Logische Schnittstellen (LIFs)

ONTAP 9

NetApp
February 12, 2026

Inhalt

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:

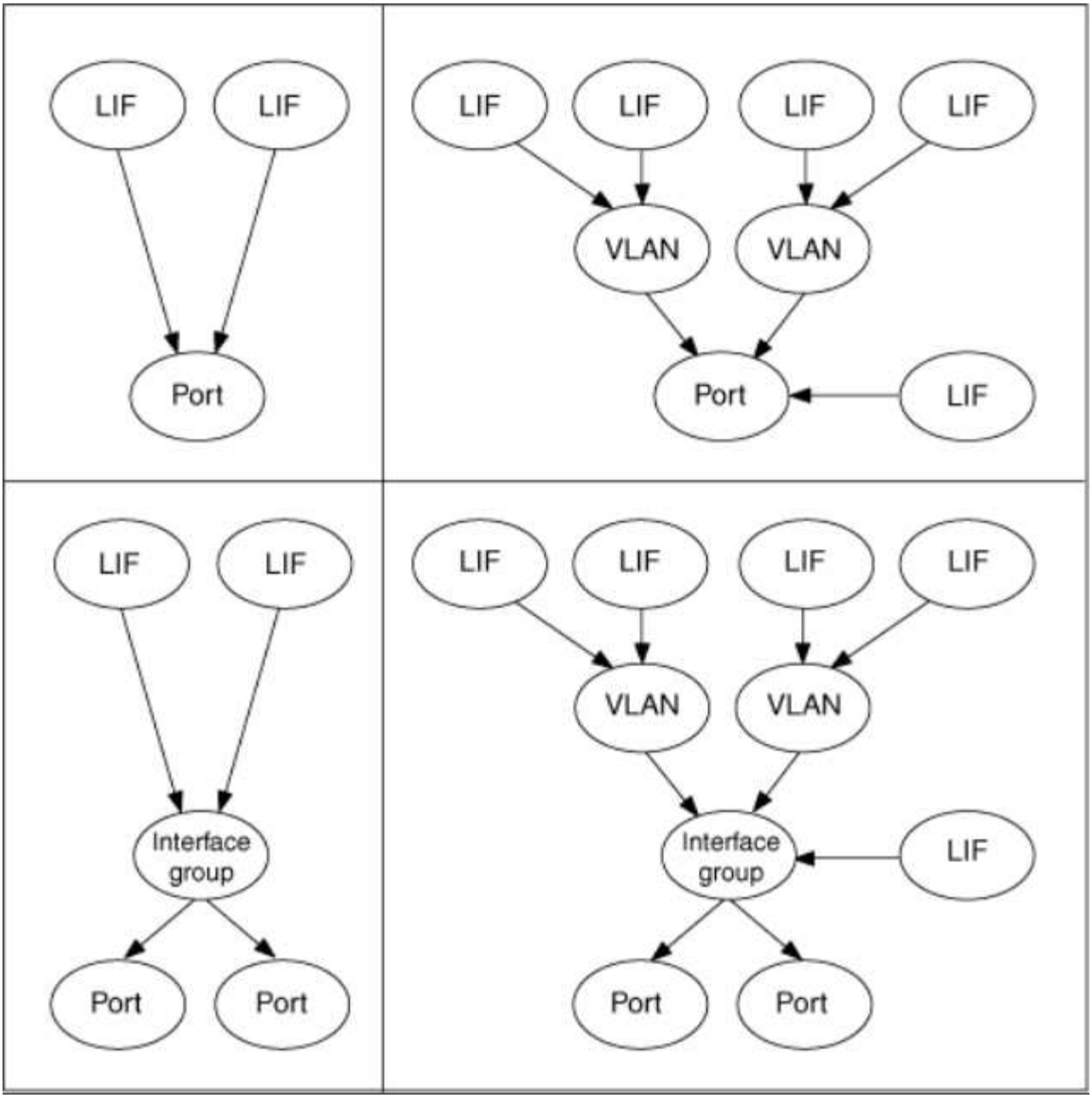
- Physische Ports, die nicht zu Interface Groups gehören
- Interface Groups
- VLANs
- Physische Ports oder Schnittstellengruppen, die VLANs hosten
- Virtuelle IP-Ports (VIP)

  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"