Netzwerk-Ports konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/networking/combine_physical_ports_to_create_interface_groups.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Netzwerk-Ports konfigurieren . . . 1
Physische Ports können kombiniert werden, um ONTAP Schnittstellengruppen zu erstellen. . . . 1
Schnittstellengruppentypen . . . 1
Eine Schnittstellengruppe oder LAG erstellen . . . 5
Einen Port zu einer Schnittstellengruppe oder einem LAG hinzufügen . . . 7
Einen Port aus einer Schnittstellengruppe oder einem LAG entfernen . . . 7
Eine Schnittstellengruppe oder LAG löschen . . . 8
ONTAP VLANs über physische Ports konfigurieren . . . 9
Eine VLAN erstellen . . . 9
Bearbeiten einer VLAN . . . 11
Löschen eines VLAN . . . 11
ONTAP Netzwerkportattribute ändern . . . 12
10GbE-Ports für ONTAP Netzwerke durch Konvertierung von 40GbE-NIC-Ports erstellen . . . 13
UTA X1143A-R6 Ports für das ONTAP Netzwerk konfigurieren . . . 14
Den UTA2-Port für die Verwendung im ONTAP Netzwerk konvertieren . . . 15
Die optischen Module CNA/UTA2 für das ONTAP Netzwerk konvertieren . . . 16
Netzwerkkarten aus ONTAP Clusterknoten entfernen . . . 17
Netzwerkports überwachen . . . 18
Den Zustand der ONTAP Netzwerkports überwachen . . . 18
Überwachung der Erreichbarkeit von ONTAP Netzwerk-Ports . . . 20
ONTAP Port-Nutzung auf einem Speichersystem . . . 23
ONTAP interne Ports . . . 26

Netzwerk-Ports konfigurieren

Physische Ports können kombiniert werden, um ONTAP Schnittstellengruppen zu erstellen.

Eine Schnittstellengruppe, auch Link-Aggregation-Gruppe (LAG) genannt, entsteht durch die Zusammenfassung von zwei oder mehr physischen Ports desselben Knotens zu einem einzigen logischen Port. Der logische Port bietet erhöhte Ausfallsicherheit, höhere Verfügbarkeit und Lastverteilung.

Schnittstellengruppentypen

Das Speichersystem unterstützt drei Arten von Schnittstellengruppen: Single-Mode, statischer Multimode und Dynamisches Multimode. Jede Schnittstellengruppe bietet unterschiedliche Stufen der Fehlertoleranz. Multimode-Schnittstellengruppen bieten Methoden zum Lastausgleich des Netzwerkverkehrs.

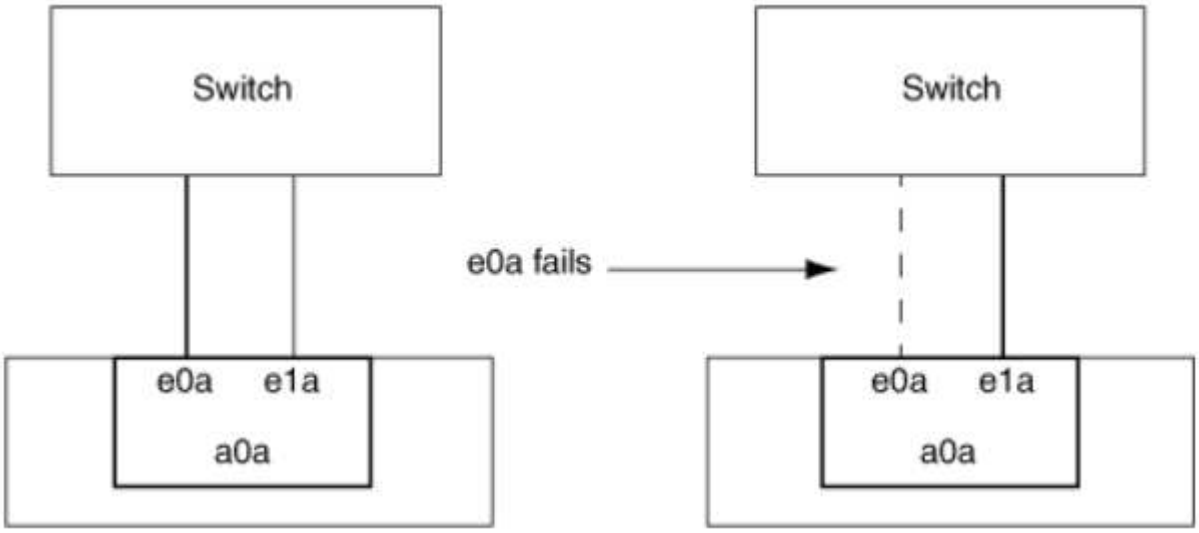
Merkmale von Einzelmodus-Schnittstellengruppen

In einer Singlemode Schnittstellengruppe ist nur eine der Schnittstellen in der Schnittstellengruppe aktiv. Die anderen Schnittstellen sind im Standby und bereit, die aktive Schnittstelle zu übernehmen, falls diese ausfällt.

Merkmale von Einzelmodus-Schnittstellengruppen:

- Im Fehlerfall überwacht der Cluster die aktive Verbindung und steuert den Failover. Da der Cluster die aktive Verbindung überwacht, ist keine Switch-Konfiguration erforderlich.
- In einer Einzelmodus-Schnittstellengruppe kann mehr als eine Schnittstelle im Standby sein.
- Wenn sich eine Single-Mode Schnittstellengruppe über mehrere Switches erstreckt, ist eine Verbindung der Switches mit einer Inter-Switch-Verbindung (ISL) erforderlich.
- Für eine Singlemode Schnittstellengruppe müssen sich die Switch-Ports im selben Broadcast-Domäne befinden.
- Link-Monitoring-ARP-Pakete mit der Quelladresse 0.0.0.0 werden über die Ports gesendet, um zu überprüfen, ob sich die Ports in derselben Broadcast-Domäne befinden.

Die folgende Abbildung zeigt ein Beispiel einer Singlemode Schnittstellengruppe. In der Abbildung gehören e0a und e1a zur a0a Singlemode Schnittstellengruppe. Wenn die aktive Schnittstelle e0a ausfällt, übernimmt die Standby-Schnittstelle e1a und hält die Verbindung zum Switch aufrecht.



Um die Einzelmodus-Funktionalität zu erreichen, wird stattdessen die Verwendung von Failover-Gruppen empfohlen. Durch die Verwendung einer Failover-Gruppe kann der zweite Port weiterhin für andere LIFs genutzt werden und muss nicht ungenutzt bleiben. Zusätzlich können Failover-Gruppen mehr als zwei Ports umfassen und Ports auf mehreren Nodes einschließen.

Merkmale statischer Multimode Schnittstellengruppen

Die Implementierung der statischer Multimode Schnittstellengruppe in ONTAP entspricht IEEE 802.3ad (statisch). Jeder Switch, der Aggregate unterstützt, aber keinen Kontrollpaketaustausch zur Konfiguration eines Aggregats ermöglicht, kann mit statischer Multimode Schnittstellengruppe verwendet werden.

Statische Multimode Schnittstellengruppen entsprechen nicht IEEE 802.3ad (dynamisch), auch bekannt als Link Aggregation Control Protocol (LACP). LACP ist äquivalent zum Port Aggregation Protocol (PAgP), dem proprietären Link Aggregation Protokoll von Cisco.

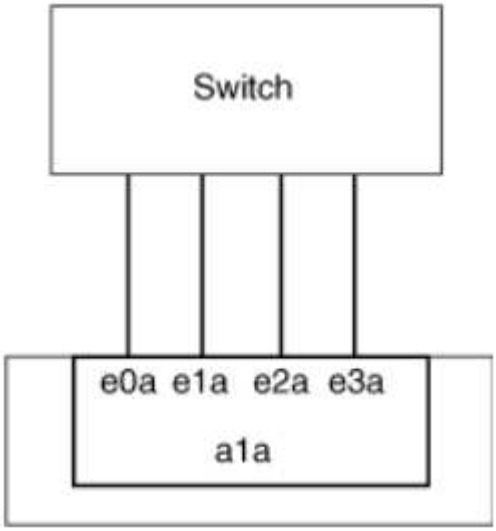
Folgende Merkmale kennzeichnen eine statische Multimode Schnittstellengruppe:

- Alle Schnittstellen in der Schnittstellengruppe sind aktiv und teilen sich eine einzige MAC-Adresse.
  - Mehrere Einzelverbindungen werden auf die Schnittstellen in der Schnittstellengruppe verteilt.
  - Jede Verbindung oder Sitzung nutzt eine Schnittstelle innerhalb der Schnittstellengruppe. Beim sequenziellen Lastverteilungsschema werden alle Sitzungen paketweise auf die verfügbaren Verbindungen verteilt und sind nicht an eine bestimmte Schnittstelle der Schnittstellengruppe gebunden.
- Statische Multimode Schnittstellengruppen können sich von einem Ausfall von bis zu "n-1" Schnittstellen erholen, wobei n die Gesamtzahl der Schnittstellen ist, die die Schnittstellengruppe bilden.
- Wenn ein Port ausfällt oder getrennt wird, wird der Datenverkehr, der über die ausgefallene Verbindung lief, automatisch auf eine der verbleibenden Schnittstellen umverteilt.
- Statische Multimode Schnittstellengruppen können einen Link-Verlust erkennen, jedoch keinen Verbindungsverlust zum Client oder Switch-Fehlkonfigurationen, die sich auf Konnektivität und Performance auswirken könnten.
- Eine statische Multimode Schnittstellengruppe erfordert einen Switch, der Link-Aggregation über mehrere Switch-Ports unterstützt. Der Switch ist so konfiguriert, dass alle Ports, an die Links einer Schnittstellengruppe angeschlossen sind, Teil eines einzigen logischen Ports sind. Einige Switches unterstützen möglicherweise keine Link-Aggregation von Ports, die für Jumbo Frames konfiguriert sind.

Weitere Informationen enthält die Dokumentation Ihres Switch-Herstellers.

- Mehrere Load-Balancing-Optionen stehen zur Verfügung, um den Datenverkehr auf die Schnittstellen einer statischer Multimode Schnittstellengruppe zu verteilen.

Die folgende Abbildung zeigt ein Beispiel einer statischen Multimode Schnittstellengruppe. Die Schnittstellen e0a, e1a, e2a und e3a gehören zur a1a Multimode Schnittstellengruppe. Alle vier Schnittstellen der a1a Multimode Schnittstellengruppe sind aktiv.



Es gibt verschiedene Technologien, die es ermöglichen, den Datenverkehr in einer einzelnen aggregierten Verbindung auf mehrere physische Switches zu verteilen. Die zur Ermöglichung dieser Funktion verwendeten Technologien variieren je nach Netzwerkprodukt. Statische Multimode Schnittstellengruppen in ONTAP entsprechen den IEEE 802.3 Standards. Wenn eine bestimmte Multiple Switch Link-Aggregation-Technologie mit den IEEE 802.3 Standards interoperiert oder diesen entspricht, sollte sie mit ONTAP funktionieren.

Der IEEE 802.3-Standard legt fest, dass das sendende Gerät in einer aggregierten Verbindung die physikalische Schnittstelle für die Übertragung bestimmt. Daher ist ONTAP nur für die Verteilung des ausgehenden Datenverkehrs zuständig und kann nicht steuern, wie eingehende Frames ankommen. Wenn die Übertragung des eingehenden Datenverkehrs in einer aggregierten Verbindung verwaltet oder gesteuert werden soll, muss diese Übertragung auf dem direkt angeschlossenen Netzwerkgerät angepasst werden.

Dynamische Multimode Schnittstellengruppe

Dynamische Multimode-Schnittstellengruppen implementieren das Link Aggregation Control Protocol (LACP), um die Gruppenzugehörigkeit an den direkt angeschlossenen Switch zu übermitteln. LACP ermöglicht die Erkennung von Verbindungsverlusten und der Unfähigkeit des Knotens, mit dem direkt angeschlossenen Switch-Port zu kommunizieren.

Die Implementierung der Dynamisches Multimode Schnittstellengruppe in ONTAP entspricht IEEE 802.3 AD (802.1 AX). ONTAP unterstützt das Port Aggregation Protocol (PAgP) nicht, ein proprietäres Link-Aggregation-Protokoll von Cisco.

Eine Dynamische Multimode Schnittstellengruppe erfordert einen Switch, der LACP unterstützt.

ONTAP implementiert LACP im nicht konfigurierbaren aktiven Modus, der gut mit Switches funktioniert, die entweder im aktiven oder passiven Modus konfiguriert sind. ONTAP implementiert die langen und kurzen LACP-Timer (zur Verwendung mit den nicht konfigurierbaren Werten 3 Sekunden und 90 Sekunden), wie in IEEE 802.3 AD (802.1AX) spezifiziert.

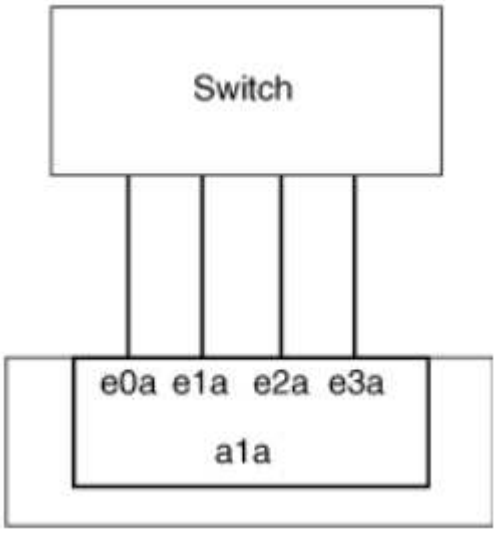
Der ONTAP Algorithmus zur Lastverteilung bestimmt den Mitgliedsport, der für die Übertragung ausgehenden Datenverkehrs verwendet wird, und steuert nicht, wie eingehende Frames empfangen werden. Der Switch bestimmt das Mitglied (den einzelnen physischen Port) seiner Portkanalgruppe, das für die Übertragung verwendet wird, basierend auf dem in der Portkanalgruppe des Switch konfigurierten Lastverteilungsalgorithmus. Daher legt die Switch-Konfiguration fest, welcher Mitgliedsport (einzelner physischer Port) des Speichersystems den Datenverkehr empfängt. Weitere Informationen zur Konfiguration des Switch finden sich in der Dokumentation Ihres Switch-Anbieters.

Wenn eine einzelne Schnittstelle keine aufeinanderfolgenden LACP-Protokollpakete empfängt, wird diese einzelne Schnittstelle in der Ausgabe des Befehls "ifgrp status" als "lag_inactive" markiert. Bestehender Datenverkehr wird automatisch auf alle verbleibenden aktiven Schnittstellen umgeleitet.

Für die Verwendung von Dynamisches Multimode Schnittstellengruppen gelten die folgenden Regeln:

- Dynamische Multimode Schnittstellengruppen sollten so konfiguriert werden, dass sie die Port-basierte, IP-basierte, MAC-basierte oder Round-Robin-Lastverteilungsmethode verwenden.
- In einer Dynamischen Multimode Schnittstellengruppe müssen alle Schnittstellen aktiv sein und eine gemeinsame MAC-Adresse verwenden.

Die folgende Abbildung zeigt ein Beispiel einer Dynamischen Multimode Schnittstellengruppe. Die Schnittstellen e0a, e1a, e2a und e3a gehören zur a1a Multimode Schnittstellengruppe. Alle vier Schnittstellen der a1a Dynamischen Multimode Schnittstellengruppe sind aktiv.



Lastausgleich in Multimode Schnittstellengruppen

Es kann sichergestellt werden, dass alle Schnittstellen einer Multimode Schnittstellengruppe gleichermaßen für ausgehenden Datenverkehr genutzt werden, indem die Methoden des IP-Adressen-, MAC-Adressen-, sequenziellen oder Port-basierten Lastausgleichs verwendet werden, um den Netzwerkverkehr gleichmäßig auf die Netzwerkports einer Multimode Schnittstellengruppe zu verteilen.

Die Methode zum Lastausgleich für eine Multimode Schnittstellengruppe kann nur bei der Erstellung der Schnittstellengruppe festgelegt werden.

Best Practice: Port-basiertes Load Balancing wird nach Möglichkeit empfohlen. Port-basiertes Load Balancing sollte verwendet werden, es sei denn, es liegt ein spezifischer Grund oder eine Einschränkung im Netzwerk vor, die dies verhindert.

Port-basierter Lastausgleich

Port-basierter Lastausgleich ist die empfohlene Methode.

Sie können den Datenverkehr auf einer Multimode Schnittstellengruppe basierend auf den Transportschicht-Ports (TCP/UDP) mithilfe der Port-basierten Lastverteilungsmethode ausgleichen.

Die Port-basierte Lastverteilungsmethode verwendet einen schnellen Hashing-Algorithmus für die Quell- und Ziel-IP-Adressen sowie die Portnummer der Transportschicht.

Lastverteilung von IP-Adresse und MAC-Adresse

Die Lastverteilung über IP-Adresse und MAC-Adresse sind die Methoden zur Angleichung des Datenverkehrs auf Multimode-Schnittstellengruppen.

Diese Lastverteilungsverfahren nutzen einen schnellen Hash-Algorithmus für die Quell- und Zieladressen (IP-Adresse und MAC-Adresse). Wenn das Ergebnis des Hash-Algorithmus einer Schnittstelle zugeordnet wird, die sich nicht im UP-Link-State befindet, wird die nächste aktive Schnittstelle verwendet.

> Die MAC-Adress-Lastverteilungsmethode sollte beim Erstellen von Schnittstellengruppen auf einem System, das direkt mit einem Router verbunden ist, nicht ausgewählt werden. In einer solchen Konfiguration ist bei jedem ausgehenden IP-Frame die Ziel-MAC-Adresse die MAC-Adresse des Routers. Dadurch wird nur eine Schnittstelle der Schnittstellengruppe verwendet.

Die Lastverteilung von IP-Adressen funktioniert für IPv4- und IPv6-Adressen auf die gleiche Weise.

Sequenzieller Lastausgleich

Sie können sequenzielles Load Balancing verwenden, um Pakete mithilfe eines Round-Robin-Algorithmus gleichmäßig auf mehrere Verbindungen zu verteilen. Die sequenzielle Option ermöglicht das Load Balancing des Datenverkehrs einer einzelnen Verbindung über mehrere Verbindungen, um den Durchsatz dieser Verbindung zu erhöhen.

Da sequenzieller Lastausgleich jedoch zu einer falschen Reihenfolge der Paketzustellung führen kann, kann dies eine extrem schlechte Leistung zur Folge haben. Daher wird sequenzieller Lastausgleich im Allgemeinen nicht empfohlen.

Eine Schnittstellengruppe oder LAG erstellen

Es besteht die Möglichkeit, eine Schnittstellengruppe oder LAG (Single-Mode, statischer Multimode oder Dynamisches Multimode (LACP)) zu erstellen, um durch die Kombination der Fähigkeiten der aggregierten Netzwerkports eine einzige Schnittstelle für Clients bereitzustellen.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager ein LAG erstellen

Schritte

1. **Netzwerk > Ethernet port > + Link Aggregation Group** auswählen, um eine LAG zu erstellen.
2. Den Knoten aus der Dropdown-Liste auswählen.
3. Wählen Sie aus den folgenden Optionen:

a. ONTAP auf **Automatische Auswahl der Broadcast-Domäne (empfohlen)**.
b. Manuelle Auswahl einer Broadcast-Domäne.

4. Wählen Sie die Ports aus, die das LAG bilden.
5. Modus auswählen:
   a. Einzeln: Es wird jeweils nur ein Port verwendet.
   b. Mehrere: Alle Ports können gleichzeitig verwendet werden.
   c. LACP: Das LACP-Protokoll legt die Ports fest, die verwendet werden können.
6. Lastverteilung auswählen:
   a. IP-basiert
   b. MAC-basiert
   c. Port
   d. Sequentiell
7. Speichern Sie Ihre Änderungen.

CLI

Die CLI dient zum Erstellen einer Schnittstellengruppe

Beim Erstellen einer Multimode Schnittstellengruppe kann eine der folgenden Lastverteilungsmethoden angegeben werden:

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

> Die MAC-Adresse einer Schnittstellengruppe wird durch die Reihenfolge der zugrunde liegenden Ports und deren Initialisierung beim Systemstart bestimmt. Es sollte daher nicht davon ausgegangen werden, dass die MAC-Adresse der Schnittstellengruppe nach Neustarts oder ONTAP Upgrades erhalten bleibt.

Schritt

Mit dem `network port ifgrp create` Befehl wird eine Schnittstellengruppe erstellt.

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

Weitere Informationen zu `network port ifgrp create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, wie eine Schnittstellengruppe namens a0a mit der Verteilungsfunktion Port und dem Modus Multimode erstellt wird:

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

Einen Port zu einer Schnittstellengruppe oder einem LAG hinzufügen

Es ist möglich, bis zu 16 physische Ports zu einer Schnittstellengruppe oder einem LAG für alle Portgeschwindigkeiten hinzuzufügen.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager einen Port zu einem LAG hinzufügen

Schritte

1. **Netzwerk > Ethernet-Port > LAG** auswählen, um ein LAG zu bearbeiten.
2. Zusätzliche Ports auf demselben Knoten können zum LAG hinzugefügt werden.
3. Speichern Sie Ihre Änderungen.

CLI

CLI verwenden, um Ports zu einer Schnittstellengruppe hinzuzufügen

Schritt

Netzwerk-Ports zur Schnittstellengruppe hinzufügen:

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

Das folgende Beispiel zeigt, wie Port e0c zu einer Schnittstellengruppe namens a0a hinzugefügt wird:

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

Ab ONTAP 9.8 werden Schnittstellengruppen automatisch etwa eine Minute nach dem Hinzufügen des ersten physischen Ports zur Schnittstellengruppe in eine geeignete Broadcast-Domäne aufgenommen. Wenn ONTAP dies nicht automatisch übernehmen soll und stattdessen die manuelle Zuordnung der ifgrp zu einer Broadcast-Domäne bevorzugt wird, ist der `-skip-broadcast-domain-placement` Parameter als Teil des `ifgrp add-port` Befehls anzugeben.

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

Einen Port aus einer Schnittstellengruppe oder einem LAG entfernen

Sie können einen Port aus einer Schnittstellengruppe entfernen, die LIFs hostet, sofern es sich nicht um den letzten Port in der Schnittstellengruppe handelt. Es besteht keine Voraussetzung, dass die Schnittstellengruppe keine LIFs hosten darf oder dass die Schnittstellengruppe nicht der Home-Port eines LIFs sein darf, solange nicht der letzte Port aus der Schnittstellengruppe entfernt wird. Wenn jedoch der letzte Port entfernt wird, müssen die LIFs zuvor aus der Schnittstellengruppe migriert oder verschoben werden.

Über diese Aufgabe

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

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager lässt sich ein Port aus einem LAG entfernen.

Schritte

1. **Netzwerk > Ethernet-Port > LAG** auswählen, um ein LAG zu bearbeiten.
2. Wählen Sie die Ports aus, die aus dem LAG entfernt werden.
3. Speichern Sie Ihre Änderungen.

CLI

CLI zur Entfernung von Ports aus einer Schnittstellengruppe verwenden

Schritt

Netzwerkports aus einer Schnittstellengruppe entfernen:

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

Weitere Informationen zu `network port ifgrp remove-port` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, wie Port e0c aus einer Schnittstellengruppe namens a0a entfernt wird:

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

Eine Schnittstellengruppe oder LAG löschen

Schnittstellengruppen oder LAGs können gelöscht werden, wenn LIFs direkt auf den zugrunde liegenden physischen Ports konfiguriert werden sollen oder wenn entschieden wird, die Schnittstellengruppe, den LAG-Modus oder die Verteilungsfunktion zu ändern.

Bevor Sie beginnen

- Die Schnittstellengruppe oder LAG darf keine LIF hosten.
- Die Schnittstellengruppe oder LAG darf weder der Home-Port noch das Failover-Ziel eines LIF sein.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager ein LAG löschen

Schritte

1. **Netzwerk > Ethernet-Port > LAG** auswählen, um ein LAG zu löschen.
2. Wählen Sie das LAG aus, das entfernt werden soll.
3. Löschen Sie den LAG.

CLI

Die CLI kann zum Löschen einer Schnittstellengruppe verwendet werden

Schritt

Mit dem `network port ifgrp delete` Befehl wird eine Schnittstellengruppe gelöscht.

Weitere Informationen zu `network port ifgrp delete` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, wie eine Schnittstellengruppe mit dem Namen a0b gelöscht wird:

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

ONTAP VLANs über physische Ports konfigurieren

VLANs können in ONTAP verwendet werden, um Netzwerke logisch zu segmentieren, indem separate Broadcast-Domänen erstellt werden, die auf Basis eines Switch-Ports definiert sind, im Gegensatz zu den traditionellen Broadcast-Domänen, die auf physischen Grenzen basieren.

Ein VLAN kann sich über mehrere physische Netzwerksegmente erstrecken. Die zu einem VLAN gehörenden Endgeräte sind durch Funktion oder Anwendung miteinander verbunden.

Beispielsweise können Endgeräte in einem VLAN nach Abteilungen wie Engineering und Accounting oder nach Projekten wie release1 und release2 gruppiert werden. Da die physische Nähe der Endgeräte in einem VLAN nicht erforderlich ist, können die Endgeräte geografisch verteilt werden, und dennoch bleibt die Broadcast-Domäne in einem Switch-Netzwerk erhalten.

In ONTAP 9.14.1 und 9.13.1 werden ungetaggte Ports, die von keiner Logical Interface (LIF) verwendet werden und keine native VLAN-Konnektivität am angeschlossenen Netzwerk-Switch besitzen, als beeinträchtigt markiert. Dies dient dazu, ungenutzte Ports zu identifizieren und stellt keinen Ausfall dar. Native VLANs ermöglichen ungetaggten Datenverkehr am ifgrp Basis-Port, beispielsweise ONTAP CFM Broadcasts. Die Konfiguration nativer VLANs auf dem Switch verhindert die Blockierung von ungetaggtem Datenverkehr.

VLANs lassen sich verwalten, indem sie erstellt, gelöscht oder Informationen darüber angezeigt werden.

> Ein VLAN sollte nicht auf einer Netzwerkschnittstelle mit demselben Bezeichner wie das native VLAN des Switches erstellt werden. Befindet sich beispielsweise die Netzwerkschnittstelle e0b im nativen VLAN 10, sollte kein VLAN e0b-10 auf dieser Schnittstelle erstellt werden.

Eine VLAN erstellen

Ein VLAN kann erstellt werden, um separate Broadcast-Domänen innerhalb derselben Netzwerkdomäne zu verwalten, indem System Manager oder der `network port vlan create` Befehl verwendet wird.

Bevor Sie beginnen

Es wurde bestätigt, dass die folgenden Anforderungen erfüllt sind:

- Die im Netzwerk eingesetzten Switches müssen entweder den IEEE 802.1Q-Standards entsprechen oder eine herstellerspezifische Implementierung von VLANs aufweisen.
- Zur Unterstützung mehrerer VLANs muss eine Endstation statisch so konfiguriert werden, dass sie zu einem oder mehreren VLANs gehört.
- Das VLAN ist nicht an einen Port angebunden, der eine Cluster-LIF hostet.
- Das VLAN ist nicht an Ports angebunden, die dem Cluster IPspace zugewiesen sind.

- Das VLAN wird nicht auf einem Schnittstellengruppen-Basis-Port erstellt, der keine Mitgliedsports enthält.

Über diese Aufgabe

Durch das Erstellen eines VLANs wird das VLAN an den Netzwerk-Port eines bestimmten Knotens in einem Cluster angebunden.

Wenn ein VLAN zum ersten Mal über einen Port konfiguriert wird, kann der Port ausfallen, was zu einer vorübergehenden Trennung des Netzwerks führt. Das anschließende Hinzufügen weiterer VLANs zum selben Port wirkt sich nicht auf den Portzustand aus.

Ein VLAN sollte nicht auf einer Netzwerkschnittstelle mit demselben Bezeichner wie das native VLAN des Switches erstellt werden. Befindet sich beispielsweise die Netzwerkschnittstelle e0b im nativen VLAN 10, sollte kein VLAN e0b-10 auf dieser Schnittstelle erstellt werden.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager ein VLAN erstellen

Ab ONTAP 9.12.0 kann die Broadcast-Domäne automatisch ausgewählt oder manuell aus der Liste ausgewählt werden. Zuvor wurden Broadcast-Domänen immer automatisch basierend auf der Layer-2-Konnektivität ausgewählt. Bei manueller Auswahl einer Broadcast-Domäne erscheint eine Warnung, dass die manuelle Auswahl einer Broadcast-Domäne zu einem Verbindungsverlust führen kann.

Schritte

1. **Netzwerk > Ethernet-Port > + VLAN** auswählen.
2. Den Knoten aus der Dropdown-Liste auswählen.
3. Wählen Sie aus den folgenden Optionen:
   a. ONTAP auf **Automatische Auswahl der Broadcast-Domäne (empfohlen)**.
   b. Manuelle Auswahl einer Broadcast-Domäne aus der Liste.
4. Wählen Sie die Ports aus, die das VLAN bilden.
5. Geben Sie die VLAN-ID an.
6. Speichern Sie Ihre Änderungen.

CLI

Die CLI wird verwendet, um eine VLAN zu erstellen

Unter bestimmten Umständen kann der VLAN-Port auf einem beeinträchtigten Port erstellt werden, ohne das Hardwareproblem oder eine Softwarefehlkonfiguration zu beheben, indem der `-ignore-health -status` Parameter des `network port modify` Befehls auf `true` gesetzt wird.

Weitere Informationen zu `network port modify` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Mit dem `network port vlan create` Befehl wird ein VLAN erstellt.
2. Es muss entweder die `vlan-name`- oder die `port`- und `vlan-id`-Option beim Erstellen eines VLANs angegeben werden. Der VLAN-Name ist eine Kombination aus dem Namen des Ports (oder der Schnittstellengruppe) und der Netzwerk-Switch VLAN-Kennung, mit einem Bindestrich

dazwischen. Zum Beispiel sind `e0c-24` und `e1c-80` gültige VLAN-Namen.

Das folgende Beispiel zeigt, wie ein VLAN `e1c-80` an den Netzwerk-Port `e1c` des Node `cluster-1-01` erstellt wird:

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

Ab ONTAP 9.8 werden VLANs automatisch etwa eine Minute nach ihrer Erstellung den entsprechenden Broadcast-Domänen zugeordnet. Wenn ONTAP dies nicht übernehmen soll und stattdessen eine manuelle Zuordnung des VLANs zu einer Broadcast-Domäne bevorzugt wird, ist der `-skip-broadcast-domain-placement` Parameter als Teil des `vlan create` Befehls anzugeben.

Weitere Informationen zu `network port vlan create` finden sich in der "ONTAP-Befehlsreferenz".

Bearbeiten einer VLAN

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

Mit System Manager ein VLAN bearbeiten

Ab ONTAP 9.12.0 kann die Broadcast-Domäne automatisch ausgewählt oder manuell aus der Liste ausgewählt werden. Zuvor wurden Broadcast-Domänen immer automatisch basierend auf der Layer-2-Konnektivität ausgewählt. Bei manueller Auswahl einer Broadcast-Domäne erscheint eine Warnung, dass die manuelle Auswahl einer Broadcast-Domäne zu einem Verbindungsverlust führen kann.

Schritte

1. **Netzwerk > Ethernet-Port > VLAN** auswählen.
2. Das Bearbeitungssymbol auswählen.
3. Führen Sie einen der folgenden Schritte aus:
   - Die Broadcast-Domäne kann geändert werden, indem eine andere aus der Liste ausgewählt wird.
   - Deaktivieren Sie das Kästchen **Aktiviert**.
4. Speichern Sie Ihre Änderungen.

Löschen eines VLAN

Möglicherweise muss ein VLAN gelöscht werden, bevor eine Netzwerkkarte aus ihrem Steckplatz entfernt wird. Beim Löschen eines VLANs wird es automatisch aus allen Failover-Regeln und -Gruppen entfernt, die es verwenden.

Bevor Sie beginnen

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

Über diese Aufgabe

Das Löschen des letzten VLAN von einem Port kann eine vorübergehende Trennung des Netzwerks vom Port verursachen.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager ein VLAN löschen

Schritte

1. **Netzwerk > Ethernet-Port > VLAN** auswählen.
2. Wählen Sie das VLAN aus, das entfernt werden soll.
3. Klicken Sie auf **Delete**.

CLI

Die CLI wird verwendet, um ein VLAN zu löschen

Schritt

Der `network port vlan delete` Befehl dient zum Löschen eines VLANs.

Das folgende Beispiel zeigt, wie ein VLAN `e1c-80` vom Netzwerk-Port `e1c` auf dem Node `cluster-1-01` gelöscht wird:

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

Weitere Informationen zu `network port vlan delete` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Netzwerkportattribute ändern

Sie können die Einstellungen für Autonegotiation, Duplex-Modus, Flusskontrolle, Geschwindigkeit und Integrität eines physischen Netzwerk-Ports anpassen.

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 von Ihnen festgelegten Werte für Duplex-Modus und Portgeschwindigkeit werden als administrative Einstellungen bezeichnet. Je nach Netzwerkbeschränkungen können die administrativen Einstellungen von den Betriebseinstellungen (das heißt, dem tatsächlich vom Port verwendeten Duplex-Modus und der Geschwindigkeit) abweichen.

- 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 Berechtigungsstufe) ändert die administrativen Einstellungen des Ports.

- Es wird nicht empfohlen, die `-up-admin`administrative Einstellung für alle Ports auf einem Knoten oder für den Port, der die letzte betriebsbereite Cluster-LIF auf einem Knoten hostet, auf false zu setzen.
- Es wird nicht empfohlen, die MTU-Größe des Management-Ports zu ändern `e0M`.

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

Schritte

1. Die Attribute eines Netzwerk-Ports ändern:

   `network port modify`

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

   Der Netzwerkport-Status wird automatisch von „Beeinträchtigt“ auf „Gut“ geändert, und dieser Port kann nun für das Hosting von LIFs verwendet werden. Die Flusssteuerung der Cluster-Ports sollte auf `none` gesetzt werden. Standardmäßig ist die Flusssteuerung auf `full` eingestellt.

Der folgende Befehl deaktiviert die Flusssteuerung am Port e0b, indem die Flusssteuerung auf „none“ gesetzt wird:

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

Weitere Informationen zu `network port modify` finden sich in der "ONTAP-Befehlsreferenz".

10GbE-Ports für ONTAP Netzwerke durch Konvertierung von 40GbE-NIC-Ports erstellen

Sie können die X1144A-R6 und die X91440A-R6 40GbE Netzwerkschnittstellenkarten (NICs) so umrüsten, dass sie vier 10GbE Ports unterstützen.

Wenn eine Hardwareplattform, die eine dieser Netzwerkkarten unterstützt, mit einem Cluster verbunden wird, der 10GbE Cluster Interconnect und Kundendatenverbindungen unterstützt, muss die Netzwerkkarte so umgerüstet werden, dass die erforderlichen 10GbE-Verbindungen bereitgestellt werden.

Bevor Sie beginnen

Es muss ein unterstütztes Breakout-Kabel verwendet werden.

Über diese Aufgabe

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

> Bei der Netzwerkkarte X1144A-R6 kann nur Port A für die vier 10GbE-Verbindungen umgerüstet werden. Nach der Umrüstung von Port A ist Port e nicht mehr verfügbar.

Schritte

1. In den Wartungsmodus wechseln.
2. Die Netzwerkkarte von 40GbE-Unterstützung auf 10GbE-Unterstützung konvertieren.

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

3. Nach der Ausführung des Konvertierungsbefehls den Knoten anhalten.
4. Das Kabel installieren oder austauschen.
5. Je nach Hardwaremodell wird der SP (Service Processor) oder BMC (Baseboard Management Controller) verwendet, um den Knoten neu zu starten, damit die Umstellung wirksam wird.

UTA X1143A-R6 Ports für das ONTAP Netzwerk konfigurieren

Standardmäßig ist der X1143A-R6 Unified-Zieladapter im FC-Zielmodus konfiguriert, Sie können seine Ports jedoch entweder als 10-Gb-Ethernet- und FCoE- (CNA-) Ports oder als 16-Gb-FC-Initiator- oder -Zielports konfigurieren. Dies erfordert unterschiedliche SFP+-Adapter.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zieldatenverkehr über denselben 10-GBE-Port. Bei FC-Konfiguration kann jedes Zwei-Port-Paar, das denselben ASIC nutzt, individuell für den FC-Ziel- oder FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter den FC-Zielmodus auf einem Zwei-Port-Paar und den FC-Initiator-Modus auf einem anderen Zwei-Port-Paar unterstützen kann. Portpaare, die mit demselben ASIC verbunden sind, müssen im selben Modus konfiguriert werden.

Im FC-Modus verhält sich der X1143A-R6 Adapter wie jedes andere FC-Gerät mit Geschwindigkeiten von bis zu 16 Gbit/s. Im CNA-Modus kann der X1143A-R6 Adapter für gleichzeitigen NIC- und FCoE-Datenverkehr über denselben 10 GbE-Port verwendet werden. Der CNA-Modus unterstützt für die FCoE-Funktion ausschließlich den FC-Zielmodus.

Um den einheitlichen Zieladapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im gleichen Personality-Modus konfiguriert werden.

Schritte

1. Portkonfiguration anzeigen:

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

2. Die Ports können nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA) konfiguriert werden:

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

3. Die entsprechenden Kabel für FC oder 10 Gbit/s Ethernet anschließen.
4. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

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

Für CNA sollte ein 10Gb Ethernet SFP verwendet werden. Für FC sollte abhängig vom angeschlossenen

FC-Fabric entweder ein 8-Gb-SFP oder ein 16-Gb-SFP verwendet werden.

Den UTA2-Port für die Verwendung im ONTAP Netzwerk konvertieren

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

Die UTA2-Persönlichkeit ist vom CNA-Modus in den FC-Modus zu ändern, wenn das physische Medium geändert werden muss, das den Port mit seinem Netzwerk verbindet, oder um die Unterstützung von FC-Initiatoren und Zieladaptern zu ermöglichen.

Vom CNA-Modus in den FC-Modus

Schritte

1. Den Adapter offline schalten:

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

2. Portmodus ändern:

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

3. Den Knoten neu starten und anschließend den Adapter online schalten:

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

4. Benachrichtigen Sie Ihren Administrator oder VIF-Manager, damit der Port je nach Bedarf gelöscht oder entfernt wird:
   - Wenn der Port als Home-Port eines LIF verwendet wird, Mitglied einer Schnittstellengruppe (ifgrp) ist oder VLANs hostet, sollte ein Administrator Folgendes tun:
     - Die LIFs verschieben, den Port aus der ifgrp entfernen oder die VLANs löschen.
     - Der Port kann manuell gelöscht werden, indem der `network port delete` Befehl ausgeführt wird. Falls der `network port delete` Befehl fehlschlägt, sollte der Administrator die Fehler beheben und dann den Befehl erneut ausführen.
   - Wenn der Port nicht als Home-Port eines LIF verwendet wird, kein Mitglied einer ifgrp ist und keine VLANs hostet, sollte der VIF Manager den Port beim Neustart aus seinen Datensätzen entfernen. Falls der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neustart manuell mit dem `network port delete` Befehl entfernen.

     Weitere Informationen zu `network port delete` finden sich in der "ONTAP-Befehlsreferenz".

5. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

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

Für CNA sollte ein 10Gb Ethernet SFP verwendet werden. Für FC sollte entweder ein 8 Gb SFP oder ein 16 Gb SFP verwendet werden, bevor die Konfiguration am Node geändert wird.

Vom FC-Modus in den CNA-Modus

Schritte

1. Den Adapter offline schalten:

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

2. Portmodus ändern:

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

3. Den Knoten neu starten
4. Es sollte überprüft werden, ob das richtige SFP+ installiert ist.

   Für CNA sollte ein 10Gb Ethernet SFP verwendet werden.

Die optischen Module CNA/UTA2 für das ONTAP Netzwerk konvertieren

Die optischen Module des Unified Zieladapter (CNA/UTA2) sind so zu wechseln, dass der für den Adapter ausgewählte Persönlichkeitsmodus unterstützt wird.

Schritte

1. Den aktuell in der Karte verwendeten SFP+ überprüfen. Anschließend den aktuellen SFP+ durch den für die gewünschte Personality (FC oder CNA) geeigneten SFP+ ersetzen.
2. Die vorhandenen optischen Module werden aus dem X1143A-R6 Adapter entfernt.
3. Die passenden Module für den bevorzugten Persönlichkeitsmodus (FC oder CNA) Optiken einsetzen.
4. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

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

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

Netzwerkkarten aus ONTAP Clusterknoten entfernen

Möglicherweise müssen Sie eine defekte Netzwerkkarte aus ihrem Steckplatz entfernen oder die Netzwerkkarte zu Wartungszwecken in einen anderen Steckplatz umstecken.

Die Vorgehensweise zum Entfernen einer Netzwerkkarte (NIC) unterscheidet sich in ONTAP 9.7 und früheren Versionen. Für das Entfernen einer Netzwerkkarte von einem ONTAP Clusterknoten mit ONTAP 9.7 oder einer früheren Version ist die entsprechende Vorgehensweise unter "Entfernen einer Netzwerkkarte aus dem Knoten (ONTAP 9.7 oder früher)" zu beachten.

Schritte

1. Den Knoten ausschalten.
2. Die Netzwerkkarte wird physisch aus ihrem Steckplatz entfernt.
3. Den Knoten einschalten.
4. Überprüfen, ob der Port gelöscht wurde:

```
network port show
```

ONTAP entfernt den Port automatisch aus allen Schnittstellengruppen. Wenn der Port das einzige Mitglied einer Schnittstellengruppe war, wird die Schnittstellengruppe gelöscht. Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

5. Falls für den Port VLANs konfiguriert waren, werden diese verschoben. Die verschobenen VLANs lassen sich mit folgendem Befehl anzeigen:

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

Die `displaced-interface show`, `displaced-vlans show` und `displaced-vlans restore` Befehle sind einzigartig und benötigen nicht den vollqualifizierten Befehlsnamen, der mit `cluster controller-replacement network` beginnt.

6. Diese VLANs werden gelöscht, können aber mit folgendem Befehl wiederhergestellt werden:

```
displaced-vlans restore
```

7. Falls für den Port LIFs konfiguriert waren, wählt ONTAP automatisch neue Home-Ports für diese LIFs auf einem anderen Port in derselben Broadcast-Domäne. Wird kein geeigneter Home-Port auf demselben Filer gefunden, gelten diese LIFs als verschoben. Verschobene LIFs lassen sich mit folgendem Befehl anzeigen:

```
displaced-interface show
```

8. Wird dem Broadcast-Bereich auf demselben Knoten ein neuer Port hinzugefügt, werden die Home-Ports

der LIFs automatisch wiederhergestellt. Alternativ lässt sich der Home-Port mit dem `network interface modify -home-port -home-node or use the displaced- interface restore` Befehl festlegen.

Verwandte Informationen

- "Cluster Controller-Ersatznetzwerk verschobene Schnittstelle löschen"
- "Netzwerkschnittstelle ändern"

Netzwerkports überwachen

Den Zustand der ONTAP Netzwerkports überwachen

Die ONTAP Verwaltung von Netzwerkports umfasst eine automatische Zustandsüberwachung sowie eine Reihe von Zustandsmonitoren, die dabei unterstützen, Netzwerkports zu identifizieren, die möglicherweise nicht für das Hosting von LIFs geeignet sind.

Über diese Aufgabe

Stellt ein Health-Monitor fest, dass ein Netzwerkport fehlerhaft ist, warnt er Administratoren durch eine EMS-Meldung oder markiert den Port als beeinträchtigt. ONTAP vermeidet das Hosten von LIFs auf beeinträchtigten Netzwerkports, wenn für diesen LIF gesunde alternative Failover-Ziele vorhanden sind. Ein Port kann aufgrund eines Soft-Failure-Ereignisses wie Link-Flapping (Verbindungen wechseln schnell zwischen aktiv und inaktiv) oder Netzwerkpartitionierung beeinträchtigt werden:

- Netzwerk-Ports im Cluster-IPspace werden als beeinträchtigt markiert, wenn sie Link-Flapping oder einen Verlust der Layer-2-(L2-)Erreichbarkeit zu anderen Netzwerk-Ports in der Broadcast-Domäne aufweisen.
- Netzwerkports in Nicht-Cluster-IPspaces werden als beeinträchtigt markiert, wenn sie Link-Flapping aufweisen.

Folgende Verhaltensweisen eines beeinträchtigten Ports sind zu beachten:

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

  Wenn ein Mitgliedsport einer Schnittstellengruppe als beeinträchtigt markiert ist, die Schnittstellengruppe jedoch weiterhin als fehlerfrei gilt, können LIFs auf dieser Schnittstellengruppe gehostet werden.

- LIFs werden automatisch von beeinträchtigten Ports auf fehlerfreie Ports migriert.
- Während eines Failover-Ereignisses wird ein beeinträchtigter Port nicht als Failover-Ziel betrachtet. Wenn keine fehlerfreien Ports verfügbar sind, hosten beeinträchtigte Ports LIFs gemäß der normalen Failover-Richtlinie.
- Sie können keine LIF auf einem eingeschränkten Port erstellen, migrieren oder zurücksetzen.

  Sie können die `ignore-health-status` Einstellung des Netzwerkports auf `true` ändern. Anschließend kann eine LIF auf den fehlerfreien Ports gehostet werden.

Schritte

1. Melden Sie sich im erweiterten Berechtigungsmodus an:

```
set -privilege advanced
```

2. Es kann geprüft werden, welche Systemüberwachungsfunktionen zur Überwachung des Netzwerkportzustands aktiviert sind:

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

   Der Gesundheitszustand eines Ports wird durch den Wert der Health Monitors bestimmt.

   Die folgenden Gesundheitsmonitore sind in ONTAP verfügbar und standardmäßig aktiviert:

   - Link-Flapping Health Monitor: Überwacht Link-Flapping

     Wenn ein Port innerhalb von fünf Minuten mehr als einmal einen Verbindungsabbruch aufweist, wird dieser Port als beeinträchtigt markiert.

   - L2 Reachability Health Monitor: Überwacht, ob alle Ports, die in derselben Broadcast-Domäne konfiguriert sind, L2-Erreichbarkeit zueinander haben.

     Dieser Health Monitor meldet L2-Erreichbarkeitsprobleme in allen IPspaces, allerdings werden nur die Ports im Cluster-IPspace als beeinträchtigt markiert.

   - CRC Monitor: Überwacht die CRC-Statistiken der Ports

     Dieser Gesundheitsmonitor kennzeichnet einen Port nicht als beeinträchtigt, sondern generiert eine EMS-Meldung, wenn eine sehr hohe CRC-Fehlerrate festgestellt wird.

   Weitere Informationen zu `network options port-health-monitor show` finden sich in der "ONTAP-Befehlsreferenz".

3. Die gewünschten Health Monitore für einen IPspace können mit dem `network options port-health-monitor modify` Befehl aktiviert oder deaktiviert werden.

   Weitere Informationen zu `network options port-health-monitor modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Detaillierter Zustand eines Ports:

   ```
   network port show -health
   ```

Die Befehlsausgabe zeigt den Gesundheitszustand des Ports, `ignore health status` die Einstellung und eine Liste der Gründe an, warum der Port als beeinträchtigt markiert ist.

Der Gesundheitszustand eines Ports kann `healthy` oder `degraded` sein.

Wenn die `ignore health status` Einstellung `true` ist, zeigt dies an, dass der Port-Integritätsstatus vom Administrator von `degraded` auf `healthy` geändert wurde.

Wenn die `ignore health status` Einstellung `false` ist, wird der Port-Gesundheitsstatus automatisch vom

System bestimmt.

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

Überwachung der Erreichbarkeit von ONTAP Netzwerk-Ports

Die Erreichbarkeitsüberwachung ist in ONTAP 9.8 und höher integriert. Mit dieser Überwachung lässt sich erkennen, wenn die physische Netzwerktopologie nicht mit der ONTAP Konfiguration übereinstimmt. In einigen Fällen kann ONTAP die Port-Erreichbarkeit wiederherstellen. In anderen Fällen sind zusätzliche Schritte erforderlich.

Über diese Aufgabe

Mit diesen Befehlen lassen sich Netzwerkfehlkonfigurationen überprüfen, diagnostizieren und beheben, die darauf zurückzuführen sind, dass die ONTAP Konfiguration weder mit der physischen Verkabelung noch mit der Netzwerk-Switch Konfiguration übereinstimmt.

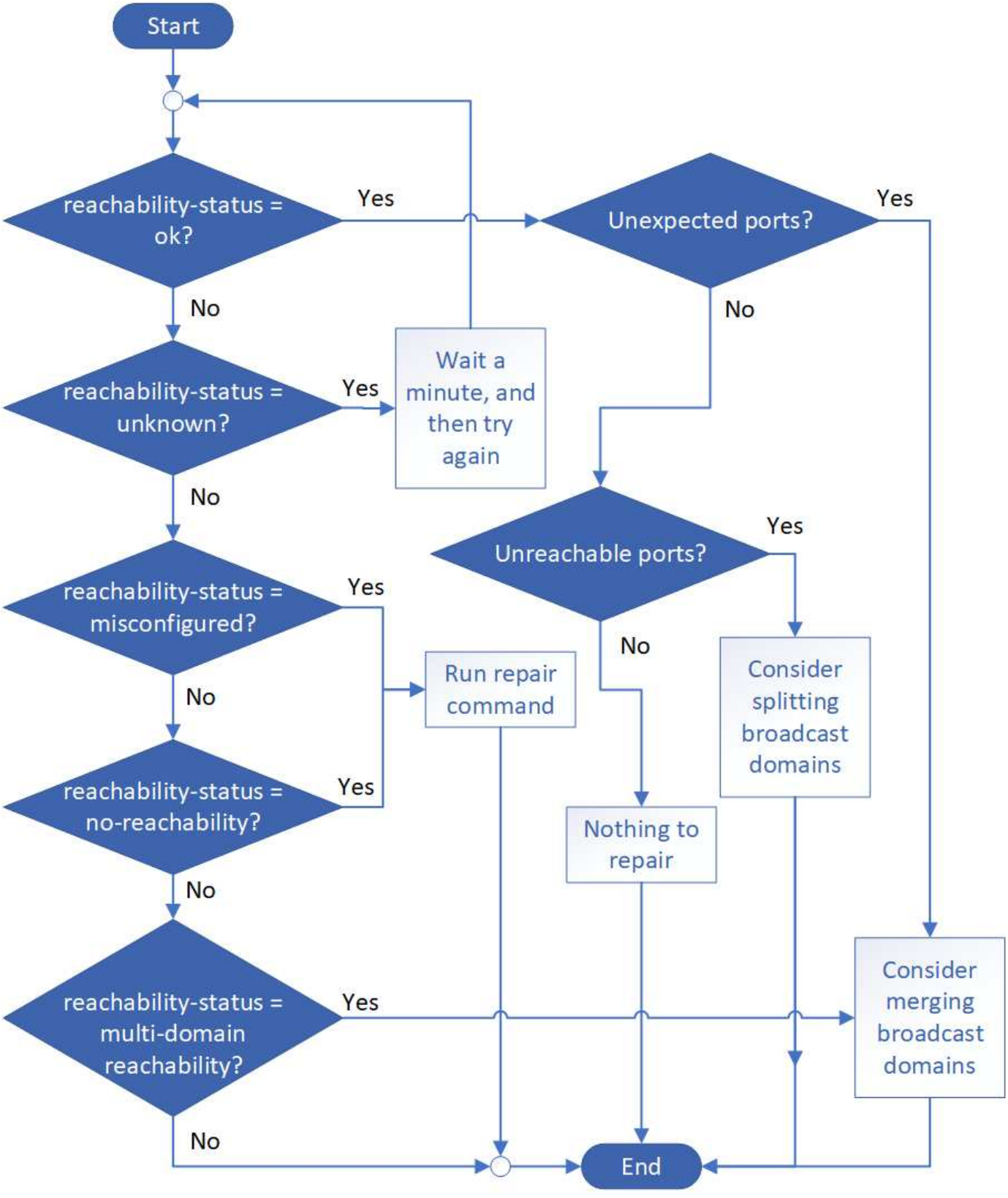
Schritt

1. Port-Erreichbarkeit anzeigen:

   ```
   network port reachability show
   ```

   Weitere Informationen zu `network port reachability show` finden sich in der "ONTAP-Befehlsreferenz".

2. Der folgende Entscheidungsbaum und die Tabelle geben Aufschluss darüber, ob ein nächster Schritt erforderlich ist.



Erreichbarkeitsstatus	Beschreibung

OK	Der Port verfügt über Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne. Wenn der Erreichbarkeitsstatus „ok“ ist, aber „unerwartete Ports“ vorhanden sind, kann das Zusammenführen einer oder mehrerer Broadcast-Domänen in Betracht gezogen werden. Weitere Informationen stehen in der folgenden Zeile *Unexpected ports*. Wenn der Erreichbarkeitsstatus „ok“ ist, aber „nicht erreichbare Ports“ vorhanden sind, kann das Aufteilen einer oder mehrerer Broadcast-Domänen in Erwägung gezogen werden. Weitere Informationen enthält die folgende Zeile *Nicht erreichbare Ports*. Wenn der Erreichbarkeitsstatus "ok" ist und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist Ihre Konfiguration korrekt.
Unerwartete Ports	Der Port ist über Layer 2 zu seiner zugewiesenen Broadcast-Domäne erreichbar; er ist jedoch auch über Layer 2 zu mindestens einer weiteren Broadcast-Domäne erreichbar. Die physische Konnektivität und die Switch-Konfiguration sollten überprüft werden, um festzustellen, ob sie fehlerhaft sind oder ob die dem Port zugewiesene Broadcast-Domäne mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden sich unter "Zusammenführen von Broadcast-Domänen".
Nicht erreichbare Ports	Wenn eine einzelne Broadcast-Domäne in zwei verschiedene Erreichbarkeitsgruppen aufgeteilt wurde, kann eine Broadcast-Domäne aufgeteilt werden, um die ONTAP Konfiguration mit der physischen Netzwerktopologie zu synchronisieren. Die Liste der nicht erreichbaren Ports definiert üblicherweise die Menge der Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollten, nachdem überprüft wurde, dass die physische und die Switch-Konfiguration korrekt sind. Weitere Informationen finden sich unter "Aufgeteilte Broadcast-Domänen".
Fehlkonfigurierte Erreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne, jedoch hat der Port Layer-2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Bei Ausführung des folgenden Befehls weist das System den Port der Broadcast-Domäne zu, zu der er erreichbar ist: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Reparatur der Port-Erreichbarkeit".
Unerreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu einer bestehenden Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Beim Ausführen des folgenden Befehls weist das System den Port einer neu automatisch erstellten Broadcast-Domäne im Default-IPspace zu: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Reparatur der Port-Erreichbarkeit". Weitere Informationen zu `network port reachability repair` finden sich in der "ONTAP-Befehlsreferenz".

Erreichbarkeit über mehrere Domänen hinweg	Der Port ist über Layer 2 zu seiner zugewiesenen Broadcast-Domäne erreichbar; er ist jedoch auch über Layer 2 zu mindestens einer weiteren Broadcast-Domäne erreichbar. Die physische Konnektivität und die Switch-Konfiguration sollten überprüft werden, um festzustellen, ob sie fehlerhaft sind oder ob die dem Port zugewiesene Broadcast-Domäne mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Zusammenführen von Broadcast-Domänen" oder "Reparatur der Port-Erreichbarkeit".
unbekannt	Wenn der Erreichbarkeitsstatus „unbekannt“ ist, einige Minuten abwarten und den Befehl erneut ausführen.

Nach der Reparatur eines Ports müssen verschobene LIFs und VLANs überprüft und behoben werden. Wenn der Port Teil einer Schnittstellengruppe war, ist es außerdem erforderlich, nachzuvollziehen, was mit dieser Schnittstellengruppe geschehen ist. Weitere Informationen finden sich unter "Reparatur der Port-Erreichbarkeit".

ONTAP Port-Nutzung auf einem Speichersystem

Mehrere bekannte Ports sind für die ONTAP Kommunikation mit bestimmten Diensten reserviert. Portkonflikte treten auf, wenn ein Portwert in Ihrer Speichernetzwerkumgebung mit dem Wert eines ONTAP Ports übereinstimmt.

Eingehender Datenverkehr

Der eingehende Datenverkehr auf Ihrem ONTAP Storage verwendet die folgenden Protokolle und Ports:

Protokoll	Port	Zweck
Alle ICMP	Alle	Die Instanz anpingen
TCP	22	Sicherer Shell-Zugriff auf die IP-Adresse der Cluster-Management-LIF oder einer Node-Management-LIF
TCP	80	Webzugriff auf die IP-Adresse der Cluster-Management-LIF
TCP/UDP	111	RPCBIND, Remote Procedure Call für NFS
UDP	123	NTP, Netzwerkzeitprotokoll
TCP	135	MSRPC, Microsoft Remote Procedure Call
TCP	139	NETBIOS-SSN, NetBIOS-Dienstsitzung für CIFS
TCP/UDP	161-162	SNMP, einfaches Netzwerkmanagementprotokoll
TCP	443	Sicherer Webseitenzugriff auf die IP-Adresse der Cluster-Management-LIF
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS über TCP mit NetBIOS Framing
TCP/UDP	635	NFS-Mount zur Interaktion mit einem entfernten Dateisystem, als ob es lokal wäre

TCP	749	Kerberos
UDP	953	Name Daemon
TCP/UDP	2049	NFS Server-Daemon
TCP	2050	NRV, NetApp Remote Volume Protocol
TCP	3260	iSCSI-Zugriff über die iSCSI-Daten-LIF
TCP/UDP	4045	NFS Sperrdaemon
TCP/UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-RPC-Rquotad
UDP	4444	KRB524, Kerberos 524
UDP	5353	Multicast DNS
TCP	10000	Datensicherung mit Network Data Management Protocol (NDMP)
TCP	11104	Cluster-Peering, bidirektionale Verwaltung von Intercluster-Verbindungssitzungen für SnapMirror
TCP	11105	Cluster-Peering, bidirektionaler SnapMirror Datentransfer über Intercluster-LIFs
SSL/TLS	30000	Akzeptiert sichere NDMP-Steuerungsverbindungen zwischen DMA und NDMP-Server über sichere Sockets (SSL/TLS). Sicherheitsscanner können eine Schwachstelle auf Port 30000 melden.

Ausgehender Verkehr

Der ausgehende Datenverkehr Ihres ONTAP Storage kann je nach Geschäftsanforderungen mithilfe einfacher oder erweiterter Regeln eingerichtet werden.

Grundlegende ausgehende Regeln

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

Protokoll	Port	Zweck
Alle ICMP	Alle	Der gesamte ausgehende Verkehr
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte ausgehende Regeln

Falls Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie mithilfe der folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch ONTAP erforderlich sind.

Active Directory

Protokoll	Port	Quelle	Ziel	Zweck
TCP	88	Node Management LIF, Daten LIF (NFS, CIFS, iSCSI)	Active Directory Gesamtstruktur	Kerberos V Authentifizierung
UDP	137	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Namensdienst
UDP	138	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Datagrammdienst
TCP	139	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Dienstsitzung
TCP	389	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	LDAP
UDP	389	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	LDAP
TCP	445	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS Framing
TCP	464	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Kerberos V-Passwort ändern und festlegen (SET_CHANGE)
UDP	464	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Kerberos Schlüsselverwaltung
TCP	749	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Ändern und Festlegen des Kerberos V Passworts (RPCSEC_GSS)

AutoSupport

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

SNMP

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

SnapMirror

Protokoll	Port	Quelle	Ziel	Zweck

TCP	11104	Intercluster-LIF	ONTAP Intercluster LIFs	Management von Intercluster-Verbindungssitzungen für SnapMirror

Sonstige Dienstleistungen

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

ONTAP interne Ports

Die folgende Tabelle listet die von ONTAP intern verwendeten Ports und deren Funktionen auf. ONTAP nutzt diese Ports für verschiedene Funktionen, wie zum Beispiel für die Herstellung der Intracluster-LIF-Kommunikation.

Diese Liste ist nicht vollständig und kann je nach Umgebung variieren.

Port/Protokoll	Komponente/Funktion
514	Syslog
900	NetApp Cluster-RPC
902	NetApp Cluster-RPC
904	NetApp Cluster-RPC
905	NetApp Cluster-RPC
910	NetApp Cluster-RPC
911	NetApp Cluster-RPC
913	NetApp Cluster-RPC

914	NetApp Cluster-RPC
915	NetApp Cluster-RPC
918	NetApp Cluster-RPC
920	NetApp Cluster-RPC
921	NetApp Cluster-RPC
924	NetApp Cluster-RPC
925	NetApp Cluster-RPC
927	NetApp Cluster-RPC
928	NetApp Cluster-RPC
929	NetApp Cluster-RPC
930	Kernel-Services und Managementfunktionen (KSMF)
931	NetApp Cluster-RPC
932	NetApp Cluster-RPC
933	NetApp Cluster-RPC
934	NetApp Cluster-RPC
935	NetApp Cluster-RPC
936	NetApp Cluster-RPC
937	NetApp Cluster-RPC
939	NetApp Cluster-RPC
940	NetApp Cluster-RPC
951	NetApp Cluster-RPC
954	NetApp Cluster-RPC
955	NetApp Cluster-RPC
956	NetApp Cluster-RPC
958	NetApp Cluster-RPC
961	NetApp Cluster-RPC
963	NetApp Cluster-RPC
964	NetApp Cluster-RPC
966	NetApp Cluster-RPC
967	NetApp Cluster-RPC
975	Key Management Interoperability Protocol (KMIP)
982	NetApp Cluster-RPC
983	NetApp Cluster-RPC
5125	Alternativer Steuerport für Festplatte

5133	Alternativer Steuerport für Festplatte
5144	Alternativer Steuerport für Festplatte
65502	Node Scope SSH
65503	LIF-Sharing
7700	Cluster Session Manager (CSM)
7810	NetApp Cluster-RPC
7811	NetApp Cluster-RPC
7812	NetApp Cluster-RPC
7813	NetApp Cluster-RPC
7814	NetApp Cluster-RPC
7815	NetApp Cluster-RPC
7816	NetApp Cluster-RPC
7817	NetApp Cluster-RPC
7818	NetApp Cluster-RPC
7819	NetApp Cluster-RPC
7820	NetApp Cluster-RPC
7821	NetApp Cluster-RPC
7822	NetApp Cluster-RPC
7823	NetApp Cluster-RPC
7824	NetApp Cluster-RPC
7835-7839 und 7845-7849	TCP-Ports für die Kommunikation innerhalb des Clusters
8023	Node Scope TELNET
8443	ONTAP S3 NAS Port für Amazon FSx
8514	Node Scope RSH
9877	KMIP Client Port (nur interner lokaler Host)
10006	TCP-Port für HA-Interconnect-Kommunikation

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.