



Konfigurieren von Netzwerkports (nur Cluster-Administratoren)

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- Konfigurieren von Netzwerkports (nur Cluster-Administratoren) 1
 - Überblick 1
 - Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen 1
 - Konfigurieren Sie VLANs über physische Ports 11
 - Netzwerkanschlussattribute ändern 15
 - MTU-Einstellung für Schnittstellengruppen-Ports ändern 16
 - Überwachen Sie den Systemzustand von Netzwerk-Ports 17
 - Überwachen Sie die Erreichbarkeit von Netzwerkports in ONTAP 9.8 und höher 19
 - Konvertieren Sie 40-GbE-NIC-Ports für 10-GbE-Konnektivität in mehrere 10-GbE-Ports 22
 - Entfernen einer NIC aus dem Knoten auf ONTAP 9.7 oder früher 23
 - Entfernen einer NIC aus dem Knoten auf ONTAP 9.8 oder höher 23

Konfigurieren von Netzwerkports (nur Cluster-Administratoren)

Überblick

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.

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

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

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

`vlan-id` Gibt die VLAN-ID im Netzwerk an. Beispiel: e1c-80 Ist ein gültiger VLAN-Name.

Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen

Eine Interface Group, auch als Link Aggregation Group (LAG) bekannt, wird erstellt, indem zwei oder mehr physische Ports in 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.

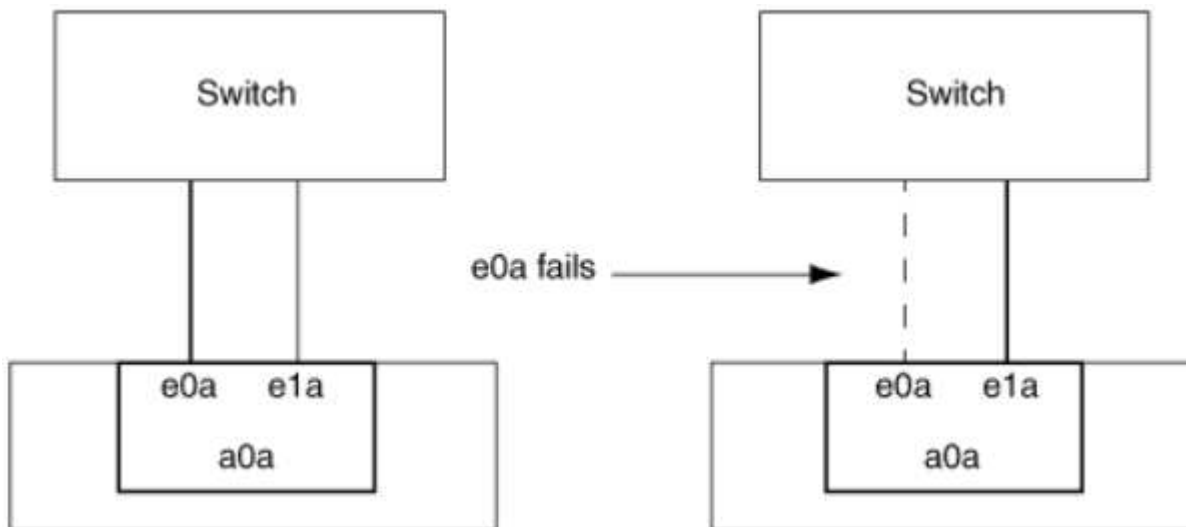
Merkmale von Single-Mode-Schnittstellengruppen

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

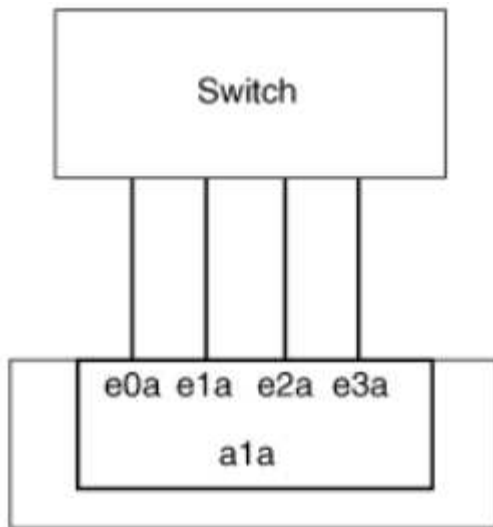
Die Implementierung der statischen Multimode-Schnittstellengruppen in ONTAP entspricht IEEE 802.3ad (statisch). Jeder Switch, der Aggregate unterstützt, aber keinen Austausch von Kontrollpaketen zur Konfiguration eines Aggregats bietet, kann mit statischen Multimode-Schnittstellengruppen verwendet werden.

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.

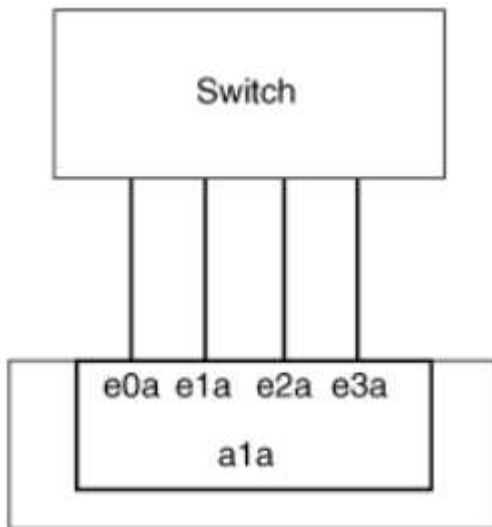
Der ONTAP-Load-Balancing-Algorithmus bestimmt den Mitgliedsport, der für die Übertragung von Outbound-Datenverkehr verwendet werden soll, und steuert nicht, wie eingehende Frames empfangen werden. Der Switch bestimmt das Mitglied (individueller physischer Port) seiner Port-Channel-Gruppe, das für die 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-Lastausgleichsmethoden 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-Schnittstellengruppen gleichermaßen für ausgehenden Datenverkehr genutzt werden, indem Sie IP-Adressen, MAC-Adressen, sequenzielle oder portbasierte Lastausgleichsmethoden verwenden, um den Netzwerkverkehr gleichmäßig über die Netzwerkanschlüsse einer Multimode-Schnittstellengruppen 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 Lastausgleichsmethode 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 Lastausgleichsmethoden 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 sequenzieller 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.

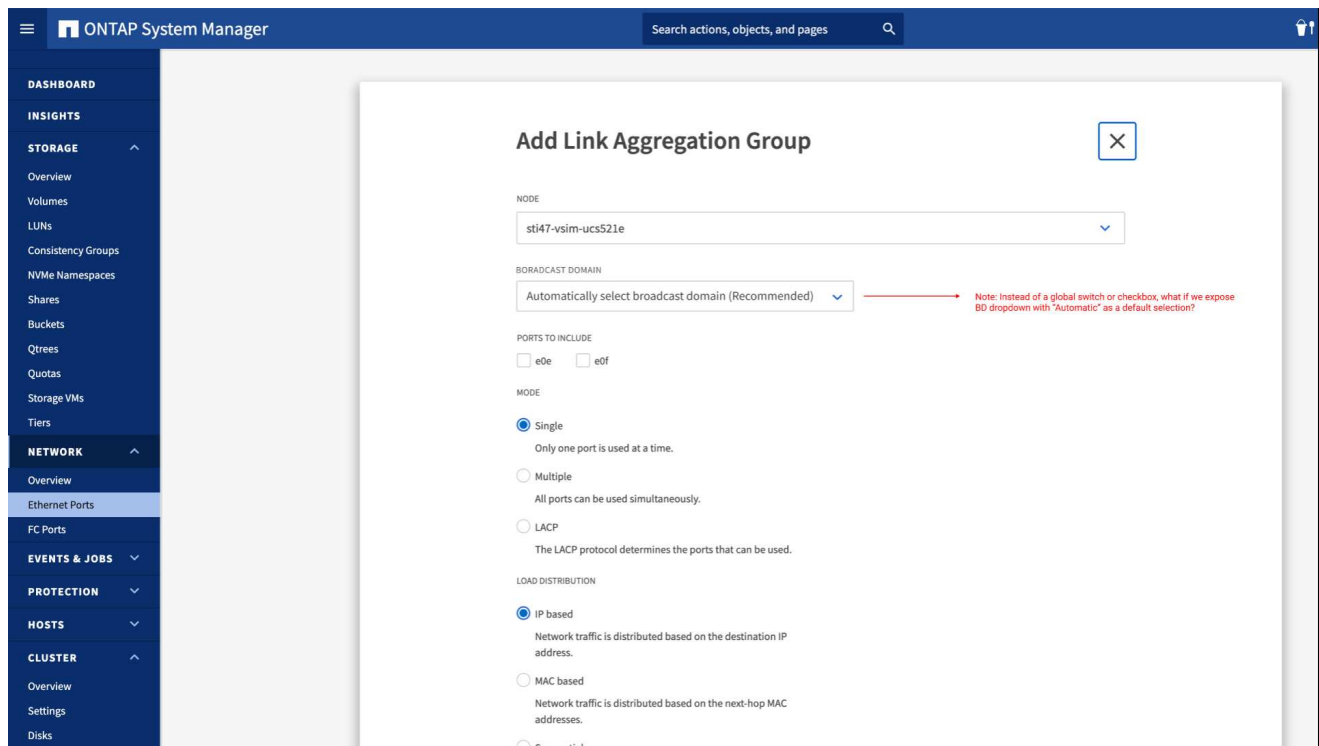
Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

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

Eine vollständige Liste der Konfigurationseinschränkungen, die für Portschnittstellen-Gruppen gelten, finden Sie im `network port ifgrp add-port` Man-Page.

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

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

Verwenden Sie die `network port ifgrp create` Befehl zum Erstellen einer Schnittstellengruppe.

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

Weitere Informationen zu diesem Befehl finden Sie unter "[ONTAP 9-Befehle](#)".

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
```

Weitere Informationen zu diesem Befehl finden Sie unter ["ONTAP 9-Befehle"](#).

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 ONTAP dies nicht tun soll und Sie das ifgrp lieber manuell in eine Broadcast-Domäne platzieren möchten, geben Sie das an `-skip-broadcast-domain-placement` Parameter als Teil des `ifgrp add-port` Befehl.

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
```

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

Verwenden Sie die `network port ifgrp delete` Befehl zum Löschen einer Schnittstellengruppe.

Weitere Informationen zu diesem Befehl finden Sie unter "[ONTAP 9-Befehle](#)".

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

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

Konfigurieren Sie VLANs über physische Ports

VLANs ermöglichen eine logische Segmentierung von Netzwerken, indem separate Broadcast-Domänen erstellt werden, die auf Switch-Port-Basis definiert sind, im Gegensatz zu herkömmlichen Broadcast-Domänen, die über physische Grenzen definiert sind.

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 geschichteten Netzwerk enthalten.

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 ein VLAN

Sie können ein VLAN erstellen, um separate Broadcast-Domänen innerhalb derselben Netzwerkdomäne zu unterhalten, indem Sie System Manager oder die verwenden `network port vlan create` Befehl.

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 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 beeinträchtigten Port erstellen möchten, ohne das Hardwareproblem oder die falsche Softwarekonfiguration zu beheben, können Sie den festlegen `-ignore-health-status` Parameter von `network port modify` Befehl als `true`.

Schritte

1. Verwenden Sie die `network port vlan create` Befehl zum Erstellen eines VLAN.
2. Sie müssen einen der angeben `vlan-name` Oder im `port` Und `vlan-id` Optionen beim Erstellen eines VLANs. Der VLAN-Name ist eine Kombination aus dem Namen des Ports (oder der Schnittstellengruppe) und der Netzwerk-Switch-VLAN-ID, mit einem Bindestrich dazwischen. Beispiel: `e0c-24` Und `e1c-80` Sind gültige VLAN-Namen.

Das folgende Beispiel zeigt, wie ein VLAN erstellt wird `e1c-80` An Netzwerk-Port angeschlossen `e1c` Auf dem Node `cluster-1-01`:

```
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 ONTAP dies nicht tun soll und das VLAN lieber manuell in eine Broadcast-Domäne platziert werden soll, geben Sie das an `-skip-broadcast-domain-placement` Parameter als Teil des `vlan create` Befehl.

Weitere Informationen zu diesem Befehl finden Sie unter ["ONTAP 9-Befehle"](#).

Bearbeiten Sie ein VLAN

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 Sie ein 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 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 die `network port vlan delete` Befehl zum Löschen eines VLANs.

Das folgende Beispiel zeigt, wie das VLAN gelöscht wird `e1c-80` Vom Netzwerk-Port `e1c` Auf dem Node `cluster-1-01`:

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

Netzwerkanschlussattribute ändern

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 einzustellen `-up-admin` Administratoreinstellung auf „false“ für alle Ports auf einem Node oder für den Port, der die letzte logische Cluster-LIF auf einem Node hostet.
- 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 die einstellen `-ignore-health-status` Feld zu „true“, 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 von Cluster-Ports auf einstellen `none`. Standardmäßig ist die Flusssteuerung auf festgelegt `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
```

MTU-Einstellung für Schnittstellengruppen-Ports ändern

Um die MTU-Einstellung für Schnittstellengruppen zu ändern, müssen Sie die MTU der Broadcast-Domäne ändern.

Die VLAN-MTU-Größe sollte mit der MTU der Broadcast-Domäne der zugrunde liegenden Schnittstellengruppen und physischen Ports übereinstimmen. Wenn für ein VLAN eine andere VLAN-Einstellung erforderlich ist, darf diese die von der zugrunde liegenden Broadcast-Domäne angegebene Größe nicht überschreiten.

Schritte

1. Ändern Sie die Einstellungen für die Broadcast-Domäne:

```
broadcast-domain modify -broadcast-domain broadcast_domain_name -mtu  
mtu_setting
```

Die folgende Warnmeldung wird angezeigt:

```
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: y
```

2. Geben Sie `y` ein, um fortzufahren.
3. Überprüfen Sie, ob die MTU-Einstellung korrekt geändert wurde:

```
network port show
```

```

network port show
(network port show)
Node: vsim-01

                                     Ignore
                                     Speed (Mbps) Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status
-----
a0a Default Default-1 up 1300 auto/1000 healthy false
e0a Default Default-1 up 1300 auto/1000 healthy false
e0b Default Default up 1500 auto/1000 healthy false
e0c Default Default up 1500 auto/1000 healthy false
e0d Default Default up 1500 auto/1000 healthy false
5 entries were displayed.

```

Überwachen Sie den Systemzustand von Netzwerk-Ports

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 Erreichbarkeit 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 den ändern `ignore-health-status` Einstellen des Netzwerkports auf `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.

3. Aktivieren oder deaktivieren Sie eine der Integritätsmonitore für einen IPspace nach Bedarf mithilfe des `network options port-health-monitor modify` Befehl.

4. Anzeigen des detaillierten Systemzustands eines Ports:

```
network port show -health
```

In der Ausgabe des Befehls wird der Systemzustand des Ports angezeigt, `ignore health status` Einstellung und eine Liste der Gründe, warum der Port als beeinträchtigt gekennzeichnet ist.

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

Wenn der `ignore health status` Einstellung lautet `true`, Zeigt an, dass der Status des Ports von geändert wurde `degraded` Bis `healthy` Vom Administrator.

Wenn der `ignore health status` Einstellung lautet `false`, Der Zustand des Ports wird automatisch vom System ermittelt.

Überwachen Sie die Erreichbarkeit von Netzwerkports in ONTAP 9.8 und höher

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

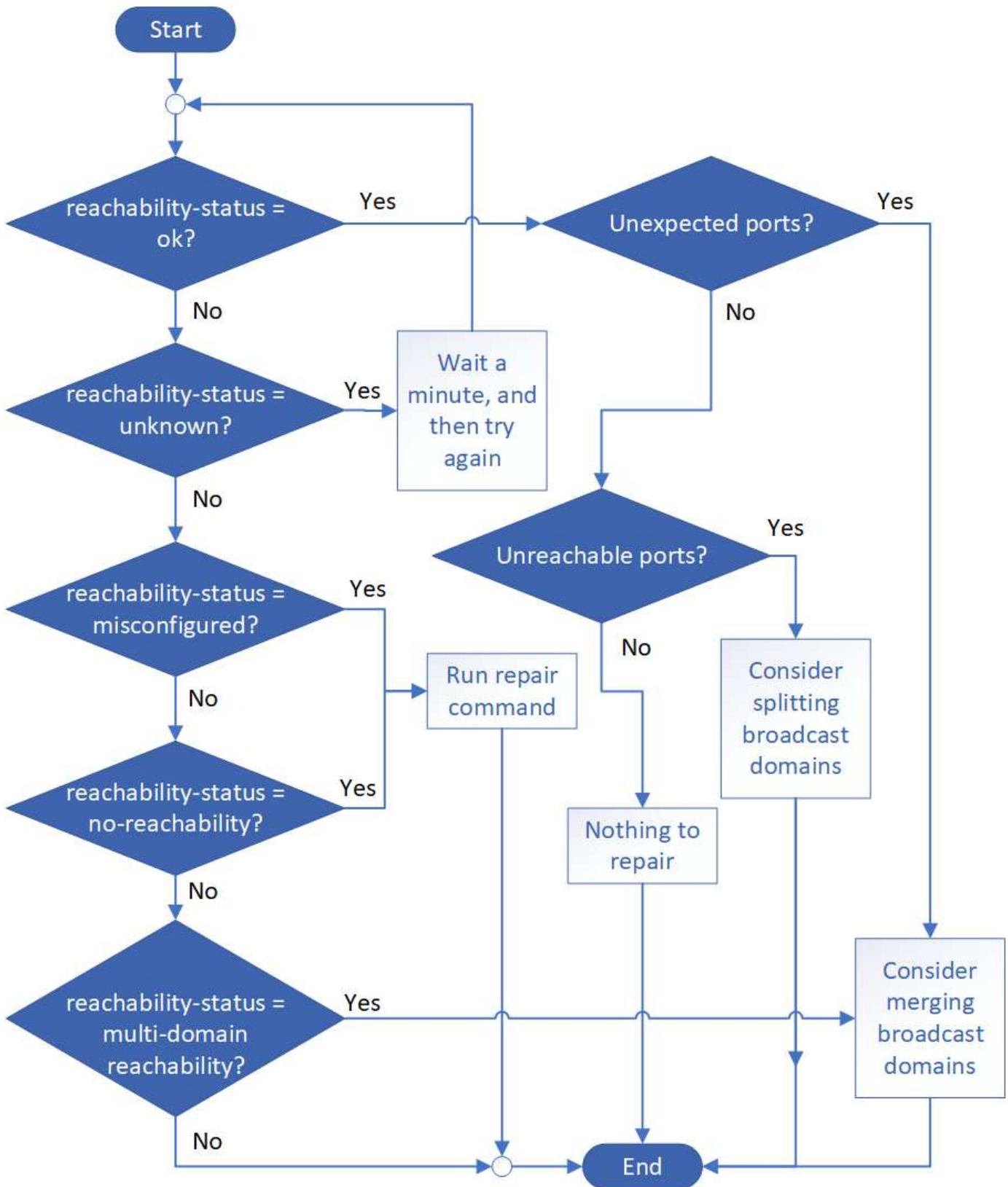
Verwenden Sie diese Befehle, um Fehlkonfigurationen in Netzwerken zu überprüfen, zu diagnostizieren und zu reparieren, die aus der ONTAP Konfiguration stammen und weder mit der physischen Verkabelung noch mit der Netzwerk-Switch-Konfiguration übereinstimmen.

Schritt

1. Port-Erreichbarkeit anzeigen:

```
network port reachability show
```

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



Erreichbarkeit-Status	Beschreibung
-----------------------	--------------

ok	<p>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 „<i>Unexpected Ports</i>“.</p> <p>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 <i>Unerreichbare Ports</i>.</p> <p>Wenn der Status „Erreichbarkeit“ „ok“ lautet und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist die Konfiguration korrekt.</p>
Unerwartete Ports	<p>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.</p> <p>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.</p> <p>Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen".</p>
Nicht erreichbare Ports	<p>Wenn eine einzelne Broadcast-Domäne in zwei unterschiedliche Wiederachabilitäts-Sets partitioniert wurde, können Sie eine Broadcast-Domäne teilen, um die ONTAP-Konfiguration mit der physischen Netzwerktopologie zu synchronisieren.</p> <p>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.</p> <p>Weitere Informationen finden Sie unter "Teilen von Broadcast-Domänen auf".</p>
Falsch konfigurierte Erreichbarkeit	<p>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.</p> <p>Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port der Broadcast-Domäne zu, der sie nachzuweisen kann:</p> <p><code>`network port reachability repair -node -port`</code> Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".</p>
Keine Erreichbarkeit	<p>Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit für eine vorhandene Broadcast-Domäne.</p> <p>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:</p> <p><code>`network port reachability repair -node -port`</code> Weitere Informationen finden Sie unter "Port-Erreichbarkeit reparieren".</p>

Multi-Domain-Erreichbarkeit	<p>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.</p> <p>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.</p> <p>Weitere Informationen finden Sie unter "Broadcast-Domänen zusammenführen" Oder "Port-Erreichbarkeit reparieren".</p>
Unbekannt	<p>Wenn der Status „unbekannt“ lautet, warten Sie einige Minuten, und versuchen Sie den Befehl erneut.</p>

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"](#).

Konvertieren Sie 40-GbE-NIC-Ports für 10-GbE-Konnektivität in mehrere 10-GbE-Ports

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.

Entfernen einer NIC aus dem Knoten auf ONTAP 9.7 oder früher

Dieses Thema bezieht sich auf ONTAP 9.7 oder früher. Sie müssen möglicherweise eine fehlerhafte NIC aus ihrem Steckplatz entfernen oder die NIC zu Wartungszwecken in einen anderen Steckplatz verschieben.

Bevor Sie beginnen

- Alle auf den NIC-Ports gehosteten LIFs müssen migriert oder gelöscht wurden.
- Bei den NIC-Ports kann es sich nicht um die Home-Ports beliebiger LIFs befinden.
- Sie müssen über erweiterte Berechtigungen verfügen, um die Ports von einer NIC löschen zu können.

Schritte

1. Löschen Sie die Ports aus der NIC:

```
network port delete
```

2. Überprüfen Sie, ob die Ports gelöscht wurden:

```
network port show
```

3. Wiederholen Sie Schritt 1, wenn in der Ausgabe des Befehls „Network Port show“ der gelöschte Port angezeigt wird.

Entfernen einer NIC aus dem Knoten auf ONTAP 9.8 oder höher

Dieses Thema bezieht sich auf ONTAP 9.8 oder höher. Sie müssen möglicherweise eine fehlerhafte NIC aus ihrem Steckplatz entfernen oder die NIC zu Wartungszwecken in einen anderen Steckplatz verschieben.

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.

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
```



Der `displaced-interface show`, `displaced-vlans show`, und `displaced-vlans restore` Befehle sind eindeutig. Sie benötigen keinen vollqualifizierten Befehlsnamen, der mit `cluster controller-replacement network` beginnt.

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 `network interface modify -home-port -home-node` oder use the `displaced-interface restore` Befehl.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.