Sie sicher, dass der VMkernel-Port für den vSAN-Netzwerkdatenverkehr auf jedem Host konfiguriert ist.
- Stellen Sie sicher, dass VLAN, MTU und Subnetz an allen Schnittstellen identisch sind.
- Stellen Sie sicher, dass Sie **`vmkping`** erfolgreich zwischen allen Hosts ausführen können. Überprüfen Sie dies mit dem Integritätsdienst.
- Wenn Sie Jumbo-Frames verwenden, stellen Sie sicher, dass Sie **`vmkping`** erfolgreich mit der Paketgröße 9000 zwischen allen Hosts ausführen können. Überprüfen Sie dies mit dem Integritätsdienst.
- Wenn Ihre vSAN-Version älter als v6.6 ist, stellen Sie sicher, dass ob Multicast im Netzwerk aktiviert ist.
- Wenn Ihre vSAN-Version älter als v6.6 ist und sich mehrere vSAN-Cluster im selben Netzwerk befinden, konfigurieren Sie Multicast so, dass eindeutige Multicast-Adressen verwendet werden.
- Wenn Ihre vSAN-Version älter als v6.6 ist und mehrere Switches umfasst, stellen Sie sicher, dass Multicast Switch-übergreifend konfiguriert ist.
- Wenn Ihre vSAN-Version älter als v6.6 und geroutet ist, stellen Sie sicher, dass PIM so konfiguriert ist, dass das Multicast-Routing zulässig ist.
- Stellen Sie sicher, dass der physische Switch die vSAN-Anforderungen (Multicast, Flusssteuerung, Interoperabilität von Funktionen) erfüllen kann.
- Stellen Sie sicher, dass das Netzwerk keine größeren Leistungsprobleme aufweist, z. B. übermäßig viele verworfene Pakete oder Pause-Frames.

- Stellen Sie sicher, dass die Netzwerklimits innerhalb akzeptabler Grenzen liegen.
- Testen Sie die vSAN-Netzwerkleistung mit **`iperf`** und stellen Sie sicher, dass Sie die Erwartungen erfüllt.