Netzwerkmanagement

ONTAP 9

NetApp
February 06, 2026

Inhalt

Netzwerkmanagement

Los geht’s

Visualisierung des ONTAP Netzwerks mit System Manager

Ab ONTAP 9.8 können Sie mit System Manager eine Grafik anzeigen, die die Komponenten und die Konfiguration des Netzwerks anzeigt. So erhalten Sie eine Anzeige der Netzwerkverbindungspfade zwischen Hosts, Ports, SVMs, Volumes und mehr. Ab ONTAP 9.12.1 können Sie die LIF- und Subnetzzuordnung im Netzwerk-Interfaces-Raster anzeigen.

Die Grafik wird angezeigt, wenn Sie **Netzwerk > Übersicht** oder im Abschnitt **Netzwerk** des Dashboards auswählen → .

In der Grafik sind die folgenden Komponentenkategorien dargestellt:

- Hosts
- Storage-Ports
- Netzwerkschnittstellen
- Storage-VMs
- Datenzugriffskomponenten

In jedem Abschnitt werden weitere Details angezeigt, die Sie mit der Maus bewegen können, oder Sie können auswählen, um Netzwerkmanagement- und Konfigurationsaufgaben durchzuführen.

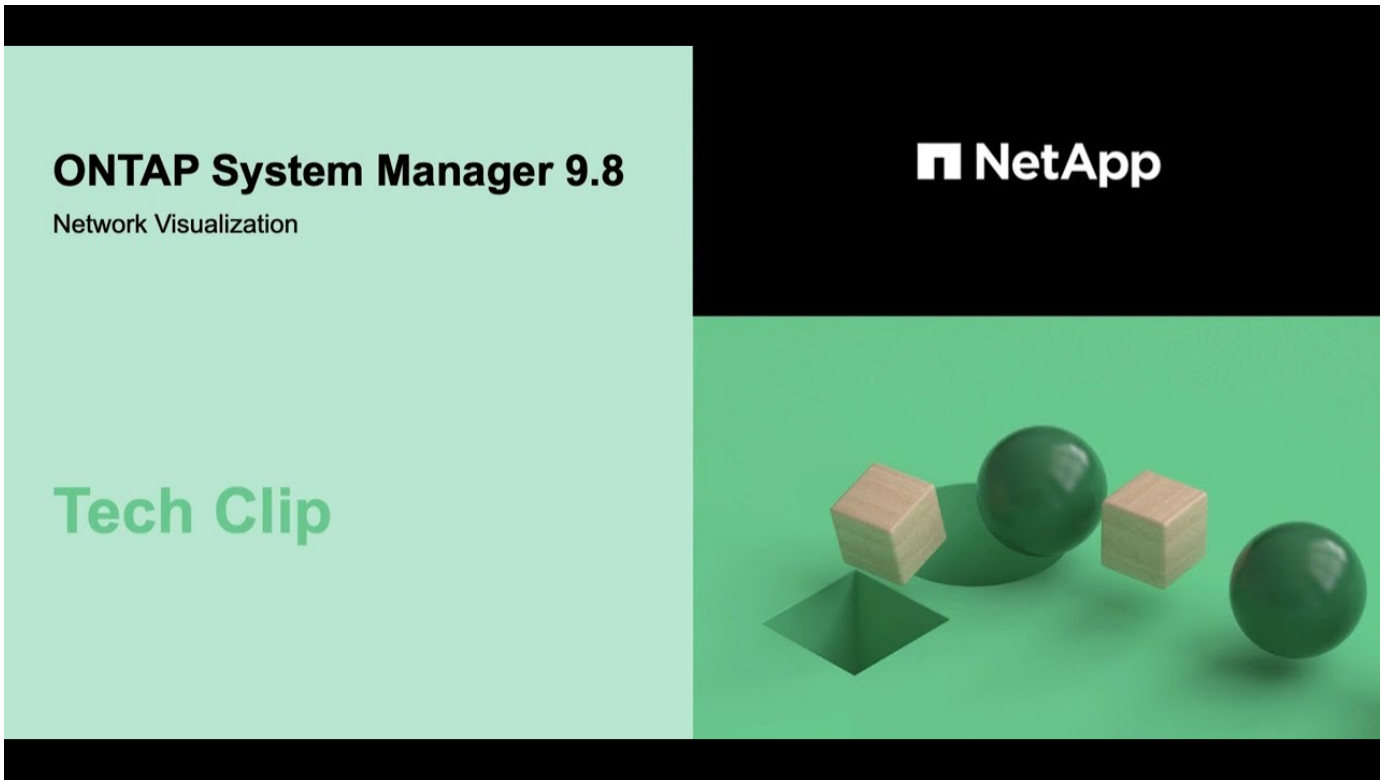
Wenn Sie klassischen System-Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), siehe "Verwalten des Netzwerks".

Beispiele

Im Folgenden sind einige Beispiele aufgeführt, wie Sie mit der Grafik interagieren können, um Details zu den einzelnen Komponenten anzuzeigen oder Aktionen zur Verwaltung Ihres Netzwerks zu initiieren:

- Klicken Sie auf einen Host, um seine Konfiguration anzuzeigen: Die damit verbundenen Ports, Netzwerkschnittstellen, Storage VMs und Datenzugriffskomponenten.
- Halten Sie die Maus über die Anzahl der Volumes in einer Storage-VM, um ein Volume auszuwählen, um seine Details anzuzeigen.
- Wählen Sie eine iSCSI-Schnittstelle aus, um ihre Leistung in der letzten Woche anzuzeigen.
- Klicken Sie neben einer Komponente auf ⋮ , um Aktionen zum Ändern dieser Komponente zu initiieren.
- Ermitteln Sie schnell, wo Probleme in Ihrem Netzwerk auftreten können, das durch ein „X“ neben ungesunden Komponenten gekennzeichnet ist.

System Manager Network Visualization Video



Erfahren Sie mehr über die Netzwerkkomponenten eines ONTAP Clusters

Sie sollten sich vor dem Einrichten des Clusters mit den Netzwerkkomponenten eines Clusters vertraut machen. Die Konfiguration der physischen Netzwerkkomponenten eines Clusters in logischen Komponenten bietet die Flexibilität und Mandantenfähigkeit von ONTAP.

Dies sind die verschiedenen Netzwerkkomponenten in einem Cluster:

- Physische Ports

  Netzwerkkarten (NICs) und Host Bus Adapter (HBAs) stellen physische Verbindungen (Ethernet und Fibre Channel) von jedem Node zu den physischen Netzwerken (Management- und Datennetzwerke) zur Verfügung.

  Informationen zu Standortanforderungen, Switch-Informationen, Anschlussverkabelungen und integrierten Controller-Anschlussverkabelungen finden Sie im Hardware Universe unter "hwu.netapp.com".

- Logische Ports

  Virtuelle lokale Netzwerke (VLANs) und Interface Groups bilden die logischen Ports. Schnittstellengruppen behandeln mehrere physische Ports als einen einzelnen Port, während VLANs einen physischen Port in mehrere separate Ports unterteilen.

- IPspaces

  IPspaces können verwendet werden, um für jede SVM in einem Cluster einen eigenen IP-Adressbereich zu erstellen. So können Clients in administrativ getrennten Netzwerkdomänen unter Verwendung überlappender IP-Adressbereiche aus demselben IP-Adressbereich des Subnetzes auf Cluster-Daten zugreifen.

- Broadcast-Domänen

  Eine Broadcast-Domäne befindet sich in einem IPspace und enthält eine Gruppe von Netzwerkports, möglicherweise von vielen Knoten im Cluster, die zum selben Layer-2-Netzwerk gehören. Die Ports in der Gruppe werden in einer SVM für den Datenverkehr verwendet.

- Subnetze

  Ein Subnetz wird innerhalb einer Broadcast-Domäne erstellt und enthält einen Pool von IP-Adressen, die zum gleichen Subnetz der Ebene 3 gehören. Dieser Pool aus IP-Adressen vereinfacht während der LIF-Erstellung die IP-Adresszuweisung.

- Logische Schnittstellen

  Eine logische Schnittstelle (LIF) ist eine IP-Adresse oder ein weltweiter Port-Name (WWPN), der einem Port zugeordnet ist. Sie ist mit Attributen wie Failover-Gruppen, Failover-Regeln und Firewall-Regeln verknüpft. Eine LIF kommuniziert über das Netzwerk über den Port (physisch oder logisch), an den es derzeit gebunden ist.

  Die verschiedenen LIFs in einem Cluster sind Daten-LIFs, Management-LIFs für Cluster-Umfang, Management-LIFs mit Node-Umfang, Intercluster LIFs und Cluster-LIFs. Die Eigentümer der LIFs sind von der SVM abhängig, wo sich das LIF befindet. Der Besitz von Daten-LIFs sind Data SVMs, LIFs zum Management von Nodes mit Node-Umfang, das Management von Cluster-Umfang und logische Intercluster-LIFs gehören den Admin-SVMs, während sich Cluster-LIFs im Besitz der Cluster-SVM befinden.

- DNS-Zonen

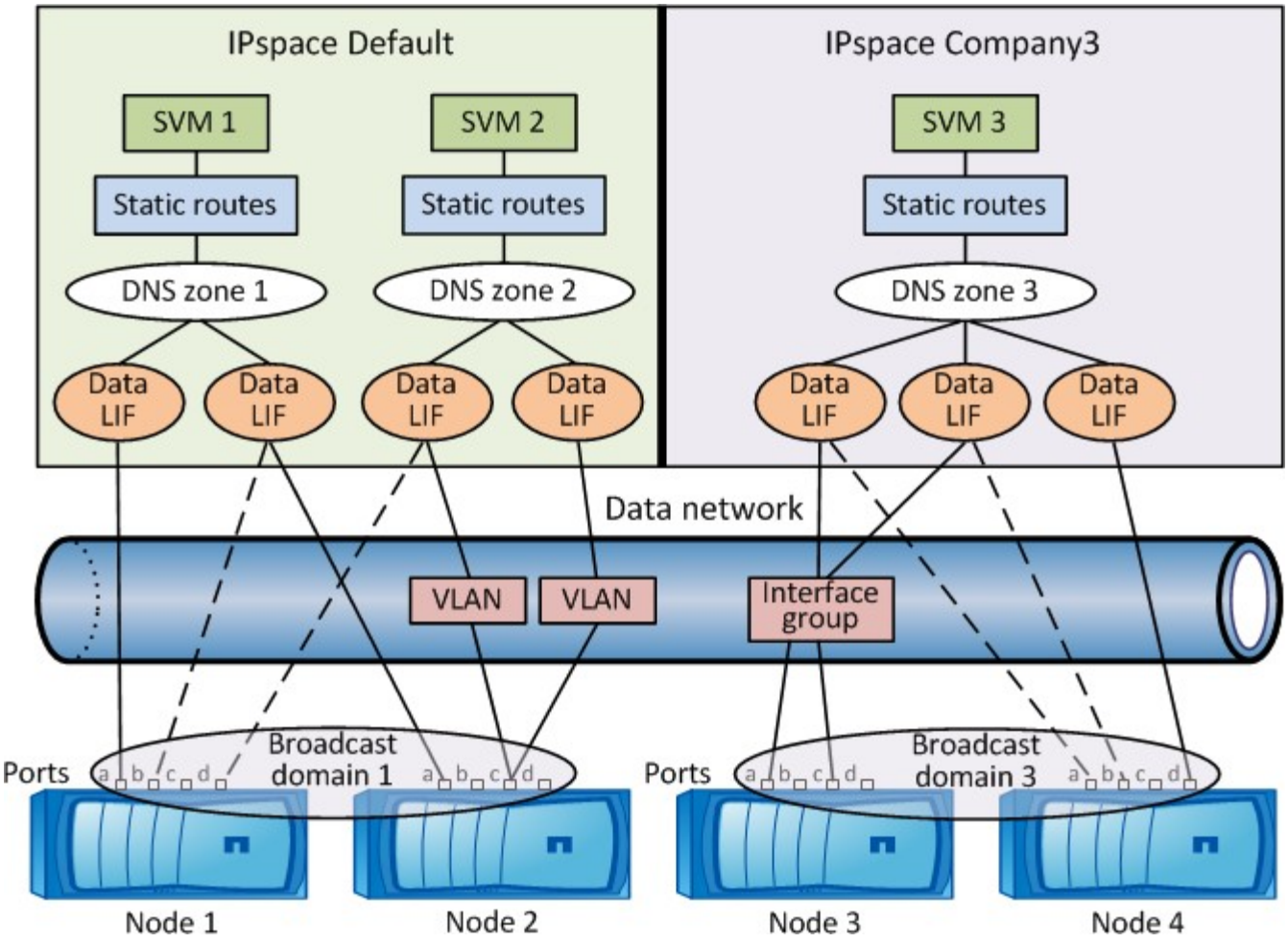
  Die DNS-Zone kann während der LIF-Erstellung angegeben werden und geben einen Namen für die LIF an, die über den DNS-Server des Clusters exportiert werden soll. Mehrere LIFs können denselben Namen teilen, wodurch die DNS-Lastausgleichfunktion IP-Adressen für den Namen gemäß Last verteilen kann.

  SVMs können mehrere DNS-Zonen aufweisen.

- Routing

  Jede SVM ist hinsichtlich des Netzwerks selbstständig. Eine SVM ist Eigentümer von LIFs und Routen, die jeden der konfigurierten externen Server erreichen können.

  Die folgende Abbildung zeigt, wie die verschiedenen Netzwerkkomponenten in einem Cluster mit vier Nodes verbunden sind:

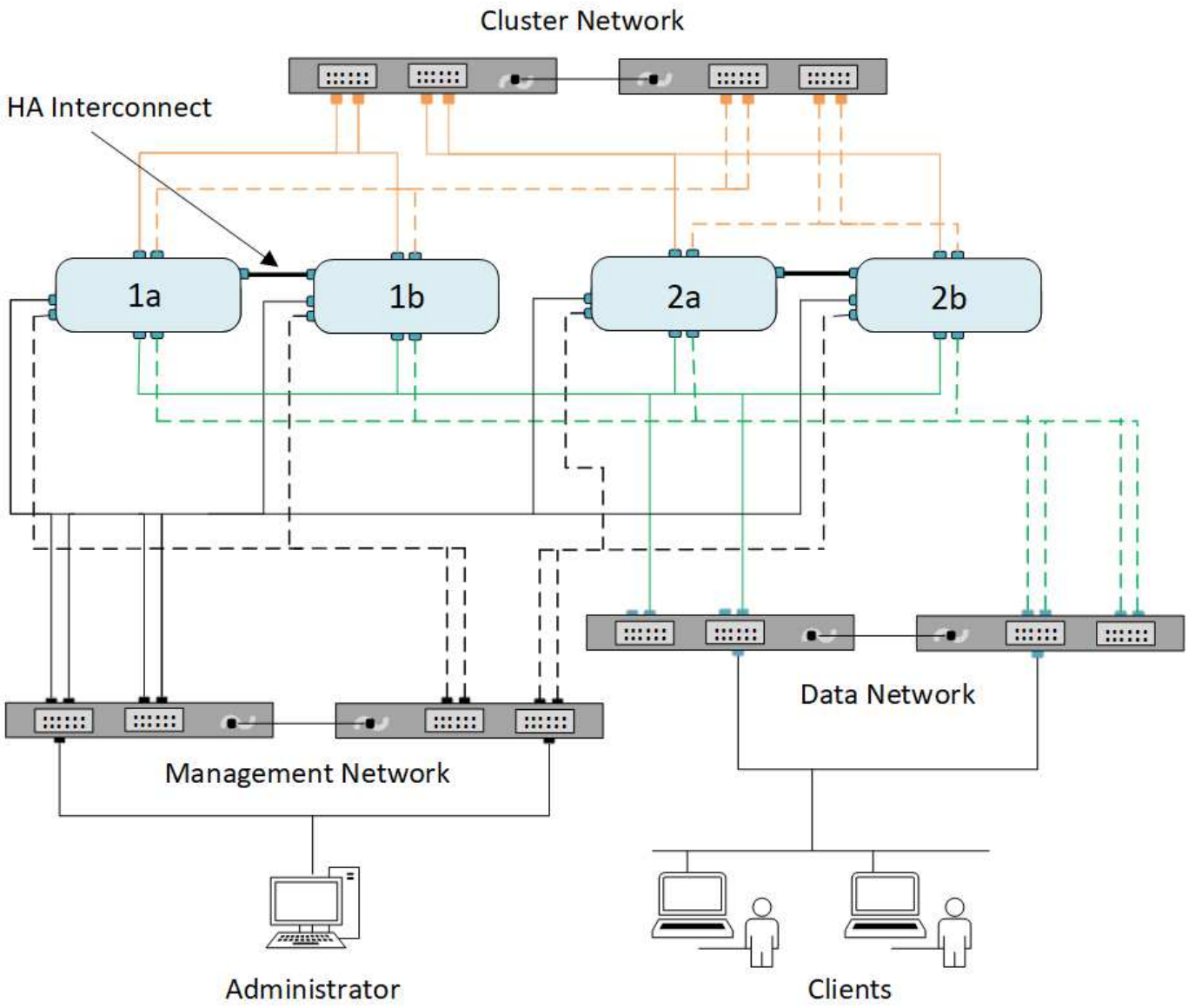


Best Practices für die ONTAP-Netzwerkverkabelung

Best Practices für die Netzwerkverkabelung trennen den Datenverkehr in die folgenden Netzwerke: Cluster, Management und Daten.

Sie sollten ein Cluster verkabeln, so dass sich der Cluster-Verkehr in einem separaten Netzwerk von allen anderen Datenverkehr befindet. Dies ist eine optionale, aber empfohlene Vorgehensweise für das Netzwerk-Management, die vom Daten- und Intracluster-Datenverkehr getrennt ist. Durch die Wartung separater Netzwerke lassen sich die Performance steigern, die Administration vereinfachen und der Zugriff auf die Nodes Sicherheits- und Managementzugriffsrechte verbessern.

Im folgenden Diagramm wird die Netzwerkverkabelung eines HA-Clusters mit vier Nodes dargestellt, der drei separate Netzwerke umfasst:



Bei der Verkabelung von Netzwerkverbindungen sollten Sie folgende Richtlinien beachten:

- Jeder Knoten sollte mit drei verschiedenen Netzwerken verbunden sein.

  Ein Netzwerk ist für das Management zuständig, eines für den Datenzugriff und eines für die Intracluster-Kommunikation. Management- und Datennetzwerke können logisch voneinander getrennt sein.

- Sie können für jeden Node mehrere Datennetzwerkverbindungen verwenden, um den Client- (Daten-) Traffic zu verbessern.
- Ein Cluster kann ohne Datennetzwerkverbindungen erstellt werden, muss aber eine Cluster-Interconnect-Verbindung enthalten.
- Zu jedem Node sollten immer mindestens zwei Cluster-Verbindungen vorhanden sein.

Weitere Informationen zur Netzwerkverkabelung finden Sie im "AFF und FAS System Documentation Center" und im "Hardware Universe".

Bestimmen Sie die LIF Failover-Richtlinie, die in einem ONTAP-Netzwerk verwendet werden soll

Broadcast-Domänen, Failover-Gruppen und Failover-Richtlinien bestimmen gemeinsam, welcher Port übernommen wird, wenn der Node oder der Port, auf dem eine LIF konfiguriert ist, ausfällt.

Eine Broadcast-Domäne listet alle Ports auf, die im selben Layer-2-Ethernet-Netzwerk erreichbar sind. Ein von einem der Ports gesendete Ethernet-Broadcast-Paket wird von allen anderen Ports in der Broadcast-Domäne angezeigt. Diese gängige Erreichbarkeit einer Broadcast-Domäne ist für LIFs wichtig, da bei einem Failover einer LIF auf einen anderen Port in der Broadcast-Domäne immer noch jeder lokale und Remote Host erreichen könnte, der über den ursprünglichen Port erreichbar war.

Failover-Gruppen definieren die Ports innerhalb einer Broadcast-Domäne, die für sich gegenseitig einen LIF Failover-Schutz bieten. Jede Broadcast-Domäne besitzt eine Failover-Gruppe, die alle Ports beinhaltet. Diese Failover-Gruppe, die alle Ports in der Broadcast-Domäne enthält, ist die Standard- und empfohlene Failover-Gruppe für das LIF. Sie können Failover-Gruppen mit kleineren, von Ihnen definierten Teilmengen erstellen, z. B. eine Failover-Gruppe von Ports, die dieselbe Link-Geschwindigkeit in einer Broadcast-Domäne haben.

Eine Failover-Richtlinie gibt an, wie eine LIF die Ports einer Failover-Gruppe verwendet, wenn ein Node oder Port ausfällt. Betrachten Sie die Failover-Richtlinie als einen Filtertyp, der auf eine Failover-Gruppe angewendet wird. Die Failover-Ziele für eine LIF (der Port-Satz, auf den eine LIF Failover-Ausfallsicherung durchführen kann) werden durch Anwenden der Failover-Richtlinie des LIF auf die Failover-Gruppe der LIF in der Broadcast-Domäne bestimmt.

Sie können die Failover-Ziele für ein LIF mit dem folgenden CLI-Befehl anzeigen:

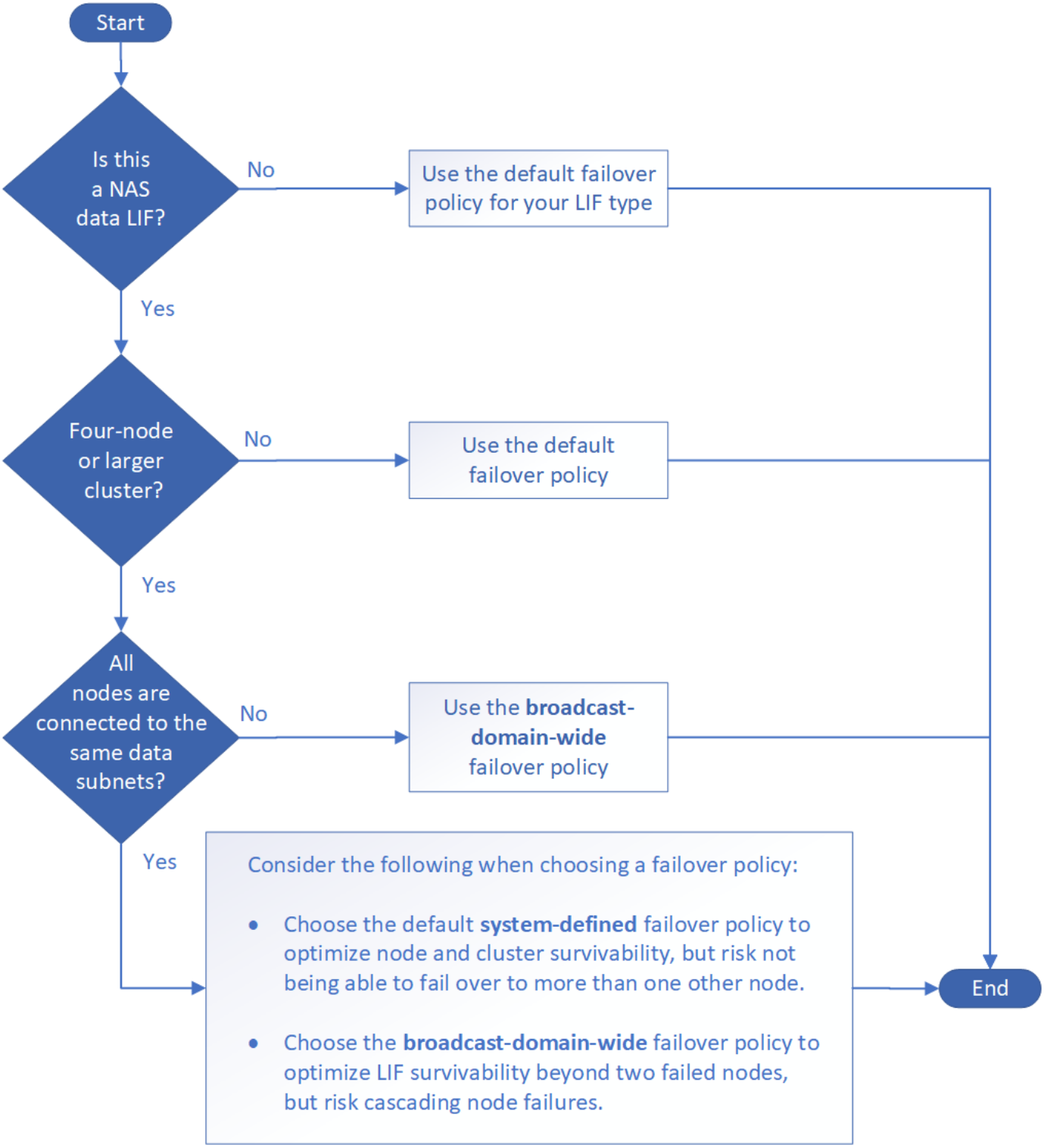
```
network interface show -failover
```

NetApp empfiehlt besonders die Verwendung der Standard-Failover-Richtlinie für Ihren LIF-Typ.

Entscheiden Sie, welche LIF Failover-Richtlinie verwendet werden soll

Entscheiden Sie, ob Sie die empfohlene Standard-Failover-Richtlinie verwenden oder ob Sie diese basierend auf Ihrem LIF-Typ und Ihrer Umgebung ändern sollten.

Entscheidungsbaum für Failover-Richtlinie



Standardmäßige Failover-Richtlinien nach LIF-Typ

LIF-Typ	Standardmäßige Failover-Richtlinie	Beschreibung
BGP LIFs	Deaktiviert	Ein Failover von LIF zu einem anderen Port ist nicht möglich.
Cluster-LIFs	Nur lokal	LIF führt nur ein Failover zu Ports auf demselben Node durch.

Cluster-Management-LIF	Broadcast-Domain Wide	LIF Failover auf Ports in derselben Broadcast-Domäne auf jedem Node im Cluster
Intercluster LIFs	Nur lokal	LIF führt nur ein Failover zu Ports auf demselben Node durch.
NAS-Daten-LIFs	Systemdefiniert	LIF Failover auf einen anderen Node, der nicht der HA-Partner ist.
Node-Management-LIFs	Nur lokal	LIF führt nur ein Failover zu Ports auf demselben Node durch.
SAN-Daten-LIFs	Deaktiviert	Ein Failover von LIF zu einem anderen Port ist nicht möglich.

Die Failover-Richtlinie „nur sfo-Partner“ ist keine Standardeinstellung, kann aber verwendet werden, wenn die LIF ein Failover auf einen Port am Home-Node oder SFO-Partner durchführen soll.

Verwandte Informationen

- "Netzwerkschnittstelle wird angezeigt"

NAS-Pfad-Failover-Workflow

Konfigurieren Sie das Failover des NAS-Pfads auf dem ONTAP-Netzwerk

Wenn Sie bereits mit grundlegenden Netzwerkkonzepten vertraut sind, können Sie die Einrichtung Ihres Netzwerks unter Umständen durch Überprüfung dieses praktischen Workflows für die NAS-Pfad-Failover-Konfiguration sparen.

Der Workflow für die Konfiguration von NAS-Pfad-Failover unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie NAS-Failover auf einem Netzwerk konfigurieren müssen, auf dem ONTAP 9.7 und früher ausgeführt wird, lesen Sie den Workflow "Failover-Workflow für NAS-Pfade (ONTAP 9.7 und früher)".

Eine NAS-LIF migriert automatisch zu einem noch intakten Netzwerk-Port, nachdem ein Verbindungsausfall auf seinem aktuellen Port auftritt. Sie können sich darauf verlassen, dass die ONTAP Standardeinstellungen das Pfad-Failover managen.

Eine SAN-LIF wird nicht migriert (es sei denn, Sie verschieben sie nach dem Link-Ausfall manuell). Stattdessen wird durch Multipathing-Technologie auf dem Host Datenverkehr an eine andere LIF umgeleitet. Weitere Informationen finden Sie unter "SAN Administration".

1 **"Füllen Sie das Arbeitsblatt aus"**

Verwenden Sie das Arbeitsblatt, um NAS-Pfad-Failover zu planen.

2 **"Erstellen von IPspaces"**

Erstellung eines eigenen IP-Adressraums für jede SVM in einem Cluster

3 **"Verschieben von Broadcast-Domänen in IPspaces"**

Verschieben Sie Broadcast-Domänen in IPspaces.

4 **"SVMs erstellen"**

SVMs erstellen, um Kunden Daten bereitzustellen

5 **"Erstellen Sie die LIFs"**

Erstellen Sie LIFs an den Ports, die Sie für den Datenzugriff verwenden möchten.

6 **"Konfigurieren Sie die DNS-Services für die SVM"**

Konfigurieren Sie DNS-Services für die SVM, bevor Sie einen NFS- oder SMB-Server erstellen.

Arbeitsblatt für NAS-Pfad-Failover im ONTAP-Netzwerk

Sie sollten alle Abschnitte des Arbeitsblatts ausfüllen, bevor Sie den NAS-Pfad-Failover konfigurieren.

Die Informationen für NAS-Failover im ONTAP-Netzwerk unterscheiden sich in ONTAP 9.7 und früheren Versionen. Wenn Sie NAS-Failover auf einem Netzwerk konfigurieren müssen, auf dem ONTAP 9.7 und früher ausgeführt wird, finden Sie "Arbeitsblatt für die NAS-Pfad-Failover-Konfiguration (ONTAP 9.7 und früher)"weitere Informationen unter .

Konfiguration von IPspace

IPspaces können verwendet werden, um für jede SVM in einem Cluster einen eigenen IP-Adressbereich zu erstellen. So können Clients in administrativ getrennten Netzwerkdomänen unter Verwendung überlappender IP-Adressbereiche aus demselben IP-Adressbereich des Subnetzes auf Cluster-Daten zugreifen.

Informationsdaten	Erforderlich?	Ihre Werte
IPspace Name die eindeutige Kennung des IPspace.	Ja.	

Konfiguration der Broadcast-Domäne

Eine Broadcast-Domänengruppe-Ports, die im selben Layer-2-Netzwerk gehören und die MTU für die Broadcast-Domain-Ports festlegt.

Broadcast-Domänen werden einem IPspace zugewiesen. Ein IPspace kann eine oder mehrere Broadcast-Domänen enthalten.

Der Port, über den eine LIF ausfällt, muss Mitglied der Failover-Gruppe für die LIF sein. Für jede von ONTAP erstellte Broadcast-Domäne wird zudem eine Failover-Gruppe mit demselben Namen erstellt, die alle Ports in der Broadcast-Domäne enthält.

Informationsdaten	Erforderlich?	Ihre Werte
IPspace Name der IPspace, dem die Broadcast-Domäne zugewiesen ist. Dieser IPspace muss vorhanden sein.	Ja.	
Broadcast-Domain Name der Name der Broadcast-Domain. Dieser Name muss im IPspace eindeutig sein.	Ja.	
MTU der maximale Wert der Übertragungseinheit für die Broadcast-Domäne, der normalerweise auf **1500** oder **9000** eingestellt ist. Der MTU-Wert wird auf alle Ports in der Broadcast-Domäne und alle Ports angewendet, die später der Broadcast-Domäne hinzugefügt werden. Der MTU-Wert sollte mit allen Geräten übereinstimmen, die mit diesem Netzwerk verbunden sind. Beachten Sie, dass für das Management des Ports und für den Traffic der Service-Prozessor (E0M) die MTU nicht mehr als 1500 Byte eingestellt sein sollte.	Ja.	
Ports Ports werden Broadcast-Domänen basierend auf der Erreichbarkeit zugewiesen. Überprüfen Sie nach Abschluss der Portzuweisung `network port reachability show` die Erreichbarkeit, indem Sie den Befehl ausführen. Es können sich bei diesen Ports um physische Ports, VLANs oder Interface Groups handeln. Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".	Ja.	

Subnetz-Konfiguration

Ein Subnetz enthält Pools mit IP-Adressen und ein Standard-Gateway, das LIFs zugewiesen werden kann, die von SVMs im IPspace verwendet werden.

- Beim Erstellen eines LIF auf einer SVM können Sie den Namen des Subnetzes angeben, anstatt eine IP-Adresse und ein Subnetz bereitzustellen.
- Da ein Subnetz mit einem Standard-Gateway konfiguriert werden kann, müssen Sie beim Erstellen einer SVM nicht in einem separaten Schritt das Standard-Gateway erstellen.

- Eine Broadcast-Domäne kann ein oder mehrere Subnetze enthalten.
- Sie können SVM-LIFs, die sich in unterschiedlichen Subnetzen befinden, konfigurieren, indem Sie mehr als ein Subnetz mit der Broadcast-Domäne des IPspaces zuordnen.
- Jedes Subnetz muss IP-Adressen enthalten, die sich nicht mit IP-Adressen überschneiden, die anderen Subnetzen im gleichen IPspace zugewiesen sind.
- Sie können SVM-Daten-LIFs bestimmte IP-Adressen zuweisen und anstelle eines Subnetzes ein Standard-Gateway für die SVM erstellen.

Informationsdaten	Erforderlich?	Ihre Werte
IPspace Name der IPspace, dem das Subnetz zugewiesen wird. Dieser IPspace muss vorhanden sein.	Ja.	
Subnetz Name der Name des Subnetzes. Dieser Name muss im IPspace eindeutig sein.	Ja.	
Broadcast-Domänenname die Broadcast-Domäne, der das Subnetz zugewiesen wird. Diese Broadcast-Domäne muss sich im angegebenen IPspace befinden.	Ja.	
Subnetzname und Maskierung des Subnetzes und der Maske, in der sich die IP-Adressen befinden.	Ja.	
Gateway Sie können ein Standard-Gateway für das Subnetz angeben. Wenn Sie beim Erstellen des Subnetzes kein Gateway zuweisen, können Sie es später zuweisen.	Nein	
IP-Adressbereiche Sie können einen Bereich von IP-Adressen oder spezifischen IP-Adressen angeben. Sie können beispielsweise einen Bereich angeben, z. B.: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` Wenn Sie keinen IP-Adressbereich angeben, können Sie LIFs den gesamten Bereich der IP-Adressen im angegebenen Subnetz zuweisen.	Nein	

Erzwingen des Updates von LIF-Zuordnungen legt fest, ob das Update von vorhandenen LIF-Zuordnungen erzwingen soll. Standardmäßig schlägt die Subnet-Erstellung fehl, wenn Service-Prozessor-Schnittstellen oder Netzwerkschnittstellen die IP-Adressen in den angegebenen Bereichen verwenden. Mit diesem Parameter werden alle manuell adressierten Schnittstellen mit dem Subnetz verknüpft und der Befehl kann erfolgreich ausgeführt werden.	Nein	

SVM-Konfiguration

Mit SVMs werden Clients und Hosts mit Daten versorgen.

Die von Ihnen aufzeichnenden Werte lauten für das Erstellen einer Standard-Daten-SVM. Wenn Sie eine MetroCluster-Quell-SVM erstellen, lesen Sie die "Installations- und Konfigurationshandbuch für Fabric-Attached MetroCluster" oder "Installations- und Konfigurationshandbuch für Stretch MetroCluster".

Informationsdaten	Erforderlich?	Ihre Werte
Geben Sie der SVM den vollständig qualifizierten Domain-Namen (FQDN) der SVM an. Dieser Name muss für Cluster-Ligen eindeutig sein.	Ja.	
Root-Volume Name des SVM-Root-Volumes.	Ja.	
Aggregat benennen Sie den Namen des Aggregats, in dem das SVM Root-Volume enthalten ist. Dieses Aggregat muss vorhanden sein.	Ja.	
Sicherheitstyp für den Sicherheitsstil für das SVM Root-Volume Mögliche Werte sind **ntfs**, **unix** und **gemischt**.	Ja.	
IPspace benennen den IPspace, dem die SVM zugewiesen ist. Dieser IPspace muss vorhanden sein.	Nein	
SVM-Sprache zur Festlegung der Standardsprache für die SVM und ihre Volumes. Wenn Sie keine Standardsprache angeben, wird die Standard-SVM-Sprache auf **C.UTF-8** gesetzt. Die Spracheinstellung der SVM bestimmt den Zeichensatz, mit dem Dateinamen und Daten aller NAS-Volumes in der SVM angezeigt werden. Sie können die Sprache nach dem Erstellen der SVM ändern.	Nein	

LIF-Konfiguration

Eine SVM stellt Daten für Clients und Hosts über eine oder mehrere logische Netzwerkschnittstellen (LIFs) bereit.

Informationsdaten	Erforderlich?	Ihre Werte
SVM benennen Sie den Namen der SVM für das LIF.	Ja.	
LIF nennt den Namen des LIF. Sie können pro Node mehrere Daten-LIFs zuweisen und jedem Node im Cluster LIFs zuweisen, sofern der Node über verfügbare Daten-Ports verfügt. Um Redundanz zu gewährleisten, sollten Sie mindestens zwei Daten-LIFs für jedes Daten-Subnetz erstellen, und die einem bestimmten Subnetz zugewiesenen LIFs sollten Home-Ports auf unterschiedlichen Nodes zugewiesen werden. **Wichtig:** Wenn Sie einen SMB-Server für das Hosting von Hyper-V oder SQL Server über SMB konfigurieren, um Lösungen für unterbrechungsfreien Betrieb zu ermöglichen, muss die SVM auf jedem Node im Cluster mindestens eine Daten-LIF haben.	Ja.	
Service-Richtlinie für LIF. Die Service-Richtlinie definiert, welche Netzwerkservices die LIF verwenden können. Für das Management des Daten- und Managementdatenverkehrs auf Daten- und System-SVMs stehen integrierte Services und Service-Richtlinien zur Verfügung.	Ja.	
Zulässige Protokolle IP-basierte LIFs benötigen keine zugelassenen Protokolle. Verwenden Sie stattdessen die Service-Richtlinien-Zeile. Legen Sie die zulässigen Protokolle für SAN LIFs auf FibreChannel-Ports fest. Dies sind die Protokolle, die diese LIF verwenden können. Die Protokolle, die das LIF verwenden, können nach Erstellen des LIF nicht mehr geändert werden. Sie sollten beim Konfigurieren des LIF alle Protokolle angeben.	Nein	
Home-Node, der Node, auf den die LIF zurückgibt, wenn das LIF auf seinen Home-Port zurückgesetzt wird. Sie sollten für jede Daten-LIF einen Home-Node aufzeichnen.	Ja.	

Home Port oder Broadcast Domain wählen eine der folgenden Optionen: **Port**: Geben Sie den Port an, zu dem die logische Schnittstelle zurückkehrt, wenn die LIF wieder auf ihren Home-Port zurückgesetzt wird. Dies erfolgt nur für die erste LIF im Subnetz eines IPspace, ansonsten ist dies nicht erforderlich. **Broadcast Domain**: Geben Sie die Broadcast-Domain an, und das System wählt den entsprechenden Port aus, auf den die logische Schnittstelle zurückkehrt, wenn das LIF auf seinen Home-Port zurückgesetzt wird.	Ja.	
Subnetz Name das Subnetz, das der SVM zugewiesen werden soll. Alle Daten-LIFs, die zur Erstellung kontinuierlich verfügbarer SMB-Verbindungen zu Applikations-Servern verwendet werden, müssen sich im selben Subnetz befinden.	Ja (bei Verwendung eines Subnetzes)	

DNS-Konfiguration

Vor der Erstellung eines NFS- oder SMB-Servers müssen Sie DNS auf der SVM konfigurieren.

Informationsdaten	Erforderlich?	Ihre Werte
Geben Sie den Namen der SVM an, auf der Sie einen NFS- oder SMB-Server erstellen möchten.	Ja.	
DNS-Domain-Name Eine Liste der Domänennamen, die bei der Durchführung der Host-to-IP-Namensauflösung an einen Host-Namen angehängt werden sollen. Geben Sie zuerst die lokale Domäne an, gefolgt von den Domänennamen, für die am häufigsten DNS-Abfragen erstellt werden.	Ja.	

IP-Adressen der DNS-Server Liste der IP-Adressen für die DNS-Server, die eine Namensauflösung für den NFS- oder SMB-Server liefern. Die aufgeführten DNS-Server müssen die Datensätze für den Servicesort (SRV) enthalten, die erforderlich sind, um die Active Directory-LDAP-Server und Domänencontroller für die Domäne zu finden, der der SMB-Server Beitritt. Der SRV-Datensatz wird verwendet, um den Namen eines Dienstes dem DNS-Computernamen eines Servers zuzuordnen, der diesen Dienst anbietet. Die Erstellung von SMB-Servern schlägt fehl, wenn ONTAP die Datensätze des Service-Speicherorts nicht durch lokale DNS-Abfragen abrufen kann. Die einfachste Möglichkeit, sicherzustellen, dass ONTAP die Active Directory SRV-Einträge finden kann, besteht darin, Active Directory-integrierte DNS-Server als SVM-DNS-Server zu konfigurieren. Sie können nicht-Active Directory-integrierte DNS-Server verwenden, sofern der DNS-Administrator die SRV-Datensätze manuell zur DNS-Zone hinzugefügt hat, die Informationen zu den Active Directory-Domänencontrollern enthält. Weitere Informationen zu den in Active Directory integrierten SRV-Datensätzen finden Sie im Thema "Die Funktionsweise von DNS-Unterstützung für Active Directory auf Microsoft TechNet".	Ja.	

Dynamische DNS-Konfiguration

Bevor Sie dynamische DNS verwenden können, um automatisch DNS-Einträge zu Ihren in Active Directory integrierten DNS-Servern hinzuzufügen, müssen Sie dynamisches DNS (DDNS) auf der SVM konfigurieren.

Für jede Daten-LIF auf der SVM werden DNS-Einträge erstellt. Durch das Erstellen mehrerer Daten-LIFS auf der SVM können Sie Client-Verbindungen zu den zugewiesenen Daten-IP-Adressen laden. DNS Load gleicht Verbindungen aus, die über den Hostnamen zu den zugewiesenen IP-Adressen erstellt werden, nach Round-Robin-Verfahren aus.

Informationsdaten	Erforderlich?	Ihre Werte
Benennen Sie die SVM, auf der Sie einen NFS- oder SMB-Server erstellen möchten.	Ja.	
Ob DDNS verwendet werden soll, gibt an, ob DDNS verwendet werden soll. Die auf der SVM konfigurierten DNS-Server müssen DDNS unterstützen. DDNS ist standardmäßig deaktiviert.	Ja.	

Ob Secure DDNS Secure DDNS verwendet werden soll, wird nur mit Active Directory-integriertem DNS unterstützt. Wenn Ihr in Active Directory integriertes DNS nur sichere DDNS-Updates erlaubt, muss der Wert für diesen Parameter wahr sein. Secure DDNS ist standardmäßig deaktiviert. Secure DDNS kann erst aktiviert werden, nachdem ein SMB-Server oder ein Active Directory-Konto für die SVM erstellt wurde.	Nein	
FQDN der DNS-Domäne der FQDN der DNS-Domäne. Sie müssen denselben Domänennamen verwenden, der für die DNS-Namensservices auf der SVM konfiguriert ist.	Nein	

Netzwerkports

Erfahren Sie mehr über die ONTAP-Netzwerk-Port-Konfiguration

Es handelt sich entweder um physische Ports (NICs) oder virtualisierte Ports, wie z. B. Interface Groups oder VLANs.

Virtuelle lokale Netzwerke (VLANs) und Interface Groups bilden die virtuellen Ports. Schnittstellengruppen behandeln mehrere physische Ports als einen einzelnen Port, während VLANs einen physischen Port in mehrere separate logische Ports unterteilen.

- Physische Ports: LIFs können direkt auf physischen Ports konfiguriert werden.
- Schnittstellengruppe: Ein Portaggregat mit zwei oder mehr physischen Ports, die als einzelner Trunk-Port fungieren. Eine Schnittstellengruppe kann Single-Mode, Multimode oder dynamischer Multimode sein.
- VLAN: Ein logischer Port, der Datenverkehr mit VLAN-Tags empfängt und sendet (IEEE 802.1Q Standard). Zu den VLAN-Port-Merkmalen gehört die VLAN-ID für den Port. Die zugrunde liegenden Ports der physischen Ports oder der Ports der Schnittstellengruppen werden als VLAN-Trunk-Ports betrachtet und die verbundenen Switch-Ports müssen so konfiguriert werden, dass sie als Trunk-Port für die VLAN-IDs konfiguriert werden.

  Der zugrunde liegende physische Port oder Schnittstellen-Gruppen-Ports für einen VLAN-Port können weiterhin LIFs hosten, die Datenverkehr ohne Tags übertragen und empfangen.

- Virtueller IP-Port (VIP): Ein logischer Port, der als Home-Port für ein VIP LIF verwendet wird. VIP-Ports werden automatisch vom System erstellt und unterstützen nur eine begrenzte Anzahl von Operationen. VIP-Ports werden ab ONTAP 9.5 unterstützt.

Die Namenskonvention für den Port ist *enumberletter*:

- Das erste Zeichen beschreibt den Porttyp. „E“ steht für Ethernet.
- Das zweite Zeichen gibt den nummerierten Steckplatz an, in dem sich der Port-Adapter befindet.
- Das dritte Zeichen gibt die Position des Ports an einem Mehrport-Adapter an. „A“ zeigt den ersten Port an, „b“ gibt den zweiten Port an, usw.

`e0b`Zeigt beispielsweise an, dass ein Ethernet-Port der zweite Port auf der Hauptplatine des Node ist.

VLANs müssen mit der Syntax benannt werden `port_name-vlan-id`.

`port_name` Gibt den physischen Port oder die Schnittstellengruppe an.

`vlan-id` Gibt die VLAN-Identifizierung im Netzwerk an. `e1c-80`Ist beispielsweise ein gültiger VLAN-Name.

Konfigurieren Sie Netzwerkports

Kombinieren Sie physische Ports, um ONTAP-Schnittstellengruppen zu erstellen

Eine Interface Group, auch bekannt als Link Aggregation Group (LAG), wird erstellt, indem zwei oder mehr physische Ports auf demselben Node zu einem einzigen logischen Port kombiniert werden. Der logische Port bietet erhöhte Ausfallsicherheit, höhere Verfügbarkeit und gemeinsame Nutzung von Lasten.

Schnittstellengruppen Typen

Das Speichersystem unterstützt drei Typen von Schnittstellengruppen: Single-Mode, statisches Multimode und dynamisches Multimode. Jede Schnittstellengruppe verfügt über verschiedene Fehlertoleranz. Multimode-Schnittstellengruppen bieten Methoden zum Lastausgleich des Netzwerkdatenverkehrs.

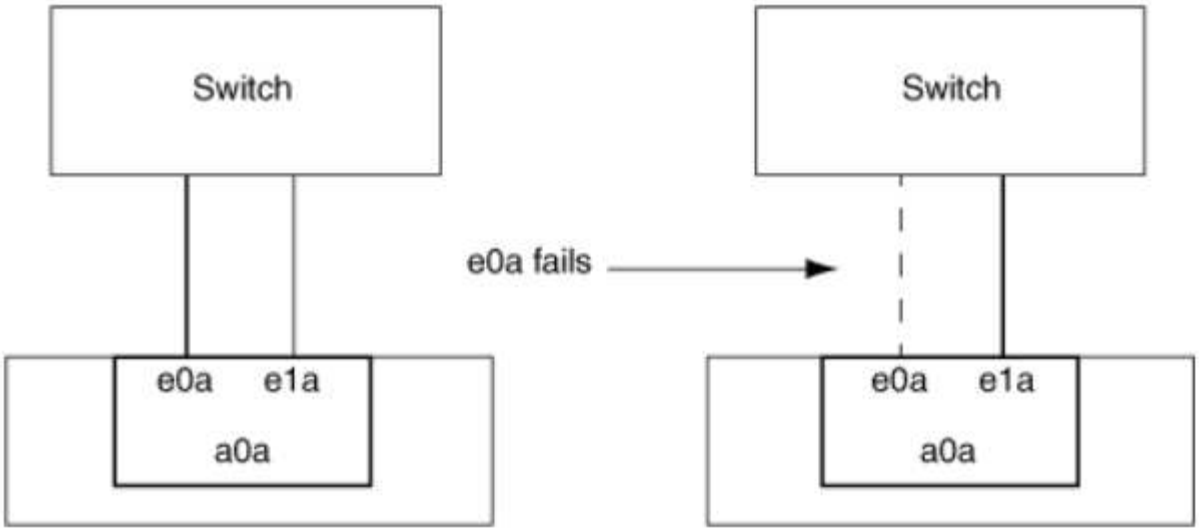
Merkmale von Single-Mode-Schnittstellengruppen

In einer Single-Mode-Schnittstellengruppe ist nur eine der Schnittstellen in der Schnittstellengruppe aktiv. Die anderen Schnittstellen befinden sich im Standby-Modus und können bei Ausfall der aktiven Schnittstelle übernehmen.

Merkmale einer Single-Mode-Schnittstellengruppen:

- Für den Failover überwacht der Cluster die aktive Verbindung und steuert den Failover. Da das Cluster die aktive Verbindung überwacht, ist keine Switch-Konfiguration erforderlich.
- Es kann mehrere Schnittstellen im Standby-Modus in einer Single-Mode-Schnittstellengruppe vorhanden sein.
- Wenn eine Single-Mode-Schnittstellengruppe mehrere Switches umfasst, müssen Sie die Switches mit einem Inter-Switch-Link (ISL) verbinden.
- Bei einer Single-Mode-Schnittstellengruppe müssen sich die Switch-Ports in derselben Broadcast-Domäne befinden.
- Link-Monitoring ARP-Pakete, die eine Quelladresse von 0.0.0.0 haben, werden über die Ports gesendet, um zu überprüfen, ob sich die Ports in derselben Broadcast-Domäne befinden.

In der folgenden Abbildung ist ein Beispiel einer Interface-Gruppe mit einem Single-Mode dargestellt. In der Abbildung sind e0a und e1a Teil der single-Mode Interface Group a0a. Wenn die aktive Schnittstelle e0a ausfällt, übernimmt die Standby e1a Schnittstelle die Übernahme und hält die Verbindung zum Switch aufrecht.



Um Single-Mode-Funktionalität durchzuführen, wird empfohlen, statt Failover-Gruppen zu verwenden. Durch Verwendung einer Failover-Gruppe kann der zweite Port weiterhin für andere LIFs verwendet werden und muss nicht ungenutzt bleiben. Darüber hinaus können Failover-Gruppen mehr als zwei Ports umfassen und Ports auf mehrere Nodes umfassen.

Merkmale statischer Multimode-Schnittstellengruppen

Die Implementierung der statischen Multimode-Schnittstellengruppen in ONTAP entspricht IEEE 802.3ad (statisch). Jeder Switch, der Aggregate unterstützt, aber keinen Austausch von Kontrollpaketen zur Konfiguration eines Aggregats bietet, kann mit statischen Multimode-Schnittstellengruppen verwendet werden.

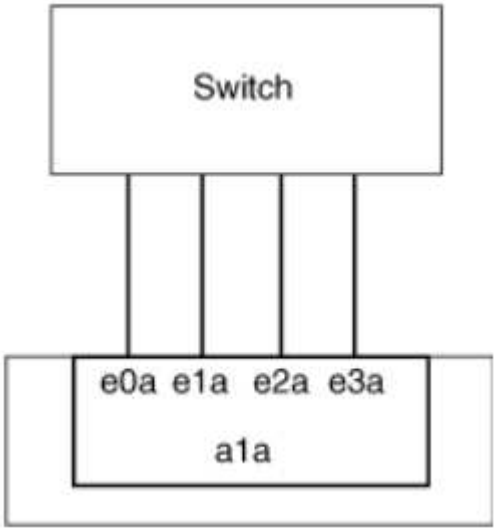
Statische Multimode-Schnittstellengruppen erfüllen nicht IEEE 802.3ad (dynamisch), auch bekannt als Link Aggregation Control Protocol (LACP). LACP entspricht dem Port Aggregation Protocol (PagP), dem proprietären Link-Aggregation-Protokoll von Cisco.

Die folgenden Merkmale sind Merkmale einer statischen Multimode-Schnittstellengruppen:

- Alle Schnittstellen in der Schnittstellengruppe sind aktiv und nutzen eine einzige MAC-Adresse.
  - Mehrere einzelne Verbindungen werden auf die Schnittstellen in der Schnittstellengruppe verteilt.
  - Jede Verbindung oder Sitzung nutzt eine Schnittstelle innerhalb der Schnittstellengruppe. Wenn Sie das sequenzielle Lastenausgleichsschema verwenden, werden alle Sitzungen auf Paket-für-Paket-Basis über verfügbare Links verteilt und sind nicht an eine bestimmte Schnittstelle von der Schnittstellengruppe gebunden.
- Statische Multimode-Schnittstellengruppen können nach einem Ausfall von bis zu „n-1“-Schnittstellen wiederherstellen, wobei n die Gesamtzahl der Schnittstellen ist, die die Schnittstellengruppe bilden.
- Wenn ein Port ausfällt oder nicht angeschlossen ist, wird der Datenverkehr, der die fehlerhafte Verbindung durchlaufen hat, automatisch an eine der verbleibenden Schnittstellen verteilt.
- Statische Multimode-Schnittstellengruppen können einen Verbindungsverlust erkennen, aber sie können keinen Verlust der Verbindung zum Client oder Switch-Fehlkonfigurationen erkennen, die sich auf Konnektivität und Leistung auswirken können.
- Eine statische Multimode-Schnittstellengruppe erfordert einen Switch, der eine Link-Aggregation über mehrere Switch-Ports unterstützt. Der Switch ist so konfiguriert, dass alle Ports, mit denen Links einer Schnittstellengruppe verbunden sind, Teil eines einzigen logischen Ports sind. Einige Switches unterstützen möglicherweise keine Link-Aggregation von Ports, die für Jumbo Frames konfiguriert sind. Weitere Informationen finden Sie in der Dokumentation des Switch-Anbieters.

- Zur Verteilung des Datenverkehrs auf die Schnittstellen einer statischen Multimode-Schnittstellengruppe stehen mehrere Optionen zur Lastverteilung zur Verfügung.

Die folgende Abbildung zeigt ein Beispiel für eine statische Multimode-Schnittstellengruppen. Die Schnittstellen e0a, e1a, e2a und e3a sind Teil der a1a Multimode-Schnittstellengruppe. Alle vier Schnittstellen in der a1a Multimode-Schnittstellengruppe sind aktiv.



Es gibt mehrere Technologien, die es ermöglichen, Datenverkehr in einer einzelnen aggregierten Verbindung über mehrere physische Switches zu verteilen. Die Technologien, die diese Funktion ermöglichen, variieren zwischen den Netzwerkprodukten. Statische Multimode-Schnittstellengruppen in ONTAP entsprechen den IEEE 802.3-Standards. Wenn eine bestimmte Technologie zur Aggregation von mehreren Switches mit den IEEE 802.3 Standards interoperabel oder entspricht, sollte sie mit ONTAP betrieben werden.

Der IEEE 802.3-Standard besagt, dass das Übertragungsgerät in einer aggregierten Verbindung die physische Schnittstelle für die Übertragung bestimmt. Daher ist ONTAP nur für die Verteilung von Outbound-Datenverkehr verantwortlich und kann nicht kontrollieren, wie eingehende Frames eintreffen. Wenn Sie die Übertragung des eingehenden Datenverkehrs über eine aggregierte Verbindung verwalten oder steuern möchten, muss diese Übertragung auf dem direkt angeschlossenen Netzwerkgerät geändert werden.

Dynamische Multimode-Schnittstellengruppen

Dynamic Multimode Interface Groups implementieren Link Aggregation Control Protocol (LACP), um eine Gruppenmitgliedschaft an den direkt angeschlossenen Switch zu kommunizieren. LACP ermöglicht es Ihnen, den Verlust des Link-Status zu erkennen und nicht die Möglichkeit, vom Node mit dem Direct-Attached Switch-Port zu kommunizieren.

Die Implementierung von Dynamic Multimode-Schnittstellengruppen in ONTAP entspricht IEEE 802.3 AD (802.1 AX). ONTAP unterstützt nicht das Port Aggregation Protocol (PagP), welches ein proprietäres Link Aggregation-Protokoll von Cisco ist.

Eine dynamische Multimode-Schnittstellengruppen erfordert einen Switch, der LACP unterstützt.

ONTAP implementiert LACP im nicht konfigurierbaren aktiv-Modus, das gut für Switches geeignet ist, die entweder im aktiven oder im passiven Modus konfiguriert sind. ONTAP implementiert die langen und kurzen LACP-Timer (zur Verwendung mit nicht konfigurierbaren Werten 3 Sekunden und 90 Sekunden), wie in IEEE 802.3 AD (802.1AX) angegeben.

Der ONTAP-Load-Balancing-Algorithmus bestimmt den Mitgliedsport, der für die Übertragung von Outbound-

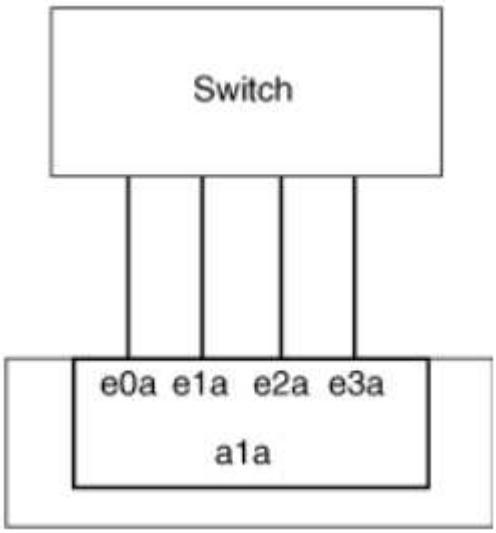
Datenverkehr verwendet werden soll, und steuert nicht, wie eingehende Frames empfangen werden. Der Switch bestimmt das Mitglied (individueller physischer Port) seiner Port-Channel-Gruppe, das für die Übertragung verwendet werden soll, basierend auf dem Lastausgleichsalgorithmus, der in der Port-Channel-Gruppe des Switches konfiguriert ist. Daher bestimmt die Switch-Konfiguration den Mitgliedsport (individueller physischer Port) des Speichersystems, über den Datenverkehr empfangen wird. Weitere Informationen zum Konfigurieren des Switches finden Sie in der Dokumentation Ihres Switch-Anbieters.

Wenn eine individuelle Schnittstelle aufeinanderfolgende LACP Protokollpakete nicht empfängt, wird diese individuelle Schnittstelle im Befehl „iffrp Status“ als „lag_inaktiv“ markiert. Vorhandener Datenverkehr wird automatisch an alle verbleibenden aktiven Schnittstellen umgeleitet.

Bei der Verwendung von dynamischen Multimode-Schnittstellengruppen gelten die folgenden Regeln:

- Dynamische Multimode-Schnittstellengruppen sollten so konfiguriert werden, dass sie die portbasierten, IP-basierten, MAC-basierten oder Round-Robin-Lastausgleichmethoden verwenden.
- In einer dynamischen Multimode-Schnittstellengruppe müssen alle Schnittstellen aktiv sein und eine einzelne MAC-Adresse gemeinsam nutzen.

Die folgende Abbildung zeigt ein Beispiel für eine dynamische Multimode-Schnittstellengruppen. Die Schnittstellen e0a, e1a, e2a und e3a sind Teil der a1a Multimode-Schnittstellengruppe. Alle vier Schnittstellen in der dynamischen multimodus-Schnittstellengruppe a1a sind aktiv.



Lastausgleich in Multimode-Schnittstellengruppen

Sie können sicherstellen, dass alle Schnittstellen einer Multimode-Schnittstellengruppe für ausgehenden Datenverkehr gleichermaßen verwendet werden, indem Sie die Methoden IP-Adresse, MAC-Adresse, sequenzieller oder portbasierter Lastverteilung verwenden, um den Netzwerkverkehr gleichmäßig über die Netzwerkports einer Multimode-Schnittstellengruppe zu verteilen.

Die Lastausgleichsmethode für eine Multimode-Schnittstellengruppe kann nur angegeben werden, wenn die Schnittstellengruppe erstellt wird.

Best Practice: Port-basierter Lastenausgleich wird empfohlen, wann immer möglich. Verwenden Sie den portbasierten Lastenausgleich, es sei denn, es gibt einen bestimmten Grund oder eine Einschränkung im Netzwerk, die dies verhindert.

Port-basierter Lastausgleich

Ein Port-basierter Lastausgleich ist die empfohlene Methode.

Mithilfe der portbasierten Lastausgleichmethode können Sie den Datenverkehr auf einer Multimode-Schnittstellengruppen basierend auf den TCP/UDP-Ports (Transport Layer) ausgleichen.

Die portbasierte Lastausgleichsmethode verwendet einen schnellen Hashing-Algorithmus auf den Quell- und Ziel-IP-Adressen zusammen mit der Port-Nummer der Transportschicht.

IP-Adresse und Lastausgleich für MAC-Adressen

IP-Adresse und MAC-Adressenlastausgleich sind die Methoden zur Gleichsetzung des Datenverkehrs auf Multimode-Schnittstellengruppen.

Diese Lastausgleichmethoden verwenden einen schnellen Hashing-Algorithmus an den Quell- und Zieladressen (IP-Adresse und MAC-Adresse). Wenn das Ergebnis des Hashing-Algorithmus einer Schnittstelle zugeordnet wird, die sich nicht im UP-Link-Status befindet, wird die nächste aktive Schnittstelle verwendet.

Wählen Sie beim Erstellen von Schnittstellengruppen auf einem System, das eine direkte Verbindung mit einem Router herstellt, nicht die Methode zum Lastausgleich der MAC-Adresse aus. In einem solchen Setup ist für jeden ausgehenden IP-Frame die Ziel-MAC-Adresse die MAC-Adresse des Routers. Daher wird nur eine Schnittstelle der Schnittstellengruppe verwendet.

Das Load Balancing für IP-Adressen funktioniert sowohl bei IPv4- als auch bei IPv6-Adressen auf die gleiche Weise.

Sequenzieller Lastausgleich

Mithilfe des sequenziellen Lastenausgleichs können Sie Pakete über einen Round-Robin-Algorithmus gleichmäßig auf mehrere Links verteilen. Mit der sequenziellen Option können Sie den Datenverkehr einer einzelnen Verbindung über mehrere Links verteilen, um den Durchsatz einer einzelnen Verbindung zu erhöhen.

Da ein sequenzieller Lastausgleich jedoch zu Paketübermittlung bei unzureichender Bestellung führen kann, kann dies zu einer extrem schlechten Performance führen. Daher wird ein sequentieller Lastenausgleich in der Regel nicht empfohlen.

Erstellen einer Interface Group oder LAG

Sie können eine Schnittstellengruppe oder LAG erstellen – Single-Mode, statischer Multimode oder dynamisches Multimode (LACP) –, um Clients eine einzige Schnittstelle bereitzustellen, indem Sie die Funktionen der aggregierten Netzwerk-Ports kombinieren.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um EINE VERZÖGERUNG zu erstellen

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > + Link Aggregation Group**, um EINE LAG zu erstellen.
2. Wählen Sie den Knoten aus der Dropdown-Liste aus.
3. Wählen Sie eine der folgenden Optionen:
   a. ONTAP to **Broadcast-Domain automatisch auswählen (empfohlen)**.
   b. So wählen Sie eine Broadcast-Domäne manuell aus:
4. Wählen Sie die Ports aus, um DIE VERZÖGERUNG zu bilden.
5. Wählen Sie den Modus:
   a. Single: Es wird jeweils nur ein Port verwendet.
   b. Mehrere: Alle Ports können gleichzeitig verwendet werden.
   c. LACP: Das LACP-Protokoll bestimmt die Ports, die verwendet werden können.
6. Wählen Sie den Lastenausgleich aus:
   a. IP-basiert
   b. MAC-basiert
   c. Port
   d. Sequenziell
7. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um eine Schnittstellengruppe zu erstellen

Beim Erstellen einer Multimode-Schnittstellengruppen können Sie eine der folgenden Load-Balancing-Methoden angeben:

- `port`: Der Netzwerkverkehr wird auf Basis der Ports der Transportschicht (TCP/UDP) verteilt. Dies ist die empfohlene Methode zum Lastausgleich.
- `mac`: Der Netzwerkverkehr wird auf Basis von MAC-Adressen verteilt.
- `ip`: Der Netzwerkverkehr wird auf Basis von IP-Adressen verteilt.
- `sequential`: Der Netzwerkverkehr wird so verteilt, wie er empfangen wird.

Die MAC-Adresse einer Schnittstellengruppe wird durch die Reihenfolge der zugrunde liegenden Ports bestimmt und wie diese Ports beim Bootup initialisiert werden. Sie sollten daher nicht davon ausgehen, dass die ifgrp MAC-Adresse bei Neustarts oder ONTAP-Upgrades erhalten bleibt.

Schritt

`network port ifgrp create`Erstellen Sie mit dem Befehl eine Schnittstellengruppe.

Schnittstellengruppen müssen mit der Syntax benannt werden `a<number><letter>`. a0a, a0b, a1c und a2a sind gültige Schnittstellengruppennamen.

Erfahren Sie mehr über `network port ifgrp create` in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, wie eine Schnittstellengruppe mit dem Namen a0a mit einer Verteilungsfunktion von Port und Multimode erstellt werden kann:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Fügen Sie einer Schnittstellengruppe oder LAG einen Port hinzu

Sie können bis zu 16 physische Ports zu einer Interface Group oder LAG für alle Port-Geschwindigkeiten hinzufügen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um einen Port zu EINEM LAG hinzuzufügen

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > LAG**, um EINE VERZÖGERUNG zu bearbeiten.
2. Wählen Sie auf demselben Node zusätzliche Ports aus, um die LAG hinzuzufügen.
3. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um Ports zu einer Schnittstellengruppe hinzuzufügen

Schritt

Fügen Sie der Schnittstellengruppe Netzwerkanschlüsse hinzu:

```
network port ifgrp add-port
```

Das folgende Beispiel zeigt, wie Port e0c einer Schnittstellengruppe mit dem Namen a0a hinzugefügt wird:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Ab ONTAP 9.8 werden Schnittstellengruppen automatisch ca. eine Minute nachdem der erste physische Port der Interface Group hinzugefügt wurde, in einer entsprechenden Broadcast-Domäne platziert. Wenn Sie dies nicht möchten, dass ONTAP den ifgrp manuell in eine Broadcast-Domäne platziert, geben Sie den `-skip-broadcast-domain-placement` Parameter als Teil des `ifgrp add-port` Befehls an.

Weitere Informationen zu `network port ifgrp add-port` und Konfigurationsbeschränkungen, die für Port-Schnittstellengruppen gelten, finden Sie im "ONTAP-Befehlsreferenz".

Entfernen Sie einen Port aus einer Schnittstellengruppe oder -LAG

Sie können einen Port von einer Schnittstellengruppe entfernen, die LIFs hostet, solange er nicht der letzte Port in der Schnittstellengruppe ist. Es ist nicht erforderlich, dass die Schnittstellengruppe keine LIFs hosten darf oder dass die Schnittstellengruppe nicht der Home Port einer LIF sein darf, vorausgesetzt, Sie entfernen nicht den letzten Port aus der Schnittstellengruppe. Wenn Sie jedoch den letzten Port entfernen, müssen Sie die LIFs zuerst von der Interface Group migrieren oder verschieben.

Über diese Aufgabe

Sie können bis zu 16 Ports (physische Schnittstellen) aus einer Interface Group oder LAG entfernen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um einen Port aus EINER LAG zu entfernen

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > LAG**, um EINE VERZÖGERUNG zu bearbeiten.
2. Wählen Sie die zu entfernenden Ports aus DER VERZÖGERUNG aus.
3. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um Ports aus einer Schnittstellengruppe zu entfernen

Schritt

Entfernen Sie Netzwerkanschlüsse aus einer Schnittstellengruppe:

```
network port ifgrp remove-port
```

Erfahren Sie mehr über `network port ifgrp remove-port` in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, wie Port e0c aus einer Schnittstellengruppe mit dem Namen a0a entfernt wird:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Löschen einer Schnittstellengruppe oder -VERZÖGERUNG

Sie können Schnittstellengruppen oder LAGs löschen, wenn Sie LIFs direkt auf den zugrunde liegenden physischen Ports konfigurieren oder sich entscheiden, die Schnittstellengruppe, DEN LAG-Modus oder die Verteilungsfunktion zu ändern.

Bevor Sie beginnen

- Die Interface-Gruppe oder LAG darf kein LIF hosten.
- Die Interface-Gruppe oder LAG darf weder der Home-Port noch das Failover-Ziel einer LIF sein.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um EINE VERZÖGERUNG zu löschen

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > LAG**, um EINE VERZÖGERUNG zu löschen.
2. Wählen Sie die VERZÖGERUNG aus, die Sie entfernen möchten.
3. LÖSCHEN Sie DIE VERZÖGERUNG.

CLI

Verwenden Sie die CLI, um eine Schnittstellengruppe zu löschen

Schritt

Mit dem `network port ifgrp delete` Befehl löschen Sie eine Schnittstellengruppe.

Erfahren Sie mehr über `network port ifgrp delete` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird gezeigt, wie eine Schnittstellengruppe mit dem Namen a0b gelöscht wird:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Konfiguration von ONTAP-VLANS über physische Ports

VLANs in ONTAP ermöglichen die logische Segmentierung von Netzwerken durch die Erstellung separater Broadcast-Domänen, die auf Switch-Port-Basis definiert werden und nicht von herkömmlichen Broadcast-Domänen, die an physischen Grenzen definiert werden.

Ein VLAN kann mehrere physische Netzwerksegmente umfassen. Die Endstationen, die zu einem VLAN gehören, werden durch Funktion oder Anwendung verknüpft.

Beispielsweise können Endstationen in einem VLAN nach Abteilungen wie Engineering und Accounting oder nach Projekten wie releas1 und release2 gruppiert werden. Da die physische Nähe der Endstationen in einem VLAN nicht unbedingt erforderlich ist, können Sie die Endstationen geographisch verteilen und die Broadcast-Domäne weiterhin in einem geswitchten Netzwerk enthalten.

In ONTAP 9.14.1 und 9.13.1 werden nicht markierte Ports, die von keiner logischen Schnittstelle (LIF) verwendet werden und denen die native VLAN-Konnektivität auf dem verbundenen Switch fehlt, als beeinträchtigt gekennzeichnet. Dies dient der Identifizierung nicht verwendeter Ports und weist nicht auf einen Ausfall hin. Native VLANs ermöglichen ungetaggten Datenverkehr auf dem ifgrp-Basisport, wie z. ONTAP CFM-Broadcasts. Konfigurieren Sie native VLANs auf dem Switch, um zu verhindern, dass nicht markierter Datenverkehr blockiert wird.

Sie können VLANs verwalten, indem Sie Informationen über sie erstellen, löschen oder anzeigen.

> Sie sollten kein VLAN auf einer Netzwerkschnittstelle mit derselben Kennung wie das native VLAN des Switches erstellen. Wenn beispielsweise die Netzwerkschnittstelle e0b auf nativem VLAN 10 ist, sollten Sie keine VLAN e0b-10 auf dieser Schnittstelle erstellen.

Erstellen Sie eine VLAN

Sie können ein VLAN erstellen, um separate Broadcast-Domänen innerhalb derselben Netzwerkdomäne mit System Manager oder dem `network port vlan create` Befehl zu verwalten.

Bevor Sie beginnen

Vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind:

- Die im Netzwerk implementierten Switches müssen entweder den IEEE 802.1Q Standards entsprechen oder über eine anbieterspezifische Implementierung von VLANs verfügen.
- Um mehrere VLANs zu unterstützen, muss eine Endstation statisch konfiguriert werden, damit sie zu einem oder mehreren VLANs gehören.
- Das VLAN ist nicht an einen Port angehängt, der eine Cluster-LIF hostet.
- Das VLAN ist nicht an Ports angeschlossen, die dem Cluster-IPspace zugewiesen sind.
- Das VLAN wird nicht auf einem Port für Schnittstellengruppen erstellt, der keine Mitgliedsports enthält.

Über diese Aufgabe

Beim Erstellen eines VLANs wird das VLAN an den Netzwerkanschluss auf einem angegebenen Node in einem Cluster angeschlossen.

Wenn Sie ein VLAN zum ersten Mal über einen Port konfigurieren, könnte der Port ausfallen, was zu einer vorübergehenden Trennung des Netzwerks führt. Nachfolgende VLAN-Erweiterungen zum selben Port wirken sich nicht auf den Portstatus aus.

Sie sollten kein VLAN auf einer Netzwerkschnittstelle mit derselben Kennung wie das native VLAN des Switches erstellen. Wenn beispielsweise die Netzwerkschnittstelle e0b auf nativem VLAN 10 ist, sollten Sie keine VLAN e0b-10 auf dieser Schnittstelle erstellen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie den System Manager, um ein VLAN zu erstellen

Ab ONTAP 9.12.0 können Sie die Broadcast-Domäne automatisch auswählen oder manuell ein aus der Liste auswählen. Zuvor wurden Broadcast-Domänen immer automatisch ausgewählt, basierend auf Layer-2-Konnektivität. Wenn Sie eine Broadcast-Domäne manuell auswählen, wird eine Warnung angezeigt, die darauf hinweist, dass die manuelle Auswahl einer Broadcast-Domäne zu einem Verbindungsverlust führen kann.

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > + VLAN**.
2. Wählen Sie den Knoten aus der Dropdown-Liste aus.
3. Wählen Sie eine der folgenden Optionen:
   a. ONTAP to **Broadcast-Domain automatisch auswählen (empfohlen)**.
   b. So wählen Sie eine Broadcast-Domäne aus der Liste manuell aus.
4. Wählen Sie die Ports aus, die das VLAN bilden sollen.
5. Geben Sie die VLAN-ID an.
6. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um ein VLAN zu erstellen

Wenn Sie unter bestimmten Umständen den VLAN-Port auf einem heruntergestuften Port erstellen möchten, ohne das Hardware-Problem oder eine Fehlkonfiguration der Software zu beheben, können Sie den `-ignore-health-status` Parameter des `network port modify` Befehls als einstellen `true`.

Erfahren Sie mehr über `network port modify` in der "ONTAP-Befehlsreferenz".

Schritte

1. Verwenden Sie den `network port vlan create` Befehl, um ein VLAN zu erstellen.
2. Sie müssen `vlan-name` `port` `vlan-id` beim Erstellen eines VLAN entweder die Optionen oder und angeben. Der VLAN-Name ist eine Kombination aus dem Namen des Ports (oder der Schnittstellengruppe) und der Netzwerk-Switch-VLAN-ID, mit einem Bindestrich dazwischen. Beispielsweise `e0c-24` `e1c-80` sind und gültige VLAN-Namen.

Das folgende Beispiel zeigt, wie ein VLAN erstellt `e1c-80` `e1c` `cluster-1-01` wird, das an den Netzwerkport auf dem Knoten angeschlossen ist:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Ab ONTAP 9.8 werden VLANs etwa eine Minute nach ihrer Erstellung automatisch in geeignete Broadcast-Domänen platziert. Wenn Sie dies nicht möchten, dass ONTAP das VLAN manuell in einer Broadcast-Domäne platziert, geben Sie den `-skip-broadcast-domain-placement` Parameter als Teil des `vlan create` Befehls an.

Erfahren Sie mehr über `network port vlan create` in der "ONTAP-Befehlsreferenz".

VLAN bearbeiten

Sie können die Broadcast-Domäne ändern oder ein VLAN deaktivieren.

Verwenden Sie System Manager, um ein VLAN zu bearbeiten

Ab ONTAP 9.12.0 können Sie die Broadcast-Domäne automatisch auswählen oder manuell ein aus der Liste auswählen. Zuvor wurden Broadcast-Domänen immer automatisch ausgewählt, basierend auf Layer 2-Konnektivität. Wenn Sie eine Broadcast-Domäne manuell auswählen, wird eine Warnung angezeigt, die darauf hinweist, dass die manuelle Auswahl einer Broadcast-Domäne zu einem Verbindungsverlust führen kann.

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > VLAN**.
2. Wählen Sie das Bearbeitungssymbol.
3. Führen Sie einen der folgenden Schritte aus:
   - Ändern Sie die Broadcast-Domäne, indem Sie eine andere aus der Liste auswählen.
   - Deaktivieren Sie das Kontrollkästchen * aktiviert*.
4. Speichern Sie die Änderungen.

Löschen eines VLAN

Möglicherweise müssen Sie ein VLAN löschen, bevor Sie einen NIC aus seinem Steckplatz entfernen. Wenn Sie ein VLAN löschen, wird es automatisch aus allen Failover-Regeln und -Gruppen entfernt, die es verwenden.

Bevor Sie beginnen

Stellen Sie sicher, dass dem VLAN keine LIFs zugewiesen sind.

Über diese Aufgabe

Das Löschen des letzten VLAN von einem Port kann zu einer vorübergehenden Trennung des Netzwerks vom Port führen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie den System Manager, um ein VLAN zu löschen

Schritte

1. Wählen Sie **Netzwerk > Ethernet-Port > VLAN**.
2. Wählen Sie das VLAN aus, das Sie entfernen möchten.
3. Klicken Sie Auf **Löschen**.

CLI

Verwenden Sie die CLI, um ein VLAN zu löschen

Schritt

Verwenden Sie den `network port vlan delete` Befehl, um ein VLAN zu löschen.

Das folgende Beispiel zeigt, wie man VLAN `e1c-80` vom Netzwerkport `e1c` auf dem Knoten löscht `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Erfahren Sie mehr über `network port vlan delete` in der "ONTAP-Befehlsreferenz".

Ändern Sie die Attribute des ONTAP-Netzwerkports

Sie können die Autonegotiation, Duplexkonfiguration, Flusskontrolle, Geschwindigkeit und Integritätseinstellungen eines physischen Netzwerkports ändern.

Bevor Sie beginnen

Der Port, den Sie ändern möchten, darf keine LIFs hosten.

Über diese Aufgabe

- Es wird nicht empfohlen, die administrativen Einstellungen der 100-GbE-, 40-GbE-, 10-GbE- oder 1-GbE-Netzwerkschnittstellen zu ändern.

  Die Werte, die Sie für den Duplexmodus und die Portgeschwindigkeit festlegen, werden als Administratoreinstellungen bezeichnet. Je nach Netzwerkeinschränkungen können die Administratoreinstellungen von den Betriebseinstellungen abweichen (d. h. den Duplexmodus und die Geschwindigkeit, die der Port tatsächlich verwendet).

- Es wird nicht empfohlen, die administrativen Einstellungen der zugrunde liegenden physischen Ports in einer Schnittstellengruppe zu ändern.

  Der `-up-admin` Parameter (verfügbar auf der erweiterten Berechtigungsebene) ändert die administrativen Einstellungen des Ports.

- Es wird nicht empfohlen, die `-up-admin` Administratoreinstellung für alle Ports an einem Node oder für den Port, der die letzte betriebliche Cluster-LIF auf einem Node hostet, auf „false“ zu setzen.
- Es wird nicht empfohlen, die MTU-Größe des Management-Ports zu ändern `e0M`.

- Die MTU-Größe eines Ports in einer Broadcast-Domäne kann nicht von dem für die Broadcast-Domäne festgelegten MTU-Wert geändert werden.
- Die MTU-Größe eines VLANs darf den Wert der MTU-Größe ihres Basis-Ports nicht überschreiten.

Schritte

1. Ändern Sie die Attribute eines Netzwerkports:

   `network port modify`

2. Sie können das `-ignore-health-status` Feld auf „true“ setzen, um anzugeben, dass das System den Integritätsstatus des Netzwerkports eines angegebenen Ports ignorieren kann.

   Der Integritätsstatus des Netzwerk-Ports wird automatisch von „beeinträchtigt“ in „ordnungsgemäß“ geändert, und dieser Port kann jetzt für das Hosting von LIFs verwendet werden. Sie sollten die Flusssteuerung der Cluster-Ports auf einstellen `none`. Standardmäßig ist die Flusssteuerung auf eingestellt `full`.

Mit dem folgenden Befehl wird die Flusssteuerung an Port e0b deaktiviert, indem die Flusskontrolle auf „none“ gesetzt wird:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Erfahren Sie mehr über `network port modify` in der "ONTAP-Befehlsreferenz".

10-GbE-Ports für ONTAP-Netzwerke werden durch Konvertieren von 40-GbE-NIC-Ports erstellt

Sie können den X1144A-R6 und die X91440A-R6 40GbE Network Interface Cards (NICs) zur Unterstützung von vier 10-GbE-Ports konvertieren.

Wenn Sie eine Hardwareplattform verbinden, die einen dieser NICs unterstützt, mit einem Cluster, das 10-GbE-Cluster-Verbindungen und Kundendatenverbindungen unterstützt, muss die NIC konvertiert werden, um die erforderlichen 10-GbE-Verbindungen bereitzustellen.

Bevor Sie beginnen

Sie müssen ein unterstütztes Breakout-Kabel verwenden.

Über diese Aufgabe

Eine vollständige Liste der Plattformen, die NICs unterstützen, finden Sie unter "Hardware Universe" .

> Auf dem X1144A-R6 NIC kann nur Port A zur Unterstützung der vier 10GbE-Verbindungen konvertiert werden. Nach der Konvertierung von Port A steht Port e nicht zur Verfügung.

Schritte

1. Wechseln Sie in den Wartungsmodus.
2. Konvertieren Sie die NIC von 40-GbE-Unterstützung zu 10-GbE-Unterstützung.

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. Halten Sie den Knoten nach Verwendung des Befehls convert.
4. Installieren oder tauschen Sie das Kabel aus.
5. Verwenden Sie je nach Hardware-Modell den SP (Service-Prozessor) oder BMC (Baseboard Management Controller), um den Node aus- und wieder einzuschalten, damit die Konvertierung wirksam wird.

Konfigurieren Sie die UTA X1143A-R6-Ports für das ONTAP-Netzwerk

Standardmäßig ist der X1143A-R6 Unified Target Adapter im FC Target-Modus konfiguriert. Sie können seine Ports jedoch entweder als 10-Gbit-Ethernet- und FCoE-Ports (CNA) oder als 16-Gbit-FC-Initiator oder als Ziel-Ports konfigurieren. Dazu sind andere SFP+-Adapter erforderlich.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zielverkehr auf demselben 10-GBE-Port. Bei Konfiguration für FC kann jedes Paar mit zwei Ports, das denselben ASIC verwendet, individuell für das FC-Ziel oder den FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter einen FC-Zielmodus auf einem Paar mit zwei Ports und einen FC-Initiator-Modus auf einem anderen Paar mit zwei Ports unterstützen kann. Die mit demselben ASIC verbundenen Port-Paare müssen im gleichen Modus konfiguriert werden.

Im FC-Modus verhält sich der X1143A-R6 Adapter wie jedes vorhandene FC-Gerät mit Geschwindigkeiten von bis zu 16 Gbit/s. Im CNA-Modus können Sie den X1143A-R6-Adapter für den gleichzeitigen NIC- und FCoE-Datenverkehr verwenden, der denselben 10-GbE-Port nutzt. Der CNA-Modus unterstützt für die FCoE-Funktion nur den FC-Zielmodus.

Um den Unified Target Adapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im selben Personality-Modus konfiguriert werden.

Schritte

1. Überprüfen Sie die Portkonfiguration:

```
system hardware unified-connect show
```

2. Konfigurieren Sie die Ports nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA):

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. Schließen Sie die entsprechenden Kabel für FC- oder 10-Gbit-Ethernet an.
4. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

   Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Für FC sollten Sie basierend auf der FC-Fabric, mit der verbunden ist, entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Konvertieren Sie den UTA2-Port zur Verwendung im ONTAP-Netzwerk

Sie können den UTA2-Port vom CNA-Modus (Converged Network Adapter) in den FC-Modus (Fibre Channel) oder umgekehrt konvertieren.

Sie sollten die UTA2-Persönlichkeit vom CNA-Modus in den FC-Modus ändern, wenn Sie das physische Medium ändern müssen, das den Port mit seinem Netzwerk verbindet oder um die FC-Initiatoren und das Ziel zu unterstützen.

Vom CNA-Modus zum FC-Modus

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Ändern des Portmodus:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. Booten Sie den Node neu, und versetzen Sie den Adapter dann in den Online-Modus:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. Benachrichtigen Sie den Administrator oder VIF-Manager, dass er den Port löschen oder entfernen soll, falls zutreffend:
   - Wenn der Port als Home Port einer logischen Schnittstelle verwendet wird, ist ein Mitglied einer Interface Group (ifgrp), oder Hosts VLANs, dann sollte ein Administrator Folgendes tun:
     - Verschieben Sie die LIFs, entfernen Sie den Port aus dem ifgrp oder löschen Sie die VLANs.
     - Löschen Sie den Port manuell, indem Sie den `network port delete` Befehl ausführen. Wenn der `network port delete` Befehl fehlschlägt, sollte der Admin die Fehler beheben und dann den Befehl erneut ausführen.
   - Wenn der Port nicht als Home-Port einer LIF verwendet wird, kein Mitglied eines ifgrp ist und keine VLANs hostet, dann sollte der VIF-Manager den Port zum Zeitpunkt des Neustarts aus seinen Datensätzen entfernen. Wenn der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neubooten mit dem `network port delete` Befehl manuell entfernen.

     Erfahren Sie mehr über `network port delete` in der "ONTAP-Befehlsreferenz".

5. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

   Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Vor dem Ändern der Konfiguration auf dem Node sollten Sie für FC entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Vom FC-Modus zum CNA-Modus

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Ändern des Portmodus:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. Booten Sie den Node neu
4. Stellen Sie sicher, dass das richtige SFP+ installiert ist.

   Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden.

Konvertieren Sie die optischen CNA/UTA2-Module für das ONTAP-Netzwerk

Sie sollten die optischen Module auf dem Unified Target Adapter (CNA/UTA2) ändern, um den Personality-Modus zu unterstützen, den Sie für den Adapter ausgewählt haben.

Schritte

1. Überprüfen Sie das aktuelle SFP+, das in der Karte verwendet wird. Ersetzen Sie dann das aktuelle SFP+ durch das entsprechende SFP+ für die bevorzugte Persönlichkeit (FC oder CNA).
2. Entfernen Sie die aktuellen optischen Module vom X1143A-R6 Adapter.
3. Setzen Sie die richtigen Module für Ihre bevorzugte Personality-Mode-Optik (FC oder CNA) ein.
4. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

   Unterstützte SFP+ Module und Cisco-Kupferkabel sind in der aufgeführt "NetApp Hardware Universe".

Entfernen Sie NICs aus ONTAP-Clusterknoten

Sie müssen möglicherweise eine fehlerhafte NIC aus ihrem Steckplatz entfernen oder die NIC zu Wartungszwecken in einen anderen Steckplatz verschieben.

> Das Verfahren zum Entfernen einer Netzwerkkarte unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie eine NIC von einem ONTAP-Clusterknoten entfernen müssen, auf dem ONTAP 9.7 und früher ausgeführt wird, lesen Sie das Verfahren "Entfernen einer NIC aus dem Knoten (ONTAP 9.7 oder früher)".

Schritte

1. Schalten Sie den Node aus.
2. Entfernen Sie die NIC physisch aus ihrem Steckplatz.
3. Schalten Sie den Node ein.

4. Überprüfen Sie, ob der Port gelöscht wurde:

```
network port show
```

ONTAP entfernt den Port automatisch von allen Interface Groups. Wenn der Port das einzige Mitglied einer Schnittstellengruppe war, wird die Schnittstellengruppe gelöscht. Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

5. Wenn auf dem Port VLANs konfiguriert waren, werden sie verschoben. Sie können Vertriebene VLANs mit dem folgenden Befehl anzeigen:

```
cluster controller-replacement network displaced-vlans show
```

Die `displaced-interface show` `displaced-vlans show` `displaced-vlans restore` Befehle , und sind eindeutig und erfordern keinen vollständig qualifizierten Befehlsnamen, der mit beginnt `cluster controller-replacement network`.

6. Diese VLANs wurden gelöscht, sind aber mit folgendem Befehl wiederhergestellt:

```
displaced-vlans restore
```

7. Wenn auf dem Port LIFs konfiguriert wären, wählt ONTAP automatisch neue Home Ports für die LIFs auf einem anderen Port der gleichen Broadcast-Domäne aus. Wenn auf dem gleichen Filer kein geeigneter Home Port gefunden wird, gelten diese LIFs als verdrängt. Sie können Vertriebene-LIFs mit dem folgenden Befehl anzeigen:

```
displaced-interface show
```

8. Wenn der Broadcast-Domäne auf demselben Node ein neuer Port hinzugefügt wird, werden die Home-Ports für die LIFs automatisch wiederhergestellt. Alternativ können Sie den Home-Port mit dem `network interface modify -home-port -home-node or use the displaced- interface restore` Befehl festlegen.

Verwandte Informationen

- "Löschen des Cluster-Controllers als Ersatz für das Netzwerk mit verschobene Schnittstelle"
- "Änderung der Netzwerkschnittstelle"

Überwachen Sie die Netzwerkanschlüsse

Überwachen Sie den Systemzustand der ONTAP-Netzwerkports

Das ONTAP Management von Netzwerk-Ports umfasst eine automatische Statusüberwachung und eine Reihe von Zustandsmonitoren, mit denen Sie Netzwerk-Ports identifizieren können, die möglicherweise nicht für das Hosting von LIFs geeignet sind.

Über diese Aufgabe

Wenn eine Systemzustandsüberwachung feststellt, dass ein Netzwerkanschluss fehlerhaft ist, werden Administratoren über eine EMS-Meldung gewarnt oder der Port wird als beeinträchtigt markiert. ONTAP vermeidet das Hosten von LIFs auf beeinträchtigten Netzwerk-Ports, wenn es gesunde alternative Failover-Ziele für diese LIF gibt. Ein Port kann aufgrund eines Soft-Failure-Ereignisses beeinträchtigt werden, z. B. das Überfüllen von Links (die schnell zwischen oben und unten hin- und herspringt) oder die Netzwerkpartitionierung:

- Netzwerkanschlüsse im IPspace des Clusters werden als beeinträchtigt markiert, wenn es zu Verbindungsverlusten oder Verlust der Reachabilität von Layer 2 (L2) zu anderen Netzwerkports in der Broadcast-Domäne kommt.
- Netzwerkports in nicht-Cluster-IPspaces werden als beeinträchtigt gekennzeichnet, wenn Link-flattern.

Sie müssen die folgenden Verhaltensweisen eines beeinträchtigten Ports kennen:

- Ein eingeschränkter Port kann nicht in ein VLAN oder eine Schnittstellengruppe aufgenommen werden.

  Wenn ein Mitglied-Port einer Interface-Gruppe als beeinträchtigt gekennzeichnet ist, die Interface-Gruppe jedoch noch als ordnungsgemäß gekennzeichnet ist, können LIFs auf dieser Interface-Gruppe gehostet werden.

- LIFs werden automatisch von Ports migriert, deren Betrieb nicht beeinträchtigt ist, auf gesunde Ports.
- Während eines Failover-Ereignisses wird ein beeinträchtigter Port nicht als Failover-Ziel betrachtet. Wenn keine ordnungsgemäßen Ports verfügbar sind, hosten degradierte Ports LIFs gemäß der normalen Failover-Richtlinie.
- Sie können eine LIF nicht zu einem beeinträchtigten Port erstellen, migrieren oder zurücksetzen.

  Sie können die `ignore-health-status` Einstellung des Netzwerkports auf ändern `true`. Sie können dann eine LIF auf den gesunden Ports hosten.

Schritte

1. Melden Sie sich im erweiterten Berechtigungsmodus an:

   ```
   set -privilege advanced
   ```

2. Überprüfen Sie, welche Integritätsmonitore für das Monitoring des Netzwerkports aktiviert sind:

   ```
   network options port-health-monitor show
   ```

   Der Integritätsstatus eines Ports wird durch den Wert der Integritätsmonitore bestimmt.

   Die folgenden Integritätsmonitore sind in ONTAP standardmäßig verfügbar und aktiviert:

   - Link-flatternder Systemzustandsüberwachung: Überwacht das Umfüllen von Links

     Wenn ein Port in fünf Minuten mehr als einmal über Verbindungsflattern verfügt, wird dieser Port als beeinträchtigt markiert.

   - L2-Statusüberwachung: Überwacht, ob alle Ports, die in derselben Broadcast-Domäne konfiguriert

sind, L2-Erreichbarkeit aufweisen

Diese Systemzustandsüberwachung meldet Probleme mit der L2-Erreichbarkeit in allen IPspaces. Es markiert jedoch nur die Ports im Cluster-IPspace als beeinträchtigt.

- CRC-Monitor: Überwacht die CRC-Statistiken auf den Ports

  Diese Systemzustandsüberwachung markiert einen Port nicht als beeinträchtigt, generiert aber eine EMS-Meldung, wenn eine sehr hohe CRC-Fehlerrate beobachtet wird.

Erfahren Sie mehr über `network options port-health-monitor show` in der "ONTAP-Befehlsreferenz".

3. Aktivieren oder deaktivieren Sie mit dem `network options port-health-monitor modify` Befehl eine der Systemzustandsüberwachungen für einen IPspace wie gewünscht.

   Erfahren Sie mehr über `network options port-health-monitor modify` in der "ONTAP-Befehlsreferenz".

4. Anzeigen des detaillierten Systemzustands eines Ports:

```
network port show -health
```

In der Befehlsausgabe werden der Systemzustand des Ports, `ignore health status` die Einstellung und die Liste der Gründe angezeigt, aus denen der Port als „beeinträchtigt“ gekennzeichnet ist.

Ein Port-Integritätsstatus kann `healthy` oder sein `degraded`.

Wenn die `ignore health status` Einstellung lautet `true`, zeigt dies an, dass der Funktionszustand des Ports `degraded` `healthy` vom Administrator von in geändert wurde.

Wenn die `ignore health status` Einstellung lautet `false`, wird der Status des Ports automatisch vom System bestimmt.

Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Überwachen Sie die Erreichbarkeit der ONTAP-Netzwerkports

Die Überwachung der Erreichbarkeit ist in ONTAP 9.8 und höher integriert. Mithilfe dieses Monitoring wird ermittelt, ob die physische Netzwerktopologie nicht mit der ONTAP Konfiguration übereinstimmt. In einigen Fällen kann ONTAP die Erreichbarkeit des Ports reparieren. In anderen Fällen sind weitere Schritte erforderlich.

Über diese Aufgabe

Verwenden Sie diese Befehle, um Fehlkonfigurationen in Netzwerken zu überprüfen, zu diagnostizieren und zu reparieren, die aus der ONTAP Konfiguration stammen und weder mit der physischen Verkabelung noch mit der Netzwerk-Switch-Konfiguration übereinstimmen.

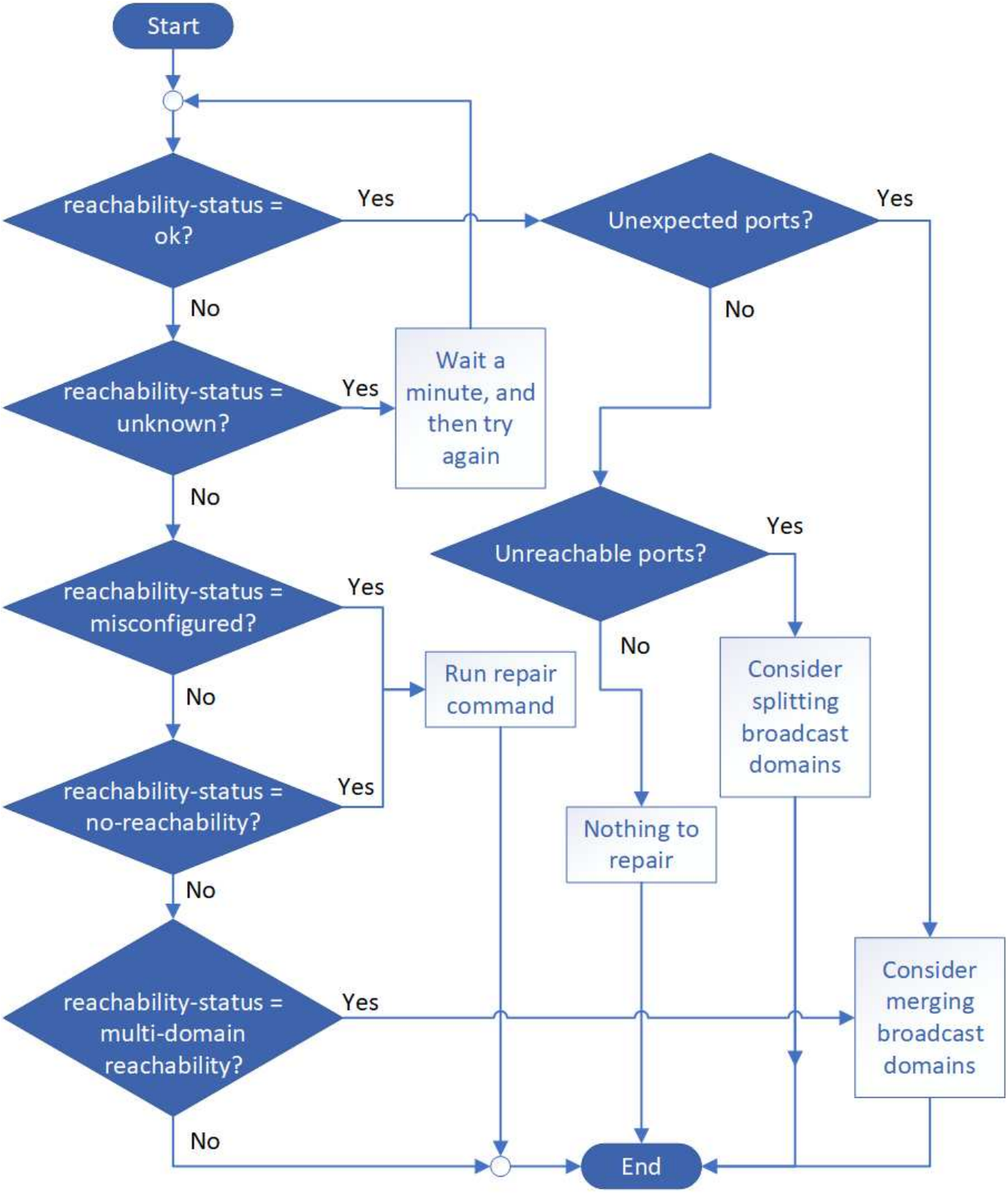
Schritt

1. Port-Erreichbarkeit anzeigen:

```
network port reachability show
```

Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".

2. Verwenden Sie die folgende Entscheidungsstruktur und die folgende Tabelle, um den nächsten Schritt zu bestimmen, falls vorhanden.



Erreichbarkeit-Status	Beschreibung

ok	Der Port verfügt über eine Layer 2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne. Wenn der Status der Erreichbarkeit „ok“ ist, aber es „unerwartete Ports“ gibt, sollten Sie eine oder mehrere Broadcast-Domänen zusammenführen. Weitere Informationen finden Sie in der folgenden Zeile „*Unexpected Ports*“. Wenn der Status „Erreichbarkeit“ „ok“ lautet, aber „nicht erreichbare Ports“ vorhanden sind, sollten Sie eine oder mehrere Broadcast-Domänen aufteilen. Weitere Informationen finden Sie in der folgenden Zeile *Unerreichbare Ports*. Wenn der Status „Erreichbarkeit“ „ok“ lautet und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist die Konfiguration korrekt.
Unerwartete Ports	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Überprüfen Sie die physische Konnektivität und die Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domain des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen".
Nicht erreichbare Ports	Wenn eine einzelne Broadcast-Domäne in zwei unterschiedliche Wiederachabilität-Sets partitioniert wurde, können Sie eine Broadcast-Domäne teilen, um die ONTAP-Konfiguration mit der physischen Netzwerktopologie zu synchronisieren. In der Regel definiert die Liste der nicht erreichbaren Ports den Satz von Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollten, nachdem Sie überprüft haben, dass die physische und die Switch-Konfiguration korrekt ist. Weitere Informationen finden Sie unter "Teilen von Broadcast-Domänen auf".
Falsch konfigurierte Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit seiner zugewiesenen Broadcast-Domäne; der Port besitzt jedoch Layer 2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port der Broadcast-Domäne zu, der sie nachzuweisen kann: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".

Keine Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit für eine vorhandene Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port einer neuen automatisch erstellten Broadcast-Domäne im Standard-IPspace zu: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren". Erfahren Sie mehr über `network port reachability repair` in der "ONTAP-Befehlsreferenz".
Multi-Domain-Erreichbarkeit	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Überprüfen Sie die physische Konnektivität und die Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domain des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen" oder "Port-Erreichbarkeit reparieren".
Unbekannt	Wenn der Status „unbekannt“ lautet, warten Sie einige Minuten, und versuchen Sie den Befehl erneut.

Nachdem Sie einen Port repariert haben, müssen Sie die vertriebenen LIFs und VLANs überprüfen und beheben. Wenn der Port Teil einer Schnittstellengruppe war, müssen Sie auch verstehen, was mit dieser Schnittstellengruppe passiert ist. Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".

Erfahren Sie mehr über die Portnutzung im ONTAP-Netzwerk

Mehrere bekannte Ports sind für die ONTAP-Kommunikation mit bestimmten Diensten reserviert. Port-Konflikte treten auf, wenn ein Portwert in Ihrer Speichernetzwerkumgebung dem Wert auf einem ONTAP-Port entspricht.

Eingehender Datenverkehr

Der Inbound-Datenverkehr im ONTAP-Speicher verwendet die folgenden Protokolle und Ports:

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
TCP	22	Sicherer Shell-Zugriff auf die IP-Adresse der Cluster-Management-LIF oder einer Node-Management-LIF
TCP	80	Zugriff auf Webseiten auf die IP-Adresse der Cluster-Management-LIF
TCP/UDP	111	RPCBIND, Remote-Prozeduraufruf für NFS
UDP	123	NTP, Network Time Protocol
TCP	135	MSRPC, Microsoft Remote Procedure Call

TCP	139	NETBIOS-SSN, NetBIOS-Servicesitzung für CIFS
TCP/UDP	161-162	SNMP, einfaches Netzwerk-Management-Protokoll
TCP	443	Sicherer Zugriff auf Webseiten auf die IP-Adresse der Cluster-Management-LIF
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
TCP/UDP	635	NFS-Mounten, um mit einem Remote-Dateisystem zu interagieren, als ob es sich um ein lokales Dateisystem handelt
TCP	749	Kerberos
UDP	953	Name Daemon
TCP/UDP	2049	NFS-Server-Daemon
TCP	2050	NRV, NetApp Remote Volume Protokoll
TCP	3260	ISCSI-Zugriff über die iSCSI-Daten-LIF
TCP/UDP	4045	NFS-Sperr-Daemon
TCP/UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS RPC rquoad
UDP	4444	KRB524, Kerberos 524
UDP	5353	Multicast-DNS
TCP	10000	Backup mit Network Data Management Protocol (NDMP)
TCP	11104	Cluster-Peering, bidirektionales Management von Intercluster-Kommunikationssitzungen für SnapMirror
TCP	11105	Cluster-Peering, bidirektionaler SnapMirror-Datentransfer mithilfe von Intercluster LIFs
SSL/TLS	30000	Akzeptiert sichere NDMP-Steuerverbindungen zwischen dem DMA- und dem NDMP-Server über sichere Sockets (SSL/TLS). Sicherheitsscanner können eine Sicherheitslücke auf Port 30000 melden.

Ausgehender Datenverkehr

Outbound-Datenverkehr auf dem ONTAP Storage können entsprechend den geschäftlichen Anforderungen anhand einfacher oder erweiterter Regeln eingerichtet werden.

Grundlegende Regeln für ausgehende Anrufe

Alle Ports können für den gesamten ausgehenden Datenverkehr über ICMP-, TCP- und UDP-Protokolle verwendet werden.

Protokoll	Port	Zweck
Alle ICMP	Alle	Gesamter abgehender Datenverkehr

Alle TCP-Protokolle	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch ONTAP erforderlich sind.

Active Directory

Protokoll	Port	Quelle	Ziel	Zweck
TCP	88	Node-Management-LIF, Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
UDP	137	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
UDP	138	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
TCP	139	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
TCP	389	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
UDP	389	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
TCP	445	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	464	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Ändern und Festlegen des Kerberos V-Passworts (SET_CHANGE)
UDP	464	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
TCP	749	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Ändern und Festlegen des Kerberos V-Passworts (RPCSEC_GSS)

AutoSupport

Protokoll	Port	Quelle	Ziel	Zweck
TCP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)

SNMP

Protokoll	Port	Quelle	Ziel	Zweck
TCP/UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps

SnapMirror

Protokoll	Port	Quelle	Ziel	Zweck
TCP	11104	Intercluster LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror

Dienstleistungen

Protokoll	Port	Quelle	Ziel	Zweck
TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
UDP	67	Node Management-LIF	DHCP	DHCP-Server
UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen
TCP	5010	Intercluster LIF	Backup-Endpunkt oder Wiederherstellungsendpunkt	Backup- und Restore-Vorgänge für die Funktion „Backup in S3“
TCP	18600 bis 18699	Node Management-LIF	Zielserver	NDMP-Kopie

Informieren Sie sich über interne ONTAP Ports

Die folgende Tabelle listet die von ONTAP intern verwendeten Ports und ihre Funktionen auf. ONTAP nutzt diese Ports für verschiedene Funktionen, beispielsweise zum Aufbau der Intracluster-LIF-Kommunikation.

Diese Liste ist nicht vollständig und kann in verschiedenen Umgebungen variieren.

Port/Protokoll	Komponente/Funktion
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC

904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC
911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC
925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
930	Kerneldienste und Verwaltungsfunktionen (KSMF)
931	NetApp Cluster RPC
932	NetApp Cluster RPC
933	NetApp Cluster RPC
934	NetApp Cluster RPC
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC

967	NetApp Cluster RPC
975	Key Management Interoperability Protocol (KMIP)
982	NetApp Cluster RPC
983	NetApp Cluster RPC
5125	Alternate Control Port für Festplatte
5133	Alternate Control Port für Festplatte
5144	Alternate Control Port für Festplatte
65502	Umfang des Node SSH
65503	LIF-Freigabe
7700	Cluster Session Manager (CSM)
7810	NetApp Cluster RPC
7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC
7822	NetApp Cluster RPC
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
7835-7839 und 7845-7849	TCP-Ports für die Kommunikation innerhalb des Clusters
8023	TELNET mit Node-Umfang
8443	ONTAP S3 NAS-Port für Amazon FSx
8514	RSH mit Node-Umfang
9877	KMIP-Client-Port (nur interner lokaler Host)
10006	TCP-Port für HA-Interconnect-Kommunikation

IPspaces

Erfahren Sie mehr über die Konfiguration des ONTAP IP-Speicherplatzes

Mit IPspaces können Sie ein einzelnes ONTAP Cluster konfigurieren, sodass Clients von mehr als einer administrativ getrennten Netzwerkdomäne auf dieses zugreifen können, selbst wenn diese Clients denselben IP-Adressbereich nutzen. Dies ermöglicht die Trennung des Client Traffic für Datenschutz und Sicherheit.

Ein IPspace definiert einen eigenen IP-Adressbereich, in dem sich Storage Virtual Machines (SVMs) befinden. Für einen IPspace definierte Ports und IP-Adressen gelten nur innerhalb dieses IPspaces. Für jede SVM innerhalb eines IPspaces wird für jede SVM eine separate Routing-Tabelle verwaltet. Daher erfolgt kein SVM- oder IPspace-Cross-Routing.

IPspaces unterstützen sowohl IPv4- als auch IPv6-Adressen in ihren Routing-Domänen.

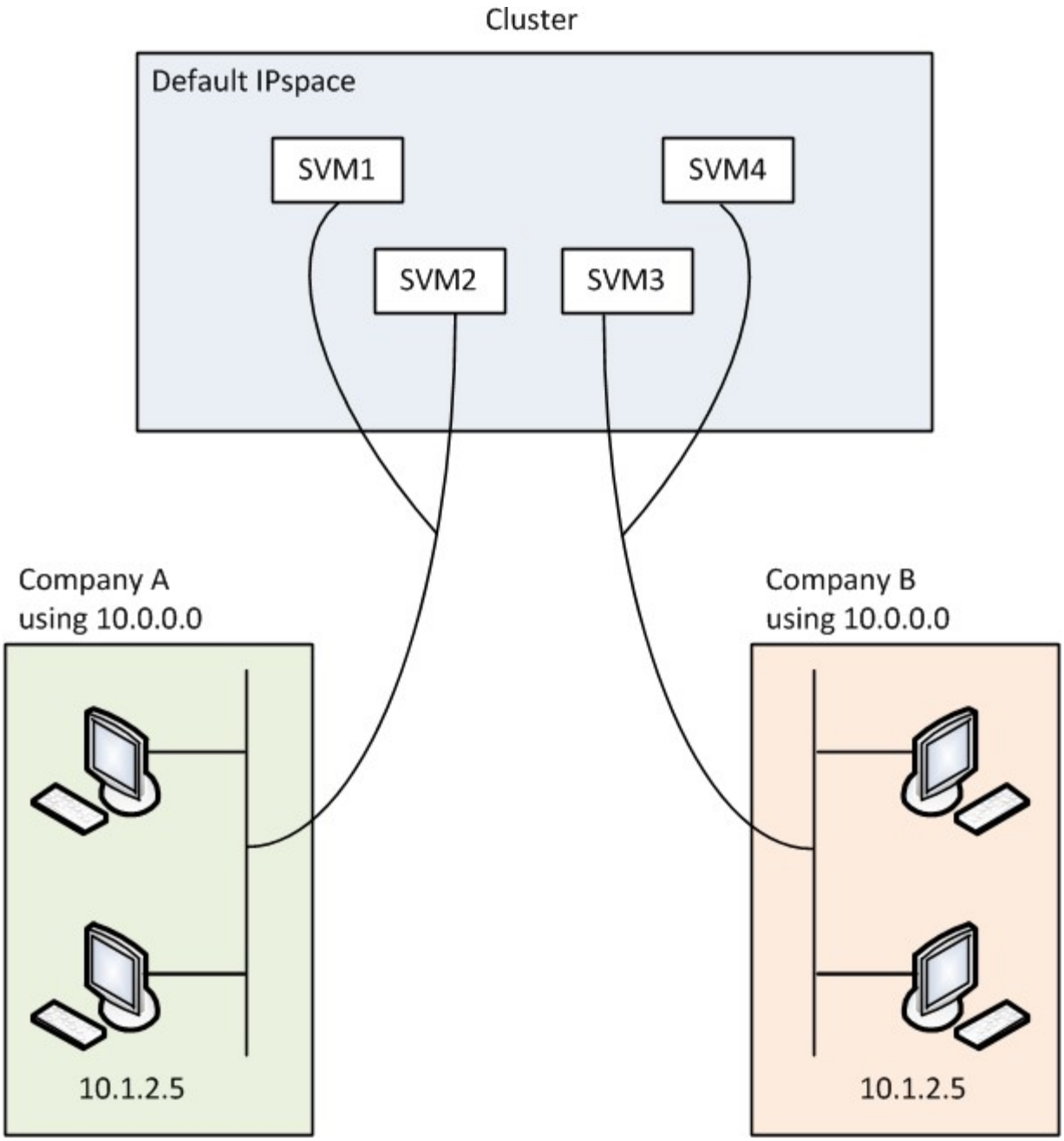
Wenn Sie Speicher für eine einzelne Organisation verwalten, müssen Sie IPspaces nicht konfigurieren. Wenn Sie Storage für mehrere Unternehmen in einem einzigen ONTAP Cluster verwalten und Sie sicher sind, dass keiner Ihrer Kunden über widersprüchliche Netzwerkkonfigurationen verfügt, dann müssen Sie auch nicht IPspaces verwenden. In vielen Fällen kann die Verwendung von Storage Virtual Machines (SVMs) mit ihren eigenen IP-Routing-Tabellen zur Trennung einzigartiger Netzwerkkonfigurationen anstelle von IPspaces genutzt werden.

Beispiel für die Verwendung von IPspaces

Eine gängige Applikation für den Einsatz von IPspaces ist, wenn ein Storage-Service-Provider (SSP) Kunden von Unternehmen A und B mit einem ONTAP Cluster am SSP-Standort verbinden muss und beide Unternehmen dieselben privaten IP-Adressbereiche nutzen.

Der SSP erstellt SVMs auf dem Cluster für jeden Kunden und bietet einen dedizierten Netzwerkpfad von zwei SVMs zu Unternehmen A Netzwerk und von den anderen zwei SVMs zu Unternehmen B Netzwerk.

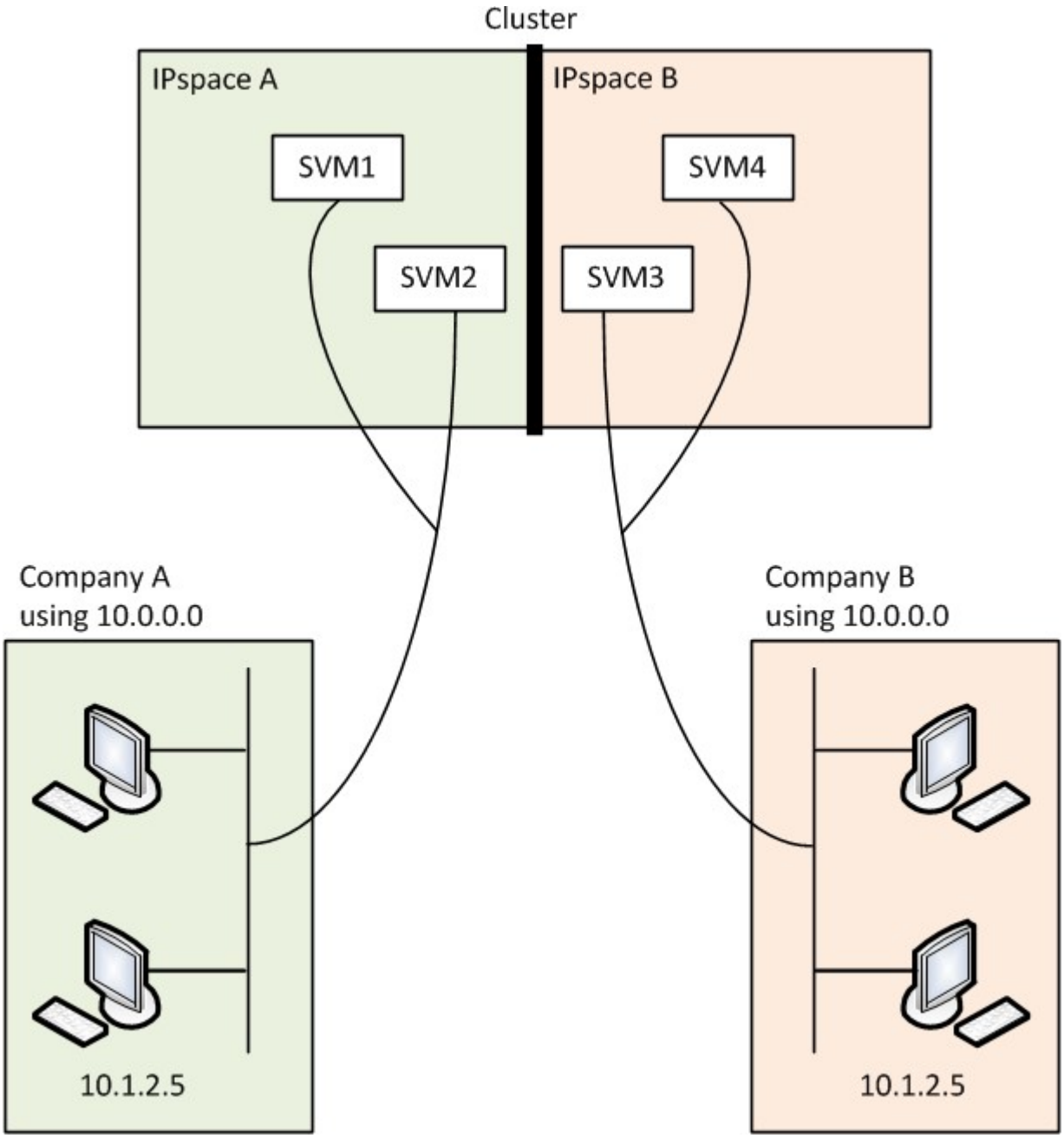
Diese Art der Bereitstellung ist in der folgenden Abbildung dargestellt, und es funktioniert, wenn beide Unternehmen nicht-private IP-Adressbereiche verwenden. Die Abbildung zeigt jedoch, dass beide Unternehmen dieselben privaten IP-Adressbereiche nutzen, was zu Problemen führt.



Beide Unternehmen verwenden die private IP-Adresse Subnetz 10.0.0.0, was die folgenden Probleme verursacht:

- Die SVMs im Cluster am SSP-Standort verfügen über widersprüchliche IP-Adressen, wenn beide Unternehmen sich entscheiden, dieselbe IP-Adresse für die jeweiligen SVMs zu verwenden.
- Selbst wenn sich beide Unternehmen einig sind, unterschiedliche IP-Adressen für ihre SVMs zu verwenden, können Schwierigkeiten auftreten.
- Zum Beispiel, wenn jeder Client im Netzwerk Von A die gleiche IP-Adresse hat wie ein Client im Netzwerk von B, können Pakete, die für einen Client im Adressraum Von A bestimmt sind, im Adressraum von B an einen Client weitergeleitet werden und umgekehrt.
- Wenn die beiden Unternehmen sich entscheiden, sich gegenseitig ausschließende Adressbereiche zu verwenden (Z. B. verwendet A 10.0.0.0 mit einer Netzmaske von 255.128.0.0 und B 10.128.0.0 mit einer Netzmaske von 255.128.0.0), Der SSP muss statische Routen auf dem Cluster konfigurieren, um Verkehr entsprechend zu A und B-Netzwerken zu leiten.

- Diese Lösung ist weder skalierbar (aufgrund statischer Routen) noch sicher (Broadcast-Datenverkehr wird an alle Schnittstellen des Clusters gesendet).um diese Probleme zu überwinden, definiert der SSP zwei IPspaces auf dem Cluster – eine für jedes Unternehmen. Da kein Cross-IPspace Traffic weitergeleitet wird, werden die Daten jedes Unternehmens sicher an das jeweilige Netzwerk weitergeleitet, auch wenn alle SVMs im Adressbereich 10.0.0.0 konfiguriert sind, wie in der folgenden Abbildung dargestellt:



Außerdem `/etc/ hosts` `/etc/hosts.equiv` `the /etc/rc` sind die IP-Adressen, auf die die verschiedenen Konfigurationsdateien verweisen, wie z. B. die Datei, die Datei und die Datei, relativ zu diesem IPspace. Daher können die IPspaces dem SSP konfliktfrei dieselbe IP-Adresse für die Konfigurations- und Authentifizierungsdaten für mehrere SVMs konfigurieren.

Standardeigenschaften von IPspaces

Beim ersten Erstellen des Clusters werden standardmäßig spezielle IPspaces erstellt. Darüber hinaus werden für jeden IPspace spezielle Storage Virtual Machines (SVMs) erstellt.

Zwei IPspaces werden automatisch erstellt, wenn das Cluster initialisiert wird:

- IP-Bereich „Standard“

  Dieser IPspace ist ein Container für Ports, Subnetze und SVMs, die Daten bereitstellen. Wenn Ihre Konfiguration keine separaten IPspaces für Clients benötigt, können in diesem IPspace alle SVMs erstellt werden. Dieser IPspace enthält auch die Cluster-Management- und Node-Management-Ports.

- IPspace „Cluster“

  Dieser IPspace enthält alle Cluster-Ports aller Nodes im Cluster. Sie wird automatisch erstellt, sobald das Cluster erstellt wird. Die Lösung bietet Konnektivität mit dem internen privaten Cluster-Netzwerk. Wenn zusätzliche Nodes dem Cluster beitreten, werden dem IPspace „Cluster“ Cluster-Ports dieser Nodes hinzugefügt.

Für jeden IPspace ist eine SVM „System“ vorhanden. Wenn Sie einen IPspace erstellen, wird eine Standard-System-SVM mit demselben Namen erstellt:

- Die System-SVM für den IPspace „Cluster“ überträgt Cluster-Datenverkehr zwischen Nodes eines Clusters im internen privaten Cluster-Netzwerk.

  Der Cluster wird vom Cluster-Administrator gemanagt, und der Name lautet „Cluster“.

- Die System-SVM für den „Standard“-IPspace überträgt den Verwaltungsdatenverkehr für das Cluster und die Nodes, einschließlich des Clusterverkehrs zwischen den Clustern.

  Der Administrator wird vom Cluster-Administrator gemanagt, und er verwendet den gleichen Namen wie das Cluster.

- Die System-SVM für einen benutzerdefinierten IPspace, den Sie erstellen, trägt den Management-Datenverkehr für diese SVM.

  Der Cluster-Administrator wird vom Cluster gemanagt, und er verwendet den gleichen Namen wie der IPspace.

Eine oder mehrere SVMs für Clients können sich in einem IPspace befinden. Jede SVM verfügt über eigene Daten-Volumes und Konfigurationen und wird unabhängig von anderen SVMs verwaltet.

Erstellen Sie IPspaces für das ONTAP-Netzwerk

IPspaces sind unterschiedliche IP-Adressbereiche, in denen sich Storage Virtual Machines (SVMs) befinden. Sie können IPspaces erstellen, wenn Ihre SVMs über eigenen sicheren Storage, eigene Administration und Routing verfügen müssen. IPspaces können verwendet werden, um für jede SVM in einem Cluster einen eigenen IP-Adressbereich zu erstellen. So können Clients in administrativ getrennten Netzwerkdomänen unter Verwendung überlappender IP-Adressbereiche aus demselben IP-Adressbereich des Subnetzes auf Cluster-Daten zugreifen.

Über diese Aufgabe

Es gibt eine clusterweite Begrenzung von 512 IPspaces. Die Cluster-weite Grenze wird auf 256 IPspaces für Cluster reduziert, die Nodes mit 6 GB RAM enthalten. Mithilfe des Hardware Universe können Sie bestimmen, ob zusätzliche Einschränkungen für Ihre Plattform gelten.

"NetApp Hardware Universe"

Ein IPspace-Name kann nicht „all“ sein, da „all“ ein systemreservierter Name ist.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Erstellen eines IPspaces:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` Ist der Name der IP-Adresse, die Sie erstellen möchten. Mit dem folgenden Befehl wird der IPspace ipspac1 auf einem Cluster erstellt:

```
network ipspace create -ipspace ipspace1
```

Erfahren Sie mehr über `network ipspace create` in der "ONTAP-Befehlsreferenz".

2. IPspaces anzeigen:

`network ipspace show`

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

Der IPspace wird zusammen mit der System-SVM für den IPspace erstellt. Die SVM des Systems führt den Management-Datenverkehr durch.

Nachdem Sie fertig sind

Wenn Sie in einem Cluster mit einer MetroCluster-Konfiguration einen IPspace erstellen, müssen IPspace-Objekte manuell auf die Partner-Cluster repliziert werden. Alle SVMs, die vor der Replizierung des IPspace erstellt und einem IPspace zugewiesen werden, werden nicht zu den Partner-Clustern repliziert.

Broadcast-Domänen werden automatisch im IPspace „Standard“ erstellt und können mit folgendem Befehl zwischen IPspaces verschoben werden:

```
network port broadcast-domain move
```

Wenn Sie beispielsweise eine Broadcast-Domäne von „Standard“ auf „ips1“ verschieben möchten, verwenden Sie den folgenden Befehl:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

Zeigen Sie IPspaces im ONTAP-Netzwerk an

Sie können die Liste der in einem Cluster vorhandenen IPspaces anzeigen und die Storage Virtual Machines (SVMs), Broadcast-Domänen und den den den einzelnen IPspace zugewiesenen Ports anzeigen.

Schritt

IPspaces und SVMs in einem Cluster anzeigen:

```
network ipspace show [-ipspace ipspace_name]
```

Mit dem folgenden Befehl werden alle IPspaces, SVMs und Broadcast-Domänen im Cluster angezeigt:

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

Mit dem folgenden Befehl werden die Knoten und Ports angezeigt, die Teil von IPspace ipspac1 sind:

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

Erfahren Sie mehr über `network ipspace show` in der "ONTAP-Befehlsreferenz".

Löschen Sie IPspaces aus dem ONTAP-Netzwerk

Wenn Sie keinen IPspace mehr benötigen, können Sie ihn löschen.

Bevor Sie beginnen

Dem IPspace, den Sie löschen möchten, dürfen keine Broadcast-Domänen, Netzwerkschnittstellen oder SVMs

zugeordnet sein.

Die systemdefinierten „Standard“- und „Cluster“-IPspaces können nicht gelöscht werden.

Schritt

Löschen eines IPspaces:

```
network ipspace delete -ipspace ipspace_name
```

Mit dem folgenden Befehl wird IPspace ipspac1 aus dem Cluster gelöscht:

```
network ipspace delete -ipspace ipspace1
```

Erfahren Sie mehr über `network ipspace delete` in der "ONTAP-Befehlsreferenz".

Broadcast-Domänen

Weitere Informationen zu ONTAP Broadcast-Domänen

Broadcast-Domänen sollen Netzwerkports gruppieren, die zum selben Layer-2-Netzwerk gehören. Die Ports in der Gruppe können dann von einer Storage Virtual Machine (SVM) für den Daten- oder Managementdatenverkehr verwendet werden.

> Die Verwaltung von Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Informationen zur Verwaltung von Broadcast-Domänen in einem Netzwerk mit ONTAP 9.7 und früher finden Sie unter "Überblick über die Broadcast-Domäne (ONTAP 9.7 und früher)".

Eine Broadcast-Domäne befindet sich in einem IPspace. Während der Cluster-Initialisierung erstellt das System zwei Standard-Broadcast-Domänen:

- Die Broadcast-Domäne „Standard“ enthält Ports, die sich im IPspace „Standard“ befinden.

  Diese Ports werden hauptsächlich zum Bereitstellen von Daten genutzt. Auch Cluster-Management- und Node-Management-Ports befinden sich in dieser Broadcast-Domäne.

- Die Broadcast-Domäne „Cluster“ enthält Ports, die sich im IPspace „Cluster“ befinden.

  Diese Ports werden für die Cluster-Kommunikation verwendet und umfassen alle Cluster-Ports aus allen Nodes im Cluster.

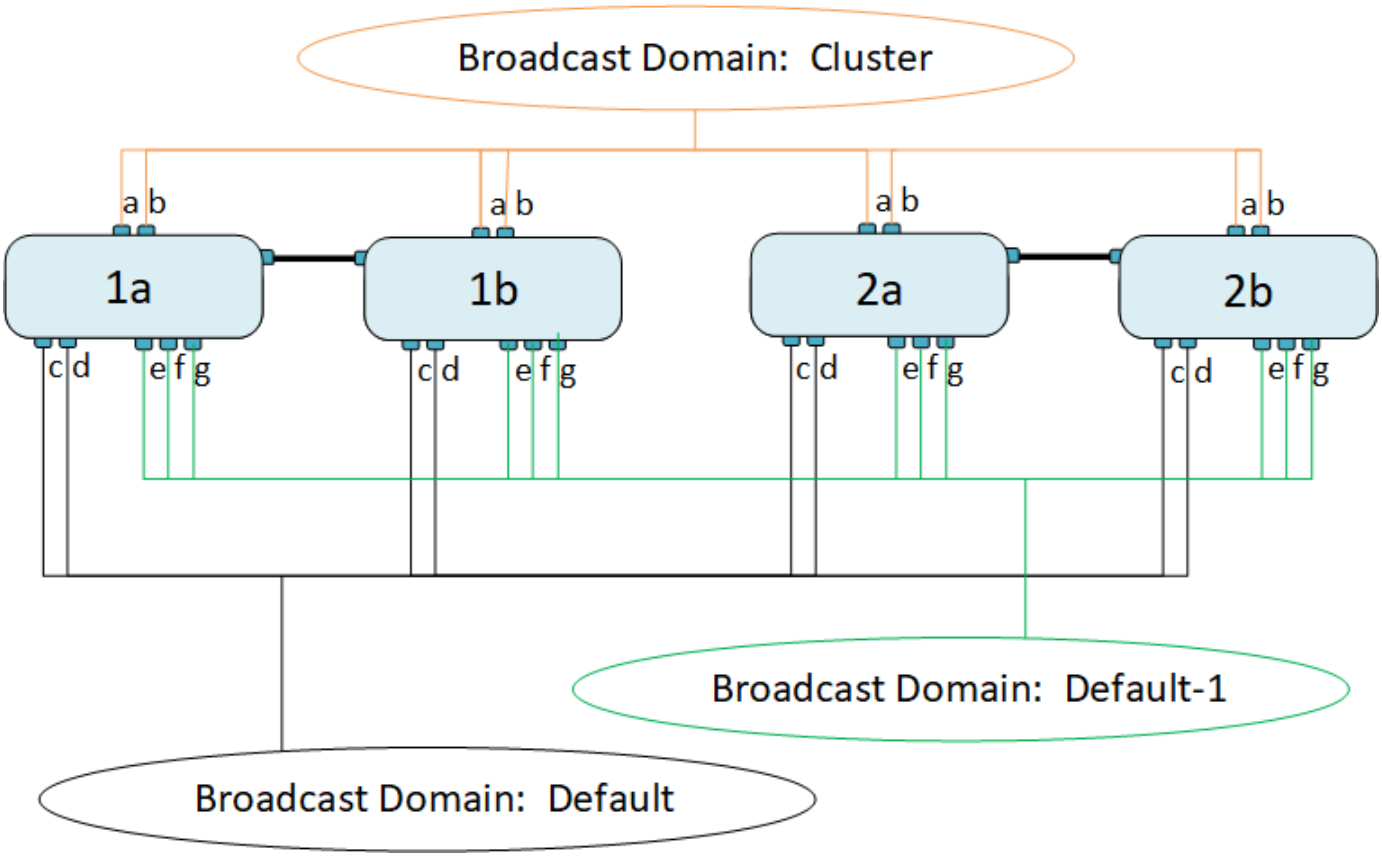
  Das System erstellt bei Bedarf zusätzliche Broadcast-Domänen im Standard-IPspace. Die Broadcast-Domäne „Standard“ enthält den Home-Port der Management-LIF sowie alle anderen Ports mit Layer-2-Erreichbarkeit dieses Ports. Zusätzliche Broadcast-Domänen werden als „Standard-1“, „Standard-2“ usw. bezeichnet.

Beispiel für die Verwendung von Broadcast-Domänen

Eine Broadcast-Domäne ist eine Reihe von Netzwerkports im gleichen IPspace, die auch Layer-2-Erreichbarkeit untereinander haben, typischerweise einschließlich Ports von vielen Knoten im Cluster.

Die Abbildung zeigt die drei Broadcast-Domänen zugewiesenen Ports in einem Cluster mit vier Nodes:

- Die Broadcast-Domäne „Cluster“ wird während der Cluster-Initialisierung automatisch erstellt und enthält Ports a und b von jedem Knoten im Cluster.
- Die Broadcast-Domäne „Standard“ wird auch während der Cluster-Initialisierung automatisch erstellt und enthält von jedem Knoten im Cluster die Ports c und d.
- Das System erstellt während der Cluster-Initialisierung automatisch zusätzliche Broadcast-Domänen basierend auf der Reachability des Layer 2-Netzwerks. Diese zusätzlichen Broadcast-Domänen haben die Namen Standard-1, Standard-2 usw.



Eine Failover-Gruppe mit demselben Namen und denselben Netzwerkports wie jede der Broadcast-Domänen wird automatisch erstellt. Diese Failover-Gruppe wird vom System automatisch verwaltet. Das bedeutet, dass beim Hinzufügen oder Entfernen von Ports aus der Broadcast-Domäne diese automatisch hinzugefügt oder aus dieser Failover-Gruppe entfernt werden.

Erstellen von ONTAP Broadcast-Domänen

Broadcast-Domänen gruppieren Netzwerk-Ports im Cluster, die zum gleichen Layer-2-Netzwerk gehören. Die Ports können dann von SVMs verwendet werden.

Broadcast-Domänen werden automatisch während der Erstellung des Clusters oder dem Beitritt zum Cluster erstellt. Ab ONTAP 9.12.0 können Sie zusätzlich zu den automatisch erstellten Broadcast-Domänen im System Manager manuell eine Broadcast-Domäne hinzufügen.

Das Verfahren zum Erstellen von Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie Broadcast-Domänen in einem Netzwerk erstellen müssen, das ONTAP 9.7 und früher ausführt, finden Sie "Erstellen einer Broadcast-Domäne (ONTAP 9.7 und früher)"weitere Informationen unter .

Bevor Sie beginnen

Die Ports, die Sie der Broadcast-Domäne hinzufügen möchten, dürfen nicht einer anderen Broadcast-Domäne angehören. Wenn die Ports, die Sie verwenden möchten, zu einer anderen Broadcast-Domäne gehören, aber nicht verwendet werden, entfernen Sie diese Ports aus der ursprünglichen Broadcast-Domäne.

Über diese Aufgabe

- Alle Broadcast-Domain-Namen müssen innerhalb eines IPspaces eindeutig sein.
- Die Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Link-Aggregationsgruppen/Interface-Gruppen (LAGs/iffrps) sein.
- Wenn die Ports, die Sie verwenden möchten, zu einer anderen Broadcast-Domäne gehören, aber nicht verwendet werden, entfernen Sie sie aus der vorhandenen Broadcast-Domäne, bevor Sie sie der neuen hinzufügen.
- Die maximale Übertragungseinheit (MTU) der Ports, die einer Broadcast-Domäne hinzugefügt wurden, wird auf den in der Broadcast-Domäne eingestellten MTU-Wert aktualisiert.
- Der MTU-Wert muss mit allen mit diesem Layer-2-Netzwerk verbundenen Geräten übereinstimmen, außer für den E0M-Port-Management-Datenverkehr.
- Wenn Sie keinen IPspace-Namen angeben, wird die Broadcast-Domäne im „Standard“-IPspace erstellt.

Um die Systemkonfiguration zu vereinfachen, wird automatisch eine Failover-Gruppe desselben Namens erstellt, die dieselben Ports enthält.

System Manager

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Broadcast-Domäne**.
2. Klicken Sie Auf + Add
3. Benennen Sie die Broadcast-Domäne.
4. Legen Sie die MTU fest.
5. Wählen Sie das IPspace aus.
6. Speichern Sie die Broadcast-Domäne.

Sie können eine Broadcast-Domäne bearbeiten oder löschen, nachdem sie hinzugefügt wurde.

CLI

Wenn Sie ONTAP 9.8 oder höher verwenden, werden Broadcast-Domänen automatisch basierend auf der Erreichbarkeit von Layer-2 erstellt. Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".

Sie können auch manuell eine Broadcast-Domäne erstellen.

Schritte

1. Anzeigen der Ports, die derzeit keiner Broadcast-Domäne zugewiesen sind:

   ```
   network port show
   ```

   Wenn die Anzeige groß ist, `network port show -broadcast-domain` zeigen Sie mit dem Befehl nur nicht zugewiesene Ports an.

2. Broadcast-Domäne erstellen:

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` Ist der Name der Broadcast-Domäne, die Sie erstellen möchten.

   b. `mtu_value` Ist die MTU-Größe für IP-Pakete; 1500 und 9000 sind typische Werte.

      Dieser Wert wird auf alle Ports angewendet, die dieser Broadcast-Domäne hinzugefügt werden.

   c. `ipspace_name` Ist der Name des IPspaces, dem diese Broadcast-Domäne hinzugefügt wird.

      Der IPspace „Standard“ wird verwendet, es sei denn, Sie geben einen Wert für diesen Parameter an.

   d. `ports_list` Ist die Liste der Ports, die der Broadcast-Domäne hinzugefügt werden.

      Die Ports werden im Format hinzugefügt `node_name:port_number`, zum Beispiel `node1:e0c`.

3. Vergewissern Sie sich, dass die Broadcast-Domäne nach Bedarf erstellt wurde:

   ```
   network port show -instance -broadcast-domain new_domain
   ```

Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Beispiel

Mit dem folgenden Befehl wird Broadcast-Domäne bcast1 im Standard-IPspace erstellt, die MTU auf 1500 festgelegt und vier Ports hinzugefügt:

`network port broadcast-domain create -broadcast-domain` *`bcast1`* `-mtu` *`1500`* `-ports` *`cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f`*

Erfahren Sie mehr über `network port broadcast-domain create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Sie können den Pool mit IP-Adressen definieren, die in der Broadcast-Domäne verfügbar sein werden, indem Sie ein Subnetz erstellen. Alternativ können Sie dem IPspace SVMs und Schnittstellen zuweisen. Weitere Informationen finden Sie unter "Cluster- und SVM-Peering".

Wenn Sie den Namen einer vorhandenen Broadcast-Domäne ändern müssen, verwenden Sie den `network port broadcast-domain rename` Befehl.

Erfahren Sie mehr über `network port broadcast-domain rename` in der "ONTAP-Befehlsreferenz".

Hinzufügen oder Entfernen von Ports aus einer ONTAP Broadcast-Domäne

Broadcast-Domänen werden automatisch während der Erstellung des Clusters oder dem Beitritt zum Cluster erstellt. Ports müssen nicht manuell aus Broadcast-Domänen entfernt werden.

Wenn sich die Erreichbarkeit des Netzwerkports entweder durch die physische Netzwerkverbindung oder durch die Switch-Konfiguration geändert hat und ein Netzwerkanschluss in eine andere Broadcast-Domäne gehört, lesen Sie das folgende Thema:

"Port-Erreichbarkeit reparieren"

Das Hinzufügen oder Entfernen von Ports für Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Informationen zum Hinzufügen oder Entfernen von Ports aus Broadcast-Domänen in einem Netzwerk mit ONTAP 9.7 und früher finden Sie unter "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne (ONTAP 9.7 und früher)".

System Manager

Ab ONTAP 9.14.1 können Sie Ethernet-Ports in Broadcast-Domänen mit System Manager neu zuweisen. Es wird empfohlen, jeden Ethernet-Port einer Broadcast-Domäne zuzuweisen. Wenn Sie also die Zuweisung eines Ethernet-Ports zu einer Broadcast-Domäne aufheben, müssen Sie ihn einer anderen Broadcast-Domäne zuweisen.

Schritte

So weisen Sie Ethernet-Ports neu zu:

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie im Abschnitt **Broadcast Domains** neben dem Domainnamen aus ⋮ .
3. Wählen Sie im Dropdown-Menü die Option **Bearbeiten** aus.
4. Deaktivieren Sie auf der Seite **Broadcast Domain bearbeiten** die Ethernet-Ports, die Sie einer anderen Domäne neu zuweisen möchten.
5. Für jeden abgewählten Port wird das Fenster **Ethernet-Port neu zuweisen** angezeigt. Wählen Sie die Broadcast-Domain aus, der Sie den Port neu zuweisen möchten, und wählen Sie dann **Neu zuweisen** aus.
6. Wählen Sie alle Ports aus, die Sie der aktuellen Broadcast-Domäne zuweisen möchten, und speichern Sie die Änderungen.

CLI

Wenn sich die Erreichbarkeit des Netzwerkports entweder durch die physische Netzwerkverbindung oder durch die Switch-Konfiguration geändert hat und ein Netzwerkanschluss in eine andere Broadcast-Domäne gehört, lesen Sie das folgende Thema:

"Port-Erreichbarkeit reparieren"

Alternativ können Sie mit dem `network port broadcast-domain add-ports` `network port broadcast-domain remove-ports` Befehl oder den Ports manuell aus Broadcast-Domänen hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Ports, die einer Broadcast-Domäne hinzugefügt werden sollen, dürfen nicht einer anderen Broadcast-Domäne angehören.
- Ports, die bereits zu einer Schnittstellengruppe gehören, können nicht einzeln einer Broadcast-Domäne hinzugefügt werden.

Über diese Aufgabe

Folgende Regeln gelten beim Hinzufügen und Entfernen von Netzwerkports:

Wenn Ports hinzugefügt werden…	Wenn Ports entfernt…
Bei den Ports kann es sich um Netzwerkports, VLANs oder Interface Groups (ifrps) handeln.	K. A.
Die Ports werden der systemdefinierten Failover-Gruppe der Broadcast-Domäne hinzugefügt.	Die Ports werden von allen Failover-Gruppen in der Broadcast-Domäne entfernt.

Die MTU der Ports wird auf den in der Broadcast-Domäne festgelegten MTU-Wert aktualisiert.	Die MTU der Ports bleibt unverändert.
Der IPspace der Ports wird auf den IPspace-Wert der Broadcast-Domain aktualisiert.	Die Ports werden in den IP-Bereich 'Default' ohne Broadcast-Domain-Attribut verschoben.

Wenn Sie den letzten Mitgliedsport einer Schnittstellengruppe mit dem `network port ifgrp remove-port` Befehl entfernen, wird der Port der Schnittstellengruppe aus der Broadcast-Domäne entfernt, da ein leerer Schnittstellengruppen-Port in einer Broadcast-Domäne nicht zulässig ist. Erfahren Sie mehr über `network port ifgrp remove-port` in der "ONTAP-Befehlsreferenz".

Schritte

1. Mit dem `network port show` Befehl können Sie die derzeit einer Broadcast-Domäne zugewiesenen oder nicht zugewiesenen Ports anzeigen.
2. Hinzufügen oder Entfernen von Netzwerk-Ports aus der Broadcast-Domäne:

Ihr Ziel ist	Verwenden…
Fügen Sie Ports zu einer Broadcast-Domäne hinzu	`network port broadcast-domain add-ports`
Entfernen Sie Ports aus einer Broadcast-Domäne	`network port broadcast-domain remove-ports`

3. Überprüfen Sie, ob die Ports der Broadcast-Domäne hinzugefügt oder entfernt wurden:

   `network port show`

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Beispiele für das Hinzufügen und Entfernen von Ports

Mit dem folgenden Befehl wird Port e0g am Node Cluster-1-01 und Port e0g am Node Cluster-1-02 zur Broadcast-Domäne bcast1 im Standard-IPspace hinzugefügt:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

Mit dem folgenden Befehl werden zwei Cluster-Ports zum Broadcast Domain Cluster im Cluster IPspace hinzugefügt:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

Mit dem folgenden Befehl wird Port e0e auf Node cluster1-01 aus Broadcast-Domäne bcast1 im Standard-IPspace entfernt:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

Erfahren Sie mehr über `network port broadcast-domain remove-ports` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Reparieren Sie die Erreichbarkeit des ONTAP-Anschlusses

Broadcast-Domänen werden automatisch erstellt. Wenn jedoch ein Port neu konfiguriert oder die Switch-Konfiguration geändert wird, muss möglicherweise ein Port in eine andere Broadcast-Domäne repariert werden (neu oder vorhanden).

ONTAP erkennt und empfiehlt Lösungen für Netzwerkverkabelungen automatisch, basierend auf der Layer-2-Erreichbarkeit von Broadcast-Domain-Komponente (ethernet-Ports).

Eine falsche Verdrahtung während kann zu einer unerwarteten Zuweisung des Broadcast-Domain-Ports führen. Ab ONTAP 9.10.1 überprüft der Cluster automatisch Netzwerkverkabelungen, indem er nach der Cluster-Einrichtung die Port-Erreichbarkeit überprüft oder wenn ein neuer Node einem vorhandenen Cluster Beitritt.

System Manager

Wenn ein Problem mit der Fähigkeit zur Port-Wiederherstellung erkannt wird, empfiehlt System Manager einen Reparaturvorgang, um das Problem zu beheben.

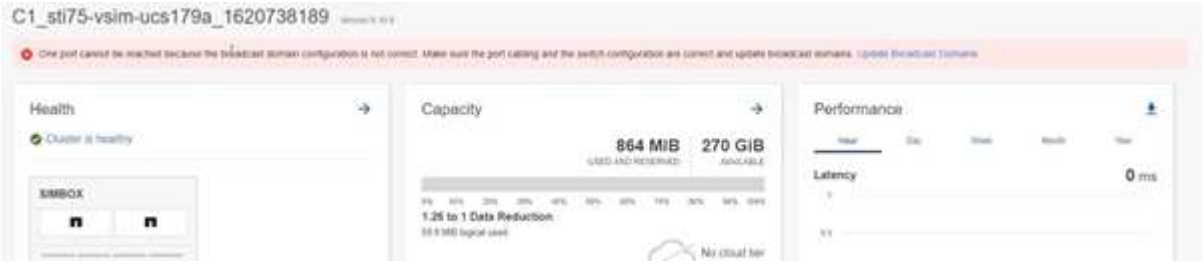
Nach der Einrichtung des Clusters werden Netzwerkverkabelungen auf dem Dashboard gemeldet.

Nach dem Verbinden eines neuen Node zu einem Cluster werden auf der Seite Nodes Netzwerkverkabelungen angezeigt.

Sie können auch den Zustand der Netzwerkverkabelung im Netzwerkdiagramm anzeigen. Die Probleme mit der Port-Erreichbarkeit werden im Netzwerkdiagramm durch ein rotes Fehlersymbol angezeigt.

Nach der Cluster-Einrichtung

Nachdem Sie den Cluster eingerichtet haben, wird im Dashboard eine Meldung angezeigt, wenn das System ein Problem mit der Netzwerkverkabelung feststellt.



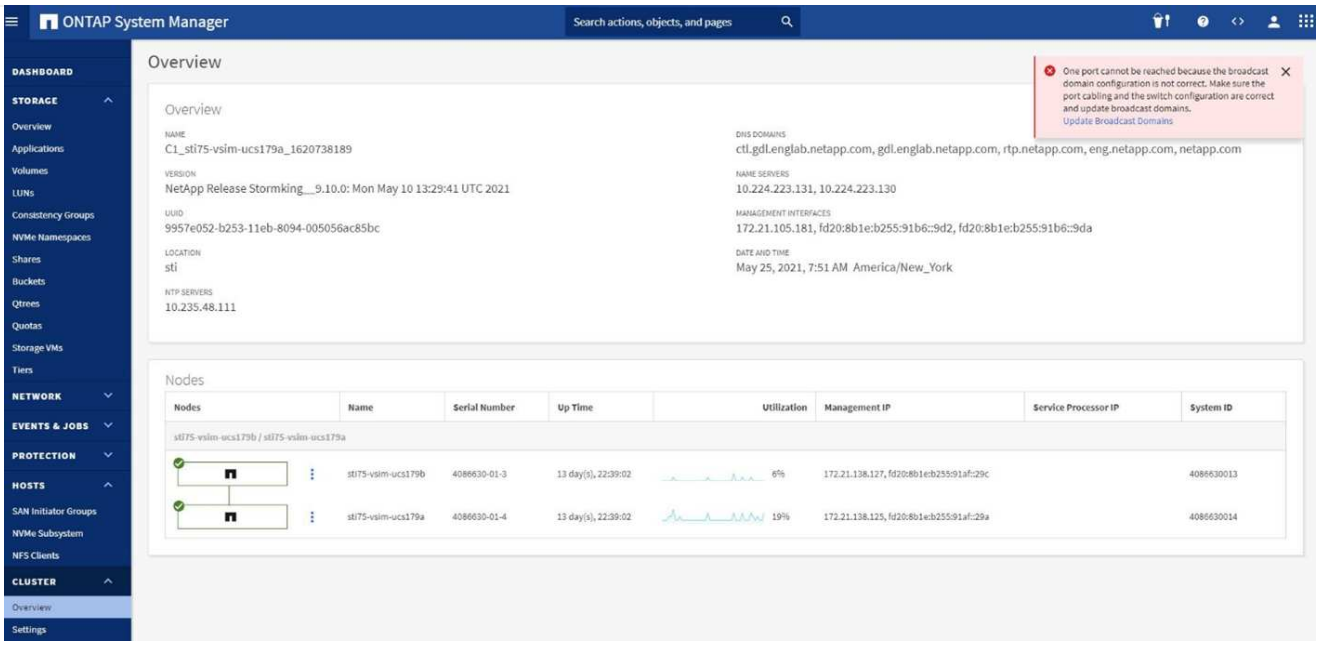
Schritte

1. Korrigieren Sie die Verkabelung wie in der Meldung vorgeschlagen.
2. Klicken Sie auf den Link, um das Dialogfeld Broadcast-Domänen aktualisieren zu starten. Das Dialogfeld Broadcast-Domänen aktualisieren wird geöffnet.

3. Überprüfen Sie die Informationen über den Port, einschließlich des Nodes, der Probleme, der aktuellen Broadcast-Domäne und der erwarteten Broadcast-Domäne.
4. Wählen Sie die Ports aus, die Sie reparieren möchten, und klicken Sie auf **Fix**. Das System verschiebt die Ports von der aktuellen Broadcast-Domäne in die erwartete Broadcast-Domäne.

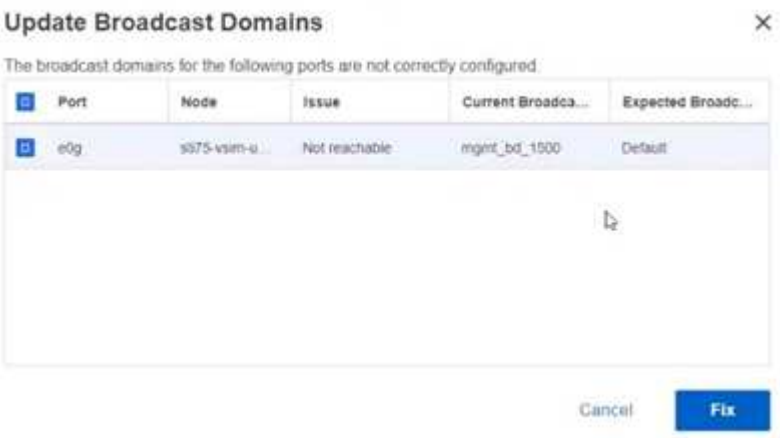
Post-Node beitreten

Nach dem Verbinden eines neuen Knotens zu einem Cluster wird auf der Seite Knoten eine Meldung angezeigt, wenn das System ein Netzwerkverkabelungsproblem erkennt.



Schritte

1. Korrigieren Sie die Verkabelung wie in der Meldung vorgeschlagen.
2. Klicken Sie auf den Link, um das Dialogfeld Broadcast-Domänen aktualisieren zu starten. Das Dialogfeld Broadcast-Domänen aktualisieren wird geöffnet.



3. Überprüfen Sie die Informationen über den Port, einschließlich des Nodes, der Probleme, der aktuellen Broadcast-Domäne und der erwarteten Broadcast-Domäne.
4. Wählen Sie die Ports aus, die Sie reparieren möchten, und klicken Sie auf **Fix**. Das System verschiebt die Ports von der aktuellen Broadcast-Domäne in die erwartete Broadcast-Domäne.

CLI

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Über diese Aufgabe

Ein Befehl steht zur Verfügung, um die Broadcast-Domänenkonfiguration für einen Port automatisch zu reparieren, der auf der von ONTAP erkannten Layer 2-Erreichbarkeit basiert.

Schritte

1. Überprüfen Sie die Switch-Konfiguration und -Verkabelung.

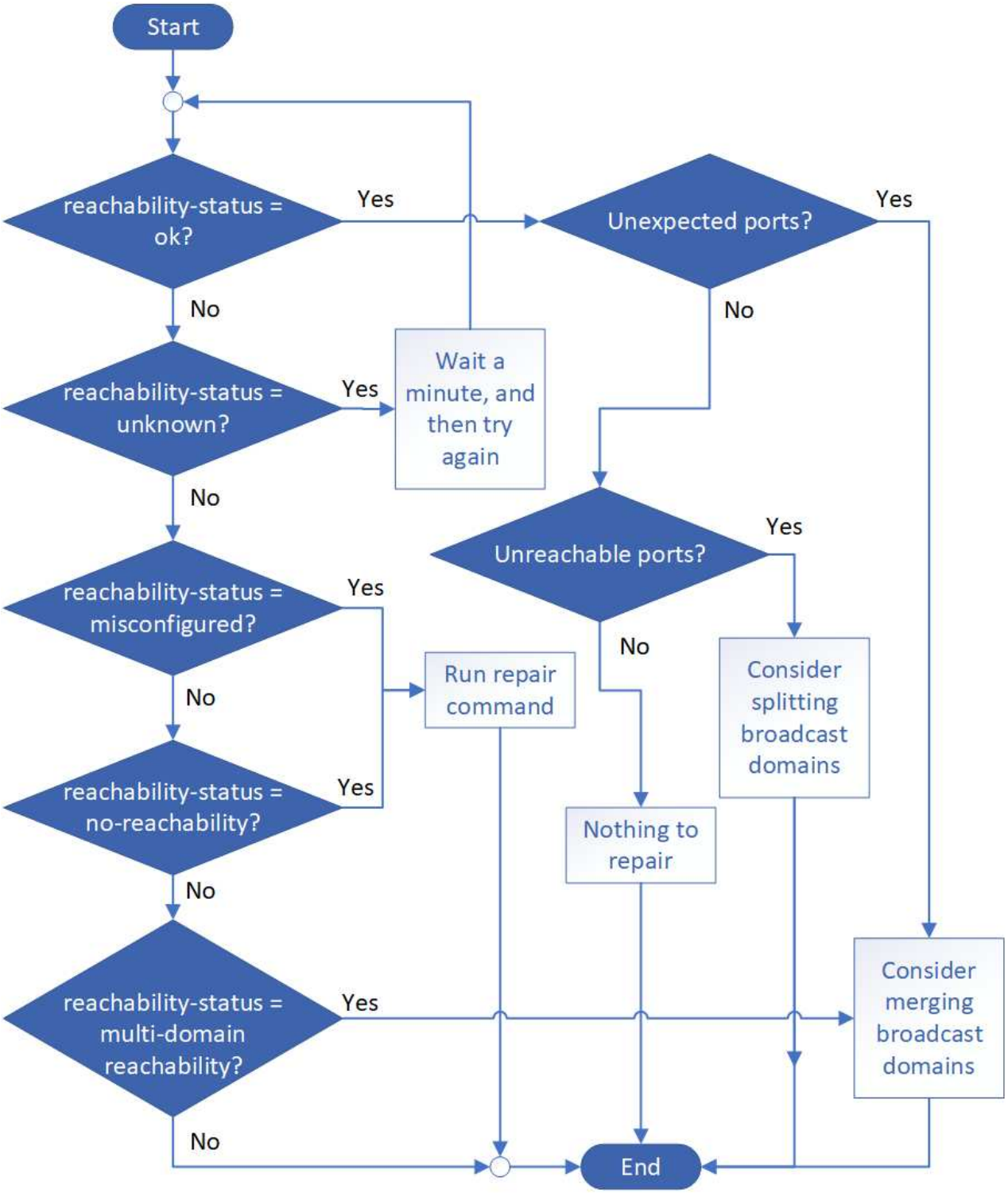
2. Überprüfen Sie die Erreichbarkeit des Ports:

   `network port reachability show -detail -node -port`

   Die Befehlsausgabe enthält Ergebnisse zur Wiederherstellung.

   Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".

3. Verwenden Sie den folgenden Entscheidungsbaum und die folgende Tabelle, um die Ergebnisse der Nachachbarkeit zu verstehen und zu bestimmen, welche, wenn überhaupt, als Nächstes zu tun.



Erreichbarkeit-Status	Beschreibung
ok	Der Port verfügt über eine Layer 2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne. Wenn der Status der Erreichbarkeit „ok“ ist, aber es „unerwartete Ports“ gibt, sollten Sie eine oder mehrere Broadcast-Domänen zusammenführen. Weitere Informationen finden Sie in der folgenden Zeile „*Unexpected Ports*“. Wenn der Status „Erreichbarkeit“ „ok“ lautet, aber „nicht erreichbare Ports“ vorhanden sind, sollten Sie eine oder mehrere Broadcast-Domänen aufteilen. Weitere Informationen finden Sie in der folgenden Zeile *Unerreichbare Ports*. Wenn der Status „Erreichbarkeit“ „ok“ lautet und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist die Konfiguration korrekt.
Unerwartete Ports	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Prüfen Sie die physische Konnektivität und Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domäne des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen".
Nicht erreichbare Ports	Wenn eine einzelne Broadcast-Domäne in zwei unterschiedliche Wiederachabilität-Sets partitioniert wurde, können Sie eine Broadcast-Domäne teilen, um die ONTAP-Konfiguration mit der physischen Netzwerktopologie zu synchronisieren. In der Regel definiert die Liste der nicht erreichbaren Ports den Satz von Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollten, nachdem Sie überprüft haben, dass die physische und die Switch-Konfiguration korrekt ist. Weitere Informationen finden Sie unter "Teilen von Broadcast-Domänen auf".
Falsch konfigurierte Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit seiner zugewiesenen Broadcast-Domäne; der Port besitzt jedoch Layer 2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port der Broadcast-Domäne zu, der sie nachzuweisen kann: `network port reachability repair -node -port`

Keine Erreichbarkeit	Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit für eine vorhandene Broadcast-Domäne. Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port einer neuen automatisch erstellten Broadcast-Domäne im Standard-IPspace zu: `network port reachability repair -node -port` **Hinweis:** Wenn alle Interface Group (ifgrp) Member Ports berichten `no-reachability`, `network port reachability repair` würde das Ausführen des Befehls auf jedem Member Port dazu führen, dass jeder von der ifgrp entfernt und in eine neue Broadcast-Domain platziert wird, was schließlich dazu führt, dass der ifgrp selbst entfernt wird. `network port reachability repair`Überprüfen Sie vor dem Ausführen des Befehls, ob die erreichbare Broadcast-Domäne des Ports basierend auf der physischen Netzwerktopologie den Erwartungen entspricht. Erfahren Sie mehr über `network port reachability repair` in der "ONTAP-Befehlsreferenz".
Multi-Domain-Erreichbarkeit	Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne. Prüfen Sie die physische Konnektivität und Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domäne des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen".
Unbekannt	Wenn der Status „unbekannt“ lautet, warten Sie einige Minuten, und versuchen Sie den Befehl erneut.

Nachdem Sie einen Port repariert haben, überprüfen Sie, ob LIFs und VLANs verschoben wurden. Wenn der Port Teil einer Schnittstellengruppe war, müssen Sie auch verstehen, was mit dieser Schnittstellengruppe passiert ist.

LIFs

Wenn ein Port repariert und in eine andere Broadcast-Domäne verschoben wird, werden alle LIFs, die auf dem reparierten Port konfiguriert wurden, automatisch einem neuen Home Port zugewiesen. Dieser Startport wird, falls möglich, aus derselben Broadcast-Domäne auf demselben Node ausgewählt. Alternativ wird ein Home-Port von einem anderen Node ausgewählt, oder wenn keine geeigneten Home-Ports vorhanden sind, wird der Home-Port gelöscht.

Wenn der Home Port eines LIF auf einen anderen Node verschoben oder gelöscht wird, gilt die LIF als „verschoben“. Sie können diese vertriebenen LIFs mit dem folgenden Befehl anzeigen:

```
displaced-interface show
```

Wenn vertriebene LIFs vorhanden sind, müssen Sie Folgendes tun:

- Stellen Sie die Homepage der vertriebenen LIF wieder her:

```
displaced-interface restore
```

- Legen Sie die Startseite der LIF manuell fest:

  ```
  network interface modify -home-port -home-node
  ```

  Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

- Entfernen Sie den Eintrag aus der Tabelle "Vertriebene-Schnittstelle", wenn Sie mit dem LIF aktuell konfiguriert Home zufrieden sind:

  ```
  displaced-interface delete
  ```

VLANs

Wenn der reparierte Port VLANs hatte, werden diese VLANs automatisch gelöscht, aber auch als „verdrängt“ aufgezeichnet. Sie können diese verschobenen VLANs anzeigen:

```
displaced-vlans show
```

Wenn vertriebene VLANs vorhanden sind, müssen Sie Folgendes tun:

- Stellen Sie die VLANs an einem anderen Port wieder her:

  ```
  displaced-vlans restore
  ```

- Entfernen Sie den Eintrag aus der Tabelle „Vertriebene-vlans“:

  ```
  displaced-vlans delete
  ```

Interface Groups

Wenn der reparierte Port Teil einer Schnittstellengruppe war, wird er von dieser Schnittstellengruppe entfernt. Wenn es der einzige Mitgliedsport war, der der Schnittstellengruppe zugewiesen wurde, wird die Schnittstellengruppe selbst entfernt.

Verwandte Informationen

- "Überprüfen Sie die Netzwerkkonfiguration nach dem Upgrade"
- "Überwachen Sie die Erreichbarkeit von Netzwerkports"
- "ONTAP-Befehlsreferenz"

Verschieben Sie ONTAP Broadcast-Domänen in IPspaces

Ab ONTAP 9.8 können Sie die Broadcast-Domänen, die das System basierend auf der Erreichbarkeit von Layer 2 erstellt hat, in die von Ihnen erstellten IPspaces verschieben.

Bevor Sie die Broadcast-Domäne verschieben, müssen Sie die Erreichbarkeit der Ports in Ihren Broadcast-Domänen überprüfen.

Durch das automatische Scannen von Ports kann bestimmt werden, welche Ports sich gegenseitig erreichen und in derselben Broadcast-Domäne platzieren können, aber dieser Scan kann den entsprechenden IPspace nicht ermitteln. Wenn die Broadcast-Domäne in einem nicht standardmäßigen IPspace gehört, müssen Sie sie

manuell verschieben, indem Sie die Schritte in diesem Abschnitt verwenden.

Bevor Sie beginnen

Broadcast-Domänen werden automatisch als Teil der Cluster-Erstellung und dem Beitritt konfiguriert. ONTAP definiert die Broadcast-Domäne „Standard“ als Satz von Ports mit Layer-2-Konnektivität zum Home Port der Managementoberfläche auf dem ersten im Cluster erstellten Node. Andere Broadcast-Domänen werden, falls erforderlich, erstellt und werden mit **Default-1**, **Default-2** usw. bezeichnet.

Wenn ein Knoten einem vorhandenen Cluster beitreten wird, werden ihre Netzwerkports basierend auf der Reachability der Ebene 2 automatisch zu bestehenden Broadcast-Domänen verbunden. Wenn sie nicht auf eine vorhandene Broadcast-Domäne hin- und wieder verfügbar sind, werden die Ports in eine oder mehrere neue Broadcast-Domänen platziert.

Über diese Aufgabe

- Ports mit Cluster-LIFs werden automatisch im IPspace „Cluster“ platziert.
- Ports, die auf den Home Port der Node-Management-LIF zugreifen können, werden in der Broadcast-Domäne „Standard“ platziert.
- Andere Broadcast-Domänen werden von ONTAP automatisch als Teil der Cluster-Erstellung oder dem Cluster-Vorgang hinzugefügt.
- Wenn Sie VLANs und Schnittstellengruppen hinzufügen, werden sie ca. eine Minute nach der Erstellung automatisch in die entsprechende Broadcast-Domäne platziert.

Schritte

1. Überprüfen Sie die Erreichbarkeit der Ports in Ihren Broadcast-Domänen. ONTAP überwacht automatisch die Reachabilität der Ebene 2. Mit dem folgenden Befehl können Sie überprüfen, ob jeder Port einer Broadcast-Domäne hinzugefügt wurde und auf „ok“-Erreichbarkeit verfügt.

   ```
   network port reachability show -detail
   ```

   Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".

2. Bei Bedarf Broadcast-Domänen in andere IPspaces verschieben:

   ```
   network port broadcast-domain move
   ```

   Beispiel: Wenn Sie eine Broadcast-Domäne von „Standard“ auf „ips1“ verschieben möchten:

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Verwandte Informationen

- "Übertragung von Broadcast-Domänen des Netzwerk-Ports"

Teilen Sie ONTAP Broadcast-Domänen auf

Wenn sich die Erreichbarkeit des Netzwerkports geändert hat, entweder durch physische Netzwerkverbindung oder durch Switch-Konfiguration, Und eine Gruppe von Netzwerkports, die zuvor in einer einzigen Broadcast-Domäne konfiguriert waren, wurde in zwei verschiedene Reachability Sets partitioniert. Sie können eine Broadcast-Domäne teilen, um die ONTAP Konfiguration mit der physischen Netzwerktopologie zu

synchronisieren.

> Das Verfahren zum Aufteilen von Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie Broadcast-Domänen in einem Netzwerk mit ONTAP 9.7 und früher aufteilen müssen, lesen Sie "Teilen von Broadcast-Domänen (ONTAP 9.7 oder früher)".

Um zu bestimmen, ob eine Broadcast-Domäne des Netzwerkports in mehrere Reachability Sets partitioniert ist, verwenden Sie den `network port reachability show -details` Befehl und achten Sie darauf, welche Ports nicht miteinander verbunden sind („unerreichbare Ports“). In der Regel definiert die Liste der nicht erreichbaren Ports den Satz von Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollen, nachdem Sie überprüft haben, dass die physische und die Switch-Konfiguration korrekt ist. Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".

Schritt

Aufteilen einer Broadcast-Domäne in zwei Broadcast-Domänen:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` Ist der Name des ipspace, in dem sich die Broadcast-Domain befindet.
- `-broadcast-domain` Ist der Name der Broadcast-Domäne, die geteilt werden soll.
- `-new-broadcast-domain` Ist der Name der neuen Broadcast-Domäne, die erstellt werden soll.
- `-ports` Ist der Knotenname und der Port, der der neuen Broadcast-Domäne hinzugefügt werden soll.

Verwandte Informationen

- "Aufteilung der Broadcast-Domäne des Netzwerk-Ports"

Zusammenführen von ONTAP Broadcast-Domänen

Wenn sich die Erreichbarkeit des Netzwerkports geändert hat, entweder durch die physische Netzwerkkonnektivität oder durch die Switch-Konfiguration und zwei Gruppen von Netzwerkports, die zuvor in mehreren Broadcast-Domänen konfiguriert waren, nun alle über eine gemeinsame Erreichbarkeit verfügen, kann das Zusammenführen zweier Broadcast-Domänen verwendet werden, um die ONTAP-Konfiguration mit der physischen Netzwerktopologie zu synchronisieren.

> Das Verfahren zum Zusammenführen von Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie Broadcast-Domänen in einem Netzwerk zusammenführen müssen, das ONTAP 9.7 und früher ausführt, finden Sie "Broadcast-Domänen zusammenführen (ONTAP 9.7 oder früher)"weitere Informationen unter .

Um festzustellen, ob mehrere Broadcast-Domänen zu einem Erreichbarkeitssatz gehören, verwenden Sie die `network port reachability show -details` Befehl und achten Sie darauf, welche in einer anderen Broadcast-Domäne konfigurierten Ports tatsächlich miteinander verbunden sind („Unerwartete Ports“). In der Regel definiert die Liste der unerwarteten Ports den Satz von Ports, die in die Broadcast-Domäne zusammengeführt werden sollen, nachdem Sie überprüft haben, ob die physische Konfiguration und die

Switch-Konfiguration korrekt sind.

Erfahren Sie mehr über `network port reachability show` in der "ONTAP-Befehlsreferenz".

Schritt

Die Ports aus einer Broadcast-Domäne in eine vorhandene Broadcast-Domäne zusammenführen:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` Ist der Name des ipspace, in dem sich die Broadcast-Domänen befinden.
- `-broadcast-domain` Ist der Name der Broadcast-Domäne, die zusammengeführt wird.
- `-into-broadcast-domain` Ist der Name der Broadcast-Domäne, die zusätzliche Ports empfängt.

Verwandte Informationen

- "Netzwerk-Port Broadcast-Domain-Merge"

Ändern Sie den MTU-Wert für Ports in einer ONTAP-Broadcast-Domäne

Sie können den MTU-Wert für eine Broadcast-Domäne ändern, um den MTU-Wert für alle Ports in dieser Broadcast-Domäne zu ändern. Dies kann getan werden, um Topologieänderungen zu unterstützen, die im Netzwerk vorgenommen wurden.

Das Verfahren zum Ändern des MTU-Werts für Broadcast-Domänenports unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie den MTU-Wert für Broadcast-Domänenports in einem Netzwerk mit ONTAP 9.7 und früher ändern müssen, lesen Sie "Ändern des MTU-Werts für Ports in einer Broadcast-Domäne (ONTAP 9.7 und früher)".

Bevor Sie beginnen

Der MTU-Wert muss mit allen mit diesem Layer-2-Netzwerk verbundenen Geräten übereinstimmen, außer für den E0M-Port-Management-Datenverkehr.

Über diese Aufgabe

Eine Änderung des MTU-Wertes führt zu einer kurzen Unterbrechung des Datenverkehrs über die betroffenen Ports. Das System zeigt eine Aufforderung an, die Sie mit y beantworten müssen, um die MTU-Änderung vorzunehmen.

Schritt

Ändern Sie den MTU-Wert für alle Ports in einer Broadcast-Domäne:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` Ist der Name der Broadcast-Domäne.
- `mtu` Ist die MTU-Größe für IP-Pakete; 1500 und 9000 sind typische Werte.

- `ipspace` Ist der Name des IPspaces, in dem sich diese Broadcast-Domäne befindet. Der IPspace „Standard“ wird verwendet, es sei denn, Sie geben einen Wert für diese Option an. Mit dem folgenden Befehl wird die MTU für alle Ports in der Broadcast-Domäne bcast1 auf 9000 geändert:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

Verwandte Informationen

- "Netzwerk-Port Broadcast-Domain ändern"

Anzeigen von ONTAP Broadcast-Domänen

Sie können die Liste der Broadcast-Domänen innerhalb jedes IPspaces in einem Cluster anzeigen. In der Ausgabe werden außerdem die Portliste und der MTU-Wert für jede Broadcast-Domäne angezeigt.

Das Verfahren zur Anzeige von Broadcast-Domänen unterscheidet sich in ONTAP 9.7 und früheren Versionen. Wenn Sie Broadcast-Domänen in einem Netzwerk anzeigen müssen, auf dem ONTAP 9.7 und früher ausgeführt wird, finden Sie weitere Informationen unter "Broadcast-Domänen anzeigen (ONTAP 9.7 oder früher)".

Schritt

Zeigen Sie die Broadcast-Domänen und die zugehörigen Ports im Cluster an:

```
network port broadcast-domain show
```

Mit dem folgenden Befehl werden alle Broadcast-Domänen und die zugehörigen Ports im Cluster angezeigt:

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

Mit dem folgenden Befehl werden die Ports in der Standard-1 Broadcast-Domäne angezeigt, die einen Aktualisierungsstatus aufweisen, was darauf hinweist, dass der Port nicht ordnungsgemäß aktualisiert werden konnte:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Default Default-1   1500
                           cluster-1-02:e0g       error
```

Verwandte Informationen

- "Netzwerk-Port Broadcast-Domain anzeigen"

ONTAP Broadcast-Domänen löschen

Wenn Sie keine Broadcast-Domain mehr benötigen, können Sie sie löschen. Dadurch werden die Ports, die dieser Broadcast-Domäne zugeordnet sind, in den „Standard“-IPspace verschoben.

Bevor Sie beginnen

Der zu löschenden Broadcast-Domäne dürfen keine Subnetze, Netzwerkschnittstellen oder SVMs zugeordnet sein.

Über diese Aufgabe

- Die vom System erstellte Broadcast-Domäne „Cluster“ kann nicht gelöscht werden.
- Beim Löschen der Broadcast-Domäne werden alle Failover-Gruppen in Verbindung mit der Broadcast-Domäne entfernt.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager eine Broadcast-Domain löschen

Die Löschoption wird nicht angezeigt, wenn die Broadcast-Domäne Ports enthält oder einem Subnetz zugeordnet ist.

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Broadcast-Domäne**.
2. Wählen Sie ⋮ **> Löschen** neben der Broadcast-Domain, die Sie entfernen möchten.

CLI

Verwenden Sie die CLI, um eine Broadcast-Domain zu löschen

Schritt

Löschen einer Broadcast-Domäne:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

Mit dem folgenden Befehl wird die Broadcast-Domäne Default-1 in IPspace ipspac1 gelöscht:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Verwandte Informationen

- "Netzwerk-Port Broadcast-Domain löschen"

Failover-Gruppen und Richtlinien

Erfahren Sie mehr über LIF Failover in ONTAP-Netzwerken

Der Begriff LIF-Failover bezieht sich auf die automatische Migration eines LIF zu einem anderen Netzwerkport als Reaktion auf einen Link-Fehler im aktuellen Port des LIF. Dies ist eine wichtige Komponente zur Hochverfügbarkeit der Verbindungen zu SVMs. Zum Konfigurieren von LIF Failover wird das Erstellen einer Failover-Gruppe, das Ändern der LIF zur Verwendung der Failover-Gruppe und das Angeben einer Failover-Richtlinie benötigt.

Eine Failover-Gruppe enthält einen Satz an Netzwerkports (physische Ports, VLANs und Interface Groups) von einem oder mehreren Nodes in einem Cluster. Die Netzwerk-Ports, die in der Failover-Gruppe vorhanden sind, definieren die Failover-Ziele, die für das LIF verfügbar sind. Einer Failover-Gruppe können Cluster-Management, Node-Management, Intercluster und NAS-Daten-LIFs zugewiesen werden.

Wenn eine LIF ohne ein gültiges Failover-Ziel konfiguriert ist, tritt ein Ausfall auf, wenn die LIF einen Failover versucht. Sie können die Failover-Konfiguration mit dem `network interface show -failover` Befehl überprüfen. Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Wenn Sie eine Broadcast-Domäne erstellen, wird automatisch eine Failover-Gruppe mit demselben Namen erstellt, die dieselben Netzwerk-Ports enthält. Diese Failover-Gruppe wird vom System automatisch verwaltet. Das bedeutet, dass beim Hinzufügen oder Entfernen von Ports aus der Broadcast-Domäne diese automatisch hinzugefügt oder aus dieser Failover-Gruppe entfernt werden. Dies wird für Administratoren, die nicht ihre eigenen Failover-Gruppen managen möchten, als effizient betrachtet.

Erstellen von ONTAP Failover-Gruppen

Sie erstellen eine Failover-Gruppe von Netzwerk-Ports, sodass ein LIF automatisch zu einem anderen Port migrieren kann, wenn am aktuellen Port des LIF ein Verbindungsfehler auftritt. Auf diese Weise kann das System den Netzwerkverkehr zu anderen verfügbaren Ports im Cluster umleiten.

Über diese Aufgabe

Mit dem `network interface failover-groups create` Befehl erstellen Sie die Gruppe und fügen der Gruppe Ports hinzu.

- Bei den Ports, die einer Failover-Gruppe hinzugefügt werden, können es sich um Netzwerk-Ports, VLANs oder Interface Groups (ifrps) handeln.
- Alle Ports, die der Failover-Gruppe hinzugefügt wurden, müssen zur gleichen Broadcast-Domäne gehören.
- Ein einzelner Port kann sich in mehreren Failover-Gruppen befinden.
- Wenn sich LIFs in unterschiedlichen VLANs oder Broadcast-Domänen befinden, müssen Failover-Gruppen für jede VLAN oder Broadcast-Domäne konfiguriert werden.
- Failover-Gruppen gelten nicht in SAN iSCSI- oder FC-Umgebungen.

Schritt

Erstellen einer Failover-Gruppe:

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* Ist der Name der SVM, die die Failover-Gruppe verwenden kann.
- *`failover_group_name`* Ist der Name der Failover-Gruppe, die Sie erstellen möchten.
- *`ports_list`* Ist die Liste der Ports, die der Failover-Gruppe hinzugefügt werden. Ports werden im Format *Node_Name>:<Port_number>* hinzugefügt, z. B. node1:e0c.

Mit dem folgenden Befehl wird die Failover-Gruppe fg3 für SVM vs3 erstellt und zwei Ports hinzugefügt:

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

Nachdem Sie fertig sind

- Sie sollten die Failover-Gruppe auf ein LIF anwenden, jetzt, wo die Failover-Gruppe erstellt wurde.
- Die Anwendung einer Failover-Gruppe, die kein gültiges Failover-Ziel für ein LIF bietet, führt zu einer Warnmeldung.

  Wenn ein LIF, das kein gültiges Failover-Ziel besitzt, ein Failover-Ziel vorschlägt, kann es zu einem Ausfall kommen.

- Erfahren Sie mehr über `network interface failover-groups create` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie ONTAP Failover-Einstellungen auf einer logischen Schnittstelle

Sie können eine LIF so konfigurieren, dass ein Failover auf eine bestimmte Gruppe von Netzwerkports durchgeführt wird, indem Sie eine Failover-Richtlinie und eine Failover-Gruppe auf die LIF anwenden. Sie können auch einen Failover eines LIF zu einem anderen Port deaktivieren.

Über diese Aufgabe

- Wenn eine LIF erstellt wird, ist standardmäßig ein LIF Failover aktiviert, und die Liste der verfügbaren Ziel-Ports wird basierend auf dem LIF-Typ und der Service-Richtlinie durch die Standard-Failover-Gruppe und die Failover-Richtlinie bestimmt.

  Ab Version 9.5 können Sie eine Service-Richtlinie für die LIF angeben, die definiert, welche Netzwerkservices die LIF verwenden können. Einige Netzwerkdienste zwingen ein LIF durch Failover-Einschränkungen.

  > Wenn sich die Service-Richtlinien einer LIF so ändern, dass Failover-Vorgänge noch weiter eingeschränkt werden, wird die Failover-Richtlinie des LIF automatisch vom System aktualisiert.

- Sie können das Failover-Verhalten der LIFs ändern, indem Sie im Befehl „Network Interface modify“ die Werte für die Parameter -Failover-Group und -Failover-Policy angeben.
- Die Änderung eines LIF, die dazu führt, dass kein gültiges Failover-Ziel für die LIF vorliegt, führt zu einer Warnmeldung.

  Wenn ein LIF, das kein gültiges Failover-Ziel besitzt, ein Failover-Ziel vorschlägt, kann es zu einem Ausfall kommen.

- Ab ONTAP 9.11.1 wird das LIF-Failover auf All-Flash-SAN-Array-Plattformen (ASA) automatisch auf neu erstellten iSCSI LIFs auf neu erstellten Storage-VMs aktiviert.

  Außerdem können Sie "Aktivieren Sie iSCSI-LIF-Failover manuell auf bereits vorhandenen iSCSI-LIFs"LIFs, die vor dem Upgrade auf ONTAP 9.11.1 oder höher erstellt wurden.

- In der folgenden Liste wird beschrieben, wie sich die Einstellung -Failover-Policy auf die Zielports auswirkt, die aus der Failover-Gruppe ausgewählt wurden:

Für iSCSI-LIF-Failover `local-only` `sfo-partner-only` `disabled` werden nur die Failover-Richtlinien, und unterstützt.

- `broadcast-domain-wide` Gilt für alle Ports auf allen Nodes in der Failover-Gruppe.
- `system-defined` Gilt nur für die Ports im Home Node von LIF und für einen anderen Node im Cluster – normalerweise ein nicht-SFO-Partner, falls vorhanden.
- `local-only` Gilt nur für diese Ports im Home Node des LIF.
- `sfo-partner-only` Gilt nur für die Ports im Home-Node der LIF und deren SFO-Partner.
- `disabled` Zeigt an, dass das LIF nicht für Failover konfiguriert ist.

Schritte

Konfigurieren Sie Failover-Einstellungen für eine vorhandene Schnittstelle:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Beispiele für die Konfiguration von Failover-Einstellungen und die Deaktivierung von Failover

Mit dem folgenden Befehl wird die Failover-Richtlinie auf Broadcast-Domain-Wide gesetzt und verwendet die Ports in der Failover-Gruppe fg3 als Failover-Ziele für LIF-Daten1 auf SVM vs3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

Mit dem folgenden Befehl wird das Failover für LIF-Daten 1 auf SVM vs3 deaktiviert:

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Verwandte Informationen

- "Netzwerkschnittstelle"

ONTAP-Befehle zum Managen von Failover-Gruppen und Richtlinien

Sie können die `network interface failover-groups` Befehle zum Verwalten von Failover-Gruppen verwenden. Sie verwenden den `network interface modify` Befehl zum Managen der Failover-Gruppen und Failover-Richtlinien, die auf eine LIF

angewendet werden.

Ihr Ziel ist	Befehl
Fügen Sie Netzwerkports zu einer Failover-Gruppe hinzu	`network interface failover-groups add-targets`
Entfernen Sie Netzwerkanschlüsse aus einer Failover-Gruppe	`network interface failover-groups remove-targets`
Ändern Sie Netzwerkports in einer Failover-Gruppe	`network interface failover-groups modify`
Zeigt die aktuellen Failover-Gruppen an	`network interface failover-groups show`
Konfigurieren Sie den Failover auf einem LIF	`network interface modify -failover -group -failover-policy`
Zeigen Sie die Failover-Gruppe und die Failover-Richtlinie an, die von den einzelnen LIFs verwendet werden	`network interface show -fields failover-group, failover-policy`
Benennen Sie eine Failover-Gruppe um	`network interface failover-groups rename`
Löschen einer Failover-Gruppe	`network interface failover-groups delete`

Das Ändern einer Failover-Gruppe, sodass sie kein gültiges Failover-Ziel für eine LIF im Cluster bietet, kann zu einem Ausfall führen, wenn ein LIF einen Failover versucht.

Verwandte Informationen

- "Netzwerkschnittstelle"

Subnetze (nur Cluster-Administratoren)

Weitere Informationen zu Subnetzen für das ONTAP-Netzwerk

Subnetze ermöglichen Ihnen die Zuweisung bestimmter IP-Adressen oder Pools für Ihre ONTAP-Netzwerkkonfiguration. Damit können Sie LIFs einfacher erstellen, indem Sie einen Subnetznamen angeben, anstatt die IP-Adresse und Netzwerkmaskenwerte angeben zu müssen.

Ein Subnetz wird innerhalb einer Broadcast-Domäne erstellt und enthält einen Pool von IP-Adressen, die zum gleichen Subnetz der Ebene 3 gehören. Beim Erstellen von LIFs werden IP-Adressen in einem Subnetz Ports in der Broadcast-Domäne zugewiesen. Wenn LIFs entfernt werden, werden die IP-Adressen an den Subnetz-Pool zurückgegeben und sind für zukünftige LIFs verfügbar.

Es wird empfohlen, Subnetze zu verwenden, da diese das Management von IP-Adressen viel einfacher machen und die Erstellung von LIFs etwas einfacher wird. Wenn Sie außerdem beim Definieren eines Subnetzes ein Gateway angeben, wird der SVM automatisch eine Standardroute hinzugefügt, wenn anhand dieses Subnetzes eine LIF erstellt wird.

Subnetze für das ONTAP-Netzwerk erstellen

Sie können ein Subnetz erstellen, um bestimmte Blöcke von IPv4- und IPv6-Adressen zuzuweisen, die später beim Erstellen von LIFs für die SVM verwendet werden.

Damit können Sie LIFs einfacher erstellen, indem Sie einen Subnetznamen angeben, anstatt für jede LIF IP-Adresse und Netzwerkmaskenwerte angeben zu müssen.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Die Broadcast-Domäne und der IPspace, in dem Sie das Subnetz hinzufügen möchten, müssen bereits vorhanden sein.

Über diese Aufgabe

- Alle Subnetznamen müssen innerhalb eines IPspaces eindeutig sein.
- Wenn Sie einem Subnetz IP-Adressbereiche hinzufügen, müssen Sie sicherstellen, dass sich im Netzwerk keine überlappenden IP-Adressen befinden, so dass unterschiedliche Subnetze oder Hosts nicht versuchen, dieselbe IP-Adresse zu verwenden.
- Wenn Sie beim Definieren eines Subnetzes ein Gateway angeben, wird der SVM automatisch eine Standardroute hinzugefügt, wenn anhand dieses Subnetzes eine LIF erstellt wird. Wenn Sie keine Subnetze verwenden oder wenn Sie beim Definieren eines Subnetzes kein Gateway angeben, müssen Sie mit dem `route create` Befehl manuell eine Route zur SVM hinzufügen.
- NetApp empfiehlt das Erstellen von Subnetzobjekten für alle LIFs auf Data SVMs. Dies ist besonders wichtig für MetroCluster-Konfigurationen, bei denen das Subnetz-Objekt es ONTAP ermöglicht, Failover-Ziele auf dem Ziel-Cluster zu bestimmen, da jedem Subnetz-Objekt eine zugeordnete Broadcast-Domäne zugeordnet ist.

Schritte

Sie können ein Subnetz mit ONTAP System Manager oder der ONTAP CLI erstellen.

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager ein Subnetz erstellen.

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Subnetze**.
2. Klicken Sie auf, + Add um ein Subnetz zu erstellen.
3. Benennen Sie das Subnetz.
4. Geben Sie die Subnetz-IP-Adresse an.
5. Stellen Sie die Subnetzmaske ein.
6. Definieren Sie den Bereich der IP-Adressen, aus denen das Subnetz besteht.
7. Falls nützlich, geben Sie ein Gateway an.
8. Wählen Sie die Broadcast-Domäne aus, zu der das Subnetz gehört.
9. Speichern Sie die Änderungen.
   a. Wenn die eingegebene IP-Adresse oder der eingegebene Bereich bereits von einer Schnittstelle verwendet wird, wird die folgende Meldung angezeigt:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Wenn Sie auf **OK** klicken, wird das vorhandene LIF dem Subnetz zugeordnet.

CLI

Verwenden Sie die CLI zum Erstellen eines Subnetzes.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` Ist der Name des Subnetzes der Ebene 3, das Sie erstellen möchten.

  Der Name kann eine Textfolge wie „Mgmt“ sein oder ein bestimmter Subnetz-IP-Wert wie 192.0.2.0/24.

- `broadcast_domain_name` Ist der Name der Broadcast-Domäne, in der sich das Subnetz befinden soll.
- `ipspace_name` Ist der Name des IPspaces, zu dem die Broadcast-Domäne gehört.

  Der IPspace „Standard“ wird verwendet, es sei denn, Sie geben einen Wert für diese Option an.

- `subnet_address` Ist die IP-Adresse und -Maske des Subnetzes, z. B. 192.0.2.0/24.
- `gateway_address` Ist das Gateway für die Standardroute des Subnetzes, z. B. 192.0.2.1.
- `ip_address_list` Ist die Liste oder der Bereich der IP-Adressen, die dem Subnetz zugewiesen werden.

  Die IP-Adressen können einzelne Adressen, eine Reihe von IP-Adressen oder eine Kombination in

einer durch Kommas getrennten Liste sein.

- Der Wert `true` kann für die `-force-update-lif-associations` Option festgelegt werden.

  Dieser Befehl schlägt fehl, wenn der Service-Prozessor oder die Netzwerkschnittstellen derzeit die IP-Adressen im angegebenen Bereich verwenden. Wenn Sie diesen Wert auf TRUE setzen, werden alle manuell adressierten Schnittstellen mit dem aktuellen Subnetz verknüpft, und der Befehl kann erfolgreich ausgeführt werden.

Mit dem folgenden Befehl wird Sub1 in Broadcast-Domäne erzeugt Standard-1 im Standard-IPspace. Es fügt eine IPv4-Subnetz-IP-Adresse und -Maske, das Gateway und eine Reihe von IP-Adressen hinzu:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

Mit dem folgenden Befehl wird Sub2 in Broadcast-Domain im IPspace „Standard“ erzeugt. Es fügt einen Bereich von IPv6-Adressen hinzu:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Sie können SVMs und Schnittstellen einem IPspace mithilfe der Adressen im Subnetz zuweisen.

Wenn Sie den Namen eines vorhandenen Subnetzes ändern müssen, verwenden Sie den `network subnet rename` Befehl.

Erfahren Sie mehr über `network subnet rename` in der "ONTAP-Befehlsreferenz".

Hinzufügen oder Entfernen von IP-Adressen aus einem Subnetz für das ONTAP-Netzwerk

Sie können IP-Adressen hinzufügen, wenn Sie zu Beginn ein Subnetz erstellen, oder Sie können IP-Adressen zu einem bereits vorhandenen Subnetz hinzufügen. Sie können auch IP-Adressen aus einem vorhandenen Subnetz entfernen. Damit können Sie nur die erforderlichen IP-Adressen für SVMs zuweisen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager IP-Adressen zu oder aus einem Subnetz hinzufügen oder entfernen

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Subnetze**.
2. Wählen Sie ⋮ **> Bearbeiten** neben dem Subnetz, das Sie ändern möchten.
3. IP-Adressen hinzufügen oder entfernen.
4. Speichern Sie die Änderungen.
   a. Wenn die eingegebene IP-Adresse oder der eingegebene Bereich bereits von einer Schnittstelle verwendet wird, wird die folgende Meldung angezeigt:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Wenn Sie auf **OK** klicken, wird das vorhandene LIF dem Subnetz zugeordnet.

CLI

Verwenden Sie die CLI, um IP-Adressen zu oder aus einem Subnetz hinzuzufügen oder zu entfernen

Über diese Aufgabe

Beim Hinzufügen von IP-Adressen wird ein Fehler angezeigt, wenn ein Service-Prozessor oder Netzwerkschnittstellen die IP-Adressen im hinzugefügten Bereich verwendet. Wenn Sie manuell adressierte Schnittstellen mit dem aktuellen Subnetz verknüpfen möchten, können Sie die `-force -update-lif-associations` Option auf einstellen `true`.

Wenn Sie die IP-Adressen entfernen, wird ein Fehler angezeigt, wenn ein Service-Prozessor oder Netzwerkschnittstellen die zu entfernenden IP-Adressen verwendet. Wenn die Schnittstellen die IP-Adressen nach dem Entfernen aus dem Subnetz weiterhin verwenden sollen, können Sie die `-force -update-lif-associations` Option auf einstellen `true`.

Schritt

IP-Adressen aus einem Subnetz hinzufügen oder entfernen:

Ihr Ziel ist	Befehl
Fügen Sie IP-Adressen zu einem Subnetz hinzu	Netzwerk-Subnetz-Add-Bereiche
Entfernen Sie IP-Adressen aus einem Subnetz	Entfernung von Netzwerksubnetzen

Mit dem folgenden Befehl werden die IP-Adressen 192.0.2.82 bis 192.0.2.85 zum Subnetz sub1 hinzugefügt:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

Mit dem folgenden Befehl wird die IP-Adresse 198.51.100.9 aus dem Subnetz sub3 entfernt:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

Wenn der aktuelle Bereich zwischen 1 und 10 und 20 bis 40 umfasst und Sie 11 bis 19 und 41 bis 50 hinzufügen möchten (was im Prinzip 1 bis 50 erlaubt), können Sie den vorhandenen Adressbereich mit dem folgenden Befehl überlappen. Dieser Befehl fügt nur die neuen Adressen hinzu und hat keine Auswirkung auf die vorhandenen Adressen:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

Erfahren Sie mehr über `network subnet add-ranges` und `network subnet remove-ranges` in der "ONTAP-Befehlsreferenz".

Ändern Sie die Subnetzeigenschaften für das ONTAP-Netzwerk

Sie können die Subnetzadresse und den Maskenwert, die Gateway-Adresse oder den IP-Adressbereich in einem vorhandenen Subnetz ändern.

Über diese Aufgabe

- Beim Ändern von IP-Adressen müssen Sie sicherstellen, dass sich keine überlappenden IP-Adressen im Netzwerk befinden, damit unterschiedliche Subnetze oder Hosts nicht versuchen, dieselbe IP-Adresse zu verwenden.
- Wenn Sie die Gateway-IP-Adresse hinzufügen oder ändern, wird das geänderte Gateway auf neue SVMs angewendet, wenn in ihnen ein LIF mit dem Subnetz erstellt wird. Es wird eine Standardroute zum Gateway für die SVM erstellt, wenn die Route nicht bereits vorhanden ist. Möglicherweise müssen Sie beim Ändern der Gateway-IP-Adresse eine neue Route zur SVM manuell hinzufügen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager Subnetzeigenschaften ändern

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Subnetze**.
2. Wählen Sie **> Bearbeiten** neben dem Subnetz, das Sie ändern möchten.
3. Nehmen Sie Änderungen vor.
4. Speichern Sie die Änderungen.
   a. Wenn die eingegebene IP-Adresse oder der eingegebene Bereich bereits von einer Schnittstelle verwendet wird, wird die folgende Meldung angezeigt:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Wenn Sie auf **OK** klicken, wird das vorhandene LIF dem Subnetz zugeordnet.

CLI

Verwenden Sie die CLI, um die Subnetzeigenschaften zu ändern

Schritt

Ändern der Subnetzeigenschaften:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` Ist der Name des Subnetzes, das Sie ändern möchten.
- `ipspace` Ist der Name des IPspaces, in dem sich das Subnetz befindet.
- `subnet` Ist die neue Adresse und Maske des Subnetzes, falls zutreffend, z. B. 192.0.2.0/24.
- `gateway` Ist das neue Gateway des Subnetzes, falls zutreffend, z. B. 192.0.2.1. Durch Eingabe von **''** wird der Gateway-Eintrag entfernt.
- `ip_ranges` Ist die neue Liste oder der neue Bereich von IP-Adressen, die dem Subnetz ggf. zugewiesen werden. Die IP-Adressen können einzelne Adressen, einen Bereich oder IP-Adressen oder eine Kombination aus einer kommagetrennten Liste sein. Der hier angegebene Bereich ersetzt die vorhandenen IP-Adressen.
- `force-update-lif-associations` Ist erforderlich, wenn Sie den IP-Adressbereich ändern. Sie können den Wert für diese Option auf **true** setzen, wenn Sie den Bereich der IP-Adressen ändern. Dieser Befehl schlägt fehl, wenn Service-Prozessor oder Netzwerkschnittstellen die IP-Adressen im angegebenen Bereich verwenden. Wenn Sie diesen Wert auf **true** setzen, werden alle manuell adressierten Schnittstellen mit dem aktuellen Subnetz verknüpft und der Befehl kann erfolgreich ausgeführt werden.

Mit dem folgenden Befehl wird die Gateway-IP-Adresse des Subnetzes sub3 geändert:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Erfahren Sie mehr über `network subnet modify` in der "ONTAP-Befehlsreferenz".

Subnetze für das ONTAP-Netzwerk anzeigen

Sie können die Liste der IP-Adressen anzeigen, die jedem Subnetz in einem IPspace zugewiesen sind. Die Ausgabe zeigt außerdem die Gesamtanzahl der in jedem Subnetz verfügbaren IP-Adressen und die Anzahl der derzeit verwendeten Adressen an.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager Subnetze anzeigen

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Subnetze**.
2. Die Liste der Subnetze anzeigen.

CLI

Verwenden Sie die CLI, um Subnetze anzuzeigen

Schritt

Die Liste der Subnetze und die zugehörigen IP-Adressbereiche anzeigen, die in diesen Subnetzen verwendet werden:

```
network subnet show
```

Mit dem folgenden Befehl werden die Subnetze und die Subnetzeigenschaften angezeigt:

```
network subnet show

IPspace: Default
Subnet                 Broadcast               Avail/
Name   Subnet          Domain    Gateway       Total   Ranges
-----  --------------- --------- ------------ --------
-----------------------
sub1   192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

Erfahren Sie mehr über `network subnet show` in der "ONTAP-Befehlsreferenz".

Subnetze aus dem ONTAP-Netzwerk löschen

Wenn Sie kein Subnetz mehr benötigen und die IP-Adressen, die dem Subnetz zugewiesen wurden, deallokalisieren möchten, können Sie es löschen.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager ein Subnetz löschen

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Subnetze**.
2. Wählen Sie ⋮ **> Löschen** neben dem Subnetz, das Sie entfernen möchten.
3. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um ein Subnetz zu löschen

Über diese Aufgabe

Sie erhalten einen Fehler, wenn ein Service-Prozessor oder Netzwerkschnittstellen derzeit IP-Adressen in den angegebenen Bereichen verwendet. Wenn die Schnittstellen auch nach dem Löschen des Subnetzes die IP-Adressen weiterhin verwenden sollen, können Sie die Option -Force-Update-lif-Associations auf „true“ setzen, um die Zuordnung des Subnetzes zu den LIFs zu entfernen.

Schritt

Subnetz löschen:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

Mit dem folgenden Befehl wird das Subnetz sub1 im IPspace ipspac1 gelöscht:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

Erfahren Sie mehr über `network subnet delete` in der "ONTAP-Befehlsreferenz".

SVMs für das ONTAP-Netzwerk erstellen

Sie müssen eine SVM erstellen, um Daten für die Clients bereitzustellen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen wissen, über welchen Sicherheitsstil das SVM-Root-Volume verfügt.

  Wenn Sie eine Hyper-V oder SQL Server über SMB-Lösung auf dieser SVM implementieren möchten, sollten Sie NTFS Sicherheitsstil für das Root-Volume verwenden. Volumes, die Hyper-V-Dateien oder SQL-Datenbankdateien enthalten, müssen zum Zeitpunkt ihrer Erstellung auf NTFS-Schutz gesetzt werden. Indem Sie den Sicherheitsstil des Root-Volumes auf NTFS einstellen, stellen Sie sicher, dass Sie nicht

versehentlich UNIX- oder Daten-Volumes im gemischten Sicherheitsstil erstellen.

- Ab ONTAP 9.13.1 können Sie die maximale Kapazität für eine Storage-VM festlegen. Sie können außerdem Warnmeldungen konfigurieren, wenn sich die SVM einem Kapazitätsschwellenwert nähert. Weitere Informationen finden Sie unter Management der SVM-Kapazität.

System Manager

Sie können mit System Manager eine Storage-VM erstellen.

Schritte

1. Wählen Sie **Storage VMs** aus.
2. Klicken Sie auf + Add , um eine Storage-VM zu erstellen.
3. Benennen Sie die Storage-VM.
4. Wählen Sie das Zugriffsprotokoll:
   - SMB/CIFS, NFS
   - ISCSI
   - FC
   - NVMe
     i. Wenn Sie **SMB/CIFS** aktivieren wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Administratorname	Geben Sie den Administratorbenutzernamen für die SMB/CIFS Storage VM an.
Passwort	Geben Sie das Administratorpasswort für die SMB/CIFS Storage-VM an.
Servername	Geben Sie den Servernamen für die SMB/CIFS-Storage-VM an.
Active Directory-Domäne	Geben Sie die Active Directory-Domäne an, die für die Benutzerauthentifizierung für die SMB/CIFS-Storage-VM verwendet werden soll.
Organisationseinheit	Geben Sie die Organisationseinheit innerhalb der Active Directory-Domäne an, die mit dem SMB/CIFS-Server verknüpft ist. „CN=Computer“ ist der Standardwert, der geändert werden kann.
Verschlüsselung der Daten beim Zugriff auf die Freigaben in der Storage-VM	Aktivieren Sie dieses Kontrollkästchen, um Daten mit SMB 3.0 zu verschlüsseln, um unberechtigten Dateizugriff auf Freigaben in der SMB/CIFS-Storage-VM zu verhindern.
Domänen	Fügen Sie die für die SMB/CIFS-Storage-VM aufgeführten Domänen hinzu, entfernen oder neu anordnen.
Name Server	Fügen Sie die Namensserver für die SMB/CIFS-Speicher-VM hinzu, entfernen Sie sie oder ordnen Sie sie neu an.

Standardsprache	Gibt die Standardeinstellung für die Sprachcodierung der Storage-VM und ihrer Volumes an. Verwenden Sie die CLI, um Einstellungen für einzelne Volumes innerhalb einer Storage VM zu ändern.
Netzwerkschnittstelle	Wählen Sie für jede für die Speicher-VM konfigurierte Netzwerkschnittstelle ein vorhandenes Subnetz aus (falls mindestens ein Subnetz vorhanden ist) oder geben Sie **ohne Subnetz** an und füllen Sie die Felder **IP-Adresse** und **Subnetzmaske** aus. Wenn nützlich, aktivieren Sie das Kontrollkästchen **Verwenden Sie dieselbe Subnetzmaske und dasselbe Gateway für alle der folgenden Schnittstellen**. Sie können zulassen, dass das System automatisch den Home-Port auswählen oder den Port, den Sie verwenden möchten, manuell aus der Liste auswählen.
Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Wenn Sie **NFS aktivieren** wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Kontrollkästchen Zugriff auf NFS-Clients zulassen	Wählen Sie dieses Kontrollkästchen aus, wenn alle Volumes, die auf der NFS Storage-VM erstellt wurden, den Root-Volume-Pfad „/“ zum Mounten und Traverse verwenden sollten. Fügen Sie der Exportrichtlinie „Standard“ Regeln hinzu, um unterbrechungsfreie Mount Traversal zu ermöglichen.

Regeln	Klicken Sie hier, + Add um Regeln zu erstellen. • Client-Spezifikation: Geben Sie die Hostnamen, IP-Adressen, Netzgruppen oder Domänen an. • Zugangsprotokolle: Wählen Sie eine Kombination der folgenden Optionen: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Zugriffsdetails: Geben Sie für jeden Benutzertyp die Zugriffsebene an, entweder schreibgeschützt, Lesen/Schreiben oder Superuser. Folgende Benutzertypen sind verfügbar: ◦ Alle ◦ Alle (als anonymer Benutzer) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Speichern Sie die Regel.
Standardsprache	Gibt die Standardeinstellung für die Sprachcodierung der Storage-VM und ihrer Volumes an. Verwenden Sie die CLI, um Einstellungen für einzelne Volumes innerhalb einer Storage VM zu ändern.
Netzwerkschnittstelle	Wählen Sie für jede für die Speicher-VM konfigurierte Netzwerkschnittstelle ein vorhandenes Subnetz aus (falls mindestens ein Subnetz vorhanden ist) oder geben Sie **ohne Subnetz** an und füllen Sie die Felder **IP-Adresse** und **Subnetzmaske** aus. Wenn nützlich, aktivieren Sie das Kontrollkästchen **Verwenden Sie dieselbe Subnetzmaske und dasselbe Gateway für alle der folgenden Schnittstellen**. Sie können zulassen, dass das System automatisch den Home-Port auswählen oder den Port, den Sie verwenden möchten, manuell aus der Liste auswählen.

Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Wenn Sie **iSCSI** aktivieren wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Netzwerkschnittstelle	Wählen Sie für jede für die Speicher-VM konfigurierte Netzwerkschnittstelle ein vorhandenes Subnetz aus (falls mindestens ein Subnetz vorhanden ist) oder geben Sie **ohne Subnetz** an und füllen Sie die Felder **IP-Adresse** und **Subnetzmaske** aus. Wenn nützlich, aktivieren Sie das Kontrollkästchen **Verwenden Sie dieselbe Subnetzmaske und dasselbe Gateway für alle der folgenden Schnittstellen**. Sie können zulassen, dass das System automatisch den Home-Port auswählen oder den Port, den Sie verwenden möchten, manuell aus der Liste auswählen.
Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Wenn Sie **FC aktivieren** wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Konfigurieren Sie FC-Ports	Wählen Sie die Netzwerkschnittstellen der Nodes aus, die in die Storage-VM einbezogen werden sollen. Es werden zwei Netzwerkschnittstellen pro Node empfohlen.
Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Wenn Sie **NVMe/FC** aktivieren wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Konfigurieren Sie FC-Ports	Wählen Sie die Netzwerkschnittstellen der Nodes aus, die in die Storage-VM einbezogen werden sollen. Es werden zwei Netzwerkschnittstellen pro Node empfohlen.
Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Wenn Sie **NVMe/TCP** aktivieren wählen, führen Sie die folgende Konfiguration aus:

Feld oder Kontrollkästchen aktivieren	Beschreibung
Netzwerkschnittstelle	Wählen Sie für jede für die Speicher-VM konfigurierte Netzwerkschnittstelle ein vorhandenes Subnetz aus (falls mindestens ein Subnetz vorhanden ist) oder geben Sie **ohne Subnetz** an und füllen Sie die Felder **IP-Adresse** und **Subnetzmaske** aus. Wenn nützlich, aktivieren Sie das Kontrollkästchen **Verwenden Sie dieselbe Subnetzmaske und dasselbe Gateway für alle der folgenden Schnittstellen**. Sie können zulassen, dass das System automatisch den Home-Port auswählen oder den Port, den Sie verwenden möchten, manuell aus der Liste auswählen.
Administratorkonto verwalten	Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Storage-VM-Administratorkonto verwalten möchten. Wenn diese Option ausgewählt ist, geben Sie den Benutzernamen und das Passwort an, bestätigen Sie das Passwort und geben Sie an, ob Sie eine Netzwerkschnittstelle für das Storage-VM-Management hinzufügen möchten.

1. Speichern Sie die Änderungen.

CLI

Verwenden Sie die ONTAP-CLI zum Erstellen eines Subnetzes.

Schritte

1. Legen Sie fest, welche Aggregate sich eignen, um das SVM-Root-Volume zu enthalten.

```
storage aggregate show -has-mroot false
```

Sie müssen ein Aggregat auswählen, das mindestens 1 GB freien Speicherplatz hat, um das Root-Volume zu enthalten. Wenn Sie beabsichtigen, NAS-Prüfungen auf der SVM zu konfigurieren, müssen Sie mindestens 3 GB zusätzlichen freien Speicherplatz auf dem Root-Aggregat haben, wobei der zusätzliche Speicherplatz verwendet wird, um das Auditing-Staging-Volume zu erstellen, wenn die Prüfung aktiviert ist.

> Wenn NAS-Auditing bereits auf einer vorhandenen SVM aktiviert ist, wird das Staging-Volume des Aggregats unmittelbar nach Abschluss der Aggregaterstellung erstellt.

2. Notieren Sie den Namen des Aggregats, auf dem Sie das SVM Root-Volume erstellen möchten.
3. Wenn Sie beim Erstellen der SVM eine Sprache angeben und den zu verwendenden Wert nicht kennen, identifizieren und notieren Sie den Wert der Sprache, die Sie angeben möchten:

   ```
   vserver create -language ?
   ```

4. Wenn Sie beim Erstellen der SVM eine Snapshot-Richtlinie angeben und den Namen der Richtlinie nicht kennen, führen Sie die verfügbaren Richtlinien auf, und identifizieren und notieren Sie den Namen der zu verwendenden Snapshot-Richtlinie:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. Wenn Sie beim Erstellen der SVM eine Kontingentrichtlinie angeben und den Namen der Richtlinie nicht kennen, führen Sie die verfügbaren Richtlinien aus und identifizieren und notieren Sie den Namen der zu verwendenden Kontingentrichtlinie:

   ```
   volume quota policy show -vserver vserver_name
   ```

6. SVM erstellen:

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. Vergewissern Sie sich, dass die SVM-Konfiguration richtig ist.

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In diesem Beispiel erstellt der Befehl im IPspace „ipspac1“ die SVM mit dem Namen „vs1“. Das Root-Volume heißt „vs1_Root“ und wird auf aggr3 mit NTFS-Sicherheitsstil erstellt.

Ab ONTAP 9.13.1 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei eine Durchsatzgrenze sowie eine Obergrenze für die Volumes in der SVM festlegen. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter Legen Sie eine Vorlage für adaptive Richtliniengruppen fest.

Logische Schnittstellen (LIFs)

LIF-Übersicht

Erfahren Sie mehr über die LIF-Konfiguration für ein ONTAP Cluster

Eine LIF (logische Schnittstelle) stellt einen Netzwerkzugriffspunkt für einen Node im Cluster dar. Sie können LIFs an Ports konfigurieren, über die das Cluster Kommunikation über das Netzwerk sendet und empfängt.

Cluster-Administrator kann zunächst erstellen, anzeigen, ändern, migrieren, wiederherstellen Oder löschen Sie

LIFs. Ein SVM-Administrator kann nur die LIFs anzeigen, die der SVM zugeordnet sind.

Eine LIF ist eine IP-Adresse oder WWPN mit entsprechenden Merkmalen, wie z. B. eine Service-Richtlinie, ein Home-Port, ein Home-Node, eine Liste von Failover-Ports auf sowie eine Firewall-Richtlinie. Sie können LIFs an Ports konfigurieren, über die das Cluster Kommunikation über das Netzwerk sendet und empfängt.

> Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

LIFs können an folgenden Ports gehostet werden:

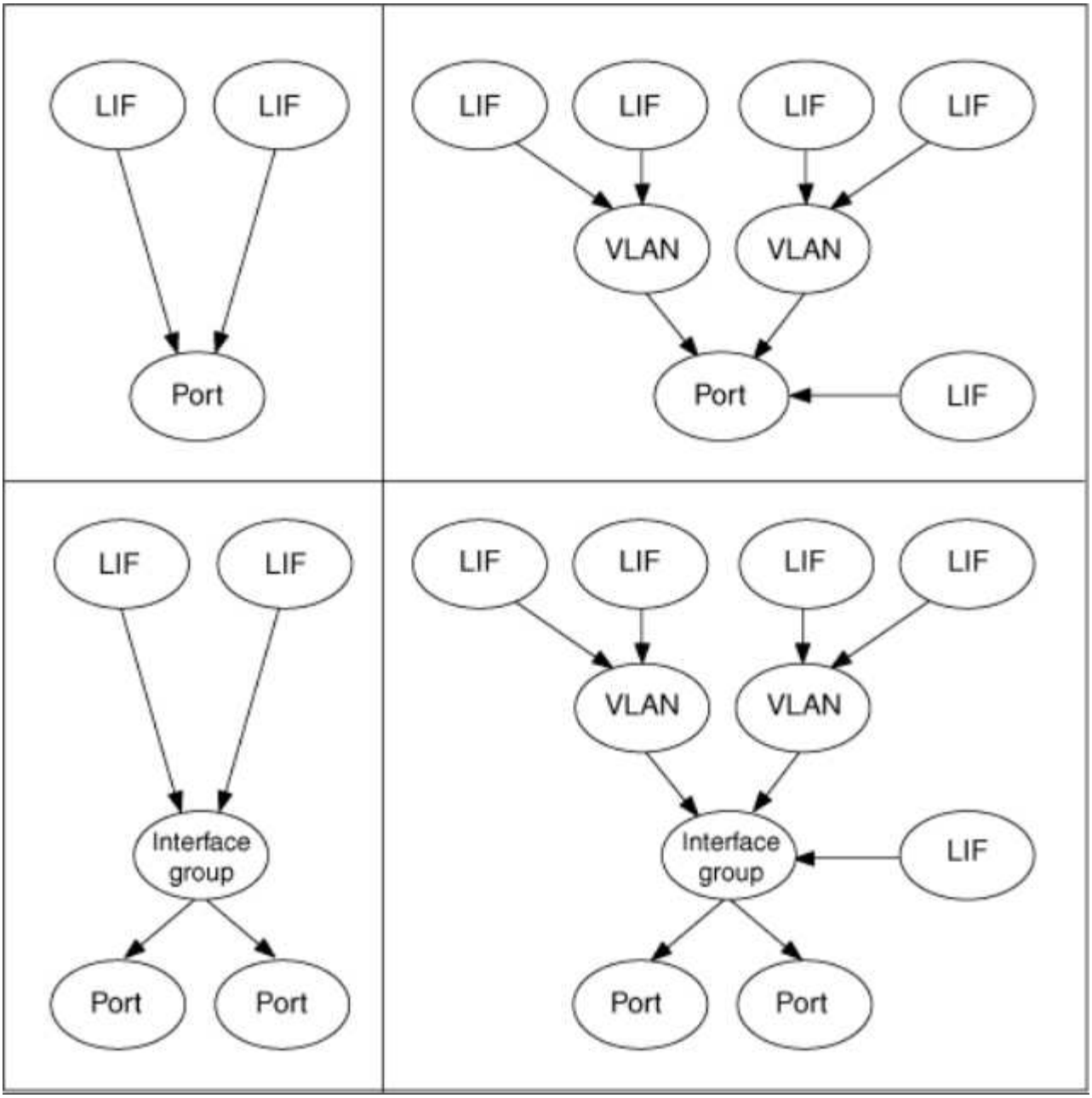
- Physische Ports, die nicht zu Interface Groups gehören
- Interface Groups
- VLANs
- Physische Ports oder Schnittstellengruppen, die VLANs hosten
- Virtuelle IP-Ports (VIP)

  Ab ONTAP 9.5 werden VIP LIFs unterstützt und auf VIP-Ports gehostet.

Während der Konfiguration von SAN-Protokollen, z. B. FC, auf einer logischen Schnittstelle wird sie einem WWPN zugewiesen.

"SAN Administration"

In der folgenden Abbildung wird die Porthierarchie in einem ONTAP-System dargestellt:



LIF Failover und Giveback

Ein LIF-Failover findet statt, wenn eine LIF von seinem Home Node oder Port zu seinem HA-Partner-Node oder -Port verschoben wird. Ein LIF-Failover kann von ONTAP automatisch oder manuell von einem Cluster-Administrator für bestimmte Ereignisse ausgelöst werden, beispielsweise durch einen physischen Ethernet-Link oder einen Node, der aus dem Quorum der replizierten Datenbank (RDB) entfernt wird. Wenn ein LIF-Failover auftritt, setzt ONTAP den normalen Betrieb auf dem Partner-Node fort, bis der Grund für das Failover behoben ist. Wenn der Home-Node oder -Port wieder in den Zustand zurückkehrt, wird die LIF vom HA-Partner zurück auf den Home Node oder Port zurückgesetzt. Diese Reversion wird als Giveback bezeichnet.

Für LIF Failover und Giveback müssen die Ports von jedem Node zur gleichen Broadcast-Domäne gehören. Um zu überprüfen, ob die relevanten Ports auf jedem Knoten zur gleichen Broadcast-Domäne gehören, siehe die folgenden Informationen:

- ONTAP 9 8 und höher: "Port-Erreichbarkeit reparieren"
- ONTAP 9.7 und früher: "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

Für LIFs mit aktiviertem LIF-Failover (automatisch oder manuell) gilt Folgendes:

- Bei LIFs mithilfe einer Datenservice-Richtlinie können Sie die Einschränkungen von Failover-Richtlinien überprüfen:
  - ONTAP 9.6 und höher: "LIFs und Service-Richtlinien in ONTAP 9.6 und höher"
  - ONTAP 9.5 und früher: "LIF-Rollen in ONTAP 9.5 und früher"
- Die automatische Zurücksetzung von LIFs geschieht, wenn die automatische Zurücksetzung auf eingestellt ist `true` und wenn der Home Port der LIF sich in einem ordnungsgemäßen Zustand befindet und die LIF hosten kann.
- Bei einer geplanten oder ungeplanten Node-Übernahme erfolgt ein Failover der LIF auf dem übernommenen Node zum HA-Partner. Der Port, über den die LIF ausfällt, wird durch VIF Manager bestimmt.
- Nachdem der Failover abgeschlossen ist, wird die LIF ordnungsgemäß ausgeführt.
- Wenn ein Giveback initiiert wird, wird das LIF wieder auf seinen Home Node und Port zurückgesetzt, wenn Auto-revert auf `true`.
- Wenn eine ethernet-Verbindung auf einem Port ausfällt, der ein oder mehrere LIFs hostet, migriert der VIF Manager die LIFs vom herunter Port zu einem anderen Port in derselben Broadcast-Domäne. Der neue Port könnte sich im selben Node oder seinem HA-Partner befinden. Wenn die Verbindung wiederhergestellt ist und die automatische Zurücksetzung auf festgelegt ist `true`, setzt der VIF Manager die LIFs zurück auf den Home Node und den Home Port.
- Wenn ein Node aus dem Quorum der replizierten Datenbank (RDB) entfernt wird, migriert der VIF Manager die LIFs vom Quorum-Node zu seinem HA-Partner. Wenn der Node zurück in das Quorum zurückkehrt und die Option zur automatischen Umrüstung auf eingestellt ist `true`, setzt der VIF Manager die LIFs zurück auf den Home Node und den Home Port.

Erfahren Sie mehr über die LIF-Kompatibilität von ONTAP mit Port-Typen

LIFs können über verschiedene Merkmale verfügen, um verschiedene Port-Typen zu unterstützen.

> Wenn Intercluster- und Management-LIFs in demselben Subnetz konfiguriert sind, kann der Managementdatenverkehr durch eine externe Firewall blockiert werden, und die AutoSupport- und NTP-Verbindungen schlagen möglicherweise fehl. Sie können das System wiederherstellen, indem Sie den `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` Befehl ausführen, um die Intercluster LIF umschalten. Sie sollten jedoch die Intercluster LIF und Management LIF in verschiedenen Subnetzen einstellen, um dieses Problem zu vermeiden.

LIF	Beschreibung
Data LIF	Eine logische Schnittstelle, die einer Storage Virtual Machine (SVM) zugewiesen ist und zur Kommunikation mit den Clients verwendet wird. Sie können mehrere Daten-LIFs an einem Port haben. Über diese Schnittstellen können Migrationen oder Failovers im gesamten Cluster erfolgen. Sie können eine Daten-LIF ändern, die als SVM-Management-LIF dient, indem Sie deren Firewallrichtlinie dem Management entsprechend anpassen. Sitzungen, die für NIS-, LDAP-, Active Directory-, WINS- und DNS-Server eingerichtet sind, verwenden Daten-LIFs.

Cluster LIF	Eine LIF, die zum Transport von Intracluster-Datenverkehr zwischen Nodes in einem Cluster verwendet wird. Cluster-LIFs müssen immer an Cluster-Ports erstellt werden. Cluster-LIFs können ein Failover zwischen Cluster-Ports auf demselben Node durchführen, können jedoch nicht migriert oder ein Failover zu einem Remote-Node durchgeführt werden. Wenn ein neuer Node einem Cluster beitreten, werden IP-Adressen automatisch generiert. Wenn Sie jedoch den Cluster-LIFs IP-Adressen manuell zuweisen möchten, müssen Sie sicherstellen, dass sich die neuen IP-Adressen im gleichen Subnetz-Bereich befinden wie die vorhandenen Cluster-LIFs.
Cluster-Management-LIF	LIF, die eine einzige Managementoberfläche für das gesamte Cluster bietet. Ein Cluster-Management-LIF kann einen Failover auf jeden Node im Cluster durchführen. Ein Failover zu Cluster- oder Intercluster-Ports ist nicht möglich
Intercluster LIF	Eine LIF, die für Cluster-übergreifende Kommunikation, Backups und Replizierung verwendet wird. Sie müssen auf jedem Node im Cluster eine Intercluster-LIF erstellen, bevor eine Cluster-Peering-Beziehung aufgebaut werden kann. Diese LIFs können nur ein Failover zu Ports im selben Node durchgeführt werden. Sie können nicht zu einem anderen Node im Cluster migriert oder ein Failover durchgeführt werden.
Node Management-LIF	Eine LIF, die eine dedizierte IP-Adresse zum Verwalten eines bestimmten Nodes in einem Cluster bietet. Das Node-Management-LIFs werden zum Zeitpunkt des Erstellen oder Beitritt zum Cluster erstellt. Diese LIFs werden für Systemwartung verwendet, wenn z. B. der Zugriff auf einen Node aus dem Cluster nicht mehr möglich ist.
VIP-LIF	Ein VIP LIF ist jede Daten-LIF, die auf einem VIP-Port erstellt wurde. Weitere Informationen finden Sie unter "Konfigurieren Sie Virtual IP (VIP) LIFs".

Verwandte Informationen

- "Änderung der Netzwerkschnittstelle"

Unterstützte LIF-Servicerichtlinien und -Rollen für Ihre ONTAP Version

Im Laufe der Zeit hat sich die Art und Weise, in der ONTAP den auf LIFs unterstützten Datenverkehr managt, geändert.

- ONTAP 9 5 und frühere Versionen verwenden LIF-Rollen und Firewall-Dienste.
- ONTAP 9 6 und höhere Versionen nutzen LIF-Servicerichtlinien:
  - ONTAP 9 5 Release führte LIF-Service-Richtlinien ein.
  - ONTAP 9.6 ersetzte LIF Rollen durch LIF Service Policies.
  - ONTAP 9.10.1 ersetzte Firewall-Services durch LIF-Servicerichtlinien.

Die Methode, die Sie konfigurieren, hängt von der Version von ONTAP ab, die Sie verwenden.

Weitere Informationen zu:

- Firewallrichtlinien finden Sie unter "Befehl: Firewall-Policy-show".
- LIF-Rollen finden Sie unter "LIF-Rollen (ONTAP 9.5 und früher)".
- LIF-Servicerichtlinien, siehe "LIFs und Service-Richtlinien (ONTAP 9.6 und höher)".

Weitere Informationen zu ONTAP LIFs und Service-Richtlinien

Sie können Service-Richtlinien (anstelle von LIF-Rollen oder Firewall-Richtlinien) LIFs zuweisen, um die Art des Datenverkehrs zu bestimmen, die für die LIFs unterstützt wird. Service-Richtlinien definieren eine Sammlung von durch ein LIF unterstützten Netzwerkservices. ONTAP bietet eine Reihe integrierter Service-Richtlinien, die einem LIF zugeordnet werden können.

Die Methode zur Verwaltung des Netzwerkverkehrs unterscheidet sich in ONTAP 9.7 und früheren Versionen. Informationen zur Verwaltung des Datenverkehrs in einem Netzwerk mit ONTAP 9.7 und früher finden Sie unter "LIF-Rollen (ONTAP 9.5 und früher)".

FCP- und NVMe/FCP-Protokolle erfordern derzeit keine Service-Policy.

Mit dem folgenden Befehl können Sie Service-Richtlinien und ihre Details anzeigen:
`network interface service-policy show`

Erfahren Sie mehr über `network interface service-policy show` in der "ONTAP-Befehlsreferenz".

Funktionen, die nicht an einen bestimmten Service gebunden sind, verwenden ein systemdefiniertes Verhalten, um LIFs für ausgehende Verbindungen auszuwählen.

Applikationen auf einer LIF mit leerer Service-Richtlinie verhalten sich möglicherweise unerwartet.

Service-Richtlinien für System-SVMs

Die Admin-SVM und jede System-SVM enthalten Servicrichtlinien, die für LIFs in dieser SVM verwendet werden können, einschließlich Management und Intercluster-LIFs. Diese Richtlinien werden automatisch vom System erstellt, wenn ein IPspace erstellt wird.

In der folgenden Tabelle sind die integrierten Richtlinien für LIFs in System-SVMs ab ONTAP 9.12.1 aufgeführt. Zeigen Sie bei anderen Versionen die Service-Richtlinien und ihre Details mithilfe des folgenden Befehls an:

```
network interface service-policy show
```

Richtlinie	Enthaltene Services	Gleichwertige Rolle	Beschreibung
Intercluster Standard	Intercluster-Core, Management-https	Intercluster	Wird von LIFs verwendet, die Intercluster-Datenverkehr transportieren. Hinweis: Service Intercluster-Core ist ab ONTAP 9.5 mit der Service-Richtlinie für Cluster net-intercluster erhältlich.
Standard-Route-Announce	Management-bgp	-	Verwendet von LIFs mit BGP-Peer-Verbindungen Hinweis: Erhältlich ab ONTAP 9.5 mit der Bezeichnung net-Route-announce Service Policy.

Standard-Management	Management-Kern, Management-https, Management-http, Management-ssh, Management-AutoSupport, Management-ems, Management-dns-Client, Management-ad-Client, Management-ldap-Client, Management-nis-Client, Management-ntp-Client, Management-Log-Forwarding	Node-Management oder Cluster-Management	Verwenden Sie diese Management-Richtlinie mit Systemaufsatzbereich, um Management-LIFs für Node- und Cluster-Umfang zu erstellen, die sich im Besitz einer System-SVM befinden. Diese LIFs können für Outbound-Verbindungen zu DNS-, AD-, LDAP- oder NIS-Servern sowie für einige zusätzliche Verbindungen zur Unterstützung von Applikationen verwendet werden, die im Auftrag des gesamten Systems ausgeführt werden. Ab ONTAP 9.12.1 können Sie den Service verwenden `management-log-forwarding`, um zu steuern, welche LIFs für die Weiterleitung von Audit-Protokollen an einen Remote-Syslog-Server verwendet werden.

In der folgenden Tabelle sind die Services aufgeführt, die LIFs ab ONTAP 9.11.1 auf einer System-SVM verwenden können:

Service	Failover-Einschränkungen	Beschreibung
Intercluster-Core	Nur Home Node	Intercluster-Kernservices
Management-Kern	-	Wichtige Management Services
Management-ssh	-	Services für SSH-Management-Zugriff
Management-http	-	Services für HTTP-Management-Zugriff
Management – https	-	Services für HTTPS-Management-Zugriff
Management-AutoSupport	-	Dienstleistungen im Zusammenhang mit dem Posten von AutoSupport Payloads
Management-bgp	Nur zu Hause-Port	Services im Zusammenhang mit BGP-Peer-Interaktionen
Backup-ndmp-Kontrolle	-	Services für NDMP-Backup-Kontrollen
Management – ems	-	Services für Management-Messaging-Zugriff
Management-ntp-Client	-	Eingeführt im ONTAP 9.10.1. Services für NTP-Client-Zugriff.

Management-ntp-Server	-	Eingeführt im ONTAP 9.10.1. Dienste für NTP-Servermanagement-Zugriff
Management-Port	-	Services für das Portmap-Management
Management-RSH-Server	-	Services für das RSH Server Management
Management-snmp-Server	-	Dienste für die SNMP-Serververwaltung
Management-Telnet-Server	-	Services für Telnet-Servermanagement
Management-Log-Forwarding	-	Eingeführt im ONTAP 9.12.1. Dienste für die Protokollweiterleitung von Audits

Service-Richtlinien für Data SVMs

Alle Daten-SVMs enthalten Service-Richtlinien, die von LIFs in dieser SVM verwendet werden können.

In der folgenden Tabelle sind die integrierten Richtlinien für LIFs in Data SVMs ab ONTAP 9.11.1 aufgeführt. Zeigen Sie bei anderen Versionen die Service-Richtlinien und ihre Details mithilfe des folgenden Befehls an:

```
network interface service-policy show
```

Richtlinie	Enthaltene Services	Äquivalent des Datenprotokolls	Beschreibung
Standard-Management	Data-Core, Management-https, Management-http, Management-ssh, Management-dns-Client, Management-ad-Client, Management-ldap-Client, Management-nis-Client	Keine	Verwenden Sie diese SVM-Richtlinie mit Umfang, um SVM-Management-LIFs zu erstellen, die sich im Besitz einer Daten-SVM befinden. Diese LIFs können verwendet werden, um SVM-Administratoren SSH oder HTTPS-Zugriff zu bieten. Falls erforderlich können diese LIFs für Outbound-Verbindungen zu externen DNS-, AD-, LDAP- oder NIS-Servern verwendet werden.
Standarddatenblöcke	Data-Core, Data-iscsi	iscsi	Verwendet von LIFs, die blockorientierten SAN-Datenverkehr transportieren. Ab ONTAP 9.10.1 ist die Richtlinie „default-Data Blocks“ veraltet. Verwenden Sie stattdessen die Service-Richtlinie „Default-Data-iscsi“.

Standarddatendateien	Data-Core, Data-fpolicy-Client, Data-dns-Server, Data-FlexCache, Data-cifs, Data-nfs, Management-dns-Client, Management-ad-Client, Management-ldap-Client, Management-nis-Client	nfs, cifs, fcache	Verwenden Sie die Richtlinie für Standarddatendateien, um NAS-LIFs zu erstellen, die dateibasierte Protokolle unterstützen. Manchmal gibt es nur eine LIF in der SVM, daher kann diese Richtlinie für ausgehende Verbindungen zu einem externen DNS-, AD-, LDAP- oder NIS-Server verwendet werden. Sie können diese Services als aus dieser Richtlinie entfernen, wenn Sie diese Verbindungen bevorzugen, verwenden Sie nur Management-LIFs.
Standard-Daten - iscsi	Data-Core, Data-iscsi	iscsi	Wird von LIFs verwendet, die iSCSI-Datenverkehr übertragen.
Standard-Daten-nvme-tcp	Daten-Core, Data-nvme-tcp	nvme-tcp	Verwendet von LIFs, die NVMe/TCP-Datenverkehr übertragen.

In der folgenden Tabelle werden die Services, die auf einer Daten-SVM verwendet werden können, zusammen mit allen Einschränkungen aufgeführt, die jeder Service der Failover-Richtlinie eines LIF seit ONTAP 9.11.1 auferlegt:

Service	Failover-Einschränkungen	Beschreibung
Management-ssh	-	Services für SSH-Management-Zugriff
Management-http	-	Eingeführt in ONTAP 9.10.1-Diensten für HTTP-Management-Zugriff
Management – https	-	Services für HTTPS-Management-Zugriff
Management-Port	-	Services für Portmap Management Access
Management-snmp-Server	-	Eingeführt in ONTAP 9.10.1 Dienste für SNMP Server Management Zugriff
Datenkern	-	Zentrale Datenservices
Daten-nfs	-	NFS-Datenservice
Daten-cifs	-	CIFS-Datenservice
FlexCache	-	FlexCache Datenservice

Daten-iscsi	Nur Home-Port für AFF/FAS; nur sfo-Partner für ASA	ISCSI-Datenservice
Backup-ndmp-Kontrolle	-	Seit der Einführung in ONTAP 9.10.1 Backup NDMP steuert der Datenservice
Daten-dns-Server	-	Eingeführt in ONTAP 9.10.1 DNS-Server-Datenservice
fpolicy-Client von Daten	-	Datendienst für die Dateiprüfung
Daten-nvme-tcp	Nur zu Hause-Port	Eingeführt im ONTAP 9.10.1 NVMe TCP-Datenservice
Daten-s3-Server	-	Simple Storage Service (S3) Server-Datenservice

Beachten Sie, wie die Service-Richtlinien den LIFs in Data SVMs zugewiesen werden:

- Wird eine Daten-SVM mit einer Liste von Datenservices erstellt, werden die integrierten Service-Richtlinien der Standarddatendateien und Standarddatenblöcke mithilfe der angegebenen Services erstellt.
- Wenn eine Daten-SVM erstellt wird, ohne eine Liste von Datenservices anzugeben, werden die integrierten Service-Richtlinien für die Standarddatendateien und Standarddatenblöcke unter Verwendung einer Standardliste der Datenservices erstellt.

  In der Liste der Standard-Datenservices sind die iSCSI-, NFS-, NVMe-, SMB- und FlexCache-Services enthalten.
- Wenn eine LIF mit einer Liste von Datenprotokollen erstellt wird, wird der logischen Schnittstelle eine Service-Richtlinie zugewiesen, die den angegebenen Datenprotokollen entspricht.
- Wenn keine entsprechende Service-Richtlinie vorhanden ist, wird eine benutzerdefinierte Service-Richtlinie erstellt.
- Wenn ein LIF ohne eine Service-Richtlinie oder eine Liste von Datenprotokollen erstellt wird, wird dem LIF standardmäßig die Standarddatenservice-Richtlinie zugewiesen.

Datenkernservice

Der Daten-Core-Service ermöglicht Komponenten, die zuvor LIFs mit der Datenrolle verwendet haben, wie erwartet auf Clustern zu arbeiten, die aktualisiert wurden, um LIFs mithilfe von Service-Richtlinien anstelle von LIF-Rollen zu verwalten (die in ONTAP 9.6 veraltet sind).

Wenn Sie Data-Core als Service angeben, werden keine Ports in der Firewall geöffnet, der Service sollte jedoch in jeder Service-Richtlinie in einer Daten-SVM enthalten sein. Die Service-Richtlinie für Standarddatendateien enthält beispielsweise standardmäßig die folgenden Dienste:

- Datenkern
- Daten-nfs
- Daten-cifs

- FlexCache

Der Daten-Core-Service sollte in die Richtlinie aufgenommen werden, damit sichergestellt ist, dass alle Applikationen, die die LIF verwenden, wie erwartet funktionieren. Die anderen drei Services können jedoch nach Bedarf entfernt werden.

Client-seitiger LIF-Service

Ab ONTAP 9.10.1 bietet ONTAP Client-seitige LIF Services für mehrere Applikationen. Diese Services bieten Kontrolle darüber, welche LIFs für Outbound-Verbindungen im Auftrag der jeweiligen Applikation verwendet werden.

Mit den folgenden neuen Services haben Administratoren die Kontrolle, welche LIFs für bestimmte Applikationen als Quelladressen verwendet werden.

Service	SVM-Einschränkungen	Beschreibung
Management-ad-Client	-	Ab ONTAP 9.11.1 stellt ONTAP den Active Directory-Client-Service für ausgehende Verbindungen zu einem externen AD-Server bereit.
Management-dns-Client	-	Ab ONTAP 9.11.1 stellt ONTAP den DNS-Client-Service für ausgehende Verbindungen zu einem externen DNS-Server bereit.
Management-ldap-Client	-	Ab ONTAP 9.11.1 stellt ONTAP den LDAP-Client-Service für ausgehende Verbindungen zu einem externen LDAP-Server bereit.
Management-nis-Client	-	Ab ONTAP 9.11.1 stellt ONTAP den NIS-Client-Service für ausgehende Verbindungen zu einem externen NIS-Server bereit.
Management-ntp-Client	Nur System	Ab ONTAP 9.10.1 bietet ONTAP den NTP-Client-Service für ausgehende Verbindungen zu einem externen NTP-Server.
fpolicy-Client von Daten	Rein Daten-beschränkt	Ab ONTAP 9.8 bietet ONTAP Client-Service für ausgehende FPolicy-Verbindungen.

Jeder der neuen Services wird automatisch in einige der integrierten Service-Richtlinien einbezogen. Allerdings können Administratoren diese aus den integrierten Richtlinien entfernen oder zu individuellen Richtlinien hinzufügen, um zu steuern, welche LIFs für ausgehende Verbindungen im Namen jeder Applikation verwendet werden.

Verwandte Informationen

- "Service-Policy für die Netzwerkschnittstelle zeigen"

Management von LIFs

Konfigurieren von Richtlinien für LIF-Dienste für ein ONTAP-Cluster

Sie können LIF-Service-Richtlinien konfigurieren, um einen einzelnen Service oder eine Liste von Services zu identifizieren, die eine LIF verwenden.

Erstellen einer Service-Richtlinie für LIFs

Sie können eine Service-Richtlinie für LIFs erstellen. Sie können einer oder mehreren LIFs eine Service-Richtlinie zuweisen, sodass diese Datenverkehr für einen einzelnen Service oder eine Liste von Services leiten kann.

Sie benötigen erweiterte Privileges, um den `network interface service-policy create` Befehl auszuführen.

Über diese Aufgabe

Für das Management des Daten- und Managementdatenverkehrs auf Daten- und System-SVMs stehen integrierte Services und Service-Richtlinien zur Verfügung. Die meisten Anwendungsfälle sind mit einer integrierten Service-Richtlinie zufrieden, anstatt eine individuelle Service-Richtlinie zu erstellen.

Sie können diese integrierten Service-Richtlinien, falls erforderlich, ändern.

Schritte

1. Zeigen Sie die im Cluster verfügbaren Services an:

   ```
   network interface service show
   ```

   Services stellen die Applikationen dar, auf die von einer logischen Schnittstelle zugegriffen wird, sowie die vom Cluster bereitgestellten Applikationen. Jeder Dienst umfasst Null oder mehr TCP- und UDP-Ports, auf denen die Anwendung zuhört.

   Die folgenden zusätzlichen Daten- und Management-Services stehen zur Verfügung:

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. Zeigen Sie die Service-Richtlinien für das Cluster an:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Service-Richtlinie erstellen:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- „Service_Name“ gibt eine Liste der Services an, die in die Richtlinie aufgenommen werden sollen.
- „IP_Address/masks“ gibt die Liste der Subnetzmaske für Adressen an, die auf die Dienste in der Service-Richtlinie zugreifen dürfen. Standardmäßig werden alle angegebenen Dienste mit einer standardmäßig zulässigen Adressliste von 0.0.0.0/0 hinzugefügt, die den Datenverkehr aus allen Subnetzen erlaubt. Wenn eine nicht standardmäßige Liste der zulässigen Adressen angegeben wird, werden LIFs mithilfe der Richtlinie konfiguriert, um alle Anforderungen mit einer Quelladresse zu blockieren, die keiner der angegebenen Masken entspricht.

  Das folgende Beispiel zeigt, wie eine Datenservicerichtlinie, *svm1_Data_Policy*, für eine SVM erstellt wird, die *NFS* und *SMB*-Dienste umfasst:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  Im folgenden Beispiel wird gezeigt, wie eine Richtlinie für Intercluster-Services erstellt wird:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Vergewissern Sie sich, dass die Service-Richtlinie erstellt wurde.

```
cluster1::> network interface service-policy show
```

   Die folgende Ausgabe zeigt die verfügbaren Service-Richtlinien:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Nachdem Sie fertig sind

Weisen Sie der Service-Richtlinie einem LIF entweder zum Zeitpunkt der Erstellung oder durch Ändern eines vorhandenen LIF zu.

Weisen Sie einer logischen Schnittstelle eine Service-Richtlinie zu

Sie können einer logischen Schnittstelle entweder zum Zeitpunkt der Erstellung der logischen Schnittstelle oder durch Ändern der logischen Schnittstelle eine Service-Richtlinie zuweisen. Eine Service-Richtlinie definiert eine Liste der Services, die zusammen mit dem LIF verwendet werden können.

Über diese Aufgabe

Sie können Service-Richtlinien für LIFs im Administrator und den Daten-SVMs zuweisen.

Schritt

Führen Sie je nachdem, wann Sie die Service-Richtlinie einem LIF zuweisen möchten, eine der folgenden Aktionen durch:

Ihr Unternehmen	Service-Richtlinie zuweisen…
Erstellen einer LIF	Netzwerkschnittstelle create -vserver svm_Name -lif <lif_Name> -Home-Node <Node_Name> -Home-Port <Port_Name> {(-Adresse <IP_address> -Netmask <IP_address>) -subnet-Name <subnet_Name>} -Service-Policy <Service_Policy_Name>
Ändern eines LIF	Netzwerkschnittstelle modify -vServer <svm_Name> -lif <lif_Name> -Service -Policy <Service_Policy_Name>

Wenn Sie eine Service-Richtlinie für eine LIF angeben, müssen Sie nicht das Datenprotokoll und die Rolle für die LIF angeben. Außerdem wird das Erstellen von LIFs unterstützt, indem die Rolle und die Datenprotokolle angegeben werden.

Eine Service-Richtlinie kann nur von LIFs in derselben SVM verwendet werden, die Sie beim Erstellen der Service-Richtlinie angegeben haben.

Beispiele

Das folgende Beispiel zeigt, wie die Service-Richtlinie eines LIF geändert wird, um die Standard-Management-Service-Richtlinie zu verwenden:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Befehle zum Verwalten von LIF-Servicrichtlinien

Verwenden Sie die `network interface service-policy` Befehle zum Managen von Richtlinien für LIF-Dienste.

Erfahren Sie mehr über `network interface service-policy` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Durch das Ändern der Service-Richtlinie einer logischen Schnittstelle in einer aktiven SnapMirror Beziehung wird der Replizierungszeitplan unterbrochen. Wenn Sie eine LIF von Intercluster nach nicht-Intercluster (oder umgekehrt) konvertieren, werden diese Änderungen nicht auf das Peering-Cluster repliziert. Um das Peer-Cluster nach dem Ändern der LIF-Service-Richtlinie zu aktualisieren, führen Sie den `snapmirror abort` Vorgang zuerst und dann Synchronisieren Sie die Replikationsbeziehung erneutaus.

Ihr Ziel ist	Befehl
Service-Policy erstellen (erweiterte Berechtigungen erforderlich)	`network interface service-policy create`
Hinzufügen eines zusätzlichen Serviceeintrags zu einer vorhandenen Servicerichtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy add-service`
Klonen einer vorhandenen Service-Richtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy clone`
Ändern eines Diensteintrags in einer vorhandenen Servicerichtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy modify-service`
Entfernen eines Diensteintrags aus einer vorhandenen Servicerichtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy remove-service`
Umbenennen einer vorhandenen Service-Richtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy rename`
Löschen einer vorhandenen Service-Richtlinie (erweiterte Berechtigungen erforderlich)	`network interface service-policy delete`
Wiederherstellen einer integrierten Service-Richtlinie in ihren Originalzustand (erweiterte Berechtigungen erforderlich)	`network interface service-policy restore-defaults`
Vorhandene Service-Richtlinien anzeigen	`network interface service-policy show`

Verwandte Informationen

- "Netzwerkschnittstellenservice anzeigen"
- "Service-Richtlinie für Netzwerkschnittstelle"
- "Snapmirror-Abbruch"

Erstellung der ONTAP LIFs

Eine SVM stellt Daten für Clients über eine oder mehrere logische Netzwerk-Schnittstellen (Logical Interfaces, LIFs) zur Verfügung. Sie müssen auf den Ports, die Sie für den Zugriff auf Daten verwenden möchten, LIFs erstellen. Eine LIF (Netzwerkschnittstelle) ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Falls eine Komponente ausfällt, kann ein LIF ein Failover auf einen anderen physischen Port durchführen oder zu einem anderen migrieren, sodass weiterhin mit dem Netzwerk kommunizieren wird.

Best Practices in sich

Mit ONTAP verbundene Switch Ports sollten als Spanning-Tree Edge Ports konfiguriert werden, um Verzögerungen während der LIF-Migration zu reduzieren.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator-up-Status konfiguriert worden sein.
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

  Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit System Manager oder dem `network subnet create` Befehl erstellt.

  Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Angabe der von einem LIF bearbeiteten Traffic-Art ist geändert. Für ONTAP 9.5 und früher verwendeten LIFs Rollen, um den Typ des Datenverkehrs anzugeben, den er verarbeiten würde. Ab ONTAP 9.6 verwenden LIFs Service-Richtlinien, um den Typ des Datenverkehrs anzugeben, den es verarbeiten würde.

Über diese Aufgabe

- Sie können NAS- und SAN-Protokolle nicht derselben logischen Schnittstelle zuweisen.

  Die unterstützten Protokolle sind SMB, NFS, FlexCache, iSCSI und FC; ISCSI und FC können nicht mit anderen Protokollen kombiniert werden. NAS- und Ethernet-basierte SAN-Protokolle können jedoch auf demselben physischen Port vorhanden sein.

  - Sie sollten keine LIFs konfigurieren, die SMB-Datenverkehr transportieren, um automatisch auf ihre Home-Nodes zurückzusetzen. Diese Empfehlung ist obligatorisch, wenn der SMB-Server eine Lösung für unterbrechungsfreien Betrieb mit Hyper-V oder SQL Server over SMB hosten soll.
- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Alle von einer SVM verwendeten Dienste für die Namenszuweisung und Hostnamenauflösung, z. B. DNS, NIS, LDAP und Active Directory Muss über mindestens eine logische Schnittstelle erreichbar sein, die den Datenverkehr der SVM bewältigt.
- Ein LIF, die Intracluster-Datenverkehr zwischen Nodes verarbeiten, sollte sich nicht im selben Subnetz wie ein LIF-Handling-Datenverkehr oder eine LIF mit Datenverkehr befinden.
- Das Erstellen eines LIF ohne gültiges Failover-Ziel führt zu einer Warnmeldung.
- Wenn Sie eine große Anzahl von LIFs im Cluster besitzen, können Sie die vom Cluster unterstützte LIF-Kapazität überprüfen:
  - System Manager: Ab ONTAP 9.12.0 können Sie den Durchsatz auf dem Netzwerk-Interface-Grid einsehen.
  - CLI: Verwenden Sie den `network interface capacity show` Befehl und die auf jedem Node unterstützte LIF-Kapazität. Verwenden Sie dazu den `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene).

    Erfahren Sie mehr über `network interface capacity show` und `network interface capacity details show` in der "ONTAP-Befehlsreferenz".

- Wenn bereits ab ONTAP 9.7 andere LIFs für die SVM im selben Subnetz vorhanden sind, müssen Sie den Home Port der LIF nicht angeben. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Home-Node in derselben Broadcast-Domäne wie die anderen LIFs, die bereits im selben Subnetz konfiguriert sind.

  Ab ONTAP 9.4 wird FC-NVMe unterstützt. Wenn Sie eine FC-NVMe-LIF erstellen, sollten Sie Folgendes beachten:

  - Das NVMe-Protokoll muss vom FC-Adapter unterstützt werden, auf dem die LIF erstellt wird.
  - FC-NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Für jede Storage Virtual Machine (SVM), die SAN unterstützt, muss eine logische Schnittstelle für den Management-Datenverkehr konfiguriert werden.
- NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
- Pro SVM kann ein Maximum von zwei NVMe LIFs für den Datenverkehr pro Node konfiguriert werden.
- Wenn Sie eine Netzwerkschnittstelle mit einem Subnetz erstellen, wählt ONTAP automatisch eine verfügbare IP-Adresse aus dem ausgewählten Subnetz aus und weist sie der Netzwerkschnittstelle zu. Sie können das Subnetz ändern, wenn es mehr als ein Subnetz gibt, aber Sie können die IP-Adresse nicht ändern.
- Wenn Sie eine SVM für eine Netzwerkschnittstelle erstellen (hinzufügen), können Sie keine IP-Adresse angeben, die sich im Bereich eines vorhandenen Subnetzes befindet. Sie erhalten einen Subnetzkonflikt. Dieses Problem tritt in anderen Workflows für eine Netzwerkschnittstelle auf, z. B. beim Erstellen oder Ändern von Clusterschnittstellen in SVM-Einstellungen oder in Cluster-Einstellungen.
- Ab ONTAP 9.10.1 `network interface` enthalten die CLI-Befehle einen `-rdma-protocols` Parameter für NFS over RDMA-Konfigurationen. Die Erstellung von Netzwerkschnittstellen für NFS über RDMA-Konfigurationen wird in System Manager ab ONTAP 9.12.1 unterstützt. Weitere Informationen finden Sie unter KONFIGURIEREN SIE LIFS für NFS über RDMA.
- Ab ONTAP 9.11.1 ist der automatische iSCSI LIF-Failover auf All-Flash SAN-Array (ASA)-Plattformen verfügbar.

  ISCSI-LIF-Failover ist automatisch aktiviert (die Failover-Richtlinie ist auf festgelegt `sfo-partner-only` und der Auto-revert-Wert ist auf eingestellt `true`) bei neu erstellten iSCSI-LIFs, wenn in der angegebenen SVM keine iSCSI-LIFs vorhanden sind oder wenn alle vorhandenen iSCSI-LIFs in der angegebenen SVM bereits mit iSCSI-LIF-Failover aktiviert sind.

  Wenn Sie nach einem Upgrade auf ONTAP 9.11.1 oder höher bereits iSCSI-LIFs in einer SVM vorhanden sind, die nicht mit der iSCSI-LIF-Failover-Funktion aktiviert wurden, und Sie neue iSCSI-LIFs in derselben SVM erstellen, übernehmen die neuen iSCSI-LIFs dieselbe Failover(`disabled`-Richtlinie) der vorhandenen iSCSI-LIFs in der SVM.

  "LIF-Failover für ASA-Plattformen"

Ab ONTAP 9.7 wählt ONTAP automatisch den Home Port einer LIF aus, solange mindestens eine LIF bereits im gleichen Subnetz in diesem IPspace vorhanden ist. ONTAP wählt einen Home-Port in derselben Broadcast-Domäne wie andere LIFs in diesem Subnetz. Sie können noch einen Home-Port angeben, dieser ist jedoch nicht mehr erforderlich (es sei denn, es sind noch keine LIFs in diesem Subnetz im angegebenen IPspace vorhanden).

Ab ONTAP 9.12.0 hängt das folgende Verfahren von der Schnittstelle ab, die Sie verwenden --System Manager oder die CLI:

System Manager

Verwenden Sie System Manager, um eine Netzwerkschnittstelle hinzuzufügen

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie + Add .
3. Wählen Sie eine der folgenden Schnittstellenrollen aus:
   a. Daten
   b. Intercluster
   c. SVM-Management
4. Wählen Sie das Protokoll aus:
   a. SMB/CIFS UND NFS
   b. ISCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Benennen Sie das LIF, oder übernehmen Sie den aus Ihrer vorherigen Auswahl generierten Namen.
6. Akzeptieren Sie den Home-Node oder wählen Sie einen aus dem Dropdown-Menü aus.
7. Wenn im IPspace der ausgewählten SVM mindestens ein Subnetz konfiguriert ist, wird das Dropdown-Menü Subnetz angezeigt.
   a. Wenn Sie ein Subnetz auswählen, wählen Sie es aus der Dropdown-Liste aus.
   b. Wenn Sie ohne Subnetz fortfahren, wird das Dropdown-Menü Broadcast-Domäne angezeigt:
      i. Geben Sie die IP-Adresse an. Wenn die IP-Adresse verwendet wird, wird eine Warnmeldung angezeigt.
      ii. Geben Sie eine Subnetzmaske an.
8. Wählen Sie den Home-Port aus der Broadcast-Domäne aus, entweder automatisch (empfohlen) oder durch Auswahl eines aus dem Dropdown-Menü. Die Steuerung des Home-Ports wird basierend auf der Broadcast-Domäne oder der Subnetzauswahl angezeigt.
9. Speichern Sie die Netzwerkschnittstelle.

CLI

Verwenden Sie die CLI, um ein LIF zu erstellen

Schritte

1. Legen Sie fest, welche Broadcast-Domänen-Ports für das LIF verwendet werden sollen.

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

Erfahren Sie mehr über `network port broadcast-domain show` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das Subnetz, das Sie für die LIFs verwenden möchten, ausreichend ungenutzte IP-Adressen enthält.

   `network subnet show -ipspace ipspace1`

   Erfahren Sie mehr über `network subnet show` in der "ONTAP-Befehlsreferenz".

3. Erstellen Sie mindestens einen LIFs an den Ports, mit denen Sie auf Daten zugreifen möchten.

   NetApp empfiehlt das Erstellen von Subnetzobjekten für alle LIFs auf Data SVMs. Dies ist besonders wichtig für MetroCluster-Konfigurationen, bei denen das Subnetz-Objekt es ONTAP ermöglicht, Failover-Ziele auf dem Ziel-Cluster zu bestimmen, da jedem Subnetz-Objekt eine zugeordnete Broadcast-Domäne zugeordnet ist. Anweisungen hierzu finden Sie unter "Erstellen Sie ein Subnetz".

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` Ist der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

     Sie können auch angeben, ob die LIF automatisch auf den Home-Node und den Home-Port zurückgesetzt werden soll. Verwenden Sie dazu die Option -Auto-revert.

   Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".

   - `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
   - Sie können eine IP-Adresse mit den `-address -netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
   - Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn

mithilfe dieses Subnetzes eine LIF erstellt wird.

- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Erfahren Sie mehr über `network route create` in der "ONTAP-Befehlsreferenz".
- `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Sie können sie jedoch `true` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.
- `-service-policy` Ab ONTAP 9.5 können Sie mit der `-service-policy` Option eine Service-Richtlinie für die LIF zuweisen. Wenn eine Service-Richtlinie für eine LIF angegeben wird, wird diese Richtlinie verwendet, um eine Standardrolle, Failover-Richtlinie und Datenprotokollliste für die LIF zu erstellen. In ONTAP 9.5 werden Service-Richtlinien nur für Cluster-übergreifende und BGP-Peer-Services unterstützt. In ONTAP 9.6 können Service-Richtlinien für mehrere Daten- und Management-Services erstellt werden.
- `-data-protocol` Ermöglicht Ihnen das Erstellen einer logischen Schnittstelle, die die FCP- oder NVMe/FC-Protokolle unterstützt. Diese Option ist beim Erstellen eines IP-LIF nicht erforderlich.

4. **Optional**: Eine IPv6-Adresse in der Option -address zuweisen:

   a. Verwenden Sie den `network ndp prefix show` Befehl, um die Liste der RA-Präfixe anzuzeigen, die an verschiedenen Schnittstellen gelernt wurden.

      Der `network ndp prefix show` Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

      Erfahren Sie mehr über `network ndp prefix show` in der "ONTAP-Befehlsreferenz".

   b. Verwenden Sie das Format `prefix::id`, um die IPv6-Adresse manuell zu erstellen.

      `prefix` Wird das Präfix an verschiedenen Schnittstellen gelernt.

      ```
      `id`Wählen Sie zum Ableiten der eine zufällige 64-Bit-
      Hexadezimalzahl aus.
      ```

5. Vergewissern Sie sich, dass die Konfiguration der LIF-Schnittstelle richtig ist.

   `network interface show -vserver vs1`

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1       up/up      10.0.0.128/24    node1     e0d
   true
   ```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

6. Vergewissern Sie sich, dass die Konfiguration der Failover-Gruppe die gewünschte Konfiguration ist.

   `network interface show -failover -vserver vs1`

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	Netzwerk-Ping
IPv6-Adresse	Netzwerk-Ping6

Beispiele

Mit dem folgenden Befehl wird eine LIF erstellt und die Werte der IP-Adresse und Netzwerkmaske anhand der `-address -netmask` Parameter und angegeben:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

Mit dem folgenden Befehl wird eine LIF erstellt und dem angegebenen Subnetz (namens client1_sub) IP-Adresse und Netzwerkmaskenwerte zugewiesen:

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

Mit dem folgenden Befehl wird eine NVMe/FC-LIF erstellt und das `nvme-fc` Datenprotokoll angegeben:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Ändern Sie ONTAP LIFs

Sie können eine LIF ändern, indem Sie die Attribute ändern, z. B. Home Node oder aktueller Node, Administrationsstatus, IP-Adresse, Netmask, Failover-Richtlinie Firewall-Richtlinie und Service-Richtlinien. Sie können auch die Adressfamilie einer logischen Schnittstelle von IPv4 zu IPv6 ändern.

Über diese Aufgabe

- Wenn Sie den Administrationsstatus einer LIF auf „down“ ändern, werden alle ausstehenden NFSv4-Sperren gehalten, bis der Administrationsstatus der LIF wieder in angezeigt wird.

  Um Sperrkonflikte zu vermeiden, die auftreten können, wenn andere LIFs versuchen, auf die gesperrten Dateien zuzugreifen, müssen Sie die NFSv4-Clients auf eine andere LIF verschieben, bevor Sie den Administratorstatus auf „down“ setzen.

- Sie können die von einer FC-LIF verwendeten Datenprotokolle nicht ändern. Sie können jedoch die Services, die einer Service-Richtlinie zugewiesen sind, ändern oder die Service-Richtlinie, die einer IP-LIF zugewiesen ist.

  Zum Ändern der von einer FC-LIF verwendeten Datenprotokolle müssen Sie die LIF löschen und neu erstellen. Um Änderungen an Service-Richtlinien an einer IP-LIF vorzunehmen, gibt es einen kurzen Ausfall, während die Updates stattfinden.

- Sie können den Home Node oder den aktuellen Node einer Management-LIF mit Node-Umfang nicht ändern.
- Wenn Sie zum Ändern der IP-Adresse und des Netzwerkmaskenwertes für eine LIF ein Subnetz verwenden, wird eine IP-Adresse aus dem angegebenen Subnetz zugewiesen. Wenn die vorherige IP-Adresse des LIF von einem anderen Subnetz stammt, wird die IP-Adresse an dieses Subnetz zurückgegeben.
- Um die Adressfamilie einer LIF von IPv4 nach IPv6 zu ändern, müssen Sie die Doppelpunkt-Notation für die IPv6-Adresse verwenden und einen neuen Wert für den `-netmask-length` Parameter hinzufügen.
- Sie können die automatisch konfigurierten Link-lokalen IPv6-Adressen nicht ändern.
- Die Änderung eines LIF, die dazu führt, dass kein gültiges Failover-Ziel für die LIF vorliegt, führt zu einer Warnmeldung.

  Wenn ein LIF, das kein gültiges Failover-Ziel besitzt, ein Failover-Ziel vorschlägt, kann es zu einem Ausfall kommen.

- Ab ONTAP 9.5 können Sie die Service-Richtlinie, die einer logischen Schnittstelle zugeordnet ist, ändern.

  In ONTAP 9.5 werden Service-Richtlinien nur für Cluster-übergreifende und BGP-Peer-Services unterstützt. In ONTAP 9.6 können Service-Richtlinien für mehrere Daten- und Management-Services erstellt werden.

- Ab ONTAP 9.11.1 ist das automatische iSCSI LIF-Failover auf All-Flash SAN-Array (ASA)-Plattformen verfügbar.

  Für bereits vorhandene iSCSI-LIFs, d. h. LIFs, die vor dem Upgrade auf 9.11.1 oder höher erstellt wurden, können Sie die Failover-Richtlinie auf ändern"Aktivieren Sie automatisches iSCSI LIF Failover".

- ONTAP verwendet das Network Time Protocol (NTP), um die Zeit im gesamten Cluster zu synchronisieren. Nach dem Ändern der LIF-IP-Adressen müssen Sie möglicherweise die NTP-Konfiguration aktualisieren,

um Synchronisierungsfehler zu vermeiden. Weitere Informationen finden Sie im"NetApp Knowledge Base: NTP-Synchronisierung schlägt nach LIF-IP-Änderung fehl" .

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Ab ONTAP 9.12.0 können Sie mit System Manager eine Netzwerkschnittstelle bearbeiten

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie ⋮ **> Bearbeiten** neben der Netzwerkschnittstelle aus, die Sie ändern möchten.
3. Ändern Sie eine oder mehrere Einstellungen der Netzwerkschnittstelle. Weitere Informationen finden Sie unter "Erstellen Sie eine LIF".
4. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um ein LIF zu ändern

Schritte

1. Ändern Sie die Attribute eines LIF mit dem `network interface modify` Befehl.

   Im folgenden Beispiel wird gezeigt, wie die IP-Adresse und Netzwerkmaske des LIF Datendisk mit einer IP-Adresse und dem Wert der Netzwerkmaske aus dem Subnetz client1_sub geändert werden:

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   Im folgenden Beispiel wird gezeigt, wie die Service-Richtlinie eines LIF geändert wird.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

2. Stellen Sie sicher, dass die IP-Adressen erreichbar sind.

Sie verwenden…	Verwenden Sie dann…
IPv4-Adressen	`network ping`
IPv6-Adressen	`network ping6`

   Erfahren Sie mehr über `network ping` in der "ONTAP-Befehlsreferenz".

Migrieren Sie ONTAP LIFs

Möglicherweise müssen Sie eine LIF zu einem anderen Port desselben Node oder eines anderen Node im Cluster migrieren, wenn der Port fehlerhaft ist oder Wartungsarbeiten erforderlich sind. Die Migration eines LIF ähnelt dem LIF Failover, allerdings ist die LIF-Migration ein manueller Vorgang, während bei einem LIF Failover die automatische Migration eines LIF als Reaktion auf einen Linkfehler am aktuellen Netzwerkport des LIF ist.

Bevor Sie beginnen

- Eine Failover-Gruppe muss für die LIFs konfiguriert worden sein.
- Der Ziel-Node und die Ports müssen betriebsbereit sein und auf dasselbe Netzwerk wie der Quellport zugreifen können.

Über diese Aufgabe

- BGP LIFs befinden sich im Home Port und können nicht zu einem anderen Node oder Port migriert werden.
- Sie müssen LIFs migrieren, die auf den Ports, die zu einer NIC gehören, zu anderen Ports im Cluster gehostet werden, bevor Sie die NIC vom Node entfernen.
- Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.
- Eine LIF mit Node-Umfang, z. B. eine Management-LIF mit Node-Umfang, Cluster-LIF und Clusterschnittstelle, kann nicht zu einem Remote Node migriert werden.
- Wenn eine NFSv4-LIF zwischen Nodes migriert wird, ergibt sich eine Verzögerung von bis zu 45 Sekunden, bevor die LIF auf einem neuen Port verfügbar ist.

  Um dieses Problem zu umgehen, verwenden Sie NFSv4.1, wo keine Verzögerung aufgetreten ist.

- Sie können iSCSI LIFs auf All-Flash SAN-Array-Plattformen (ASA) mit ONTAP 9.11.1 oder höher migrieren.

  Die Migration von iSCSI LIFs ist auf Ports am Home-Node oder am HA-Partner begrenzt.

- Wenn es sich bei Ihrer Plattform nicht um eine All-Flash SAN-Array (ASA)-Plattform handelt, auf der ONTAP Version 9.11.1 oder höher ausgeführt wird, können Sie iSCSI LIFs nicht von einem Node auf einen anderen Node migrieren.

  Um diese Einschränkung zu umgehen, müssen Sie auf dem Ziel-Node eine iSCSI-LIF erstellen. Erfahren Sie mehr über "Erstellen von iSCSI-LIFs".

- Wenn Sie eine LIF (Netzwerkschnittstelle) für NFS über RDMA migrieren möchten, müssen Sie sicherstellen, dass der Ziel-Port RoCE-fähig ist. Sie müssen ONTAP 9.10.1 oder höher ausführen, um eine LIF mit der CLI zu migrieren, oder ONTAP 9.12.1 für die Migration mit System Manager. Wenn Sie in System Manager Ihren RoCE-fähigen Ziel-Port ausgewählt haben, müssen Sie das Kontrollkästchen neben **RoCE-Ports verwenden** aktivieren, um die Migration erfolgreich abzuschließen. Erfahren Sie mehr über "Konfigurieren von LIFs für NFS über RDMA".
- Beim Migrieren der Quell- oder Ziel-LIF schlägt der Copy-Offload von VMware VAAI fehl. Weitere Informationen zum Offload von Kopien:
  - "NFS-Umgebungen"
  - "SAN-Umgebungen"

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um eine Netzwerkschnittstelle zu migrieren

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie ⋮ **> Migrate** neben der Netzwerkschnittstelle aus, die Sie ändern möchten.

   ⓘ Wählen Sie für eine iSCSI-LIF im Dialogfeld **Migrate Interface** den Zielknoten und den Port des HA-Partners aus.

   Wenn Sie die iSCSI-LIF dauerhaft migrieren möchten, aktivieren Sie das Kontrollkästchen. Das iSCSI LIF muss offline sein, bevor es dauerhaft migriert wird. Darüber hinaus kann eine iSCSI LIF, sobald sie dauerhaft migriert ist, nicht rückgängig gemacht werden. Es gibt keine Option zum Zurücksetzen.

3. Klicken Sie Auf * Migrieren*.
4. Speichern Sie die Änderungen.

CLI

Verwenden Sie die CLI, um eine LIF zu migrieren

Schritt

Je nachdem, ob Sie eine bestimmte LIF oder alle LIFs migrieren möchten, führen Sie die entsprechende Aktion durch:

Migration…	Geben Sie den folgenden Befehl ein…
Ein spezifisches LIF	`network interface migrate`
Alle Daten- und Cluster-Management-LIFs auf einem Node	`network interface migrate-all`
Alle LIFs abseits eines Ports	`network interface migrate-all -node <node> -port <port>`

Das folgende Beispiel zeigt, wie eine LIF mit dem Namen `datalif1` auf der SVM `vs0` zum Port auf migriert `e0d` `node0b` wird:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

Das folgende Beispiel zeigt, wie alle Daten- und Cluster-Management-LIFs vom aktuellen (lokalen) Node migriert werden:

```
network interface migrate-all -node local
```

Verwandte Informationen

- "Migration der Netzwerkschnittstelle"

Zurücksetzen einer LIF auf seinen Home Port nach einem ONTAP Node Failover oder einer Port-Migration

Sie können eine LIF nach einem Failover auf ihren Home Port zurücksetzen oder sie wird entweder manuell oder automatisch zu einem anderen Port migriert. Wenn der Home-Port einer bestimmten LIF nicht verfügbar ist, bleibt das LIF im aktuellen Port des Ports und wird nicht zurückgesetzt.

Über diese Aufgabe

- Wenn Sie den Home Port eines LIF administrativ vor dem Einstellen der Option zur automatischen Rückstellung in den Zustand „up“ versetzen, wird das LIF nicht wieder zum Home Port zurückgegeben.
- Das LIF kehrt nicht automatisch zurück, es sei denn, die Option „Auto-revert“ ist auf „true“ gesetzt.
- Sie müssen sicherstellen, dass die Option „Auto-revert“ aktiviert ist, damit die LIFs auf die Home-Ports zurückgesetzt werden können.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager, um eine Netzwerkschnittstelle auf ihren Startport zurück zu setzen

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie ⋮ **> revert** neben der Netzwerkschnittstelle aus, die Sie ändern möchten.
3. Wählen Sie **revert** aus, um eine Netzwerkschnittstelle auf ihren Startport zurückzusetzen.

CLI

Verwenden Sie die CLI, um eine LIF auf ihren Home-Port zurück zu stellen

Schritt

Zurücksetzen eines LIF auf seinen Home Port manuell oder automatisch:

Wenn Sie eine LIF auf seinen Home-Port zurücksetzen möchten…	Geben Sie dann den folgenden Befehl ein…
Manuell	`network interface revert -vserver vserver_name -lif lif_name`
Automatisch	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

Erfahren Sie mehr über `network interface` in der "ONTAP-Befehlsreferenz".

Stellen Sie eine falsch konfigurierte ONTAP LIF wieder her

Ein Cluster kann nicht erstellt werden, wenn das Cluster-Netzwerk mit einem Switch verbunden ist, aber nicht alle im Cluster IPspace konfigurierten Ports können die anderen Ports erreichen, die im IP-Speicherplatz des Clusters konfiguriert sind.

Über diese Aufgabe

Wenn in einem Cluster mit Switches eine Cluster-Netzwerkschnittstelle (LIF) auf dem falschen Port konfiguriert ist oder ein Cluster-Port in das falsche Netzwerk integriert ist, `cluster create` kann der Befehl mit der folgenden Fehlermeldung fehlschlagen:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Erfahren Sie mehr über `cluster create` in der "ONTAP-Befehlsreferenz".

Die Ergebnisse des `network port show` Befehls können zeigen, dass dem Cluster-IPspace mehrere Ports hinzugefügt werden, da sie mit einem Port verbunden sind, der mit einer Cluster-LIF konfiguriert ist. Die Ergebnisse der `network port reachability show -detail` Der Befehl zeigt an, welche Ports keine Verbindung zueinander haben.

Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Um eine auf einem Port konfigurierte Cluster-LIF von wiederherzustellen, die für die anderen Ports, die mit Cluster-LIFs konfiguriert sind, nicht erreichbar ist, führen Sie die folgenden Schritte aus:

Schritte

1. Setzen Sie den Home-Port der Cluster-LIF auf den richtigen Port zurück:

   ```
   network port modify -home-port
   ```

   Erfahren Sie mehr über `network port modify` in der "ONTAP-Befehlsreferenz".

2. Entfernen Sie die Ports, für die keine Cluster-LIFs konfiguriert sind, aus der Cluster-Broadcast-Domäne:

   ```
   network port broadcast-domain remove-ports
   ```

   Erfahren Sie mehr über `network port broadcast-domain remove-ports` in der "ONTAP-Befehlsreferenz".

3. Erstellen des Clusters:

   ```
   cluster create
   ```

Ergebnis

Nach Abschluss der Cluster-Erstellung erkennt das System die korrekte Konfiguration und platziert die Ports in die richtigen Broadcast-Domänen.

Verwandte Informationen

- "Netzwerk-Port-Erreichbarkeit anzeigen"

Löschen Sie die ONTAP LIFs

Sie können eine nicht mehr benötigte Netzwerkschnittstelle (LIF) löschen.

Bevor Sie beginnen

Die zu löschenden LIFs dürfen nicht verwendet werden.

Schritte

1. Markieren Sie die LIFs, die Sie administrativ unten löschen möchten, mit folgendem Befehl:

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. `network interface delete`Löschen Sie mit dem Befehl eine oder alle LIFs:

Wenn Sie löschen möchten…	Geben Sie den Befehl ein …
Ein spezifisches LIF	`network interface delete -vserver vserver_name -lif lif_name`
Alle LIFs	`network interface delete -vserver vserver_name -lif *`

   Erfahren Sie mehr über `network interface delete` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird der LIF-mgmtlif2 gelöscht:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. `network interface show`Bestätigen Sie mit dem Befehl das Löschen der LIF.

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie ONTAP Virtual IP (VIP) LIFs

Einige Datacenter der nächsten Generation verwenden IP-Netzwerkmechanismen (Layer-3), die ein Failover von LIFs über Subnetze erfordern. ONTAP unterstützt virtuelle IP-Daten-LIFs (VIP) und das zugehörige Routing-Protokoll, das Border Gateway Protocol (BGP), um die Failover-Anforderungen dieser Netzwerke der nächsten Generation zu erfüllen.

Über diese Aufgabe

Eine VIP-Daten-LIF ist eine LIF, die nicht zu einem Subnetz gehört und über alle Ports erreichbar ist, die ein BGP LIF im gleichen IPspace hosten. Ein VIP-Daten-LIF beseitigt die Abhängigkeit eines Hosts von einzelnen Netzwerkschnittstellen. Da mehrere physische Adapter den Datenverkehr übertragen, konzentriert sich die gesamte Last nicht auf einen einzelnen Adapter und das zugehörige Subnetz. Die Existenz einer VIP-Daten-LIF wird Peer-Router über das Routing-Protokoll Border Gateway Protocol (BGP) angekündigt.

VIP-Daten-LIFs bieten die folgenden Vorteile:

- LIF-Portabilität über eine Broadcast-Domäne oder ein Subnetz hinaus: VIP-Daten-LIFs können ein Failover auf ein beliebiges Subnetz im Netzwerk durchführen, indem der aktuelle Speicherort der einzelnen VIP-Daten-LIFs Router über BGP angekündigt wird.
- Aggregatdurchsatz: VIP-Daten-LIFs unterstützen den Gesamtdurchsatz, der die Bandbreite des einzelnen Ports überschreitet, da die VIP LIFs Daten gleichzeitig von mehreren Subnetzen oder Ports senden oder empfangen können.

Border Gateway Protocol (BGP) einrichten

Vor der Erstellung von VIP-LIFs müssen Sie BGP einrichten. Dies ist das Routingprotokoll, das für die Ankündigung der Existenz einer VIP-LIF an Peer-Router verwendet wird.

Ab ONTAP 9.9.1 bietet VIP optionale Standard-Routenautomatisierung mit BGP-Peer-Gruppen, um die Konfiguration zu vereinfachen.

ONTAP hat eine einfache Möglichkeit, Standardrouten mit den BGP-Peers als Next-Hop-Router zu erlernen, wenn sich der BGP-Peer im selben Subnetz befindet. Um die Funktion zu verwenden, setzen Sie das `-use-peer-as-next-hop` Attribut auf `true`. Standardmäßig ist dieses Attribut `false` .

Wenn Sie statische Routen konfiguriert haben, werden diese immer noch vor diesen automatisierten Standardrouten bevorzugt.

Bevor Sie beginnen

Der Peer-Router muss so konfiguriert sein, dass er eine BGP-Verbindung von der BGP-LIF für die konfigurierte autonome Systemnummer (ASN) akzeptiert.

> ONTAP verarbeitet keine eingehenden Routenankündigungen vom Router. Daher sollten Sie den Peer-Router so konfigurieren, dass keine Route-Updates an das Cluster gesendet werden. Dies verkürzt die Zeit, die für die Kommunikation mit dem Peer benötigt wird, um voll funktionsfähig zu werden, und reduziert die interne Speichernutzung innerhalb von ONTAP.

Über diese Aufgabe

Beim Einrichten von BGP ist optional die Erstellung einer BGP-Konfiguration, das Erstellen einer BGP-LIF und das Erstellen einer BGP-Peer-Gruppe erforderlich. ONTAP erstellt automatisch eine Standard-BGP-Konfiguration mit Standardwerten, wenn die erste BGP-Peer-Gruppe auf einem bestimmten Knoten erstellt wird.

Ein BGP LIF wird zur Einrichtung von BGP TCP-Sitzungen mit Peer-Routern verwendet. Für einen Peer-Router ist eine BGP LIF der nächste Hop, um eine VIP-LIF zu erreichen. Für das BGP LIF ist ein Failover deaktiviert. Eine BGP-Peer-Gruppe stellt die VIP-Routen für alle SVMs im von der Peer-Gruppe verwendeten IPspace bereit. Der von der Peer-Gruppe verwendete IPspace wird vom BGP-LIF geerbt.

Ab ONTAP 9.16.1 wird die MD5-Authentifizierung auf BGP-Peer-Gruppen zum Schutz von BGP-Sitzungen unterstützt. Wenn MD5 aktiviert ist, können BGP-Sitzungen nur unter autorisierten Peers eingerichtet und verarbeitet werden, um mögliche Unterbrechungen der Sitzung durch einen nicht autorisierten Schauspieler zu

verhindern.

Die Befehle und `network bgp peer-group modify` wurden um folgende Felder erweitert `network bgp peer-group create`:

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Mit diesen Parametern können Sie eine BGP-Peer-Gruppe mit einer MD5-Signatur für erhöhte Sicherheit konfigurieren. Die folgenden Anforderungen gelten für die Verwendung der MD5-Authentifizierung:

- Sie können den Parameter nur angeben `-md5-secret`, wenn der `-md5-enabled` Parameter auf eingestellt ist `true`.
- IPsec muss global aktiviert sein, bevor Sie die MD5-BGP-Authentifizierung aktivieren können. Das BGP-LIF ist nicht für eine aktive IPsec-Konfiguration erforderlich. Siehe "Konfigurieren Sie IP-Sicherheit (IPsec) über die Verschlüsselung über das Netzwerk".
- NetApp empfiehlt, MD5 auf dem Router zu konfigurieren, bevor Sie es auf dem ONTAP-Controller konfigurieren.

Ab ONTAP 9.9 wurden diese Felder hinzugefügt:

- `-asn` Oder `-peer-asn` (4-Byte-Wert) das Attribut selbst ist nicht neu, aber es verwendet jetzt eine 4-Byte-Ganzzahl.
- `-med`
- `-use-peer-as-next-hop`

Sie können erweiterte Routenauswahl mit Multi-Exit Discriminator (MED) Unterstützung für die Pfadpriorisierung vornehmen. MED ist ein optionales Attribut in der BGP-Aktualisierungsmeldung, das Routern anweist, die beste Route für den Datenverkehr auszuwählen. Bei MED handelt es sich um eine unsignierte 32-Bit-Ganzzahl (0 - 4294967295); niedrigere Werte werden bevorzugt.

Ab ONTAP 9.8 wurden die folgenden Felder dem `network bgp peer-group` Befehl hinzugefügt:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Mit diesen BGP-Attributen können Sie DIE ATTRIBUTE ALS Pfad und Community für die BGP-Peer-Gruppe konfigurieren.

> Während ONTAP die oben genannten BGP-Attribute unterstützt, müssen Router diese nicht anerkennen. NetApp empfiehlt dringend, zu bestätigen, welche Attribute von Ihrem Router unterstützt werden, und BGP-Peer-Gruppen entsprechend zu konfigurieren. Weitere Informationen finden Sie in der von Ihrem Router bereitgestellten BGP-Dokumentation.

Schritte

1. Melden Sie sich bei der erweiterten Berechtigungsebene an:

   ```
   set -privilege advanced
   ```

2. Optional: Erstellen Sie eine BGP-Konfiguration oder ändern Sie die Standard-BGP-Konfiguration des Clusters, indem Sie eine der folgenden Aktionen durchführen:

   a. BGP-Konfiguration erstellen:

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

   - Der `-routerid` Parameter akzeptiert einen gepunkteten Dezimalwert von 32 Bit, der nur innerhalb einer AS-Domäne eindeutig sein muss. NetApp empfiehlt, die Node-Management-IP-Adresse (v4) zu verwenden, für `<router_id>` die eine Eindeutigkeit garantiert.
   - Obwohl ONTAP BGP 32-Bit-ASN-Zahlen unterstützt, wird nur die Standard-Dezimalschreibweise unterstützt. Gepunktete ASN-Notation, z. B. 65000.1 statt 4259840001 für eine private ASN, wird nicht unterstützt.

   Beispiel mit einem 2-Byte-ASN:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

   Beispiel mit einem 4-Byte-ASN:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

   a. Ändern der Standard-BGP-Konfiguration:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

   - `<asn_number>` Gibt die ASN-Nummer an. Ab ONTAP 9.8 unterstützt ASN für BGP eine nicht-negative Ganzzahl mit 2 Bytes. Dies ist eine 16-Bit-Zahl (1 bis 65534 verfügbare Werte). Ab ONTAP 9.9.1 unterstützt ASN für BGP eine nicht-negative 4-Byte-Ganzzahl (1 bis 4294967295). Der Standard-ASN ist 65501. ASN 23456 ist für die Einrichtung von ONTAP-Sitzungen mit Kollegen reserviert, die keine 4-Byte-ASN-Funktion ankündigen.
   - `<hold_time>` Gibt die Haltezeit in Sekunden an. Der Standardwert ist 180s.

   ONTAP unterstützt nur eine globale `<asn_number>`, `<hold_time>` und `<router_id>`, auch wenn Sie BGP für mehrere IPspaces konfigurieren. Der BGP und alle IP-Routing-Informationen sind vollständig in einem IPspace isoliert. Ein IPspace entspricht einer virtuellen Routing- und Forwarding-Instanz (VRF).

3. BGP-LIF für die System-SVM erstellen:

   Im Standard-IPspace ist der SVM-Name der Cluster-Name. Bei zusätzlichen IPspaces ist der Name der SVM mit dem IPspace-Namen identisch.

   ```
   network interface create -vserver <system_svm> -lif <lif_name> -service
   -policy default-route-announce -home-node <home_node> -home-port
   <home_port> -address <ip_address> -netmask <netmask>
   ```

   Sie können die `default-route-announce` Service-Richtlinie für die BGP-LIF oder jede benutzerdefinierte Service-Richtlinie verwenden, die den Service „Management-bgp“ enthält.

   ```
   network interface create -vserver cluster1 -lif bgp1 -service-policy
   default-route-announce -home-node cluster1-01 -home-port e0c -address
   10.10.10.100 -netmask 255.255.255.0
   ```

4. Erstellen Sie eine BGP-Peer-Gruppe, die zum Erstellen von BGP-Sitzungen mit den Remote Peer Routern verwendet wird, und konfigurieren Sie die VIP-Routinginformationen, die den Peer-Routern angekündigt werden:

   Beispiel 1: Erstellen Sie eine Peer-Gruppe ohne automatische Standardroute

   In diesem Fall muss der Administrator eine statische Route zum BGP-Peer erstellen.

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
   type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
   {-community BGP community list <0-65535>:<0-65535>}
   ```

   ```
   network bgp peer-group create -peer-group group1 -ipspace Default -bgp
   -lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
   -asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
   9000:900,8000:800
   ```

   Beispiel 2: Erstellen Sie eine Peer-Gruppe mit einer automatischen Standardroute

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
   preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
   prepend-count <integer>} {-med <integer>} {-community BGP community list
   <0-65535>:<0-65535>}
   ```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Beispiel 3: Erstellen Sie eine Peer-Gruppe mit aktiviertem MD5

a. IPsec aktivieren:

```
security ipsec config modify -is-enabled true
```

b. Erstellen Sie die BGP-Peer-Gruppe mit aktiviertem MD5:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Beispiel mit einem Hex-Schlüssel:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657400
```

Beispiel mit einem String:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Nachdem Sie die BGP-Peer-Gruppe erstellt haben, wird beim Ausführen des Befehls ein virtueller ethernet-Port (beginnend mit v0a..v0z,v1a…) aufgelistet `network port show`. Die MTU dieser Schnittstelle wird immer unter 1500 gemeldet. Die tatsächlich für den Datenverkehr verwendete MTU wird vom physischen Port (BGP LIF) abgeleitet, der beim Senden des Datenverkehrs ermittelt wird. Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Virtuelle IP-Datenschnittstelle (VIP) erstellen

Die Existenz einer VIP-Daten-LIF wird Peer-Router über das Routing-Protokoll Border Gateway Protocol (BGP) angekündigt.

Bevor Sie beginnen

- Die BGP-Peer-Gruppe muss eingerichtet werden und die BGP-Sitzung für die SVM, auf der die LIF erstellt werden soll, muss aktiv sein.

- Für jeden ausgehenden VIP-Datenverkehr für die SVM muss eine statische Route zum BGP-Router oder einem anderen Router im Subnetz des BGP-LIF erstellt werden.
- Sie sollten Multipath-Routing aktivieren, damit der ausgehende VIP-Verkehr alle verfügbaren Routen nutzen kann.

  Wenn die Multipath-Weiterleitung nicht aktiviert ist, wird der gesamte ausgehende VIP-Datenverkehr von einer einzigen Schnittstelle geleitet.

Schritte

1. Schnittstelle für VIP-Daten erstellen:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role data
   -data-protocol
   {nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
   <ip_address> -is-vip true -failover-policy broadcast-domain-wide
   ```

   Ein VIP-Port wird automatisch ausgewählt, wenn Sie den Home-Port nicht mit dem `network interface create` Befehl angeben.

   Standardmäßig gehört die VIP Daten-LIF zu jedem IPspace der vom System erstellten Broadcast-Domäne namens „VIP“. Sie können die VIP-Broadcast-Domäne nicht ändern.

   Ein VIP-Daten-LIF ist auf allen Ports, die eine BGP LIF eines IPspace hosten, gleichzeitig erreichbar. Wenn keine aktive BGP-Sitzung für die SVM der VIP auf dem lokalen Knoten vorhanden ist, erfolgt ein Failover der LIF der VIP-Daten zum nächsten VIP-Port auf dem Node, auf dem eine BGP-Sitzung für diese SVM eingerichtet wurde.

2. Vergewissern Sie sich, dass die BGP-Sitzung den Status „up“ für die SVM der VIP-Daten-LIF aufweist:

   ```
   network bgp vserver-status show

   Node        Vserver  bgp status
           ----------  -------- ---------
           node1       vs1      up
   ```

   Wenn der BGP-Status `down` für die SVM auf einem Node lautet, erfolgt ein Failover der VIP-Daten-LIF auf einen anderen Node, bei dem der BGP-Status für die SVM aktiviert ist. Wenn der BGP-Status `down` in allen Nodes lautet, kann die LIF für VIP-Daten nicht überall gehostet werden, und hat den LIF-Status als ausgefallen.

Befehle zum Verwalten des BGP

Ab ONTAP 9.5 verwenden Sie die `network bgp` Befehle, um die BGP-Sitzungen in ONTAP zu verwalten.

Verwalten der BGP-Konfiguration

Ihr Ziel ist	Befehl

Erstellen einer BGP-Konfiguration	`network bgp config create`
BGP-Konfiguration ändern	`network bgp config modify`
BGP-Konfiguration löschen	`network bgp config delete`
Zeigt die BGP-Konfiguration an	`network bgp config show`
Zeigt den BGP-Status für die SVM der VIP-LIF an	`network bgp vserver-status show`

Verwalten von BGP-Standardwerten

Ihr Ziel ist	Befehl
BGP-Standardwerte ändern	`network bgp defaults modify`
Anzeigen von BGP-Standardwerten	`network bgp defaults show`

Verwalten von BGP-Peer-Gruppen

Ihr Ziel ist	Befehl
Erstellen Sie eine BGP-Peer-Gruppe	`network bgp peer-group create`
Ändern einer BGP-Peer-Gruppe	`network bgp peer-group modify`
Löschen einer BGP-Peer-Gruppe	`network bgp peer-group delete`
Informationen zu BGP-Peer-Gruppen anzeigen	`network bgp peer-group show`
Benennen Sie eine BGP-Peer-Gruppe um	`network bgp peer-group rename`

Verwalten von BGP-Peer-Gruppen mit MD5

Ab ONTAP 9.16.1 können Sie die MD5-Authentifizierung in einer vorhandenen BGP-Peer-Gruppe aktivieren oder deaktivieren.

> Wenn Sie MD5 auf einer vorhandenen BGP-Peer-Gruppe aktivieren oder deaktivieren, wird die BGP-Verbindung beendet und neu erstellt, um die MD5-Konfigurationsänderungen anzuwenden.

Ihr Ziel ist	Befehl
Aktivieren Sie MD5 in einer vorhandenen BGP-Peer-Gruppe	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Deaktivieren Sie MD5 in einer vorhandenen BGP-Peer-Gruppe	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

- "Netzwerk-bgp"
- "Netzwerkschnittstelle"
- "Sicherheit IPSec-Konfiguration ändern"

Lasten des Netzwerks ausgleichen

Optimieren Sie den ONTAP-Netzwerkverkehr mithilfe des DNS-Lastausgleichs

Sie können Ihr Cluster so konfigurieren, dass Client-Anforderungen von entsprechend geladenen LIFs erfüllt werden. Dies führt zu einer ausgewogeneren Auslastung von LIFs und Ports, was wiederum eine bessere Performance des Clusters ermöglicht.

Der DNS-Lastausgleich hilft bei der Auswahl einer entsprechend ausgelasteten Daten-LIF und beim Ausgleichen von Datenverkehr im Benutzernetzwerk über alle verfügbaren Ports (physische Ports, Interface Groups und VLANs).

Beim DNS-Lastausgleich sind LIFs mit der Lastverteilungszone einer SVM verbunden. Ein DNS-Server für den gesamten Standort wird so konfiguriert, dass er alle DNS-Anfragen weitergibt und die am wenigsten geladene LIF auf Basis des Netzwerk-Traffic und der Verfügbarkeit der Port-Ressourcen (CPU-Auslastung, Durchsatz, offene Verbindungen usw.) zurückgibt. Der DNS-Lastausgleich bietet folgende Vorteile:

- Neue Client-Verbindungen, die auf verfügbare Ressourcen abgestimmt sind.
- Es sind keine manuellen Eingriffe erforderlich, um zu entscheiden, welche LIFs beim Mounten einer bestimmten SVM zu verwenden sind.
- DNS-Lastausgleich unterstützt NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1 SMB 3.0 und S3.

Erfahren Sie mehr über den DNS-Lastausgleich für das ONTAP-Netzwerk

Clients mounten eine SVM durch Angabe einer IP-Adresse (zugeordnet zu einer LIF) oder eines Host-Namens (zugeordnet mit mehreren IP-Adressen). Standardmäßig werden vom Site-weiten DNS-Server LIFs Round Robin-Verfahren ausgewählt, um den Workload auf alle LIFs gleichmäßig zu verteilen.

Der Round-Robin-Lastausgleich kann zu einer Überprovisionierung einiger LIFs führen, sodass Sie die Möglichkeit haben, eine DNS-Load-Balancing-Zone zu verwenden, die die Host-Name-Auflösung in einer SVM übernimmt. Mithilfe einer DNS-Lastausgleichzone wird ein besserer Ausgleich der neuen Clientverbindungen über verfügbare Ressourcen hinweg gewährleistet, was zu einer verbesserten Leistung des Clusters führt.

Eine DNS-Lastausgleichzone ist ein DNS-Server im Cluster, der die Last auf allen LIFs dynamisch bewertet und eine entsprechend geladene LIF zurückgibt. In einer Load Balancing Zone weist DNS jeder logischen Schnittstelle ein Gewicht (Metrik) zu, das auf der Last basiert.

Jeder LIF wird basierend auf der Port-Last und der CPU-Auslastung des Home Node ein Gewicht zugewiesen. LIFs, die auf weniger geladenen Ports arbeiten, haben eine höhere Wahrscheinlichkeit, dass sie in eine DNS-Abfrage zurückgegeben werden. Gewichte können auch manuell zugewiesen werden.

DNS-Lastausgleichzonen für das ONTAP-Netzwerk erstellen

Sie können eine DNS-Lastausgleichzone erstellen, um die dynamische Auswahl einer

logischen Schnittstelle gemäß der Last, d. h. der Anzahl der Clients, die auf einem LIF gemountet sind, zu vereinfachen. Sie können eine Load Balancing-Zone erstellen, während Sie eine Daten-LIF erstellen.

Bevor Sie beginnen

Der DNS-Forwarder auf dem standortweiten DNS-Server muss so konfiguriert sein, dass alle Anfragen für die Lastausgleichszone an die konfigurierten LIFs weitergehen.

Der"NetApp Knowledge Base: So richten Sie DNS-Lastausgleich im Cluster-Modus ein" enthält weitere Informationen zum Konfigurieren des DNS-Lastausgleichs mithilfe der bedingten Weiterleitung.

Über diese Aufgabe

- Jede logische Datenschnittstelle kann auf DNS-Abfragen für einen DNS-Namen für den Lastenausgleichsbereich reagieren.
- Eine DNS-Load-Balancing-Zone muss einen eindeutigen Namen im Cluster haben, und der Zonenname muss die folgenden Anforderungen erfüllen:
  - Er darf maximal 256 Zeichen lang sein.
  - Es sollte mindestens einen Zeitraum enthalten.
  - Das erste und das letzte Zeichen dürfen kein Punkt oder ein anderes Sonderzeichen sein.
  - Es dürfen keine Leerzeichen zwischen Zeichen enthalten.
  - Jede Beschriftung im DNS-Namen darf 63 Zeichen nicht überschreiten.

    Eine Bezeichnung ist der Text, der vor oder nach dem Zeitraum erscheint. Beispielsweise verfügt die DNS-Zone mit dem Namen storage.company.com über drei Bezeichnungen.

Schritt

Verwenden Sie den `network interface create` Befehl mit der `dns-zone` Option, um eine DNS-Lastausgleichszone zu erstellen. Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Wenn die Lastausgleichzone bereits vorhanden ist, wird ihr das LIF hinzugefügt.

Im folgenden Beispiel wird gezeigt, wie beim Erstellen der LIF eine DNS-Lastausgleichszone mit `lif1` dem Namen storage.company.com erstellt wird:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Fügen Sie eine ONTAP LIF hinzu oder entfernen Sie sie aus einer Lastverteilungszone

Sie können eine LIF hinzufügen oder aus der DNS-Load-Balancing-Zone einer Virtual Machine (SVM) entfernen. Sie können auch alle LIFs gleichzeitig aus einer Lastausgleichzone entfernen.

Bevor Sie beginnen

- Alle LIFs in einer Lastverteilungszone sollten zur gleichen SVM gehören.
- Ein LIF kann nur Teil einer DNS-Load-Balancing-Zone sein.
- Failover-Gruppen für jedes Subnetz müssen eingerichtet worden sein, wenn die LIFs zu unterschiedlichen Subnetzen gehören.

Über diese Aufgabe

Eine LIF, die sich im Status „Administratoren inaktiv“ befindet, wird vorübergehend aus der DNS-Load-Balancing-Zone entfernt. Wenn das LIF wieder zum Administrationsstatus zurückkehrt, wird das LIF automatisch der DNS-Load-Balancing-Zone hinzugefügt.

Schritt

Fügen Sie ein LIF zu einer Lastverteilung hinzu oder entfernen Sie diese aus einer Zone:

Ihr Ziel ist	Eingeben…
Fügen Sie eine LIF hinzu	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Beispiel: `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`
Entfernen eines einzelnen LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none` Beispiel: `network interface modify -vserver vs1 -lif data1 -dns-zone none`
Entfernen Sie alle LIFs	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none` Beispiel: `network interface modify -vserver vs0 -lif * -dns-zone none` Sie können eine SVM aus einer Lastverteilungszone entfernen, indem Sie alle LIFs in der SVM aus dieser Zone entfernen.

Verwandte Informationen

- "Änderung der Netzwerkschnittstelle"

Konfigurieren Sie die DNS-Dienste für das ONTAP-Netzwerk

Vor dem Erstellen eines NFS- oder SMB-Servers müssen Sie die DNS-Services für die SVM konfigurieren. Im Allgemeinen sind die DNS-Namensserver die in Active Directory integrierten DNS-Server für die Domäne, der der NFS- oder SMB-Server Beitritt.

Über diese Aufgabe

In Active Directory integrierte DNS-Server enthalten die Service Location Records (SRV) für die Domain-LDAP- und Domain-Controller-Server. Wenn die SVM die Active Directory LDAP-Server und Domänen-Controller nicht finden kann, schlägt die Einrichtung des NFS- oder SMB-Servers fehl.

SVMs verwenden die Hosts Name Services ns-Switch-Datenbank, um zu ermitteln, welche Services verwendet werden sollen, und in welcher Reihenfolge beim Suchen von Informationen zu Hosts. Die beiden unterstützten Namensdienste für die Host-Datenbank sind Dateien und dns.

Bevor Sie den SMB-Server erstellen, müssen Sie sicherstellen, dass dns eine der Quellen ist.

Verwenden Sie die Statistics-UI, um die Statistiken für DNS-Namensdienste für den mgwd-Prozess und SECD-Prozess anzuzeigen.

Schritte

1. Bestimmen Sie, welche aktuelle Konfiguration für die Host Name Services-Datenbank ist. In diesem Beispiel verwendet die Datenbank des Hostnamens Service die Standardeinstellungen.

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. Führen Sie bei Bedarf die folgenden Aktionen durch.

   a. Fügen Sie den DNS-Namensservice der Host-Servicedatendatenbank in der gewünschten Reihenfolge hinzu, oder ordnen Sie die Quellen neu an.

      In diesem Beispiel ist die Host-Datenbank so konfiguriert, dass sie DNS- und lokale Dateien in dieser Reihenfolge verwendet.

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. Vergewissern Sie sich, dass die Konfiguration der Namensdienste richtig ist.

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. Konfigurieren Sie DNS-Dienste.

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

   Der Name-Service dns create Befehl vserver Services führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Nameserver nicht kontaktieren kann.

4. Vergewissern Sie sich, dass die DNS-Konfiguration korrekt ist und der Dienst aktiviert ist.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Überprüfen Sie den Status der Namensserver.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Konfigurieren Sie dynamisches DNS auf der SVM

Wenn der in Active Directory integrierte DNS-Server die DNS-Einträge eines NFS- oder SMB-Servers dynamisch in DNS registrieren soll, müssen Sie DDNS (Dynamic DNS) auf der SVM konfigurieren.

Bevor Sie beginnen

Auf der SVM müssen DNS-Namensservices konfiguriert werden. Wenn Sie sichere DDNS verwenden, müssen Sie die in Active Directory integrierten DNS-Namensserver verwenden, und Sie müssen entweder einen NFS- oder SMB-Server oder ein Active Directory-Konto für die SVM erstellt haben.

Über diese Aufgabe

Der angegebene vollständig qualifizierte Domänenname (FQDN) muss eindeutig sein:

Der angegebene vollständig qualifizierte Domänenname (FQDN) muss eindeutig sein:

- Bei NFS `-vserver-fqdn` `vserver services name-service dns dynamic-update` wird der in als Teil des Befehls angegebene Wert zum registrierten FQDN für die LIFs.
- Für SMB werden die Werte, die als NetBIOS-Name des CIFS-Servers und der vollständig qualifizierte CIFS-Domänenname angegeben sind, der registrierte FQDN für die LIFs. Dies ist in ONTAP nicht konfigurierbar. Im folgenden Szenario lautet der LIF-FQDN „CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Um einen Konfigurationsfehler bei einem SVM-FQDN zu vermeiden, der nicht den RFC-Regeln für DDNS-Updates entspricht, verwenden Sie einen FQDN-Namen, der RFC-kompatibel ist. Weitere Informationen finden Sie unter "RFC 1123".

Schritte

1. Konfigurieren Sie DDNS auf der SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates
   ```

   ```
   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Sternchen kann nicht als Teil des benutzerdefinierten FQDN verwendet werden. Beispiel: `*.netapp.com` Ist ungültig.

2. Überprüfen Sie, ob die DDNS-Konfiguration korrekt ist:

   ```
   vserver services name-service dns dynamic-update show
   ```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Konfigurieren Sie dynamische DNS-Dienste für das ONTAP-Netzwerk

Wenn der in Active Directory integrierte DNS-Server die DNS-Einträge eines NFS- oder SMB-Servers dynamisch in DNS registrieren soll, müssen Sie DDNS (Dynamic DNS) auf der SVM konfigurieren.

Bevor Sie beginnen

Auf der SVM müssen DNS-Namensservices konfiguriert werden. Wenn Sie sichere DDNS verwenden, müssen Sie die in Active Directory integrierten DNS-Namensserver verwenden, und Sie müssen entweder einen NFS- oder SMB-Server oder ein Active Directory-Konto für die SVM erstellt haben.

Über diese Aufgabe

Der angegebene FQDN muss eindeutig sein.

> Um einen Konfigurationsfehler bei einem SVM-FQDN zu vermeiden, der nicht den RFC-Regeln für DDNS-Updates entspricht, verwenden Sie einen FQDN-Namen, der RFC-kompatibel ist.

Schritte

1. Konfigurieren Sie DDNS auf der SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Sternchen kann nicht als Teil des benutzerdefinierten FQDN verwendet werden. Beispiel: `*.netapp.com` Ist ungültig.

2. Überprüfen Sie, ob die DDNS-Konfiguration korrekt ist:

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Auflösung des Hostnamens

Erfahren Sie mehr über die Auflösung von Hostnamen für das ONTAP-Netzwerk

ONTAP muss Hostnamen in numerische IP-Adressen übersetzen können, um den Zugriff auf Clients und den Zugriff auf Dienste zu ermöglichen. Sie müssen Storage Virtual Machines (SVMs) konfigurieren, damit Sie lokale oder externe Name Services verwenden können, um Host-Informationen zu beheben. ONTAP unterstützt die Konfiguration eines externen DNS-Servers oder die Konfiguration der lokalen Hostdatei für die Auflösung des Host-Namens.

Bei Verwendung eines externen DNS-Servers können Sie Dynamic DNS (DDNS) konfigurieren, der automatisch neue oder geänderte DNS-Informationen aus Ihrem Speichersystem an den DNS-Server sendet. Ohne dynamische DNS-Updates müssen Sie die DNS-Informationen (DNS-Name und IP-Adresse) manuell zu den identifizierten DNS-Servern hinzufügen, wenn ein neues System online geschaltet wird oder sich vorhandene DNS-Informationen ändern. Dieser Prozess ist langsam und fehleranfällig. Während der Disaster

Recovery kann die manuelle Konfiguration zu langen Ausfallzeiten führen.

Konfigurieren Sie DNS für die Auflösung von Hostnamen für das ONTAP-Netzwerk

Sie verwenden DNS, um auf lokale oder Remote-Quellen für Hostinformationen zuzugreifen. Sie müssen DNS konfigurieren, um auf eine oder beide Quellen zugreifen zu können.

ONTAP muss in der Lage sein, die Host-Informationen zu suchen, um Clients ordnungsgemäßen Zugriff zu ermöglichen. Sie müssen Name Services konfigurieren, damit ONTAP auf lokale oder externe DNS-Services zugreifen kann, um die Hostinformationen abzurufen.

ONTAP speichert Informationen zur Konfiguration des Namensservice in einer Tabelle, die der `/etc/nsswitch.conf` Datei auf UNIX-Systemen entspricht.

Konfigurieren Sie eine SVM und Daten-LIFs für die Host-Name-Auflösung mithilfe eines externen DNS-Servers

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst.

Bevor Sie beginnen

Ein standortweiter DNS-Server muss für die Suche nach Hostnamen verfügbar sein.

Sie sollten mehrere DNS-Server konfigurieren, um Single Point of Failure zu vermeiden. `vserver services name-service dns create`Wenn Sie nur einen DNS-Servernamen eingeben, gibt der Befehl eine Warnung aus.

Über diese Aufgabe

Konfigurieren Sie dynamische DNS-DiensteWeitere Informationen zum Konfigurieren von dynamischem DNS auf der SVM finden Sie unter.

Schritte

1. DNS auf der SVM aktivieren:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

Mit dem folgenden Befehl werden externe DNS-Server auf der SVM vs1 aktiviert:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

Der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsprüfung durch und meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

2. Überprüfen Sie den Status der Namensserver mit dem `vserver services name-service dns check` Befehl.

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

Informationen zu Service-Richtlinien, die sich auf DNS beziehen, finden Sie unter "LIFs und Service-Richtlinien in ONTAP 9.6 und höher".

Konfigurieren Sie die Tabelle „Namensdienst-Switch“ für die Host-Name-Auflösung

Sie müssen die Tabelle des Namensdienstschalters richtig konfigurieren, damit ONTAP zum Abrufen von Hostinformationen den lokalen oder externen Namensservice konsultieren kann.

Bevor Sie beginnen

Sie müssen sich für die Host-Zuordnung in Ihrer Umgebung entscheiden, welchen Namensservice Sie verwenden möchten.

Schritte

1. Fügen Sie die erforderlichen Einträge zur Tabelle des Namensdienstschalters hinzu:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Vergewissern Sie sich, dass die Tabelle des Namensdienstschalters die erwarteten Einträge in der gewünschten Reihenfolge enthält:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Beispiel

Im folgenden Beispiel wird ein Eintrag in der Switch-Tabelle für den Namensservice für SVM vs1 so geändert, dass er zuerst die Datei der lokalen Hosts und dann einen externen DNS-Server zum Auflösen der Hostnamen verwendet:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAP-Befehle zum Verwalten der Tabelle ONTAP-Hosts

Ein Cluster-Administrator kann die Einträge für den Host-Namen in der Hosttabelle der SVM (Storage Virtual Machine) hinzufügen, ändern, löschen und anzeigen. Ein SVM-Administrator kann die Hostnameneinträge nur für die zugewiesene SVM konfigurieren.

Befehle zum Verwalten von lokalen Host-Name-Einträgen

Mit dem `vserver services name-service dns hosts` Befehl können Sie DNS-Hosttabelleneinträge erstellen, ändern oder löschen.

Wenn Sie die DNS-Hostnamen erstellen oder ändern, können Sie mehrere Alias-Adressen, die durch Kommas getrennt sind, angeben.

Ihr Ziel ist	Befehl
Erstellen Sie einen DNS-Hostnamen	`vserver services name-service dns hosts create`
Ändern eines DNS-Host-Namens	`vserver services name-service dns hosts modify`
Löschen Sie einen DNS-Hostnamen	`vserver services name-service dns hosts delete`

Weitere Informationen zu den `vserver services name-service dns hosts` Befehlen finden Sie im "ONTAP-Befehlsreferenz".

Sicherheit für das Netzwerk

Konfigurieren Sie die ONTAP-Netzwerksicherheit mit FIPS für alle SSL-Verbindungen

ONTAP erfüllt die Anforderungen des Federal Information Processing Standards (FIPS) 140-2 für alle SSL-Verbindungen. Sie können den SSL-FIPS-Modus ein- und ausschalten, SSL-Protokolle global festlegen und alle schwachen Verschlüsselungsverfahren innerhalb von ONTAP deaktivieren.

Bei SSL auf ONTAP ist die FIPS-Compliance standardmäßig deaktiviert und die folgenden TLS-Protokolle aktiviert:

- TLSv1.3 (ab ONTAP 9.11.1)
- TLSv1.2

In früheren ONTAP-Versionen waren standardmäßig die folgenden TLS-Protokolle aktiviert:

- TLSv1.1 (standardmäßig deaktiviert ab ONTAP 9.12.1)
- TLSv1 (standardmäßig deaktiviert, beginnend mit ONTAP 9.8)

Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP mit externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Crypto for SSL verwendet.

Wenn Administratorkonten auf SVMs mit einem öffentlichen SSH-Schlüssel zugreifen möchten, müssen Sie vor Aktivierung des SSL-FIPS-Modus sicherstellen, dass der Host Key-Algorithmus unterstützt wird.

Hinweis: die Unterstützung des Host Key Algorithmus hat sich in ONTAP 9.11.1 und späteren Versionen geändert.

Version von ONTAP	Unterstützte Schlüsseltypen	Nicht unterstützte Schlüsseltypen
9.11.1 und höher	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + SSH-rsa

Bestehende öffentliche SSH-Konten ohne die unterstützten Schlüsselalgorithmen müssen vor der Aktivierung von FIPS mit einem unterstützten Schlüsseltyp neu konfiguriert werden oder die Administratorauthentifizierung schlägt fehl.

Weitere Informationen finden Sie unter "Aktivieren Sie SSH-Konten für öffentliche Schlüssel".

ONTAP 9.18.1 führt die Unterstützung für die Post-Quantum-Computing-Kryptographiealgorithmen ML-KEM, ML-DSA und SLH-DSA für SSL ein und bietet damit eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Quantencomputerangriffe. Diese Algorithmen sind nur verfügbar, wennFIPS ist deaktiviert Die Post-Quanten-Kryptographiealgorithmen werden ausgehandelt, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

Aktivieren Sie FIPS

Es wird empfohlen, dass alle sicheren Benutzer ihre Sicherheitskonfiguration unmittelbar nach der Installation oder Aktualisierung des Systems anpassen. Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP mit externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Crypto for SSL verwendet.

> Wenn FIPS aktiviert ist, können Sie kein Zertifikat mit einer RSA-Schlüssellänge von 4096 installieren oder erstellen.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. FIPS aktivieren:

   ```
   security config modify * -is-fips-enabled true
   ```

3. Wenn Sie dazu aufgefordert werden, fortzufahren, geben Sie ein `y`
4. Ab ONTAP 9.9.1 ist kein Neustart erforderlich. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster einzeln manuell neu.

Beispiel

Wenn ONTAP 9.9.1 oder höher ausgeführt wird, wird die Warnmeldung nicht angezeigt.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Weitere Informationen zur `security config modify` Konfiguration des SSL-FIPS-Modus finden Sie in "ONTAP-Befehlsreferenz".

FIPS deaktivieren

Ab ONTAP 9.18.1 unterstützt SSL in ONTAP die Post-Quantum-Computing-Kryptographiealgorithmen ML-KEM, ML-DSA und SLH-DSA. Diese Algorithmen sind nur verfügbar, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Deaktivieren Sie FIPS, indem Sie Folgendes eingeben:

   ```
   security config modify -is-fips-enabled false
   ```

3. Wenn Sie aufgefordert werden, fortzufahren, geben `y`Sie .
4. Ab ONTAP 9.9.1 ist kein Neustart erforderlich. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster manuell neu.

Wenn Sie das SSLv3-Protokoll verwenden müssen, müssen Sie FIPS mit dem oben beschriebenen Verfahren deaktivieren. SSLv3 kann nur aktiviert werden, wenn FIPS deaktiviert ist.

Sie können SSLv3 mit folgendem Befehl aktivieren. Wenn Sie ONTAP 9.9.1 oder eine neuere Version verwenden, wird Ihnen diese Warnmeldung nicht angezeigt.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Den FIPS-Compliance-Status anzeigen

Sie sehen, ob im gesamten Cluster die aktuellen Sicherheitseinstellungen ausgeführt werden.

Schritte

1. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster einzeln manuell neu.
2. Den aktuellen Compliance-Status anzeigen:

   `security config show`

   ```
   cluster1::> security config show
   Cluster    Supported
   FIPS Mode  Protocols Supported Cipher Suites
   ---------- ---------
   ------------------------------------------------------------
   false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
   TLS_RSA_WITH_AES_128_CCM_8,
              TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                        TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_RSA_WITH_AES_128_CBC_SHA256,
   TLS_RSA_WITH_AES_256_CCM,
                        TLS_RSA_WITH_AES_256_CCM_8,
                        ...
   ```

   Erfahren Sie mehr über `security config show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "FIPS 203: Standard für einen modulgitterbasierten Schlüsselkapselungsmechanismus (ML-KEM)"
- "FIPS 204: Modulgitterbasierter digitaler Signaturstandard (ML-DSA)"
- "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)"

Konfigurieren Sie die IPsec-Verschlüsselung während der Übertragung

Bereiten Sie die Verwendung der IP-Sicherheit im ONTAP-Netzwerk vor

Ab ONTAP 9.8 haben Sie die Möglichkeit, IP-Sicherheit (IPsec) zum Schutz Ihres Netzwerkverkehrs zu verwenden. IPsec ist eine von mehreren Data-in-Motion- oder in-Flight-Verschlüsselungsoptionen, die mit ONTAP verfügbar sind. Sie sollten die IPsec-Konfiguration vorbereiten, bevor Sie sie in einer Produktionsumgebung verwenden.

Implementierung der IP-Sicherheit in ONTAP

IPsec ist ein Internetstandard, der von der IETF verwaltet wird. Es bietet Datenverschlüsselung und -Integrität sowie Authentifizierung für den Datenverkehr, der auf IP-Ebene zwischen den Netzwerkendpunkten fließt.

Mit ONTAP sichert IPsec den gesamten IP-Datenverkehr zwischen ONTAP und den verschiedenen Clients, einschließlich der NFS-, SMB- und iSCSI-Protokolle. Neben Datenschutz und Datenintegrität ist der Netzwerkverkehr vor mehreren Angriffen wie Replay- und man-in-the-Middle-Angriffen geschützt. ONTAP verwendet die Implementierung des IPsec-Transportmodus. Er nutzt das IKE-Protokoll (Internet Key Exchange) Version 2 für die Verhandlung des Schlüsselmaterials zwischen ONTAP und den Clients, die entweder IPv4 oder IPv6 verwenden.

Wenn die IPsec-Funktion auf einem Cluster aktiviert ist, erfordert das Netzwerk einen oder mehrere Einträge in der ONTAP-Sicherheitsrichtliniendatenbank (SPD), die den verschiedenen Datenverkehrseigenschaften entsprechen. Diese Einträge werden den spezifischen Schutzdetails zugeordnet, die zum Verarbeiten und Senden der Daten erforderlich sind (z. B. Chiffre Suite und Authentifizierungsmethode). Ein entsprechender SPD-Eintrag ist ebenfalls bei jedem Client erforderlich.

Für bestimmte Arten von Datenverkehr ist möglicherweise eine andere Option zur Verschlüsselung von Daten in Bewegung vorzuziehen. Für die Verschlüsselung von NetApp SnapMirror- und Cluster-Peering-Datenverkehr wird beispielsweise das TLS-Protokoll (Transport Layer Security) anstelle von IPsec empfohlen. Das liegt daran, dass TLS in den meisten Situationen eine bessere Leistung bietet.

Verwandte Informationen

- "Internet Engineering Task Force"
- "RFC 4301: Sicherheitsarchitektur für das Internet Protocol"

Weiterentwicklung der ONTAP IPsec-Implementierung

IPsec wurde erstmals mit ONTAP 9.8 eingeführt. Die Implementierung wurde in nachfolgenden ONTAP Versionen wie unten beschrieben weiterentwickelt.

ONTAP 9.18.1

Die Unterstützung für IPsec-Hardware-Offloading wurde auf IPv6-Datenverkehr erweitert.

ONTAP 9.17.1

Die Unterstützung für IPsec-Hardware-Offload wird erweitert auf "Link-Aggregationsgruppen" . "Postquanten-Pre-Shared Keys (PPKs)" werden für die IPsec-Pre-Shared Keys (PSK)-Authentifizierung unterstützt.

ONTAP 9.16.1

Mehrere kryptografische Vorgänge, wie Verschlüsselungs- und Integritätsprüfungen, können auf eine unterstützte NIC-Karte verlagert werden. Weitere Informationen finden Sie unter IPsec-Hardware-Offload-Funktion .

ONTAP 9.12.1

Die Unterstützung von IPsec-Front-End-Hostprotokollen ist in MetroCluster-IP- und MetroCluster-Fabric-Attached-Konfigurationen verfügbar. Die durch MetroCluster Cluster bereitgestellte IPsec-Unterstützung für Cluster ist auf Front-End-Host-Datenverkehr beschränkt und wird auf MetroCluster LIFs nicht unterstützt.

ONTAP 9.10.1

Zusätzlich zu den PSKs können Zertifikate für die IPsec-Authentifizierung verwendet werden. Vor ONTAP 9.10.1 werden nur PSKs für die Authentifizierung unterstützt.

ONTAP 9.9.1

Die von IPsec verwendeten Verschlüsselungsalgorithmen sind nach FIPS 140-2 validiert. Diese Algorithmen werden vom NetApp Cryptographic Module in ONTAP verarbeitet, das die FIPS 140-2-2-Validierung führt.

ONTAP 9,8

Die Unterstützung für IPsec wird basierend auf der Implementierung des Transportmodus zunächst verfügbar.

IPsec-Hardware-Offload-Funktion

Wenn Sie ONTAP 9.16.1 oder höher verwenden, haben Sie die Möglichkeit, bestimmte rechenintensive Vorgänge, wie z. B. Verschlüsselungs- und Integritätsprüfungen, auf eine am Storage-Node installierte NIC-Karte (Network Interface Controller) zu übertragen. Der Durchsatz für auf die NIC-Karte ausgelagerte Vorgänge beträgt etwa 5 % oder weniger. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.

Anforderungen und Empfehlungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Anforderungen beachten.

Unterstützte Ethernet-Karten

Sie dürfen nur unterstützte Ethernet-Karten installieren und verwenden. Die folgenden Ethernet-Karten werden ab ONTAP 9.16.1 unterstützt:

- X50131A (2P, 40G/100G/200G/400G Ethernet-Controller)
- X60132A (4p, 10G/25G Ethernet-Controller)

ONTAP 9.17.1 fügt Unterstützung für die folgenden Ethernet-Karten hinzu:

- X50135A (2p, 40G/100G Ethernet-Controller)
- X60135A (2p, 40G/100G Ethernet-Controller)

Die Karten X50131A und X50135A werden auf den folgenden Plattformen unterstützt:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Die Karten X60132A und X60135A werden auf den folgenden Plattformen unterstützt:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Sehen Sie sich die "NetApp Hardware Universe" für weitere Informationen zu den unterstützten Plattformen und Karten.

Umfang des Clusters

Die IPsec-Hardware-Offload-Funktion ist global für den Cluster konfiguriert. Und so wird der Befehl beispielsweise `security ipsec config` auf alle Nodes im Cluster angewendet.

Konsistente Konfiguration

Unterstützte NIC-Karten sollten auf allen Knoten im Cluster installiert werden. Wenn eine unterstützte NIC-Karte nur auf einigen Nodes verfügbar ist, wird nach einem Failover eine deutliche Performance-Verschlechterung angezeigt, wenn einige der LIFs nicht auf einer Offload-fähigen NIC gehostet werden.

Anti-Replay deaktivieren

Sie müssen den IPsec-Anti-Replay-Schutz auf ONTAP (Standardkonfiguration) und den IPsec-Clients deaktivieren. Wenn diese Option nicht deaktiviert ist, werden Fragmentierung und Multi-Path (redundante Route) nicht unterstützt.

Wenn die ONTAP-IPsec-Konfiguration von der Standardeinstellung auf Anti-Replay-Schutz aktivieren geändert wurde, verwenden Sie diesen Befehl, um sie zu deaktivieren:

```
security ipsec config modify -replay-window 0
```

Sie müssen sicherstellen, dass der IPsec-Anti-Replay-Schutz auf Ihrem Client deaktiviert ist. Informationen zur Deaktivierung des Anti-Replay-Schutzes finden Sie in der IPsec-Dokumentation für Ihren Client.

Einschränkungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Einschränkungen berücksichtigen.

IPv6

Ab ONTAP 9.18.1 wird IPv6 für die IPsec-Hardware-Offload-Funktion unterstützt. Vor ONTAP 9.18.1 unterstützt die IPsec-Hardware-Auslagerung kein IPv6.

Erweiterte Sequenznummern

Die erweiterten IPsec-Sequenznummern werden von der Hardware-Offload-Funktion nicht unterstützt. Es werden nur die normalen 32-Bit-Sequenznummern verwendet.

Link-Aggregation

Ab ONTAP 9.17.1 können Sie die IPsec-Hardware-Offload-Funktion mit einem "Link-Aggregationsgruppe" .

Vor Version 9.17.1 unterstützt die IPsec-Hardware-Offload-Funktion keine Link-Aggregation. Sie kann nicht mit

einer Schnittstelle oder Link-Aggregationsgruppe verwendet werden, die über das `network port ifgrp` Befehle an der ONTAP CLI.

Konfigurationsunterstützung in der ONTAP-CLI

In ONTAP 9.16.1 werden drei vorhandene CLI-Befehle aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen. "Konfigurieren Sie die IP-Sicherheit in ONTAP"Weitere Informationen finden Sie unter.

ONTAP-Befehl	Aktualisieren
`security ipsec config show`	Der boolesche Parameter `Offload Enabled` zeigt den aktuellen NIC-Offload-Status an.
`security ipsec config modify`	Mit dem Parameter `is-offload-enabled` kann die NIC-Offload-Funktion aktiviert oder deaktiviert werden.
`security ipsec config show-ipsecsa`	Vier neue Zähler wurden hinzugefügt, um den ein- und ausgehenden Datenverkehr in Byte und Paketen anzuzeigen.

Konfigurationsunterstützung in der ONTAP-REST-API

Zwei vorhandene REST-API-Endpunkte werden in ONTAP 9.16.1 aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen.

REST-Endpunkt	Aktualisieren
`/api/security/ipsec`	Der Parameter `offload_enabled` wurde hinzugefügt und ist mit der PATCH-Methode verfügbar.
`/api/security/ipsec/security_association`	Zwei neue Zählerwerte wurden hinzugefügt, um die Gesamtzahl der von der Offload-Funktion verarbeiteten Bytes und Pakete zu verfolgen.

Weitere Informationen zur ONTAP REST-API einschließlich "Neuerungen an der ONTAP REST-API"finden Sie in der Dokumentation zur ONTAP Automatisierung. Weitere Informationen zu finden Sie auch in der Dokumentation zur ONTAP-Automatisierung "IPsec-Endpunkte".

Verwandte Informationen

- "Sicherheit IPSec"

Konfigurieren Sie die IP-Sicherheit für das ONTAP-Netzwerk

Zum Konfigurieren und Aktivieren der IPsec-Verschlüsselung während der Übertragung auf Ihrem ONTAP-Cluster sind mehrere Aufgaben erforderlich.

Überprüfen Sie die "Bereiten Sie sich auf die Verwendung der IP-Sicherheit vor"Einstellungen, bevor Sie IPsec konfigurieren. Sie müssen beispielsweise entscheiden, ob Sie die ab ONTAP 9.16.1 verfügbare IPsec-Hardware-Offload-Funktion verwenden möchten.

Aktivieren Sie IPsec auf dem Cluster

Sie können IPsec auf dem Cluster aktivieren, um sicherzustellen, dass Daten während der Übertragung kontinuierlich verschlüsselt und sicher sind.

Schritte

1. Ermitteln, ob IPsec bereits aktiviert ist:

   `security ipsec config show`

   Wenn das Ergebnis enthält `IPsec Enabled: false`, fahren Sie mit dem nächsten Schritt fort.

2. IPsec aktivieren:

   `security ipsec config modify -is-enabled true`

   Sie können die IPsec-Hardware-Offload-Funktion mit dem booleschen Parameter aktivieren `is-offload-enabled`.

3. Führen Sie den Ermittlungsbefehl erneut aus:

   `security ipsec config show`

   Das Ergebnis enthält nun `IPsec Enabled: true`.

Bereiten Sie die IPsec-Richtlinienerstellung mit Zertifikatauthentifizierung vor

Sie können diesen Schritt überspringen, wenn Sie nur PSKs (Pre-Shared Keys) zur Authentifizierung verwenden und keine Zertifikatauthentifizierung verwenden.

Bevor Sie eine IPsec-Richtlinie erstellen, die Zertifikate für die Authentifizierung verwendet, müssen Sie überprüfen, ob die folgenden Voraussetzungen erfüllt sind:

- Sowohl ONTAP als auch der Client müssen das CA-Zertifikat der anderen Partei installiert haben, damit die Zertifikate der Endeinheit (entweder ONTAP oder der Client) von beiden Seiten verifiziert werden können
- Für die ONTAP LIF, die an der Richtlinie teilnimmt, wird ein Zertifikat installiert

ONTAP LIFs können Zertifikate gemeinsam nutzen. Es ist keine 1:1-Zuordnung zwischen Zertifikaten und LIFs erforderlich.

Schritte

1. Installieren Sie alle während der gegenseitigen Authentifizierung verwendeten CA-Zertifikate, einschließlich ONTAP- und Client-seitiger CAS, in das ONTAP-Zertifikatsmanagement, sofern sie nicht bereits installiert ist (wie bei einer selbstsignierten ONTAP-Root-CA).

   Beispielbefehl

   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Um sicherzustellen, dass sich die installierte CA während der Authentifizierung im IPsec-CA-Suchpfad befindet, fügen Sie mithilfe des `security ipsec ca-certificate add` Befehls die ONTAP-Zertifizierungsstelle für die Zertifikatsverwaltung zum IPsec-Modul hinzu.

   Beispielbefehl

   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Erstellen und installieren Sie ein Zertifikat zur Verwendung durch die LIF von ONTAP. Die Emittent-CA dieses Zertifikats muss bereits in ONTAP installiert und zu IPsec hinzugefügt werden.

   Beispielbefehl

   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

Weitere Informationen zu Zertifikaten in ONTAP finden Sie in den Befehlen für Sicherheitszertifikate in der Dokumentation zu ONTAP 9.

Security Policy Database (SPD) definieren

IPsec erfordert einen SPD-Eintrag, bevor der Datenverkehr im Netzwerk fließen kann. Dies gilt unabhängig davon, ob Sie ein PSK oder ein Zertifikat zur Authentifizierung verwenden.

Schritte

1. Mit dem `security ipsec policy create` Befehl können Sie:
   a. Wählen Sie die ONTAP-IP-Adresse oder das Subnetz der IP-Adressen aus, die am IPsec-Transport beteiligt werden sollen.
   b. Wählen Sie die Client-IP-Adressen aus, die eine Verbindung zu den ONTAP-IP-Adressen herstellen.

      Der Client muss Internet Key Exchange Version 2 (IKEv2) mit einem vorab freigegebenen Schlüssel (PSK) unterstützen.

   c. Wählen Sie optional die detaillierten Datenverkehrsparameter aus, z. B. die Protokolle der oberen Schicht (UDP, TCP, ICMP usw.), die lokalen Portnummern und die Remote-Portnummern, um den Datenverkehr zu schützen. Die entsprechenden Parameter sind `protocols` , `local-ports` Und `remote-ports` jeweils.

      Überspringen Sie diesen Schritt, um den gesamten Datenverkehr zwischen der ONTAP-IP-Adresse und der Client-IP-Adresse zu schützen. Der Schutz des gesamten Datenverkehrs ist die Standardeinstellung.

   d. Geben Sie entweder PSK oder Public-Key-Infrastruktur (PKI) für den `auth-method` Parameter für die gewünschte Authentifizierungsmethode ein.
      i. Wenn Sie eine PSK eingeben, fügen Sie die Parameter ein, und drücken Sie dann <enter>, um die Aufforderung zur Eingabe und Überprüfung der zuvor freigegebenen Taste zu drücken.

         Die `local-identity` Parameter und `remote-identity` sind optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

      ii. Wenn Sie eine PKI eingeben, müssen Sie auch die `cert-name` `local-identity` `remote-identity` Parameter , , eingeben. Wenn die Identität des externen Zertifikats unbekannt ist oder mehrere Client-Identitäten erwartet werden, geben Sie die spezielle Identität ein `ANYTHING`.
   e. Ab ONTAP 9.17.1 können Sie optional eine Post-Quantum Pre-Shared Key (PPK)-Identität mit dem `ppk-identity` Parameter. PPKs bieten eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Quantencomputerangriffe. Wenn Sie eine PPK-Identität eingeben, werden Sie aufgefordert, das PPK-Geheimnis einzugeben. PPKs werden nur für die PSK-Authentifizierung unterstützt.

Erfahren Sie mehr über `security ipsec policy create` im "ONTAP-Befehlsreferenz" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Der IP-Verkehr kann erst zwischen Client und Server übertragen werden, wenn sowohl ONTAP als auch der Client die entsprechenden IPsec-Richtlinien eingerichtet haben und die Authentifizierungsdaten (entweder PSK oder Zertifikat) auf beiden Seiten vorhanden sind.

Verwenden Sie IPsec-Identitäten

Bei der Authentifizierungsmethode für vorinstallierte Schlüssel sind lokale und Remote-Identitäten optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

Für die PKI/Zertifikat-Authentifizierungsmethode sind sowohl lokale als auch Remote-Identitäten zwingend erforderlich. Die Identitäten geben an, welche Identität innerhalb des Zertifikats jeder Seite zertifiziert ist und für den Überprüfungsprozess verwendet wird. Wenn die Remote-Identität unbekannt ist oder wenn es viele verschiedene Identitäten sein könnte, verwenden Sie die spezielle Identität `ANYTHING`.

Über diese Aufgabe

Innerhalb von ONTAP werden Identitäten durch Ändern des SPD-Eintrags oder während der Erstellung der SPD-Richtlinie festgelegt. Beim SPD kann es sich um einen Identitätsnamen im IP-Adressenformat oder String-Format handelt.

Schritte

1. Verwenden Sie den folgenden Befehl, um eine vorhandene SPD-Identitätseinstellung zu ändern:

```
security ipsec policy modify
```

Beispielbefehl

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsec Konfiguration für mehrere Clients

Wenn eine kleine Anzahl von Clients IPsec nutzen muss, reicht die Verwendung eines einzelnen SPD-Eintrags für jeden Client aus. Wenn jedoch Hunderte oder gar Tausende von Clients IPsec nutzen müssen, empfiehlt NetApp die Verwendung einer IPsec Konfiguration für mehrere Clients.

Über diese Aufgabe

ONTAP unterstützt die Verbindung mehrerer Clients über mehrere Netzwerke mit einer einzelnen SVM-IP-Adresse, wobei IPsec aktiviert ist. Dies lässt sich mit einer der folgenden Methoden erreichen:

- **Subnetz-Konfiguration**

  Damit alle Clients in einem bestimmten Subnetz (z. B. 192.168.134.0/24) über einen einzigen SPD-Richtlinieneintrag eine Verbindung zu einer einzelnen SVM-IP-Adresse herstellen `remote-ip-subnets` können, müssen Sie das im Subnetz-Formular angeben. Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben.

  > Bei der Verwendung eines einzelnen Richtlinieneintrags in einer Subnetzkonfiguration teilen IPsec-Clients in diesem Subnetz die IPsec-Identität und den vorab gemeinsam genutzten Schlüssel (PSK). Dies gilt jedoch nicht für die Zertifikatauthentifizierung. Bei der Verwendung von Zertifikaten kann jeder Client sein eigenes eindeutiges Zertifikat oder ein freigegebenes Zertifikat zur Authentifizierung verwenden. ONTAP IPsec überprüft die Gültigkeit des Zertifikats auf der Grundlage des CAS, das auf seinem lokalen Vertrauensspeicher installiert ist. ONTAP unterstützt auch die Überprüfung der Zertifikatsperrliste (Certificate Revocation List, CRL).

- **Alle Clients konfigurieren** zulassen

  Damit jeder Client unabhängig von seiner Quell-IP-Adresse eine Verbindung zur IPsec-fähigen SVM-IP-Adresse `0.0.0.0/0` herstellen kann, verwenden Sie bei der Angabe des `remote-ip-subnets` Felds den Platzhalter.

  Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben. Für die Zertifikatauthentifizierung können Sie eingeben `ANYTHING`.

  Wenn der `0.0.0.0/0` Platzhalter verwendet wird, müssen Sie außerdem eine bestimmte lokale oder Remote-Portnummer konfigurieren, die verwendet werden soll. `NFS port 2049`Beispiel: .

  Schritte

  a. Verwenden Sie einen der folgenden Befehle, um IPsec für mehrere Clients zu konfigurieren.

     i. Wenn Sie **Subnetz-Konfiguration** zur Unterstützung mehrerer IPsec-Clients verwenden:

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     Beispielbefehl

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. Wenn Sie **allow all Clients Configuration** verwenden, um mehrere IPsec-Clients zu unterstützen:

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

  Beispielbefehl

  ```
  security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
  IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
  -identity ontap_side_identity -remote-identity client_side_identity
  ```

Zeigt IPsec-Statistiken an

Während der Verhandlung kann ein Sicherheitskanal, der als IKE-Sicherheitszuordnung (SA) bezeichnet wird, zwischen der ONTAP SVM-IP-Adresse und der Client-IP-Adresse eingerichtet werden. IPsec SAS werden auf beiden Endpunkten installiert, um die eigentliche Datenverschlüsselung und -Entschlüsselung zu ermöglichen. Sie können Statistikbefehle verwenden, um den Status von IPsec SAS und IKE SAS zu überprüfen.

Wenn Sie die IPsec-Hardware-Offload-Funktion verwenden, werden mit dem Befehl mehrere neue Zähler angezeigt `security ipsec config show-ipsecsa`.

Beispielbefehle

IKE SA-Beispielbefehl:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA-Beispielbefehl und -Ausgabe:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA-Beispielbefehl und -Ausgabe:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheit IPSec"

Konfigurieren der ONTAP Backend-Cluster-Netzwerkverschlüsselung

Ab ONTAP 9.18.1 können Sie die Transport Layer Security (TLS)-Verschlüsselung für Daten während der Übertragung im Backend-Cluster-Netzwerk konfigurieren. Diese Verschlüsselung schützt Kundendaten, die in ONTAP gespeichert sind, während der Übertragung zwischen ONTAP Knoten im Backend-Clusternetzwerk.

Über diese Aufgabe

- Die Backend-Cluster-Netzwerkverschlüsselung ist standardmäßig deaktiviert.
- Wenn die Verschlüsselung des Backend-Cluster-Netzwerks aktiviert ist, werden alle in ONTAP gespeicherten Kundendaten bei der Übertragung zwischen ONTAP Knoten im Backend-Cluster-Netzwerk verschlüsselt. Bestimmte Netzwerkdaten im Cluster, wie z. B. Daten des Kontrollpfads, sind nicht verschlüsselt.
- Standardmäßig verwendet die Backend-Cluster-Netzwerkverschlüsselung automatisch generierte Zertifikate für jeden Knoten im Cluster. Du kannstCluster-Netzwerkverschlüsselungszertifikate verwalten Auf jedem Knoten soll ein benutzerdefiniertes Zertifikat verwendet werden.

Bevor Sie beginnen

- Sie müssen ONTAP Administrator sein. `admin` Berechtigungsstufe zum Ausführen der folgenden Aufgaben.
- Auf allen Knoten im Cluster muss ONTAP 9.18.1 oder höher ausgeführt werden, um die Backend-Cluster-Netzwerkverschlüsselung zu aktivieren.

Verschlüsselung für die Cluster-Netzwerkkommunikation aktivieren oder deaktivieren

Schritte

1. Den aktuellen Verschlüsselungsstatus des Clusternetzwerks anzeigen:

   ```
   security cluster-network show
   ```

   Dieser Befehl zeigt den aktuellen Status der Cluster-Netzwerkverschlüsselung an:

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Aktivieren oder Deaktivieren der TLS-Backend-Cluster-Netzwerkverschlüsselung:

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Dieser Befehl aktiviert oder deaktiviert die verschlüsselte Kommunikation für Kundendaten, die sich

während der Übertragung im Backend-Cluster-Netzwerk befinden.

Cluster-Netzwerkverschlüsselungszertifikate verwalten

1. Aktuelle Informationen zum Cluster-Netzwerkverschlüsselungszertifikat anzeigen:

```
security cluster-network certificate show
```

Dieser Befehl zeigt die aktuellen Informationen zum Cluster-Netzwerkverschlüsselungszertifikat an:

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

Für jeden Knoten im Cluster werden die Zertifikats- und Zertifizierungsstellennamen (CA-Namen) angezeigt.

2. Ändern des Clusternetzwerk-Verschlüsselungszertifikats für einen Knoten:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Dieser Befehl ändert das Clusternetzwerk-Verschlüsselungszertifikat für einen bestimmten Knoten. Das Zertifikat muss vor Ausführung dieses Befehls installiert und von einer installierten Zertifizierungsstelle signiert werden. Weitere Informationen zur Zertifikatsverwaltung finden Sie unter"Managen Sie ONTAP Zertifikate mit System Manager" Die Wenn `-name` Wenn kein Zertifikat angegeben ist, wird das automatisch generierte Standardzertifikat verwendet.

Konfiguration von Firewallrichtlinien für LIFs im ONTAP Netzwerk

Die Einrichtung einer Firewall verbessert die Clustersicherheit und hilft, unbefugten Zugriff auf das Storage-System zu verhindern. Standardmäßig ist die integrierte Firewall so konfiguriert, dass der Remote-Zugriff auf einen bestimmten Satz von IP-Services für Daten, Management und logische Intercluster-Schnittstellen möglich ist.

Ab ONTAP 9.10.1:

- Firewallrichtlinien sind veraltet und werden durch LIF-Servicerichtlinien ersetzt. Zuvor wurde die integrierte Firewall mithilfe von Firewallrichtlinien gemanagt. Diese Funktion wird nun mithilfe einer LIF-Service-

Richtlinie realisiert.

- Alle Firewall-Richtlinien sind leer und öffnen keine Ports in der zugrunde liegenden Firewall. Stattdessen müssen alle Ports mithilfe einer LIF-Service-Richtlinie geöffnet werden.
- Nach einem Upgrade auf 9.10.1 oder höher ist keine Aktion erforderlich, da die Umstellung von Firewallrichtlinien auf LIF-Servicrichtlinien erfolgt. Das System erstellt automatisch die LIF-Servicrichtlinien entsprechend den in der früheren ONTAP Version verwendeten Firewall-Richtlinien. Wenn Sie Skripts oder andere Tools verwenden, mit denen benutzerdefinierte Firewallrichtlinien erstellt und gemanagt werden, müssen Sie diese Skripte möglicherweise aktualisieren, um stattdessen benutzerdefinierte Service-Richtlinien zu erstellen.

Weitere Informationen finden Sie unter "LIFs und Service-Richtlinien in ONTAP 9.6 und höher".

Über Firewallrichtlinien kann der Zugriff auf Management-Serviceprotokolle wie SSH, HTTP, HTTPS, Telnet, NTP, gesteuert werden. NDMP, NDMPS, RSH, DNS ODER SNMP Firewallrichtlinien können nicht für Datenprotokolle wie NFS oder SMB eingerichtet werden.

Für Firewallservices und -Richtlinien gibt es folgende Managementoptionen:

- Aktivieren oder Deaktivieren des Firewallservice
- Anzeigen der aktuellen Konfiguration des Firewallservice
- Erstellen einer neuen Firewallrichtlinie unter Angabe von Richtliniennamen und Netzwerkservices
- Anwenden einer Firewallrichtlinie auf eine logische Schnittstelle
- Erstellen einer neuen Firewallrichtlinie als exakte Kopie einer vorhandenen Richtlinie

  Verwenden einer Richtlinienkopie zum Erstellen einer Richtlinie mit ähnlichen Merkmalen innerhalb derselben SVM oder zum Kopieren dieser Richtlinie zu einer anderen SVM

- Anzeigen von Informationen zu Firewallrichtlinien
- Ändern der IP-Adressen und Netmasks, die von einer Firewallrichtlinie verwendet werden
- Löschen einer Firewallrichtlinie, die von keinem LIF verwendet wird

Firewall-Richtlinien und LIFs

Mithilfe von LIF-Firewallrichtlinien wird der Zugriff auf das Cluster über jede logische Schnittstelle beschränkt. Sie müssen verstehen, wie sich die Standard-Firewall-Richtlinie auf den Systemzugriff über jeden logischen Typ auswirkt, und wie Sie eine Firewall-Richtlinie anpassen können, um die Sicherheit über LIF zu erhöhen oder zu verringern.

Beim Konfigurieren einer LIF mit dem `network interface create` `network interface modify` Befehl oder `-firewall-policy` bestimmt der für den Parameter angegebene Wert die Service-Protokolle und IP-Adressen, die Zugriff auf die LIF erlauben. Erfahren Sie mehr über `network interface` in der "ONTAP-Befehlsreferenz".

In vielen Fällen können Sie den standardmäßigen Firewallrichtlinienwert akzeptieren. In anderen Fällen müssen Sie den Zugriff auf bestimmte IP-Adressen und bestimmte Management-Service-Protokolle einschränken. Die verfügbaren Management-Service-Protokolle umfassen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS UND SNMP

Die Firewallrichtlinie für alle Cluster-LIFs ist standardmäßig aktiviert `""` und kann nicht geändert werden.

In der folgenden Tabelle werden die Standard-Firewall-Richtlinien beschrieben, die jeder logischen

Schnittstelle zugewiesen werden. Dies ist abhängig von ihrer Rolle (ONTAP 9.5 und früher) oder Service-Richtlinie (ONTAP 9.6 und höher) bei der Erstellung des logischen Schnittstelle.

Firewallrichtlinie	Standard-Service-Protokolle	Standardzugriff	LIFs werden angewendet auf
Management	dns, http, https, ndmp, NDMPs, ntp, snmp, SSH	Beliebige Adresse (0.0.0.0/0)	Cluster-Management, SVM-Management und Node-Management-LIFs
management nfs	dns, http, https, ndmp, NDMPs, ntp, portmap, snmp, SSH	Beliebige Adresse (0.0.0.0/0)	Daten-LIFs unterstützen zudem den SVM-Managementzugriff
Intercluster	https, ndmp, NDMPs	Beliebige Adresse (0.0.0.0/0)	Alle LIFs zwischen Clustern
Daten	dns, ndmp, NDMPs, Port-Map	Beliebige Adresse (0.0.0.0/0)	Alle Daten-LIFs

Konfiguration des Portmap-Dienstes

Der Portmap-Dienst ordnet RPC-Dienste den Ports zu, auf denen sie zuhören.

Der Portmap-Service war in ONTAP 9.3 und früher immer zugänglich, war von ONTAP 9.4 bis ONTAP 9.6 konfigurierbar und wird ab ONTAP 9.7 automatisch gemanagt.

- In ONTAP 9.3 und früher war der portmap-Dienst (rpcbind) in Netzwerkkonfigurationen, die sich auf die integrierte ONTAP-Firewall statt auf eine Firewall eines Drittanbieters stützten, immer über Port 111 zugänglich.
- Von ONTAP 9.4 bis ONTAP 9.6 können Sie Firewallrichtlinien ändern, um zu steuern, ob der Portmap-Service auf bestimmten LIFs zugegriffen werden kann.
- Ab ONTAP 9.7 wird der Port Map Firewall-Service eingestellt. Stattdessen wird der Port-Map automatisch für alle LIFs geöffnet, die den NFS-Service unterstützen.

Portmap-Dienst ist in der Firewall in ONTAP 9.4 bis ONTAP 9.6 konfigurierbar.

Der restliche Teil dieses Themas erläutert, wie der Port Map Firewall-Service für ONTAP 9.4 bis ONTAP 9.6 Versionen konfiguriert wird.

Je nach Konfiguration können Sie den Zugriff auf den Service für bestimmte Arten von LIFs, in der Regel Management-Schnittstellen und Intercluster LIFs, unzulassen. In manchen Fällen kann der Zugriff auf Daten-LIFs sogar unzulässig sein.

Welches Verhalten können Sie erwarten

Das Verhalten von ONTAP 9.4 bis ONTAP 9.6 ermöglicht einen nahtlosen Übergang bei einem Upgrade. Wenn bereits über bestimmte LIFs auf den Portmap-Service zugegriffen wird, ist dieser über diese LIFs hinweg weiterhin zugänglich. Wie in ONTAP 9.3 und früheren Versionen können Sie die Services angeben, auf die in der Firewall-Richtlinie für den LIF-Typ zugegriffen werden kann.

Alle Nodes im Cluster müssen ONTAP 9.4 bis ONTAP 9.6 ausführen, damit das Verhalten wirksam wird. Nur der eingehende Datenverkehr ist betroffen.

Die neuen Regeln lauten wie folgt:

- Bei einem Upgrade auf Version 9.4 bis 9.6 fügt ONTAP den Portmap-Service allen vorhandenen Firewall-Richtlinien hinzu – Standard oder benutzerdefiniert.
- Wenn Sie ein neues Cluster oder einen neuen IPspace erstellen, fügt ONTAP den Portmap-Service nur der Standarddatenrichtlinie hinzu, nicht jedoch den standardmäßigen Management- oder Cluster-Richtlinien.
- Sie können den Portmap-Dienst je nach Bedarf den Standard- oder benutzerdefinierten Richtlinien hinzufügen und den Dienst nach Bedarf entfernen.

So fügen Sie den Portmap-Dienst hinzu oder entfernen ihn

Um den Portmap-Service einer SVM oder Cluster-Firewallrichtlinie hinzuzufügen (Zugriff innerhalb der Firewall), geben Sie ein:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Um den Portmap-Service von einer SVM oder einer Cluster-Firewallrichtlinie zu entfernen (Zugriff innerhalb der Firewall), geben Sie ein:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Sie können mit dem Befehl „Ändern“ der Netzwerkschnittstelle die Firewallrichtlinie auf eine vorhandene LIF anwenden. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Erstellen Sie eine Firewallrichtlinie und weisen Sie sie einer logischen Schnittstelle zu

Jedem LIF werden Standard-Firewallrichtlinien zugewiesen, wenn Sie das LIF erstellen. In vielen Fällen funktionieren die Standard-Firewall-Einstellungen gut und Sie müssen sie nicht ändern. Wenn Sie die Netzwerkservices oder IP-Adressen ändern möchten, die auf eine LIF zugreifen können, können Sie eine benutzerdefinierte Firewallrichtlinie erstellen und dieser LIF zuweisen.

Über diese Aufgabe

- Sie können keine Firewallrichtlinie mit dem `policy` Namen `data`, , `intercluster` `cluster`oder erstellen `mgmt`.

  Diese Werte sind den systemdefinierten Firewallrichtlinien vorbehalten.

- Sie können keine Firewallrichtlinie für Cluster-LIFs festlegen oder ändern.

  Die Firewallrichtlinie für Cluster-LIFs ist für alle Service-Typen auf 0.0.0.0/0 festgelegt.

- Wenn Sie einen Dienst aus einer Richtlinie entfernen müssen, müssen Sie die vorhandene Firewallrichtlinie löschen und eine neue Richtlinie erstellen.
- Wenn IPv6 auf dem Cluster aktiviert ist, können Sie Firewallrichtlinien mit IPv6-Adressen erstellen.

  Nachdem IPv6 aktiviert ist, `data` `intercluster` `mgmt`enthalten , und Firewallrichtlinien ::/0, den IPv6-Platzhalter, in ihrer Liste der akzeptierten Adressen.

- Wenn Sie zur Konfiguration der Datensicherungsfunktionen in allen Clustern System Manager verwenden, müssen Sie sicherstellen, dass die Cluster-übergreifenden LIF-IP-Adressen in der Liste „zulässig“ aufgeführt sind und dass HTTPS-Service sowohl auf den Intercluster LIFs als auch auf den Firewalls Ihres

Unternehmens zulässig ist.

Standardmäßig `intercluster` erlaubt die Firewallrichtlinie den Zugriff von allen IP-Adressen (0.0.0.0/0 oder ::/0 für IPv6) und aktiviert HTTPS-, NDMP- und NDMPS-Dienste. Wenn Sie diese Standardrichtlinie ändern oder eine eigene Firewallrichtlinie für Intercluster-LIFs erstellen, müssen Sie der Liste „zulässig“ jede Intercluster-LIF-IP-Adresse hinzufügen und den HTTPS-Service aktivieren.

- Ab ONTAP 9.6 werden die HTTPS- und SSH-Firewall-Services nicht unterstützt.

  In ONTAP 9.6 `management-https` `management-ssh` sind die und LIF-Services für HTTPS- und SSH-Managementzugriff verfügbar.

Schritte

1. Erstellen Sie eine Firewallrichtlinie, die für LIFs auf einer bestimmten SVM zur Verfügung steht:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Mit diesem Befehl können Sie mehrere Male mehr als einen Netzwerkdienst und eine Liste zulässiger IP-Adressen für jeden Dienst in der Firewall-Richtlinie hinzufügen.

2. Überprüfen Sie mit dem `system services firewall policy show` Befehl, ob die Richtlinie ordnungsgemäß hinzugefügt wurde.
3. Wenden Sie die Firewallrichtlinie auf ein LIF an:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Überprüfen Sie mit dem `network interface show -fields firewall-policy` Befehl, ob die Richtlinie korrekt zum LIF hinzugefügt wurde.

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Beispiel zum Erstellen einer Firewallrichtlinie und Zuweisen zu einer logischen Schnittstelle

Mit dem folgenden Befehl wird eine Firewall-Richtlinie namens Data_http erstellt, die den HTTP- und HTTPS-Protokollzugriff über IP-Adressen im Subnetz 10.10 ermöglicht, diese Richtlinie auf die LIF namens data1 in SVM vs1 anwendet und dann alle Firewallrichtlinien des Clusters zeigt:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

ONTAP-Befehle zum Managen von Firewallservices und -Richtlinien

Sie können den `system services firewall` Firewall-Service mit den Befehlen managen, die `system services firewall policy` Befehle zum Verwalten von Firewallrichtlinien und den `network interface modify` Befehl zum Verwalten von Firewalleinstellungen für LIFs.

Ab ONTAP 9.10.1:

- Firewallrichtlinien sind veraltet und werden durch LIF-Servicerichtlinien ersetzt. Zuvor wurde die integrierte Firewall mithilfe von Firewallrichtlinien gemanagt. Diese Funktion wird nun mithilfe einer LIF-Service-Richtlinie realisiert.
- Alle Firewall-Richtlinien sind leer und öffnen keine Ports in der zugrunde liegenden Firewall. Stattdessen müssen alle Ports mithilfe einer LIF-Service-Richtlinie geöffnet werden.
- Nach einem Upgrade auf 9.10.1 oder höher ist keine Aktion erforderlich, da die Umstellung von Firewallrichtlinien auf LIF-Servicrichtlinien erfolgt. Das System erstellt automatisch die LIF-Servicrichtlinien entsprechend den in der früheren ONTAP Version verwendeten Firewall-Richtlinien. Wenn Sie Skripts oder andere Tools verwenden, mit denen benutzerdefinierte Firewallrichtlinien erstellt und gemanagt werden, müssen Sie diese Skripte möglicherweise aktualisieren, um stattdessen benutzerdefinierte Service-Richtlinien zu erstellen.

Weitere Informationen finden Sie unter "LIFs und Service-Richtlinien in ONTAP 9.6 und höher".

Ihr Ziel ist	Befehl
Aktivieren oder Deaktivieren des Firewallservice	`system services firewall modify`
Zeigt die aktuelle Konfiguration für den Firewallservice an	`system services firewall show`
Erstellen Sie eine Firewallrichtlinie oder fügen Sie einen Service zu einer vorhandenen Firewallrichtlinie hinzu	`system services firewall policy create`
Wenden Sie eine Firewallrichtlinie auf ein LIF an	`network interface modify -lif lifname -firewall-policy`
Ändern Sie die IP-Adressen und Netmasks, die einer Firewallrichtlinie zugeordnet sind	`system services firewall policy modify`
Zeigt Informationen zu Firewallrichtlinien an	`system services firewall policy show`
Erstellen Sie eine neue Firewallrichtlinie als exakte Kopie einer vorhandenen Richtlinie	`system services firewall policy clone`
Löschen Sie eine Firewallrichtlinie, die von keinem LIF verwendet wird	`system services firewall policy delete`

Verwandte Informationen

- "Firewall für Systemdienste"
- "Änderung der Netzwerkschnittstelle"

QoS-Kennzeichnung (nur Cluster-Administratoren)

Erfahren Sie mehr über ONTAP-Netzwerk Quality of Service (QoS)

Mithilfe der Markierung für die Netzwerkqualität (Quality of Service, QoS) können Sie verschiedene Datenverkehrstypen basierend auf den Netzwerkbedingungen priorisieren, um die Netzwerkressourcen effektiv zu nutzen. Sie können den differenzierten Service Code Point (DSCP)-Wert der ausgehenden IP-Pakete für die unterstützten Traffic-Typen pro IPspace festlegen.

DSCP-Kennzeichnung für UC-Konformität

Sie können die Markierung des differenzierten Dienstcodepunktes (DSCP) für ausgehenden (ausgehenden) IP-Paketverkehr für ein bestimmtes Protokoll mit einem Standard- oder vom Benutzer bereitgestellten DSCP-Code aktivieren. Die DSCP-Kennzeichnung ist ein Mechanismus zur Klassifizierung und Verwaltung des Netzwerkdatenverkehrs und ist eine Komponente der Unified Capability (UC)-Compliance.

Die DSCP-Markierung (auch bekannt als *QoS-Markierung* oder *Quality of Service-Markierung*) wird durch die Bereitstellung eines IPspace-, Protokoll- und DSCP-Wertes aktiviert. Die Protokolle, auf die DSCP-Kennzeichnung angewendet werden kann, sind NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet und SNMP

Wenn Sie keinen DSCP-Wert angeben, wenn Sie die DSCP-Markierung für ein bestimmtes Protokoll aktivieren, wird ein Standardwert verwendet:

- Der Standardwert für Datenprotokolle/Datenverkehr ist 0x0A (10).
- Der Standardwert für Steuerungsprotokolle/-Verkehr ist 0x30 (48).

Kennungswerte der ONTAP-Netzwerk-QoS ändern

Sie können die Qualitätskennungswerte (QoS) für verschiedene Protokolle für jeden IPspace ändern.

Bevor Sie beginnen

Alle Nodes im Cluster müssen dieselbe Version von ONTAP ausführen.

Schritt

Ändern Sie QoS-Markierungswerte mit dem `network qos-marking modify` Befehl.

- Der `-ipspace` Parameter gibt den IPspace an, für den der QoS-Markierungseintrag geändert werden soll.
- Der `-protocol` Parameter gibt das Protokoll an, für das der QoS-Markierungseintrag geändert werden soll.
- Der `-dscp` Parameter gibt den DSCP-Wert (Differentiated Services Code Point) an. Die möglichen Werte liegen zwischen 0 und 63.
- Mit dem `-is-enabled` Parameter wird die QoS-Markierung für das angegebene Protokoll im vom

`-ipspace` Parameter angegebenen IPspace aktiviert bzw. deaktiviert.

Mit dem folgenden Befehl wird die QoS-Markierung für das NFS-Protokoll im standardmäßigen IPspace aktiviert:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

Mit dem folgenden Befehl wird der DSCP-Wert für das NFS-Protokoll im standardmäßigen IPspace auf 20 gesetzt:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Erfahren Sie mehr über `network qos-marking modify` und mögliche Werte des Protokolls im "ONTAP-Befehlsreferenz".

Anzeigen von Kennwerten der ONTAP-Netzwerk-QoS

Sie können die QoS-Markierungswerte für verschiedene Protokolle für jeden IPspace anzeigen.

Schritt

Zeigt QoS-Markierungswerte mit dem `network qos-marking show` Befehl an.

Mit dem folgenden Befehl wird die QoS-Markierung für alle Protokolle im Standard-IPspace angezeigt:

```
network qos-marking show -ipspace Default
IPspace              Protocol           DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                 10  false
                     FTP                  48  false
                     HTTP-admin           48  false
                     HTTP-filesrv         10  false
                     NDMP                 10  false
                     NFS                  10  true
                     SNMP                 48  false
                     SSH                  48  false
                     SnapMirror           10  false
                     Telnet               48  false
                     iSCSI                10  false
11 entries were displayed.
```

Erfahren Sie mehr über `network qos-marking show` in der "ONTAP-Befehlsreferenz".

Verwalten von SNMP (nur Cluster-Administratoren)

Erfahren Sie mehr über SNMP im ONTAP-Netzwerk

SNMP lässt sich konfigurieren, um SVMs in Ihrem Cluster zu überwachen und Probleme zu vermeiden, bevor sie auftreten, und um auf Probleme zu reagieren, falls diese auftreten. Beim Management von SNMP müssen SNMP-Benutzer konfiguriert und SNMP traphost-Ziele (Management-Workstations) für alle SNMP-Ereignisse konfiguriert werden. SNMP ist standardmäßig auf Daten-LIFs deaktiviert.

Sie können schreibgeschützte SNMP-Benutzer in der Daten-SVM erstellen und managen. Daten-LIFs müssen konfiguriert werden, um SNMP-Anforderungen auf der SVM zu empfangen.

SNMP-Netzwerkmanagement-Workstations oder -Manager können den SVM-SNMP-Agent zur Information abfragen. Der SNMP-Agent sammelt Informationen und leitet sie an die SNMP-Manager weiter. Der SNMP-Agent erzeugt auch Trap-Benachrichtigungen, wenn bestimmte Ereignisse auftreten. Der SNMP-Agent auf der SVM hat schreibgeschützte Berechtigungen. Er kann nicht für bestimmte Vorgänge oder zur Durchführung von Korrekturmaßnahmen als Antwort auf einen Trap verwendet werden. ONTAP stellt einen SNMP-Agent bereit, der mit SNMP-Versionen v1, v2c und v3 kompatibel ist. SNMPv3 bietet erweiterte Sicherheit durch Nutzung von Passphrases und Verschlüsselung.

Weitere Informationen zur SNMP-Unterstützung in ONTAP-Systemen finden Sie unter "TR-4220: SNMP-Unterstützung in Data ONTAP".

MIB-Übersicht

Eine MIB (Management Information Base) ist eine Textdatei, die SNMP-Objekte und Traps beschreibt.

MIBs beschreiben die Struktur der Managementdaten des Storage-Systems und verwenden einen hierarchischen Namespace mit Objekt-IDs (OIDs). Jede OID identifiziert eine Variable, die über SNMP gelesen werden kann.

Da MIBs keine Konfigurationsdateien sind und ONTAP diese Dateien nicht liest, wird die SNMP-Funktionalität von MIBs nicht beeinflusst. ONTAP bietet die folgende MIB-Datei:

- Ein NetApp Custom MIB (`netapp.mib`)

ONTAP unterstützt IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) und ICMP (RFC 2466) MIBs, die sowohl IPv4- als auch IPv6-Daten enthalten, werden unterstützt.

ONTAP bietet auch einen kurzen Querverweis zwischen Objektkennungen (OIDs) und Objektkurznamen in der `traps.dat` Datei.

> Die neuesten Versionen der Dateien ONTAP MIBs und `traps.dat `stehen auf der NetApp Support-Website zur Verfügung. Allerdings entsprechen die Versionen dieser Dateien auf der Support-Website nicht unbedingt den SNMP-Fähigkeiten Ihrer ONTAP-Version. Diese Dateien werden bereitgestellt, um Ihnen zu helfen, SNMP-Funktionen in der neuesten ONTAP-Version zu bewerten.

SNMP-Traps

SNMP-Traps erfassen System Monitoring Informationen, die als asynchrone Benachrichtigung vom SNMP-

Agent an den SNMP-Manager gesendet werden.

Es gibt drei Arten von SNMP-Traps: Standard, integrierte und benutzerdefinierte definiert. Benutzerdefinierte Traps werden in ONTAP nicht unterstützt.

Ein Trap kann verwendet werden, um regelmäßig auf betriebliche Schwellenwerte oder Fehler zu überprüfen, die in der MIB definiert sind. Wenn ein Schwellenwert erreicht wird oder ein Fehler erkannt wird, sendet der SNMP-Agent eine Meldung (Trap) an die Traphosts, die sie über das Ereignis alarmieren.

ONTAP unterstützt SNMPv1- und SNMPv3-Traps. ONTAP unterstützt keine SNMPv2c-Traps und -Informationen.

Standard-SNMP-Traps

Diese Traps sind in RFC 1215 definiert. Es gibt fünf Standard-SNMP-Traps, die von ONTAP unterstützt werden: Coldstart, warmstart, LinkDown, linkup und AuthentifizierungFailure.

Der Trap für die Authentifizierungsausfältung ist standardmäßig deaktiviert. Sie müssen den Befehl verwenden `system snmp authtrap` , um den Trap zu aktivieren. Erfahren Sie mehr über `system snmp authtrap` in der "ONTAP-Befehlsreferenz".

Integrierte SNMP-Traps

Integrierte Traps sind in ONTAP vordefiniert und werden bei Auftreten eines Ereignisses automatisch an die Netzwerk-Management-Stationen in der traphost-Liste gesendet. Diese Traps wie diskFailedShutdown, cpuTooBusy und VolumeNearlyFull sind in der benutzerdefinierten MIB definiert.

Jeder integrierte Trap wird durch einen eindeutigen Trap-Code identifiziert.

Erstellen Sie SNMP-Communitys für das ONTAP-Netzwerk

Sie können bei der Verwendung von SNMPv1 und SNMPv2c eine SNMP-Community erstellen, die als Authentifizierungsmechanismus zwischen der Management Station und der Storage Virtual Machine (SVM) fungiert.

Durch die Erstellung von SNMP Communities in einer Daten-SVM können Sie Befehle wie `snmpwalk` und `snmpget` für die Daten-LIFs ausführen.

Über diese Aufgabe

- Bei Neuinstallationen von ONTAP sind SNMPv1 und SNMPv2c standardmäßig deaktiviert.

  SNMPv1 und SNMPv2c sind aktiviert, nachdem Sie eine SNMP-Community erstellt haben.

- ONTAP unterstützt schreibgeschützte Communitys.
- Standardmäßig ist der SNMP-Service für die Firewall-Richtlinie „Daten“, die Daten-LIFs zugewiesen ist `deny`, auf festgelegt.

  Sie müssen eine neue Firewallrichtlinie mit SNMP-Dienst auf `allow` erstellen, wenn Sie einen SNMP-Benutzer für eine Daten-SVM erstellen.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- Sie können SNMP Communities für SNMPv1- und SNMPv2c-Benutzer sowohl für die Admin-SVM als auch für die Daten-SVM erstellen.
- Da eine SVM nicht Teil des SNMP-Standards ist, müssen Abfragen zu Daten-LIFs die NetApp-Root-OID (1.3.6.1.4.1.789) enthalten, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789` z. B. .

Schritte

1. Erstellen Sie eine SNMP-Community mit dem `system snmp community add` Befehl. Mit dem folgenden Befehl wird gezeigt, wie eine SNMP-Community in dem Admin-SVM-Cluster-1 erstellt wird:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

   Mit dem folgenden Befehl wird gezeigt, wie eine SNMP-Community in der Data SVM vs1 erstellt wird:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Überprüfen Sie, dass die Communities erstellt wurden, indem Sie den System snmp Community show Befehl verwenden.

   Der folgende Befehl zeigt die beiden Gemeinschaften, die für SNMPv1 und SNMPv2c erstellt wurden:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Überprüfen Sie mit dem `system services firewall policy show` Befehl, ob SNMP als Dienst in der Firewallrichtlinie „Daten“ zulässig ist.

   Der folgende Befehl zeigt an, dass der snmp-Dienst in der Standard-Firewall-Richtlinie „Daten“ nicht erlaubt ist (der snmp-Dienst ist nur in der „Management“ Firewall-Richtlinie zulässig):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Erstellen Sie eine neue Firewallrichtlinie, die den Zugriff über `snmp` den Service mit dem `system services firewall policy create` Befehl ermöglicht.

   Mit den folgenden Befehlen wird eine neue Daten-Firewall-Richtlinie namens „data1“ erstellt, die den ermöglicht `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Wenden Sie die Firewallrichtlinie auf eine logische Datenschnittstelle an, indem Sie den Befehl mit dem Parameter „-Firewall-Policy“ verwenden `network interface modify`.

Mit dem folgenden Befehl wird die neue „data1“ Firewallrichtlinie zu LIF „Daten1“ zugewiesen:

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie SNMPv3-Benutzer in einem ONTAP-Cluster

SNMPv3 ist ein sicheres Protokoll im Vergleich zu SNMPv1 und SNMPv2c. Um SNMPv3 zu verwenden, müssen Sie einen SNMPv3-Benutzer konfigurieren, um die SNMP-Dienstprogramme vom SNMP-Manager aus auszuführen.

Schritt

Verwenden Sie die `security login create` Befehl zum Erstellen eines SNMPv3-Benutzers.

Sie werden aufgefordert, folgende Informationen einzugeben:

- Engine ID: Standard und Empfohlener Wert ist lokale Engine ID
- Authentifizierungsprotokoll
- Authentifizierungspasswort
- Datenschutzprotokoll
- Passwort für das Datenschutzprotokoll

Ergebnis

Der SNMPv3-Benutzer kann sich über den SNMP-Manager über den Benutzernamen und das Kennwort anmelden und die Befehle des SNMP-Dienstprogramms ausführen.

SNMPv3-Sicherheitsparameter

SNMPv3 umfasst eine Authentifizierungsfunktion, die bei Auswahl von Benutzern erfordert, dass sie beim Aufrufen eines Befehls ihren Namen, ein Authentifizierungsprotokoll, einen Authentifizierungsschlüssel und den gewünschten Sicherheitsgrad eingeben.

In der folgenden Tabelle sind die SNMPv3-Sicherheitsparameter aufgelistet:

Parameter	Befehlszeilenoption	Beschreibung
EngineID	-E EngineID	Engine-ID des SNMP-Agenten. Der Standardwert ist Local EngineID (empfohlen).
Sicherheitsname	-U Name	Der Benutzername darf maximal 32 Zeichen enthalten.
AuthProtocol	-A {None} SHA-256	Authentifizierungstyp kann keine, MD5, SHA oder SHA-256 sein.

AuthKey	-EINE PASSPHRASE	Passphrase mit mindestens acht Zeichen.
Sicherheitsstufe	• L {authNoPriv}	Sicherheitsstufe kann Authentifizierung, Datenschutz, Authentifizierung, Datenschutz oder keine Authentifizierung sein. Kein Datenschutz.
PrivProtocol	-X { none} aes128	Das Datenschutzprotokoll kann keine, des oder aes128 sein
Privatpasswort	-X-Passwort	Passwort mit mindestens acht Zeichen.

Beispiele für unterschiedliche Sicherheitsstufen

Dieses Beispiel zeigt, wie ein SNMPv3-Benutzer, der mit unterschiedlichen Sicherheitsstufen erstellt `snmpwalk` wurde, die SNMP-Client-seitigen Befehle wie, verwenden kann, um die Clusterobjekte abzufragen.

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

Sie müssen `snmpwalk` 5.3.1 oder höher verwenden, wenn das Authentifizierungsprotokoll SHA ist.

Sicherheitsstufe: AuthPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3-Benutzers mit der authPriv-Sicherheitsstufe.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS-Modus

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3-Benutzer, der den snmpwalk-Befehl ausführt:

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Sicherheitsstufe: AuthNoPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3-Benutzers mit der autauthNoPriv-Sicherheitsstufe.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS-Modus

FIPS erlaubt Ihnen nicht, **none** für das Datenschutzprotokoll zu wählen. Daher ist es nicht möglich, einen authNoPriv.-SNMPv3-Benutzer im FIPS-Modus zu konfigurieren.

Snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3-Benutzer, der den snmpwalk-Befehl ausführt:

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder

einigen Objekten aus der Tabelle abrufen.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Sicherheitsstufe: NoAuthNoPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3-Benutzers mit der Sicherheitsstufe noAuthNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS-Modus

FIPS erlaubt Ihnen nicht, **none** für das Datenschutzprotokoll zu wählen.

Snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3-Benutzer, der den snmpwalk-Befehl ausführt:

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie Traphosts für SNMP im ONTAP-Netzwerk

Sie können traphost (SNMP Manager) so konfigurieren, dass Benachrichtigungen (SNMP Trap PDUs) empfangen werden, wenn SNMP Traps im Cluster generiert werden. Sie

können entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des SNMP traphost angeben.

Bevor Sie beginnen

- SNMP- und SNMP-Traps müssen auf dem Cluster aktiviert sein.

  SNMP- und SNMP-Traps sind standardmäßig aktiviert.

- Für das Auflösen der traphost-Namen muss auf dem Cluster DNS konfiguriert sein.
- IPv6 muss auf dem Cluster aktiviert sein, um SNMP-Traphosts mithilfe von IPv6-Adressen zu konfigurieren.
- Beim Erstellen von Traphosts müssen Sie die Authentifizierung eines vordefinierten benutzerbasierten Sicherheitsmodells (USM) und die Datenschutzanmeldeinformationen angegeben haben.

Schritt

Hinzufügen eines SNMP traphost:

```
system snmp traphost add
```

Traps können nur gesendet werden, wenn mindestens eine SNMP Management Station als traphost angegeben ist.

Mit dem folgenden Befehl wird ein neuer SNMPv3 traphost mit dem Namen yyy.example.com mit einem bekannten USM-Benutzer hinzugefügt:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

Mit dem folgenden Befehl wird ein traphost unter Verwendung der IPv6-Adresse des Hosts hinzugefügt:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Überprüfen Sie SNMP-Polling in einem ONTAP-Cluster

Nachdem Sie SNMP konfiguriert haben, sollten Sie überprüfen, dass Sie den Cluster anfragen können.

Über diese Aufgabe

Um einen Cluster abzufragen, müssen Sie einen Drittanbieter-Befehl wie verwenden `snmpwalk` .

Schritte

1. Senden Sie einen SNMP-Befehl, um den Cluster von einem anderen Cluster abzufragen.

   Verwenden Sie für Systeme, die SNMPv1 ausführen, `snmpwalk -v version -c community_stringip_address_or_host_name system` den CLI-Befehl, um den Inhalt der MIB

(Management Information Base) zu ermitteln.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Bei Systemen, auf denen SNMPv2c ausgeführt `snmpwalk -v version -c community_stringip_address_or_host_name system` wird, verwenden Sie den CLI-Befehl, um den Inhalt der MIB (Management Information Base) zu ermitteln.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Verwenden Sie für Systeme, die SNMPv3 ausführen, `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` den CLI-Befehl, um den Inhalt der MIB (Management Information Base) zu ermitteln.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

ONTAP-Befehle zum Verwalten von SNMP, Traps und Traphosts

Sie können die `system snmp` Befehle zum Verwalten von SNMP, Traps und Traphosts verwenden. Sie können die `security` Befehle verwenden, um SNMP-Benutzer pro SVM zu verwalten. Sie können die `event` Befehle verwenden, um Ereignisse im Zusammenhang mit SNMP-Traps zu verwalten.

Befehle zum Konfigurieren von SNMP

Ihr Ziel ist	Befehl
Aktivieren Sie SNMP auf dem Cluster	`options -option-name snmp.enable -option-value on` Der SNMP-Service muss unter der Management (Mgmt) Firewall-Richtlinie zugelassen werden. Sie können überprüfen, ob SNMP zulässig ist, indem Sie den Befehl System Services Firewall Policy show verwenden.
Deaktivieren Sie SNMP auf dem Cluster	`options -option-name snmp.enable -option-value off`

Befehle zum Verwalten von SNMP v1-, v2c- und v3-Benutzern

Ihr Ziel ist	Befehl
Konfigurieren Sie SNMP-Benutzer	`security login create`
Anzeigen von SNMP-Benutzern	`security snmpusers`Und `security login show -application snmp`

Löschen Sie SNMP-Benutzer	`security login delete`
Ändern Sie den Namen der Zugriffskontrollrolle einer Anmeldemethode für SNMP-Benutzer	`security login modify`

Befehle zur Bereitstellung von Kontakt- und Standortinformationen

Ihr Ziel ist	Befehl
Zeigt die Kontaktinformationen des Clusters an oder ändern sie	`system snmp contact`
Zeigt die Standortdetails des Clusters an oder ändern sie	`system snmp location`

Befehle zum Verwalten von SNMP-Communitys

Ihr Ziel ist	Befehl
Fügen Sie eine schreibgeschützte Community (ro) für eine SVM oder alle SVMs im Cluster hinzu	`system snmp community add`
Löschen Sie eine Community oder alle Communities	`system snmp community delete`
Zeigen Sie die Liste aller Communitys an	`system snmp community show`

Da SVMs nicht Teil des SNMP-Standards sind, müssen Abfragen zu Daten-LIFs beispielsweise die NetApp-Root-OID (1.3.6.1.4.1.789) enthalten `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Befehl zum Anzeigen von SNMP-Optionswerten

Ihr Ziel ist	Befehl
Zeigen Sie die aktuellen Werte aller SNMP-Optionen an, einschließlich Clusterkontakt, Kontaktstelle, ob das Cluster zum Senden von Traps konfiguriert ist, die Liste der Traphosts, Liste der Communities und Zugriffsteuerungsarten	`system snmp show`

Befehle zum Verwalten von SNMP-Traps und traphosts

Ihr Ziel ist	Befehl
Aktivieren Sie SNMP-Traps die vom Cluster gesendet werden	`system snmp init -init 1`

Deaktivieren Sie SNMP-Traps die vom Cluster gesendet werden	`system snmp init -init 0`
Fügen Sie einen traphost hinzu, der SNMP-Benachrichtigungen für bestimmte Ereignisse im Cluster erhält	`system snmp traphost add`
Löschen Sie einen traphost	`system snmp traphost delete`
Zeigt die Liste der Traphosts an	`system snmp traphost show`

Befehle zum Verwalten von Ereignissen im Zusammenhang mit SNMP-Traps

Ihr Ziel ist	Befehl
Zeigen Sie die Ereignisse an, für die SNMP-Traps (integriert) generiert werden	`event route show` Verwenden Sie den `-snmp-support true` Parameter, um nur SNMP-bezogene Ereignisse anzuzeigen. Mit dem `instance -messagename <message>` Parameter werden eine detaillierte Beschreibung des Ereignisses und etwaige Korrekturmaßnahmen angezeigt. Das Routing einzelner SNMP-Trap-Ereignisse zu bestimmten traphost-Zielen wird nicht unterstützt. Alle SNMP-Trap-Ereignisse werden an alle traphost-Ziele gesendet.
Zeigt eine Liste der SNMP-Trap-Verlaufsdatensätze an, bei denen es sich um Ereignisbenachrichtigungen handelt, die an SNMP-Traps gesendet wurden	`event snmphistory show`
Löschen Sie einen SNMP-Trap-Verlaufsdatensatz	`event snmphistory delete`

Verwandte Informationen

- "System-snmp"
- "Sicherheits-SNMP-Benutzer"
- "Sicherheit"
- "Ereignis"
- "Sicherheitsanmeldung"

Routing in einer SVM managen

Erfahren Sie mehr über SVM-Routing im ONTAP Netzwerk

Die Routing-Tabelle für eine SVM bestimmt den Netzwerkpfad, den die SVM für die Kommunikation mit einem Ziel verwendet. Es ist wichtig zu verstehen, wie Routing-Tabellen funktionieren, so dass Sie Netzwerkprobleme verhindern können, bevor sie auftreten.

Die Routingregeln lauten wie folgt:

- ONTAP leitet Datenverkehr über die am häufigsten verfügbare Route.
- ONTAP leitet den Datenverkehr über eine Standard-Gateway-Route (mit 0 Bit Netzmaske) als letztes Resort weiter, wenn keine speziellen Routen verfügbar sind.

Bei Routen mit demselben Ziel, derselben Netmask und Metrik kann nicht garantiert werden, dass das System nach einem Neustart oder nach einem Upgrade die gleiche Route verwendet. Dies ist insbesondere ein Problem, wenn Sie mehrere Standardrouten konfiguriert haben.

Es empfiehlt sich, für eine SVM nur eine Standardroute zu konfigurieren. Um Störungen zu vermeiden, sollten Sie sicherstellen, dass die Standardroute alle Netzwerkadressen erreichen kann, die über eine spezifischere Route nicht erreichbar sind. Weitere Informationen finden Sie unter"NetApp Knowledge Base: SU134 – Der Netzwerkzugriff kann durch eine falsche Routing-Konfiguration in Clustered ONTAP unterbrochen werden"

Erstellen Sie statische Routen für das ONTAP-Netzwerk

Sie können innerhalb einer Storage Virtual Machine (SVM) statische Routen erstellen, um zu steuern, wie LIFs das Netzwerk für Outbound-Datenverkehr verwenden.

Wenn Sie einen Routeneintrag erstellen, der einer SVM zugeordnet ist, wird diese Route von allen LIFs verwendet, die sich im Besitz der angegebenen SVM befinden und sich im gleichen Subnetz wie das Gateway befinden.

Schritt

`network route create`Erstellen Sie mit dem Befehl eine Route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

Erfahren Sie mehr über `network route create` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie Multipath-Routing für das ONTAP-Netzwerk

Wenn mehrere Routen dieselbe Metrik für ein Ziel haben, wird nur eine der Routen für ausgehenden Datenverkehr ausgewählt. Dies führt dazu, dass andere Routen für das Senden von ausgehendem Datenverkehr nicht genutzt werden. Sie können das Multipath-Routing so aktivieren, dass die Lastverteilung über alle verfügbaren Routen im

Verhältnis zu ihren Kennzahlen erfolgt, im Gegensatz zum ECMP-Routing, das die Lastverteilung über die verfügbaren Routen derselben Metrik ausgleicht.

Schritte

1. Melden Sie sich bei der erweiterten Berechtigungsebene an:

   ```
   set -privilege advanced
   ```

2. Multipath-Routing aktivieren:

   ```
   network options multipath-routing modify -is-enabled true
   ```

   Das Multipath-Routing ist für alle Nodes im Cluster aktiviert.

   ```
   network options multipath-routing modify -is-enabled true
   ```

   Erfahren Sie mehr über `network options multipath-routing modify` in der "ONTAP-Befehlsreferenz".

Löschen Sie statische Routen aus dem ONTAP-Netzwerk

Sie können eine nicht benötigte statische Route von einer Storage Virtual Machine (SVM) löschen.

Schritt

```
`network route delete`Löschen Sie mit dem Befehl eine statische Route.
```

Im folgenden Beispiel wird eine statische Route gelöscht, die SVM vs0 mit einem Gateway von 10.63.0.1 und einer Ziel-IP-Adresse von 0.0.0.0/0 verknüpft ist:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

Erfahren Sie mehr über `network route delete` in der "ONTAP-Befehlsreferenz".

Anzeigen von ONTAP Routing-Informationen

Sie können Informationen über die Routing-Konfiguration für jede SVM auf Ihrem Cluster anzeigen. So können Sie Routingprobleme im Zusammenhang mit Verbindungsproblemen zwischen Client-Applikationen oder -Services und einer LIF auf einem Node im Cluster diagnostizieren.

Schritte

1. Mit dem `network route show` Befehl werden Routen innerhalb einer oder mehrerer SVMs angezeigt. Das folgende Beispiel zeigt eine in der vs0 SVM konfigurierte Route:

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Mit dem `network route show-lifs` Befehl können Sie die Zuordnung von Routen und LIFs innerhalb einer oder mehrerer SVMs anzeigen.

   Das folgende Beispiel zeigt LIFs mit Routen, die sich im Besitz der vs0 SVM befinden:

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   Erfahren Sie mehr über `network route show` und `network route show-lifs` in der "ONTAP-Befehlsreferenz".

3. Verwenden Sie den `network route active-entry show` Befehl, um installierte Routen auf einem oder mehreren Nodes, SVMs, Subnetzen oder Routen mit angegebenen Zielen anzuzeigen.

   Das folgende Beispiel zeigt alle installierten Routen auf einer bestimmten SVM:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
```

```
---------------------  ------------------  ---------   ------  -----
default                fd20:8b1e:b255:814e::1
                                           e0d             20  UGS
fd20:8b1e:b255:814e::/64
                       link#4              e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination            Gateway             Interface   Metric  Flags
---------------------  ------------------  ---------   ------  -----
127.0.0.1              127.0.0.1           lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination            Gateway             Interface   Metric  Flags
---------------------  ------------------  ---------   ------  -----
127.0.10.1             127.0.20.1          losk            10  UHS
127.0.20.1             127.0.20.1          losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination            Gateway             Interface   Metric  Flags
---------------------  ------------------  ---------   ------  -----
default                fd20:8b1e:b255:814e::1
                                           e0d             20  UGS
fd20:8b1e:b255:814e::/64
                       link#4              e0d              0  UC
fd20:8b1e:b255:814e::1 link#4              e0d              0  UHL
11 entries were displayed.
```

Erfahren Sie mehr über `network route active-entry show` in der "ONTAP-Befehlsreferenz".

Entfernen Sie dynamische Routen aus Routing-Tabellen für das ONTAP-Netzwerk

Wenn ICMP-Umleitungen für IPv4 und IPv6 empfangen werden, werden dynamische Routen zur Routing-Tabelle hinzugefügt. Standardmäßig werden die dynamischen Routen nach 300 Sekunden entfernt. Wenn Sie dynamische Routen für einen anderen Zeitraum beibehalten möchten, können Sie den Zeitwert ändern.

Über diese Aufgabe

Sie können den Timeout-Wert zwischen 0 und 65,535 Sekunden einstellen. Wenn Sie den Wert auf 0 setzen, laufen die Routen nie ab. Durch das Entfernen dynamischer Routen wird ein Verlust der Verbindung durch die Persistenz ungültiger Routen verhindert.

Schritte

1. Zeigt den aktuellen Zeitüberschreitungswert an.
   - Für IPv4:

     ```
     network tuning icmp show
     ```

   - Für IPv6:

     ```
     network tuning icmp6 show
     ```

2. Ändern Sie den Timeout-Wert.
   - Für IPv4:

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - Für IPv6:

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. Überprüfen Sie, ob der Zeitüberschreitungswert korrekt geändert wurde.
   - Für IPv4:

     ```
     network tuning icmp show
     ```

   - Für IPv6:

     ```
     network tuning icmp6 show
     ```

Erfahren Sie mehr über `network tuning icmp` in der "ONTAP-Befehlsreferenz".

Informationen zum ONTAP-Netzwerk

Zeigen Sie ONTAP-Netzwerkinformationen an

Über die CLI können Sie Informationen zu Ports, LIFs, Routen, Failover-Regeln, Failover-Gruppen, Firewall-Regeln, DNS, NIS und Verbindungen. Ab ONTAP 9.8 können Sie auch die Daten herunterladen, die in System Manager über Ihr Netzwerk angezeigt werden.

Diese Informationen können in Situationen, z. B. bei der Neukonfiguration von Netzwerkeinstellungen oder bei der Fehlerbehebung im Cluster nützlich sein.

Als Cluster-Administrator können Sie alle verfügbaren Netzwerkinformationen anzeigen. Als SVM-Administrator können Sie nur die Informationen anzeigen, die mit Ihren zugewiesenen SVMs verbunden sind.

Wenn Sie in System Manager Informationen in einer *Listenansicht* anzeigen, können Sie auf **Download** klicken und die Liste der angezeigten Objekte wird heruntergeladen.

- Die Liste wird im CSV-Format (Comma Separated values) heruntergeladen.
- Es werden nur die Daten in den sichtbaren Spalten heruntergeladen.
- Der CSV-Dateiname ist mit dem Objektnamen und einem Zeitstempel formatiert.

Zeigen Sie Informationen zu ONTAP-Netzwerkports an

Sie können Informationen über einen bestimmten Port oder über alle Ports auf allen Nodes im Cluster anzeigen.

Über diese Aufgabe

Folgende Informationen werden angezeigt:

- Node-Name
- Port-Name
- IP-Name
- Name der Broadcast-Domäne
- Verbindungsstatus (auf oder ab)
- MTU-Einstellung
- Einstellung der Portgeschwindigkeit und Betriebsstatus (1 Gigabit oder 10 Gigabit pro Sekunde)
- Einstellung für automatische Aushandlung (wahr oder falsch)
- Duplexmodus und Betriebsstatus (halb oder voll)
- Falls zutreffend, Interface Group des Ports
- Gegebenenfalls werden die VLAN-Tag-Informationen des Ports angezeigt
- Systemzustand des Ports (Systemzustand oder beeinträchtigt)
- Gründe für einen Port, der als „beeinträchtigt“ markiert wird

Wenn keine Daten für ein Feld verfügbar sind (z. B. die Betriebsduplex- und -Geschwindigkeit für einen inaktiven Port wären nicht verfügbar), wird der Feldwert als angezeigt `-`.

Schritt

Zeigen Sie mit dem `network port show` Befehl Informationen zu Netzwerk-Ports an.

Sie können detaillierte Informationen für jeden Port anzeigen, indem Sie den `-instance` Parameter angeben. Oder Sie erhalten spezifische Informationen, indem `-fields` Sie Feldnamen mit dem Parameter angeben.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie ONTAP VLAN-Informationen an

Sie können Informationen zu einem bestimmten VLAN oder zu allen VLANs im Cluster anzeigen.

Über diese Aufgabe

Sie können detaillierte Informationen für jedes VLAN anzeigen, indem Sie den `-instance` Parameter angeben. Sie können bestimmte Informationen anzeigen, indem `-fields` Sie mit dem Parameter Feldnamen angeben.

Schritt

Mit dem `network port vlan show` Befehl werden Informationen zu VLANs angezeigt. Mit dem folgenden Befehl werden Informationen zu allen VLANs im Cluster angezeigt:

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

Erfahren Sie mehr über `network port vlan show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie Informationen zu ONTAP-Schnittstellengruppen an

Sie können Informationen über eine Schnittstellengruppe anzeigen, um deren Konfiguration zu bestimmen.

Über diese Aufgabe

Folgende Informationen werden angezeigt:

- Node, auf dem sich die Schnittstellengruppe befindet
- Liste der Netzwerkports, die in der Schnittstellengruppe enthalten sind
- Der Name der Schnittstellengruppe
- Verteilungsfunktion (MAC, IP, Port oder sequenziell)
- Media Access Control (MAC)-Adresse der Interface Group
- Port-Aktivitätsstatus; das heißt, ob alle aggregierten Ports aktiv sind (volle Teilnahme), ob einige aktiv sind (Teilteilbeteiligung) oder ob keine aktiv sind

Schritt

Mit dem `network port ifgrp show` Befehl werden Informationen zu Schnittstellengruppen angezeigt.

Sie können detaillierte Informationen zu jedem Node anzeigen, indem Sie den `-instance` Parameter angeben. Sie können bestimmte Informationen anzeigen, indem `-fields` Sie mit dem Parameter Feldnamen angeben.

Mit dem folgenden Befehl werden Informationen zu allen Schnittstellengruppen im Cluster angezeigt:

```
network port ifgrp show
         Port     Distribution                   Active
Node     IfGrp    Function     MAC Address       Ports   Ports
-------- -------- ------------ ----------------- ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2 full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66 full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e full    e7a, e7b
```

Mit dem folgenden Befehl werden detaillierte Schnittstellengruppeninformationen für einen einzelnen Node angezeigt:

```
network port ifgrp show -instance -node cluster-1-01

                Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

Erfahren Sie mehr über `network port ifgrp show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie LIF-Informationen zu ONTAP an

Sie können ausführliche Informationen über ein LIF anzeigen, um seine Konfiguration zu ermitteln.

Diese Informationen können Sie auch zur Diagnose einfacher LIF-Probleme einsetzen, beispielsweise durch die Überprüfung auf doppelte IP-Adressen oder durch die Überprüfung, ob der Netzwerk-Port zum richtigen Subnetz gehört. SVM-Administratoren (Storage Virtual Machine) können nur die Informationen über die mit der SVM verknüpften LIFs anzeigen.

Über diese Aufgabe

Folgende Informationen werden angezeigt:

- Der logischen Schnittstelle zugeordnete IP-Adresse
- Administrationsstatus des LIF
- Betriebsstatus des LIF

  Der Betriebsstatus von Daten-LIFs wird durch den Status der SVM bestimmt, der den Daten-LIFs zugeordnet ist. Wenn die SVM angehalten wird, ändert sich der Betriebsstatus der LIF in „down“. Wenn die SVM wieder gestartet wird, ändert sich der Betriebsstatus in „up“

- Node und der Port, auf dem sich die LIF befindet

Wenn keine Daten für ein Feld verfügbar sind (z. B. wenn keine erweiterten Statusinformationen vorhanden sind), wird der Feldwert als angezeigt `-`.

Schritt

Zeigt LIF-Informationen mit dem `network interface show` Befehl an.

Sie können ausführliche Informationen zu jeder LIF anzeigen, indem Sie den Parameter „-Instance“ angeben oder bestimmte Informationen abrufen, indem Sie mithilfe des Parameters -fields Feldnamen angeben.

Mit dem folgenden Befehl werden allgemeine Informationen zu allen LIFs in einem Cluster angezeigt:

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

Mit dem folgenden Befehl werden ausführliche Informationen zu einem einzelnen LIF angezeigt:

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
              Operational Status: up
                 Extended Status: -
                         Is Home: false
                 Network Address: 192.0.2.128
                         Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Anzeigen von Routinginformationen für das ONTAP-Netzwerk

Sie können Informationen zu Routen innerhalb einer SVM anzeigen.

Schritt

Geben Sie je nach Art der Routing-Informationen den entsprechenden Befehl ein:

So zeigen Sie Informationen über…	Eingeben…
Statische Routen pro SVM	`network route show`

LIFs an jeder Route, pro SVM	`network route show-lifs`

Sie können detaillierte Informationen zu jeder Route anzeigen, indem Sie den `-instance` Parameter angeben. Mit dem folgenden Befehl werden die statischen Routen innerhalb der SVMs in Cluster-1 angezeigt:

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

Mit dem folgenden Befehl werden die Zuordnung statischer Routen und logischer Schnittstellen (LIFs) in allen SVMs im Cluster-1 angezeigt:

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Erfahren Sie mehr über `network route show` und `network route show-lifs` in der "ONTAP-Befehlsreferenz".

Zeigen Sie die Einträge der ONTAP-DNS-Host-Tabelle an

Die DNS-Host-Tabelleneinträge ordnen Hostnamen IP-Adressen zu. Sie können die Hostnamen und Alias-Namen sowie die IP-Adresse anzeigen, die sie für alle SVMs in einem Cluster zuweisen.

Schritt

Zeigen Sie die Host-Namenseinträge für alle SVMs mithilfe des Befehls „vserver Services Name-Service dns Hosts show“ an.

Im folgenden Beispiel werden die Einträge der Hosttabelle angezeigt:

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst.

Zeigen Sie Informationen zur Konfiguration der ONTAP DNS-Domain an

Sie können die DNS-Domänenkonfiguration einer oder mehrerer Storage Virtual Machines (SVMs) in Ihrem Cluster anzeigen, um zu überprüfen, ob sie ordnungsgemäß konfiguriert ist.

Schritt

Anzeigen der DNS-Domänenkonfigurationen mit dem `vserver services name-service dns show` Befehl.

Mit dem folgenden Befehl werden die DNS-Konfigurationen für alle SVMs im Cluster angezeigt:

```
vserver services name-service dns show
                                                        Name
Vserver         State     Domains                       Servers
--------------- --------- ----------------------------- -------------
cluster-1        enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs1             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs2             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs3             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
```

Mit dem folgenden Befehl werden detaillierte DNS-Konfigurationsinformationen für SVM vs1 angezeigt:

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

Zeigen Sie Informationen zu ONTAP Failover-Gruppen an

Sie können Informationen zu Failover-Gruppen anzeigen, einschließlich der Liste der Nodes und Ports in jeder Failover-Gruppe, ob das Failover aktiviert oder deaktiviert ist, und den Typ der Failover-Richtlinie, die auf die einzelnen LIFs angewendet wird.

Schritte

1. Zeigen Sie mit dem `network interface failover-groups show` Befehl die Zielports für jede Failover-Gruppe an.

   Mit dem folgenden Befehl werden Informationen zu allen Failover-Gruppen auf einem Cluster mit zwei Nodes angezeigt:

```
network interface failover-groups show
                              Failover
Vserver         Group         Targets
--------------- ------------- --------------------------------
Cluster
                Cluster
                              cluster1-01:e0a, cluster1-01:e0b,
                              cluster1-02:e0a, cluster1-02:e0b
vs1
                Default
                              cluster1-01:e0c, cluster1-01:e0d,
                              cluster1-01:e0e, cluster1-02:e0c,
                              cluster1-02:e0d, cluster1-02:e0e
```

Erfahren Sie mehr über `network interface failover-groups show` in der "ONTAP-Befehlsreferenz".

2. Zeigen Sie mit dem `network interface failover-groups show` Befehl die Ziel-Ports und die Broadcast-Domäne für eine bestimmte Failover-Gruppe an.

   Mit dem folgenden Befehl werden ausführliche Informationen zu Failover-Gruppendata12 für SVM vs4 angezeigt:

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Zeigen Sie mit dem `network interface show` Befehl die Failover-Einstellungen an, die von allen LIFs verwendet werden.

   Mit dem folgenden Befehl werden die Failover-Richtlinie und die Failover-Gruppe angezeigt, die von den einzelnen LIFs verwendet werden:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -----------------  ---------------------  -------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie die ONTAP LIF Failover-Ziele an

Unter Umständen müssen Sie prüfen, ob die Failover-Richtlinien und die Failover-Gruppen einer LIF ordnungsgemäß konfiguriert sind. Um eine Fehlkonfiguration der Failover-Regeln zu vermeiden, können Sie die Failover-Ziele für eine einzelne LIF oder für alle LIFs anzeigen.

Über diese Aufgabe

Durch Anzeigen von LIF Failover-Zielen können Sie Folgendes überprüfen:

- Gibt an, ob die LIFs mit der korrekten Failover-Gruppe und der korrekten Failover-Richtlinie konfiguriert sind
- Gibt an, ob die resultierende Liste der Failover-Ziel-Ports für jede LIF geeignet ist
- Gibt an, ob das Failover-Ziel einer Daten-LIF kein Management-Port (E0M) ist

Schritt

Zeigen Sie mit der `failover` Option des `network interface show` Befehls die Failover-Ziele eines LIF an.

Mit dem folgenden Befehl werden Informationen zu den Failover-Zielen für alle LIFs in einem Cluster mit zwei Nodes angezeigt. In der `Failover Targets` Zeile werden die (priorisierte) Liste der Node-Port-Kombinationen für eine bestimmte LIF angezeigt.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie ONTAP LIFs in einer Lastverteilungszone an

Sie können überprüfen, ob eine Load-Balancing-Zone korrekt konfiguriert ist, indem Sie alle zu ihr gehörenden LIFs anzeigen. Sie können auch die Load Balancing-Zone einer bestimmten LIF oder die Load-Balancing-Zonen für alle LIFs anzeigen.

Schritt

Zeigt die LIFs und Lastverteilungsdetails an, die Sie mit einem der folgenden Befehle benötigen

Anzeige…	Eingeben…
LIFs in einer bestimmten Lastverteilungszone	`network interface show -dns-zone zone_name` `zone_name` Gibt den Namen der Lastausgleichszone an.
Die Lastverteilungszone eines bestimmten LIF	`network interface show -lif lif_name -fields dns-zone`
Die Lastverteilungszonen aller LIFs	`network interface show -fields dns-zone`

Beispiele für das Anzeigen von Lastverteilungszonen für LIFs

Mit dem folgenden Befehl werden die Details zu allen LIFs in der Lastausgleichzone storage.company.com für SVM vs0 angezeigt:

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network           Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask      Node      Port    Home
--------- ---------- ---------- ----------------- --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

Mit dem folgenden Befehl werden die DNS-Zone-Details der LIF-Daten angezeigt.3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

Mit dem folgenden Befehl werden die Liste aller LIFs im Cluster und der entsprechenden DNS-Zonen angezeigt:

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Zeigen Sie ONTAP-Cluster-Verbindungen an

Sie können alle aktiven Verbindungen im Cluster anzeigen oder die Anzahl der aktiven Verbindungen auf dem Node nach Client, logischer Schnittstelle, Protokoll oder Service zählen. Sie können auch alle Listening-Verbindungen im Cluster anzeigen.

Aktive Verbindungen nach Client anzeigen (nur Cluster-Administratoren)

Sie können die aktiven Verbindungen nach Client anzeigen, um den Node zu überprüfen, den ein bestimmter Client nutzt, und um mögliche Ungleichgewichte zwischen den Client-Zählungen pro Node anzuzeigen.

Über diese Aufgabe

Die Anzahl der aktiven Verbindungen nach Client ist in den folgenden Szenarien nützlich:

- Suchen eines überlasteten oder überlasteten Knotens
- Bestimmen, warum der Zugriff eines bestimmten Clients auf ein Volume langsam ist.

  Sie können Details zu dem Node anzeigen, auf den der Client zugreift, und ihn dann mit dem Node vergleichen, auf dem sich das Volume befindet. Wenn der Zugriff auf das Volume ein Durchlaufen des Cluster-Netzwerks erfordert, kommt es möglicherweise zu einer verringerten Performance, weil der Remote-Zugriff auf das Volume auf einem überzeichneten Remote-Node möglich ist.

- Dabei wird sichergestellt, dass alle Nodes gleichermaßen für den Datenzugriff verwendet werden.
- Suchen von Clients, die eine unerwartet hohe Anzahl von Verbindungen haben.
- Überprüfung, ob bestimmte Clients Verbindungen zu einem Node haben.

Schritt

Zeigt mit dem `network connections active show-clients` Befehl die Anzahl der aktiven Verbindungen durch den Client auf einem Node an.

Erfahren Sie mehr über `network connections active show-clients` in der "ONTAP-Befehlsreferenz".

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253               1
        vs0             192.0.2.252               2
        Cluster         192.10.2.124              5
node1   vs0             192.0.2.250               1
        vs0             192.0.2.252               3
        Cluster         192.10.2.123              4
node2   vs1             customer.example.com      1
        vs1             192.0.2.245               3
        Cluster         192.10.2.122              4
node3   vs1             customer.example.org      1
        vs1             customer.example.net      3
        Cluster         192.10.2.121              4
```

Aktive Verbindungen nach Protokoll anzeigen (nur Cluster-Administratoren)

Sie können eine Anzahl der aktiven Verbindungen nach Protokoll (TCP oder UDP) auf einem Knoten anzeigen, um die Verwendung von Protokollen innerhalb des Clusters zu vergleichen.

Über diese Aufgabe

Die Anzahl der aktiven Verbindungen nach Protokoll ist in folgenden Szenarien nützlich:

- Suche nach UDP-Clients, die ihre Verbindung verlieren.

  Wenn sich ein Knoten in der Nähe seines Verbindungslimits befindet, sind UDP-Clients die ersten, die fallengelassen werden.

- Überprüfung, ob keine anderen Protokolle verwendet werden.

Schritt

Zeigt mit dem `network connections active show-protocols` Befehl die Anzahl der aktiven Verbindungen nach Protokoll auf einem Node an.

Erfahren Sie mehr über `network connections active show-protocols` in der "ONTAP-Befehlsreferenz".

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

Aktive Verbindungen nach Service anzeigen (nur Cluster-Administratoren)

Sie können für jeden Node in einem Cluster die Anzahl der aktiven Verbindungen nach Servicetyp (z. B. nach NFS, SMB, Mount usw.) anzeigen. Mithilfe dieser Funktion können Sie die Nutzung von Services innerhalb des Clusters vergleichen, sodass der primäre Workload eines Node bestimmt wird.

Über diese Aufgabe

Die Anzahl der aktiven Verbindungen nach Dienst ist in den folgenden Szenarien nützlich:

- Überprüfung, ob alle Nodes für die entsprechenden Services genutzt werden und ob der Lastausgleich für diesen Service funktioniert
- Überprüfung, ob keine anderen Dienste genutzt werden. Mit dem `network connections active show-services` Befehl wird die Anzahl der aktiven Verbindungen nach Dienst auf einem Node angezeigt.

Erfahren Sie mehr über `network connections active show-services` in der "ONTAP-Befehlsreferenz".

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

Anzeigen aktiver Verbindungen nach LIF auf einem Node und einer SVM

Sie können die Anzahl der aktiven Verbindungen für jede logische Schnittstelle, nach Node und Storage Virtual Machine (SVM) anzeigen, um Verbindungsungleichgewichte zwischen LIFs innerhalb des Clusters anzuzeigen.

Über diese Aufgabe

Die Anzahl der aktiven Verbindungen nach LIF ist in den folgenden Szenarien nützlich:

- Suchen eines überlasteten LIF durch Vergleichen der Anzahl der Verbindungen pro LIF
- Überprüfen, ob der DNS-Lastausgleich für alle Daten-LIFs funktioniert
- Vergleichen der Anzahl von Verbindungen mit den verschiedenen SVMs, um die am häufigsten verwendeten SVMs zu finden

Schritt

Mit dem `network connections active show-lifs` Befehl wird die Anzahl der aktiven Verbindungen pro LIF nach SVM und Node angezeigt.

Erfahren Sie mehr über `network connections active show-lifs` in der "ONTAP-Befehlsreferenz".

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Zeigt aktive Verbindungen in einem Cluster an

Sie können Informationen über die aktiven Verbindungen in einem Cluster anzeigen, um Informationen zu LIFs, Ports, Remote-Host, Service, Storage Virtual Machines (SVMs) und Protokollen, die von einzelnen Verbindungen verwendet werden, anzuzeigen.

Über diese Aufgabe

Die Anzeigen der aktiven Verbindungen in einem Cluster ist in den folgenden Szenarien nützlich:

- Überprüfung, ob einzelne Clients das richtige Protokoll und den korrekten Service auf dem richtigen Node verwenden
- Wenn ein Client mit einer bestimmten Kombination aus Node, Protokoll und Service Probleme beim Datenzugriff hat, können Sie mit diesem Befehl einen ähnlichen Client zum Konfigurations- oder Paketverfolgung-Vergleich finden.

Schritt

Mit dem `network connections active show` Befehl können Sie die aktiven Verbindungen in einem Cluster anzeigen.

Erfahren Sie mehr über `network connections active show` in der "ONTAP-Befehlsreferenz".

Mit dem folgenden Befehl werden die aktiven Verbindungen auf dem Node node1 angezeigt:

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

Mit dem folgenden Befehl werden die aktiven Verbindungen auf der SVM vs1 angezeigt:

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Anzeige von Hörverbindungen in einem Cluster

Sie können Informationen zu den Hörverbindungen in einem Cluster anzeigen, um die LIFs und Ports anzuzeigen, die Verbindungen für ein bestimmtes Protokoll und einen bestimmten Service akzeptieren.

Über diese Aufgabe

Die Anzeige der Hörverbindungen in einem Cluster ist in den folgenden Szenarien nützlich:

- Überprüfen, ob das gewünschte Protokoll oder der gewünschte Service eine LIF angehört, wenn Client-Verbindungen zu dieser LIF konsistent ausfallen.
- Überprüfen, ob an jeder Cluster-LIF ein UDP/rclopcp-Listener geöffnet wird, wenn der Remote-Datenzugriff auf ein Volume auf einem Node über eine LIF auf einem anderen Node fehlschlägt.
- Überprüfen, ob ein UDP/rclopcp Listener an jeder Cluster LIF geöffnet wird, wenn SnapMirror Transfers zwischen zwei Nodes im selben Cluster ausfallen.
- Überprüfung, ob ein TCP/ctlopcp Listener an jeder intercluster LIF geöffnet wird, wenn SnapMirror Transfers zwischen zwei Knoten verschiedener Cluster ausfallen.

Schritt

Mit dem `network connections listening show` Befehl können Sie die Listening-Verbindungen pro Knoten anzeigen.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

Erfahren Sie mehr über `network connections listening show` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Diagnose von Netzwerkproblemen

Sie können Probleme in Ihrem Netzwerk mithilfe von Befehlen wie `ping`, `traceroute`, `ndp`, und diagnostizieren `tcpdump`. Sie können auch Befehle wie `ping6` und verwenden `traceroute6`, um IPv6-Probleme zu diagnostizieren.

Ihr Ziel ist	Diesen Befehl eingeben…
Testen Sie, ob der Node andere Hosts im Netzwerk erreichen kann	`network ping`
Testen Sie, ob der Node andere Hosts im IPv6-Netzwerk erreichen kann	`network ping6`
Verfolgen Sie die Route, die die IPv4-Pakete zu einem Netzwerkknoten führen	`network traceroute`
Verfolgen Sie die Route, die die IPv6-Pakete zu einem Netzwerkknoten führen	`network traceroute6`
Managen des Neighbor Discovery Protocol (NDP)	`network ndp`
Zeigen Sie Statistiken zu Paketen an, die auf einer bestimmten Netzwerkschnittstelle oder auf allen Netzwerkschnittstellen empfangen und gesendet werden	`run -node` *`node_name`* `ifstat` **Hinweis**: Dieser Befehl ist aus der Nodeshell verfügbar.
Anzeigen von Informationen zu benachbarten Geräten, die von jedem Node und Port im Cluster erkannt werden, einschließlich des Remote-Gerätetyps und der Geräteplattform	`network device-discovery show`

Anzeigen des CDP-Nachbarn des Knotens (ONTAP unterstützt nur CDP1-Werbeanzeigen)	`run -node node_name cdpd show-neighbors` **Hinweis**: Dieser Befehl ist aus der Nodeshell verfügbar.
Verfolgen Sie die Pakete, die im Netzwerk gesendet und empfangen werden	`network tcpdump start -node node-name -port port_name` **Hinweis**: Dieser Befehl ist aus der Nodeshell verfügbar.
Messung von Latenz und Durchsatz zwischen Cluster- oder Intracluster-Nodes	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` Weitere Informationen finden Sie im "Performance Management".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "Netzwerk-Ping"
- "Netzwerk-Traceroute"
- "Netzwerkgeräte-Erkennung anzeigen"
- "Netzwerk-ndp"

Zeigen Sie die Netzwerkkonnektivität mit Protokollen zur Erkennung von Nachbarn an

Zeigen Sie die ONTAP-Netzwerkkonnektivität mit Protokollen zur Erkennung von Nachbarn an

In einem Datacenter können Sie mithilfe von „Neighbor“-Erkennungsprotokollen die Netzwerkverbindung zwischen zwei physischen oder virtuellen Systemen und ihren Netzwerkschnittstellen anzeigen. ONTAP unterstützt zwei Protokolle für die „Neighbor“-Erkennung: Das Cisco Discovery Protocol (CDP) und das Link Layer Discovery Protocol (LLDP).

Mithilfe von Nachbarprotokollprotokollen können Sie Informationen zu direkt verbundenen protokollfähigen Geräten in einem Netzwerk automatisch erkennen und anzeigen. Jedes Gerät gibt Informationen zu Identifikation, Funktionen und Konnektivität an. Diese Informationen werden in Ethernet-Frames an eine Multicast-MAC-Adresse übertragen und von allen benachbarten protokollfähigen Geräten empfangen.

Damit zwei Geräte zu „Nachbarn“ werden, muss jedes Protokoll aktiviert und korrekt konfiguriert sein. Die Funktion des Erkennungsprotokolls ist auf direkt verbundene Netzwerke beschränkt. Zur Nachbarn können protokollfähige Geräte wie Switches, Router, Bridges usw. gehören. ONTAP unterstützt zwei Nachbarprotokoll, die einzeln oder gemeinsam verwendet werden können.

- Cisco Discovery Protocol (CDP)*

CDP ist ein von Cisco Systems entwickeltes proprietäres Link-Layer-Protokoll. Sie ist in ONTAP standardmäßig für Cluster-Ports aktiviert, muss jedoch explizit für Daten-Ports aktiviert sein.

Link Layer Discovery Protocol (LLDP)

LLDP ist ein anbieterneutrales Protokoll, das im Standarddokument IEEE 802.1AB angegeben ist. Sie muss explizit für alle Ports aktiviert sein.

Verwenden Sie CDP, um ONTAP-Netzwerkverbindungen zu erkennen

Die Verwendung von CDP zur Erkennung von Netzwerkverbindungen besteht aus der Überprüfung von Bereitstellungsüberlegungen, der Nutzung von Datenports, der Anzeige von Nachbargeräten und der Anpassung der CDP-Konfigurationswerte nach Bedarf. CDP ist standardmäßig auf Cluster-Ports aktiviert.

CDP muss auch auf Switches und Routern aktiviert sein, bevor Informationen zu Nachbargeräten angezeigt werden können.

Version von ONTAP	Beschreibung
9.10.1 und früher	CDP kann außerdem von der Systemzustandsüberwachung der Cluster-Switches verwendet werden, um die Cluster- und Management-Netzwerk-Switches automatisch zu erkennen.
9.11.1 und höher	CDP kann außerdem von der Systemzustandsüberwachung der Cluster-Switches verwendet werden, um die Switches für das Cluster-, Storage- und Management-Netzwerk automatisch zu erkennen.

Verwandte Informationen

"Systemadministration"

Überlegungen zur Verwendung von CDP

Standardmäßig senden CDP-kompatible Geräte CDPv2-Werbeanzeigen. CDP-kompatible Geräte senden CDPv1-Werbeanzeigen nur dann, wenn sie CDPv1-Werbeanzeigen erhalten. ONTAP unterstützt nur CDPv1. Wenn ein ONTAP-Knoten CDPv1-Werbeanzeigen sendet, senden CDP-kompatible benachbarte Geräte daher CDP1-Werbeanzeigen zurück.

Vor der Aktivierung von CDP auf einem Knoten sollten Sie die folgenden Informationen berücksichtigen:

- CDP wird für alle Ports unterstützt.
- CDP-Werbeanzeigen werden von Ports gesendet und empfangen, die sich im up-Zustand befinden.
- CDP muss auf den Sende- und Empfangsgeräten für das Senden und Empfangen von CDP-Werbeanzeigen aktiviert sein.
- CDP-Werbeanzeigen werden in regelmäßigen Abständen gesendet, und Sie können das Zeitintervall konfigurieren.
- Wenn IP-Adressen für eine LIF geändert werden, sendet der Node die aktualisierten Informationen in der nächsten CDP-Ankündigung.
- ONTAP 9.10.1 und früher:
  - CDP ist immer auf Cluster-Ports aktiviert.
  - CDP ist standardmäßig auf allen nicht-Cluster-Ports deaktiviert.
- ONTAP 9.11.1 und höher:
  - CDP ist immer auf Cluster- und Storage-Ports aktiviert.

- CDP ist standardmäßig auf allen nicht-Cluster- und nicht-Storage-Ports deaktiviert.

> Wenn LIFs auf dem Node geändert werden, werden die CDP-Informationen manchmal nicht auf der Seite des empfangenden Geräts (z. B. ein Switch) aktualisiert. Wenn ein solches Problem auftritt, sollten Sie die Netzwerkschnittstelle des Node mit dem Status „down“ und dann mit dem Status „up“ konfigurieren.

- In CDP-Werbeanzeigen werden nur IPv4-Adressen beworben.
- Bei physischen Netzwerk-Ports mit VLANs werden alle auf den VLANs dieses Ports konfigurierten LIFs angekündigt.
- Bei physischen Ports, die Teil einer Schnittstellengruppe sind, werden alle in dieser Schnittstellengruppe konfigurierten IP-Adressen auf jedem physischen Port angekündigt.
- Bei einer Interface Group, die VLANs hostet, werden alle in der Interface Group konfigurierten LIFs und VLANs auf den einzelnen Netzwerk-Ports angekündigt.
- Da CDP-Pakete auf nicht mehr als 1500 Byte beschränkt sind, können bei Ports, die mit einer großen Anzahl von LIFs konfiguriert sind, nur eine Teilmenge dieser IP-Adressen auf dem benachbarten Switch gemeldet werden.

CDP aktivieren oder deaktivieren

Um Anzeigen zu ermitteln und an CDP-konforme benachbarte Geräte zu senden, muss CDP auf jedem Knoten des Clusters aktiviert sein.

Standardmäßig ist CDP in ONTAP 9.10.1 und früher auf allen Cluster-Ports eines Knotens aktiviert und auf allen nicht-Cluster-Ports eines Knotens deaktiviert.

Standardmäßig ist CDP in ONTAP 9.11.1 und höher auf allen Cluster- und Speicherports eines Knotens aktiviert und auf allen nicht-Cluster- und nicht-Speicherports eines Node deaktiviert.

Über diese Aufgabe

Die `cdpd.enable` Option steuert, ob CDP auf den Ports eines Knotens aktiviert oder deaktiviert ist:

- Für ONTAP 9.10.1 und frühere Versionen ermöglicht ON CDP für nicht-Cluster-Ports.
- Für ONTAP 9.11.1 und höher ermöglicht ON CDP auf nicht-Cluster- und nicht-Storage-Ports.
- Bei ONTAP 9.10.1 und älteren Versionen deaktiviert CDP für nicht-Cluster-Ports; Sie können CDP bei Cluster-Ports nicht deaktivieren.
- Bei ONTAP 9.11.1 und höher deaktiviert Off CDP für nicht-Cluster- und nicht-Speicherports; CDP kann bei Cluster-Ports nicht deaktiviert werden.

Wenn CDP auf einem Port deaktiviert ist, der mit einem CDP-kompatiblen Gerät verbunden ist, kann der Netzwerkverkehr möglicherweise nicht optimiert werden.

Schritte

1. Aktuelle CDP-Einstellung für einen Knoten oder für alle Knoten in einem Cluster anzeigen:

So zeigen Sie die CDP-Einstellung an:	Eingeben…
Ein Node	`run - node <node_name> options cdpd.enable`

Alle Nodes in einem Cluster	`options cdpd.enable`

2. Aktivieren oder Deaktivieren von CDP an allen Ports eines Knotens oder an allen Ports aller Knoten in einem Cluster:

So aktivieren oder deaktivieren Sie CDP ein:	Eingeben…
Ein Node	`run -node node_name options cdpd.enable {on or off}`
Alle Nodes in einem Cluster	`options cdpd.enable {on or off}`

Anzeigen von CDP-Nachbarinformationen

Sie können Informationen über die benachbarten Geräte anzeigen, die mit jedem Port des Clusters verbunden sind, sofern der Port mit einem CDP-kompatiblen Gerät verbunden ist. Sie können mit dem `network device-discovery show -protocol cdp` Befehl Nachbarinformationen anzeigen. Erfahren Sie mehr über `network device-discovery show` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

In ONTAP 9.10.1 und früher, da CDP immer für Cluster-Ports aktiviert ist, werden CDP-Nachinformationen immer für diese Ports angezeigt. CDP muss auf nicht-Cluster-Ports aktiviert sein, damit für diese Ports „Nachbar"-Informationen angezeigt werden können.

In ONTAP 9.11.1 und höher wird CDP immer für Cluster- und Storage-Ports aktiviert, sodass CDP-Nachinformationen immer für diese Ports angezeigt werden. CDP muss auf nicht-Cluster- und nicht-Storage-Ports aktiviert sein, damit für diese Ports Nachbar-Informationen angezeigt werden können.

Schritt

Informationen zu allen CDP-kompatiblen Geräten anzeigen, die mit den Ports eines Knotens im Cluster verbunden sind:

```
network device-discovery show -node node -protocol cdp
```

Mit dem folgenden Befehl werden die Nachbarn angezeigt, die mit den Ports auf dem Node sti2650-212 verbunden sind:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

Die Ausgabe listet die Cisco-Geräte auf, die mit jedem Port des angegebenen Knotens verbunden sind.

Konfigurieren Sie die Haltezeit für CDP-Nachrichten

Die Haltezeit ist der Zeitraum, für den CDP-Werbeanzeigen im Cache von benachbarten CDP-kompatiblen Geräten gespeichert werden. Die Haltezeit wird in jedem CDP1-Paket angekündigt und wird aktualisiert, sobald ein CDPv1-Paket von einem Node empfangen wird.

- Der Wert der `cdpd.holdtime` Option sollte auf beiden Nodes eines HA-Paars auf den gleichen Wert eingestellt werden.
- Der Standardwert für die Haltezeit beträgt 180 Sekunden, Sie können jedoch Werte zwischen 10 Sekunden und 255 Sekunden eingeben.
- Wenn eine IP-Adresse entfernt wird, bevor die Haltezeit abgelaufen ist, werden die CDP-Informationen bis zum Ablauf der Haltezeit zwischengespeichert.

Schritte

1. Zeigen Sie die aktuelle CDP-Haltezeit für einen Knoten oder für alle Knoten in einem Cluster an:

So zeigen Sie die Haltezeit von…	Eingeben…
Ein Node	`run -node node_name options cdpd.holdtime`

Alle Nodes in einem Cluster	`options cdpd.holdtime`

2. Konfigurieren Sie die CDP-Haltezeit auf allen Ports eines Node oder auf allen Ports aller Knoten in einem Cluster:

So stellen Sie die Haltezeit ein:	Eingeben…
Ein Node	`run -node node_name options cdpd.holdtime holdtime`
Alle Nodes in einem Cluster	`options cdpd.holdtime holdtime`

Stellen Sie das Intervall für das Senden von CDP-Werbeanzeigen ein

CDP-Anzeigen werden regelmäßig an CDP-Nachbarn gesendet. Sie können das Intervall für das Senden von CDP-Anzeigen in Abhängigkeit von Netzwerkverkehr und Änderungen in der Netzwerktopologie erhöhen oder verringern.

- Der Wert der `cdpd.interval` Option sollte auf beiden Nodes eines HA-Paars auf den gleichen Wert eingestellt werden.
- Das Standardintervall beträgt 60 Sekunden, Sie können jedoch einen Wert von 5 Sekunden bis 900 Sekunden eingeben.

Schritte

1. Anzeige des aktuellen CDP-Zeitintervalls für einen Knoten oder für alle Knoten in einem Cluster:

So zeigen Sie das Intervall für…	Eingeben…
Ein Node	`run -node node_name options cdpd.interval`
Alle Nodes in einem Cluster	`options cdpd.interval`

2. Konfigurieren Sie das Intervall für das Senden von CDP-Werbeanzeigen für alle Ports eines Node oder für alle Ports aller Nodes in einem Cluster:

So legen Sie das Intervall für…	Eingeben…
Ein Node	`run -node node_name options cdpd.interval interval`
Alle Nodes in einem Cluster	`options cdpd.interval interval`

CDP-Statistiken anzeigen oder löschen

Sie können die CDP-Statistiken für den Cluster und nicht-Cluster-Ports auf jedem Node anzeigen, um potenzielle Netzwerkverbindungsprobleme zu erkennen. CDP-Statistiken werden seit der letzten Freigabe

kumulativ erfasst.

Über diese Aufgabe

In ONTAP 9.10.1 und früher, da CDP immer für Ports aktiviert ist, werden CDP-Statistiken immer für Verkehr auf diesen Ports angezeigt. CDP muss auf Ports aktiviert sein, damit Statistiken für diese Ports angezeigt werden können.

In ONTAP 9.11.1 und höher, da CDP immer für Cluster- und Speicherports aktiviert ist, werden CDP-Statistiken immer für den Datenverkehr auf diesen Ports angezeigt. CDP muss auf nicht-Cluster- oder nicht-Storage-Ports aktiviert sein, damit Statistiken für diese Ports angezeigt werden können.

Schritt

Aktuelle CDP-Statistiken für alle Ports auf einem Knoten anzeigen oder löschen:

Ihr Ziel ist	Eingeben…
Zeigen Sie die CDP-Statistiken an	`run -node node_name cdpd show-stats`
Löschen Sie die CDP-Statistiken	`run -node node_name cdpd zero-stats`

Beispiel zum Anzeigen und Löschen von Statistiken

Der folgende Befehl zeigt die CDP-Statistiken vor dem Löschen an. Die Ausgabe zeigt die Gesamtanzahl der Pakete an, die seit dem letzten Löschen der Statistiken gesendet und empfangen wurden.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:        0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:          0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:     0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:         0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:    0  | Other errors:         0

OTHER
 Init failures:       0
```

Mit dem folgenden Befehl werden die CDP-Statistiken gelöscht:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

Nachdem die Statistiken gelöscht wurden, beginnen sie sich zu sammeln, nachdem die nächste CDP-Anzeige gesendet oder empfangen wurde.

Verbinden mit Ethernet-Switches, die CDP nicht unterstützen

Mehrere Switches von Anbietern unterstützen CDP nicht. Siehe die"NetApp Knowledge Base: ONTAP Geräteerkennung zeigt Knoten anstelle des Switches an" für weitere Details.

Es gibt zwei Möglichkeiten, dieses Problem zu lösen:

- Deaktivieren Sie CDP, und aktivieren Sie LLDP, falls unterstützt. Weitere Informationen finden Sie unter "Verwenden Sie LLDP, um die Netzwerkverbindung zu erkennen" .
- Konfigurieren Sie einen MAC-Adresspaketfilter auf den Switches, um CDP-Ankündigungen zu löschen.

Verwenden Sie LLDP, um ONTAP-Netzwerkverbindungen zu erkennen

Die Verwendung von LLDP zur Erkennung von Netzwerkverbindungen besteht aus der Überprüfung von Bereitstellungsüberlegungen, der Aktivierung auf allen Ports, der Anzeige von Nachbargeräten und der Anpassung der LLDP-Konfigurationswerte nach Bedarf.

LLDP muss auch auf Switches und Routern aktiviert sein, bevor Informationen zu Nachbargeräten angezeigt werden können.

ONTAP meldet derzeit folgende TLVs (Type-length-value Structures):

- Chassis-ID
- Port-ID
- Time-to-Live (TTL)
- Systemname

  Der Systemname TLV wird nicht an CNA-Geräte gesendet.

Bestimmte konvergierte Netzwerkadapter (CNAs) wie der X1143-Adapter und die UTA2 Onboard Ports

enthalten Offload-Unterstützung für LLDP:

- LLDP-Offload wird für Data Center Bridging (DCB) genutzt.
- Angezeigte Informationen können sich zwischen dem Cluster und dem Switch unterscheiden.

  Die vom Switch angezeigten Chassis-ID- und Port-ID-Daten unterscheiden sich möglicherweise von CNA- und nicht-CNA-Ports.

Beispiel:

- Für nicht-CNA-Ports:
  - Die Chassis-ID ist eine feste MAC-Adresse von einer der Ports auf dem Node
  - Die Port-ID ist der Port-Name des entsprechenden Ports auf dem Node
- Für CNA-Ports:
  - Die Chassis-ID und die Port-ID sind die MAC-Adressen der entsprechenden Ports auf dem Node.

Für diese Port-Typen sind die vom Cluster angezeigten Daten jedoch konsistent.

Die LLDP-Spezifikation definiert den Zugriff auf die gesammelten Informationen über eine SNMP-MIB. Allerdings unterstützt ONTAP derzeit nicht die LLDP MIB.

LLDP aktivieren oder deaktivieren

Um Anzeigen zu ermitteln und an LLDP-konforme benachbarte Geräte zu senden, muss LLDP auf jedem Knoten des Clusters aktiviert sein. Ab ONTAP 9.7 ist LLDP standardmäßig auf allen Ports eines Knotens aktiviert.

Über diese Aufgabe

Für ONTAP 9.10.1 und frühere Versionen `lldp.enable` steuert die Option, ob LLDP auf den Ports eines Knotens aktiviert oder deaktiviert ist:

- `on` Aktiviert LLDP auf allen Ports.
- `off` Deaktiviert LLDP an allen Ports.

Für ONTAP 9.11.1 und höher `lldp.enable` steuert die Option, ob LLDP auf den nicht-Cluster- und nicht-Speicher-Ports eines Knotens aktiviert oder deaktiviert ist:

- `on` Aktiviert LLDP auf allen nicht-Cluster- und nicht-Speicher-Ports.
- `off` Deaktiviert LLDP auf allen nicht-Cluster- und nicht-Speicher-Ports.

Schritte

1. Aktuelle LLDP-Einstellung für einen Knoten oder für alle Knoten in einem Cluster anzeigen:
   - Ein Node: `run -node node_name options lldp.enable`
   - Alle Knoten: Optionen `lldp.enable`
2. Aktivieren oder Deaktivieren von LLDP an allen Ports eines Knotens oder an allen Ports aller Knoten in einem Cluster:

So aktivieren oder deaktivieren Sie LLDP ein:	Eingeben…
Ein Node	`run -node node_name options lldp.enable {on
off}`	Alle Nodes in einem Cluster
`options lldp.enable {on	off}`

- Einzelner Node:

```
run -node node_name options lldp.enable {on|off}
```

- Alle Nodes:

```
options lldp.enable {on|off}
```

Anzeigen von LLDP-Nachbarinformationen

Sie können Informationen über die benachbarten Geräte anzeigen, die mit jedem Port des Knotens des Clusters verbunden sind, sofern der Port mit einem LLDP-kompatiblen Gerät verbunden ist. Sie verwenden den Befehl Network Device-Discovery show, um Nachbarinformationen anzuzeigen.

Schritt

1. Informationen zu allen LLDP-kompatiblen Geräten anzeigen, die mit den Ports eines Knotens im Cluster verbunden sind:

```
network device-discovery show -node node -protocol lldp
```

Mit dem folgenden Befehl werden die Nachbarn angezeigt, die mit den Ports auf dem Node „Cluster-1_01“ verbunden sind. Die Ausgabe listet die LLDP-fähigen Geräte auf, die mit jedem Port des angegebenen Knotens verbunden sind. Wenn die `-protocol` Option weggelassen wird, werden in der Ausgabe auch CDP-fähige Geräte aufgelistet.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Passen Sie das Intervall für die Übertragung von LLDP-Anzeigen an

LLDP-Anzeigen werden regelmäßig an LLDP-Nachbarn gesendet. Sie können das Intervall für das Senden von LLDP-Anzeigen in Abhängigkeit von Netzwerkverkehr und Änderungen in der Netzwerktopologie erhöhen oder verringern.

Über diese Aufgabe

Das von IEEE empfohlene Standardintervall beträgt 30 Sekunden, Sie können jedoch einen Wert von 5 Sekunden bis 300 Sekunden eingeben.

Schritte

1. Anzeige des aktuellen LLDP-Zeitintervalls für einen Knoten oder für alle Knoten in einem Cluster:
   - Einzelner Node:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - Alle Nodes:

     ```
     options lldp.xmit.interval
     ```

2. Passen Sie das Intervall für das Senden von LLDP-Werbeanzeigen für alle Ports eines Knotens oder für alle Ports aller Knoten in einem Cluster an:
   - Einzelner Node:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - Alle Nodes:

     ```
     options lldp.xmit.interval <interval>
     ```

Passen Sie den Zeitwert für LLDP-Anzeigen an

Time-to-Live (TTL) ist der Zeitraum, in dem LLDP-Anzeigen in benachbarten LLDP-kompatiblen Geräten im Cache gespeichert werden. TTL wird in jedem LLDP-Paket angekündigt und wird aktualisiert, sobald ein LLDP-Paket von einem Node empfangen wird. TTL kann in ausgehenden LLDP-Frames geändert werden.

Über diese Aufgabe

- TTL ist ein berechneter Wert, das Produkt des Übertragungsintervalls (`lldp.xmit.interval` (`lldp.xmit.hold`) und der Hold-Multiplikator) plus eins.
- Der Standardwert für Hold Multiplikator ist 4, Sie können aber Werte zwischen 1 und 100 eingeben.
- Die Standard-TTL beträgt daher 121 Sekunden, wie von IEEE empfohlen, aber durch die Anpassung des Übertragungsintervalls und die Speicherung von Multiplikatorwerten können Sie einen Wert für ausgehende Frames von 6 Sekunden auf 30001 Sekunden festlegen.
- Wenn eine IP-Adresse entfernt wird, bevor die TTL abläuft, werden die LLDP-Informationen im Cache gespeichert, bis die TTL abläuft.

Schritte

1. Zeigt den aktuellen Hold-Multiplikator-Wert für einen Node oder für alle Nodes in einem Cluster an:
   - Einzelner Node:

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - Alle Nodes:

     ```
     options lldp.xmit.hold
     ```

2. Passen Sie den Hold-Multiplikator-Wert an alle Ports eines Knotens oder auf allen Ports aller Knoten in einem Cluster an:
   - Einzelner Node:

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - Alle Nodes:

     ```
     options lldp.xmit.hold <hold_value>
     ```

LLDP-Statistiken anzeigen oder löschen

Sie können die LLDP-Statistiken für den Cluster und nicht-Cluster-Ports auf jedem Node anzeigen, um potenzielle Netzwerkverbindungsprobleme zu erkennen. LLDP-Statistiken werden seit der letzten Freigabe kumulativ erfasst.

Über diese Aufgabe

Für ONTAP 9.10.1 und früher, da LLDP immer für Cluster-Ports aktiviert ist, werden LLDP-Statistiken immer für

den Verkehr auf diesen Ports angezeigt. LLDP muss auf nicht-Cluster-Ports aktiviert sein, damit Statistiken für diese Ports angezeigt werden können.

Für ONTAP 9.11.1 und höher, da LLDP immer für Cluster- und Speicherports aktiviert ist, werden LLDP-Statistiken immer für den Datenverkehr auf diesen Ports angezeigt. LLDP muss auf nicht-Cluster- und nicht-Speicherports aktiviert sein, damit Statistiken für diese Ports angezeigt werden können.

Schritt

Aktuelle LLDP-Statistiken für alle Ports auf einem Knoten anzeigen oder löschen:

Ihr Ziel ist	Eingeben…
Zeigen Sie die LLDP-Statistiken an	`run -node node_name lldp stats`
Löschen Sie die LLDP-Statistiken	`run -node node_name lldp stats -z`

Beispiel für das Anzeigen und Löschen von Statistiken

Der folgende Befehl zeigt die LLDP-Statistiken vor dem Löschen an. Die Ausgabe zeigt die Gesamtanzahl der Pakete an, die seit dem letzten Löschen der Statistiken gesendet und empfangen wurden.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

Mit dem folgenden Befehl werden die LLDP-Statistiken gelöscht.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

Nachdem die Statistiken gelöscht wurden, beginnen sie sich zu sammeln, nachdem die nächste LLDP-Anzeige

gesendet oder empfangen wurde.