Configurare le porte di rete

ONTAP 9

NetApp
February 12, 2026

Sommario

Configurare le porte di rete . . . 1
- Combinare porte fisiche per creare gruppi di interfacce ONTAP . . . 1
  - Tipi di gruppi di interfacce . . . 1
  - Creare un gruppo di interfacce o un LAG . . . 5
  - Aggiungere una porta a un gruppo di interfacce o LAG . . . 7
  - Rimuovere una porta da un gruppo di interfacce o LAG . . . 7
  - Eliminare un gruppo di interfacce o un LAG . . . 8
- Configurare LE VLAN ONTAP su porte fisiche . . . 9
  - Creare una VLAN . . . 10
  - Modificare una VLAN . . . 12
  - Eliminare una VLAN . . . 12
- Modificare gli attributi delle porte di rete ONTAP . . . 13
- Creare porte 10GbE per reti ONTAP convertendo 40GbE porte NIC . . . 14
- Configurare le porte UTA X1143A-R6 per la rete ONTAP . . . 15
- Convertire la porta UTA2 per l'utilizzo nella rete ONTAP . . . 16
- Convertire i moduli ottici CNA/UTA2 per la rete ONTAP . . . 18
- Rimozione delle schede di rete dai nodi del cluster ONTAP . . . 18
- Monitorare le porte di rete . . . 19
  - Monitorare lo stato delle porte di rete ONTAP . . . 19
  - Monitorare la raggiungibilità delle porte di rete ONTAP . . . 21
  - Informazioni sull'utilizzo delle porte sulla rete ONTAP . . . 25
  - Informazioni sulle porte interne di ONTAP . . . 28

Configurare le porte di rete

Combinare porte fisiche per creare gruppi di interfacce ONTAP

Un gruppo di interfacce, noto anche come LAG (link Aggregation Group), viene creato combinando due o più porte fisiche sullo stesso nodo in una singola porta logica. La porta logica offre maggiore resilienza, maggiore disponibilità e condivisione del carico.

Tipi di gruppi di interfacce

Il sistema storage supporta tre tipi di gruppi di interfacce: Single-mode, static multimode e Dynamic Multimode. Ciascun gruppo di interfacce fornisce diversi livelli di tolleranza agli errori. I gruppi di interfacce multimodali forniscono metodi per il bilanciamento del carico del traffico di rete.

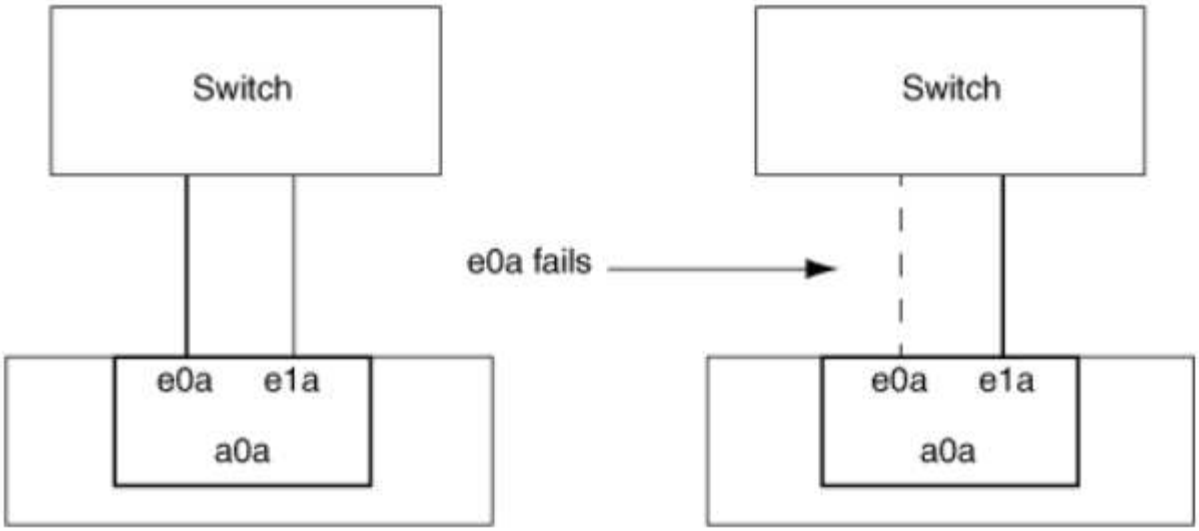
Caratteristiche dei gruppi di interfacce single-mode

In un gruppo di interfacce a modalità singola, è attiva solo una delle interfacce del gruppo di interfacce. Le altre interfacce sono in standby, pronte per essere utilizzate in caso di guasto dell'interfaccia attiva.

Caratteristiche di un gruppo di interfacce single-mode:

- Per il failover, il cluster monitora il collegamento attivo e controlla il failover. Poiché il cluster monitora il collegamento attivo, non è necessaria alcuna configurazione dello switch.
- In un gruppo di interfacce a modalità singola, in standby possono essere presenti più interfacce.
- Se un gruppo di interfacce single-mode si estende su più switch, è necessario collegare gli switch con un collegamento Inter-Switch (ISL).
- Per un gruppo di interfacce a modalità singola, le porte dello switch devono trovarsi nello stesso dominio di trasmissione.
- I pacchetti ARP per il monitoraggio dei collegamenti, che hanno un indirizzo di origine 0.0.0.0, vengono inviati sulle porte per verificare che le porte si trovino nello stesso dominio di trasmissione.

La figura riportata di seguito mostra un esempio di gruppo di interfacce a modalità singola. Nella figura, e0a ed e1a fanno parte del gruppo di interfacce single-mode di a0a. Se l'interfaccia attiva, e0a, si guasta, l'interfaccia e1a di standby assume il controllo e mantiene la connessione allo switch.



Per ottenere la funzionalità single-mode, si consiglia di utilizzare i gruppi di failover. Utilizzando un gruppo di failover, la seconda porta può ancora essere utilizzata per altre LIF e non deve rimanere inutilizzata. Inoltre, i gruppi di failover possono estendersi su più di due porte e possono estendersi su più nodi.

Caratteristiche dei gruppi di interfacce statiche multimodali

L'implementazione del gruppo di interfacce statiche multimodali in ONTAP è conforme allo standard IEEE 802.3ad (statico). Qualsiasi switch che supporti gli aggregati, ma non dispone di uno scambio di pacchetti di controllo per la configurazione di un aggregato, può essere utilizzato con gruppi di interfacce statiche multimodali.

I gruppi di interfacce statiche multimodali non sono conformi allo standard IEEE 802.3ad (dinamico), noto anche come link Aggregation Control Protocol (LACP). LACP è equivalente al protocollo di aggregazione delle porte (PAgP), il protocollo di aggregazione dei collegamenti proprietario di Cisco.

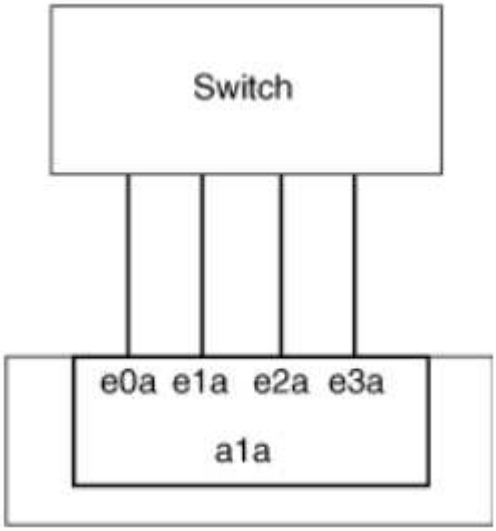
Di seguito sono riportate le caratteristiche di un gruppo di interfacce statiche multimodali:

- Tutte le interfacce del gruppo di interfacce sono attive e condividono un singolo indirizzo MAC.
  - Più connessioni individuali sono distribuite tra le interfacce nel gruppo di interfacce.
  - Ogni connessione o sessione utilizza un'interfaccia all'interno del gruppo di interfacce. Quando si utilizza lo schema di bilanciamento del carico sequenziale, tutte le sessioni vengono distribuite tra i collegamenti disponibili pacchetti per pacchetto e non sono associate a una particolare interfaccia del gruppo di interfacce.
- I gruppi di interfacce statiche multimodali possono essere ripristinati da un guasto di un massimo di interfacce "n-1", dove n è il numero totale di interfacce che formano il gruppo di interfacce.
- Se una porta non funziona o viene scollegata, il traffico che stava attraversando il collegamento guasto viene automaticamente ridistribuito a una delle interfacce rimanenti.
- I gruppi di interfacce statiche multimodali possono rilevare una perdita di collegamento, ma non possono rilevare una perdita di connettività al client o configurazioni errate dello switch che potrebbero influire sulla connettività e sulle prestazioni.
- Un gruppo di interfacce statiche multimodali richiede uno switch che supporti l'aggregazione di collegamenti su più porte di switch. Lo switch è configurato in modo che tutte le porte a cui sono collegati i collegamenti di un gruppo di interfacce facciano parte di una singola porta logica. Alcuni switch potrebbero non supportare l'aggregazione di collegamenti delle porte configurate per i frame jumbo. Per ulteriori

informazioni, consultare la documentazione del fornitore dello switch.

- Sono disponibili diverse opzioni di bilanciamento del carico per distribuire il traffico tra le interfacce di un gruppo di interfacce statiche multimodali.

La figura riportata di seguito mostra un esempio di gruppo di interfacce multimodali statiche. Le interfacce e0a, e1a, e2a e e3a fanno parte del gruppo di interfacce multimodali a1a. Tutte e quattro le interfacce nel gruppo di interfacce multimode a1a sono attive.



Esistono diverse tecnologie che consentono di distribuire il traffico in un singolo collegamento aggregato su più switch fisici. Le tecnologie utilizzate per abilitare questa funzionalità variano a seconda dei prodotti di rete. I gruppi di interfacce statiche multimodali in ONTAP sono conformi agli standard IEEE 802.3. Se si dice che una particolare tecnologia di aggregazione di collegamenti a switch multipli interagiti con o sia conforme agli standard IEEE 802.3, dovrebbe funzionare con ONTAP.

Lo standard IEEE 802.3 stabilisce che la periferica trasmittente in un collegamento aggregato determina l'interfaccia fisica per la trasmissione. Pertanto, ONTAP è responsabile solo della distribuzione del traffico in uscita e non può controllare il modo in cui arrivano i frame in entrata. Se si desidera gestire o controllare la trasmissione del traffico in entrata su un collegamento aggregato, tale trasmissione deve essere modificata sul dispositivo di rete direttamente connesso.

Gruppo di interfacce Multimode dinamiche

I gruppi di interfacce dinamiche multimodali implementano il protocollo LACP (link Aggregation Control Protocol) per comunicare l'appartenenza del gruppo allo switch direttamente collegato. LACP consente di rilevare lo stato di perdita del collegamento e l'impossibilità per il nodo di comunicare con la porta dello switch direct-attached.

L'implementazione del gruppo di interfacce multimodali dinamiche in ONTAP è conforme allo standard IEEE 802.3 ad (802.1 AX). ONTAP non supporta il protocollo di aggregazione delle porte (PAgP), un protocollo di aggregazione dei collegamenti proprietario di Cisco.

Un gruppo di interfacce multimodali dinamiche richiede uno switch che supporti LACP.

ONTAP implementa LACP in modalità attiva non configurabile che funziona bene con gli switch configurati in modalità attiva o passiva. ONTAP implementa i timer LACP lunghi e brevi (per l'utilizzo con valori non configurabili 3 secondi e 90 secondi), come specificato in IEEE 802.3 ad (802.1AX).

L'algoritmo di bilanciamento del carico ONTAP determina la porta membro da utilizzare per trasmettere il

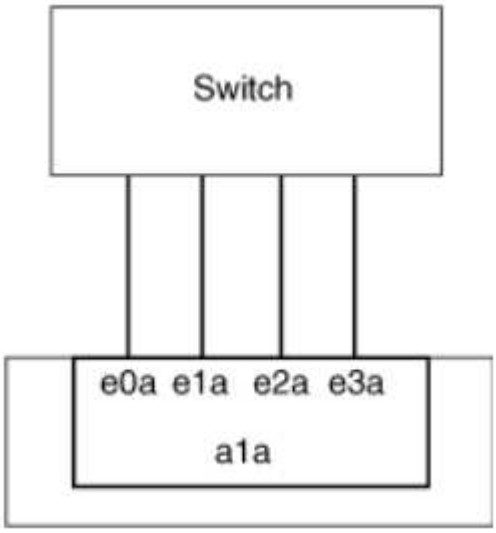
traffico in uscita e non controlla la modalità di ricezione dei frame in entrata. Lo switch determina il membro (singola porta fisica) del proprio gruppo di canali di porte da utilizzare per la trasmissione, in base all'algoritmo di bilanciamento del carico configurato nel gruppo di canali di porte dello switch. Pertanto, la configurazione dello switch determina la porta membro (singola porta fisica) del sistema di storage per ricevere il traffico. Per ulteriori informazioni sulla configurazione dello switch, consultare la documentazione del fornitore dello switch.

Se una singola interfaccia non riesce a ricevere pacchetti di protocollo LACP successivi, quella singola interfaccia viene contrassegnata come "lag_inactive" nell'output del comando "ifgrp status". Il traffico esistente viene automaticamente reindirizzato a tutte le interfacce attive rimanenti.

Quando si utilizzano gruppi di interfacce multimodali dinamiche, si applicano le seguenti regole:

- I gruppi di interfacce multimodali dinamiche devono essere configurati per utilizzare i metodi di bilanciamento del carico basati su porta, IP, MAC o round robin.
- In un gruppo di interfacce multimodali dinamiche, tutte le interfacce devono essere attive e condividere un singolo indirizzo MAC.

La figura riportata di seguito mostra un esempio di gruppo di interfacce multimodali dinamiche. Le interfacce e0a, e1a, e2a e e3a fanno parte del gruppo di interfacce multimodali a1a. Tutte e quattro le interfacce nel gruppo di interfacce dinamiche multimodali a1a sono attive.



Bilanciamento del carico in gruppi di interfacce multimodali

È possibile garantire che tutte le interfacce di un gruppo di interfacce multimodale siano utilizzate allo stesso modo per il traffico in uscita utilizzando l'indirizzo IP, l'indirizzo MAC, i metodi di bilanciamento del carico sequenziali o basati su porta per distribuire il traffico di rete in modo equo sulle porte di rete di un gruppo di interfacce multimode.

Il metodo di bilanciamento del carico per un gruppo di interfacce multimodali può essere specificato solo quando viene creato il gruppo di interfacce.

Best Practice: Si consiglia di eseguire il bilanciamento del carico basato su porta quando possibile. Utilizzare il bilanciamento del carico basato su porta, a meno che non vi sia un motivo o una limitazione specifica nella rete che lo impedisca.

Bilanciamento del carico basato su porta

Il metodo consigliato è il bilanciamento del carico basato su porta.

È possibile equalizzare il traffico su un gruppo di interfacce multimodali in base alle porte TCP/UDP (Transport Layer) utilizzando il metodo di bilanciamento del carico basato su porta.

Il metodo di bilanciamento del carico basato su porta utilizza un algoritmo di hashing rapido sugli indirizzi IP di origine e di destinazione insieme al numero di porta del layer di trasporto.

Bilanciamento del carico degli indirizzi IP e MAC

Il bilanciamento del carico degli indirizzi IP e MAC è un metodo per equalizzare il traffico su gruppi di interfacce multimodali.

Questi metodi di bilanciamento del carico utilizzano un algoritmo di hashing rapido sugli indirizzi di origine e di destinazione (indirizzo IP e indirizzo MAC). Se il risultato dell'algoritmo di hashing viene mappato su un'interfaccia che non si trova nello stato UP link, viene utilizzata la successiva interfaccia attiva.

> Non selezionare il metodo di bilanciamento del carico dell'indirizzo MAC quando si creano gruppi di interfacce su un sistema che si connette direttamente a un router. In tale configurazione, per ogni frame IP in uscita, l'indirizzo MAC di destinazione è l'indirizzo MAC del router. Di conseguenza, viene utilizzata una sola interfaccia del gruppo di interfacce.

Il bilanciamento del carico degli indirizzi IP funziona allo stesso modo per gli indirizzi IPv4 e IPv6.

Bilanciamento sequenziale del carico

È possibile utilizzare il bilanciamento del carico sequenziale per distribuire in modo uguale pacchetti tra più link utilizzando un algoritmo round robin. È possibile utilizzare l'opzione sequenziale per il bilanciamento del carico del traffico di una singola connessione su più collegamenti per aumentare il throughput di una singola connessione.

Tuttavia, poiché il bilanciamento del carico sequenziale può causare l'erogazione di pacchetti fuori servizio, le performance possono risultare estremamente scarse. Pertanto, il bilanciamento del carico sequenziale non è generalmente consigliato.

Creare un gruppo di interfacce o un LAG

È possibile creare un gruppo di interfacce o un LAG (single-mode, static multimode o Dynamic Multimode (LACP)) per presentare una singola interfaccia ai client combinando le funzionalità delle porte di rete aggregate.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per creare un LAG

Fasi

1. Selezionare **Network > Ethernet port > + link Aggregation Group** per creare un LAG.
2. Selezionare il nodo dall'elenco a discesa.
3. Scegliere tra le seguenti opzioni:
   a. ONTAP (Seleziona dominio broadcast) per **selezionare automaticamente il dominio di broadcast (scelta consigliata)**.
   b. Per selezionare manualmente un dominio di trasmissione.
4. Selezionare le porte per il LAG.
5. Selezionare la modalità:
   a. Singolo: Viene utilizzata una sola porta alla volta.
   b. Multiplo: Tutte le porte possono essere utilizzate contemporaneamente.
   c. LACP: Il protocollo LACP determina le porte che è possibile utilizzare.
6. Selezionare il bilanciamento del carico:
   a. Basato su IP
   b. Basato SU MAC
   c. Porta
   d. Sequenziale
7. Salvare le modifiche.

CLI

Utilizzare la CLI per creare un gruppo di interfacce

Quando si crea un gruppo di interfacce multimodali, è possibile specificare uno dei seguenti metodi di bilanciamento del carico:

- `port`: Il traffico di rete viene distribuito in base alle porte TCP/UDP (Transport Layer). Si tratta del metodo consigliato per il bilanciamento del carico.
- `mac`: Il traffico di rete viene distribuito in base agli indirizzi MAC.
- `ip`: Il traffico di rete viene distribuito in base agli indirizzi IP.
- `sequential`: Il traffico di rete viene distribuito man mano che viene ricevuto.

> L'indirizzo MAC di un gruppo di interfacce è determinato dall'ordine delle porte sottostanti e dalla modalità di inizializzazione di queste porte durante l'avvio. Pertanto, non si deve presumere che l'indirizzo MAC di ifgrp sia persistente durante i riavvii o gli aggiornamenti ONTAP.

Fase

Utilizzare `network port ifgrp create` per creare un gruppo di interfacce.

I gruppi di interfacce devono essere denominati utilizzando la sintassi `a<number><letter>`. Ad

esempio, a0a, a0b, a1c e a2a sono nomi di gruppi di interfacce validi.

Ulteriori informazioni su `network port ifgrp create` nella "Riferimento al comando ONTAP".

Nell'esempio seguente viene illustrato come creare un gruppo di interfacce denominato a0a con una funzione di distribuzione di porta e una modalità di multimode:

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

Aggiungere una porta a un gruppo di interfacce o LAG

È possibile aggiungere fino a 16 porte fisiche a un gruppo di interfacce o LAG per tutte le velocità delle porte.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per aggiungere una porta a un LAG

Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG*) per modificare un LAG.
2. Selezionare porte aggiuntive sullo stesso nodo da aggiungere al LAG.
3. Salvare le modifiche.

CLI

Utilizzare la CLI per aggiungere porte a un gruppo di interfacce

Fase

Aggiungere le porte di rete al gruppo di interfacce:

`network port ifgrp add-port`

Nell'esempio seguente viene illustrato come aggiungere la porta e0c a un gruppo di interfacce denominato a0a:

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

A partire da ONTAP 9.8, i gruppi di interfacce vengono inseriti automaticamente in un dominio di trasmissione appropriato circa un minuto dopo l'aggiunta della prima porta fisica al gruppo di interfacce. Se non si desidera che ONTAP esegua questa operazione e si preferisce inserire manualmente ifgrp in un dominio di trasmissione, specificare `-skip-broadcast-domain-placement` come parte di `ifgrp add-port` comando.

Ulteriori informazioni sulle limitazioni di configurazione e sulle `network port ifgrp add-port` limitazioni che si applicano ai gruppi di interfacce delle porte in "Riferimento al comando ONTAP".

Rimuovere una porta da un gruppo di interfacce o LAG

È possibile rimuovere una porta da un gruppo di interfacce che ospita le LIF, purché non sia l'ultima porta del

gruppo di interfacce. Non è necessario che il gruppo di interfacce non debba ospitare LIF o che il gruppo di interfacce non debba essere la porta home di una LIF, considerando che non si sta rimuovendo l'ultima porta dal gruppo di interfacce. Tuttavia, se si rimuove l'ultima porta, è necessario migrare o spostare i file LIF dal gruppo di interfacce.

A proposito di questa attività

È possibile rimuovere fino a 16 porte (interfacce fisiche) da un gruppo di interfacce o LAG.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per rimuovere una porta da un LAG

Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG*) per modificare un LAG.
2. Selezionare le porte da rimuovere dal LAG.
3. Salvare le modifiche.

CLI

Utilizzare la CLI per rimuovere le porte da un gruppo di interfacce

Fase

Rimuovere le porte di rete da un gruppo di interfacce:

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

Ulteriori informazioni su `network port ifgrp remove-port` nella "Riferimento al comando ONTAP".

Nell'esempio seguente viene illustrato come rimuovere la porta e0c da un gruppo di interfacce denominato a0a:

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

Eliminare un gruppo di interfacce o un LAG

È possibile eliminare i gruppi di interfacce o i LAG se si desidera configurare le LIF direttamente sulle porte fisiche sottostanti o si decide di modificare il gruppo di interfacce o la modalità LAG o la funzione di distribuzione.

Prima di iniziare

- Il gruppo di interfacce o il LAG non deve ospitare una LIF.
- Il gruppo di interfacce o LAG non deve essere né la porta home né la destinazione di failover di una LIF.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per eliminare un LAG

Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG*) per eliminare un LAG.
2. Selezionare il LAG che si desidera rimuovere.
3. Eliminare il LAG.

CLI

Utilizzare la CLI per eliminare un gruppo di interfacce

Fase

Utilizzare `network port ifgrp delete` comando per eliminare un gruppo di interfacce.

Ulteriori informazioni su `network port ifgrp delete` nella "Riferimento al comando ONTAP".

Nell'esempio seguente viene illustrato come eliminare un gruppo di interfacce denominato a0b:

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

Configurare LE VLAN ONTAP su porte fisiche

È possibile utilizzare le VLAN in ONTAP per fornire la segmentazione logica delle reti creando domini di broadcast separati definiti in base alla porta dello switch rispetto ai domini di broadcast tradizionali, definiti in base ai confini fisici.

Una VLAN può estendersi su più segmenti di rete fisici. Le stazioni finali appartenenti a una VLAN sono correlate in base alla funzione o all'applicazione.

Ad esempio, le stazioni finali in una VLAN possono essere raggruppate in base a reparti, ad esempio tecnici e contabili, o in base a progetti, ad esempio release1 e release2. Poiché la prossimità fisica delle stazioni finali non è essenziale in una VLAN, è possibile disperdere le stazioni finali geograficamente e contenere ancora il dominio di trasmissione in una rete commutata.

In ONTAP 9.14.1 e 9.13.1, le porte non contrassegnate che non sono utilizzate da alcuna interfaccia logica (LIF) e che non dispongono di connettività VLAN nativa sullo switch connesso vengono contrassegnate come degradate. Ciò serve ad identificare le porte inutilizzate e non indica un'interruzione. Le VLAN native consentono il traffico non taggato sulla porta base ifgrp, come le trasmissioni ONTAP CFM. Configurare le VLAN native sullo switch per impedire il blocco del traffico non taggato.

È possibile gestire le VLAN creando, eliminando o visualizzando le relative informazioni.

> Non creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non creare una VLAN e0b-10 su tale interfaccia.

Creare una VLAN

È possibile creare una VLAN per mantenere domini di trasmissione separati all'interno dello stesso dominio di rete utilizzando System Manager o l' `network port vlan create` comando.

Prima di iniziare

Verificare che siano soddisfatti i seguenti requisiti:

- Gli switch implementati nella rete devono essere conformi agli standard IEEE 802.1Q o disporre di un'implementazione delle VLAN specifica del vendor.
- Per supportare più VLAN, una stazione finale deve essere configurata staticamente per appartenere a una o più VLAN.
- La VLAN non è collegata a una porta che ospita una LIF del cluster.
- La VLAN non è collegata alle porte assegnate a Cluster IPSpace.
- La VLAN non viene creata su una porta del gruppo di interfacce che non contiene porte membro.

A proposito di questa attività

La creazione di una VLAN collega la VLAN alla porta di rete di un nodo specificato in un cluster.

Quando si configura una VLAN su una porta per la prima volta, la porta potrebbe spegnersi, causando una disconnessione temporanea della rete. Le successive aggiunte di VLAN alla stessa porta non influiscono sullo stato della porta.

> Non creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non creare una VLAN e0b-10 su tale interfaccia.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per creare una VLAN

A partire da ONTAP 9.12.0, è possibile selezionare automaticamente il dominio di trasmissione o manualmente dall'elenco. In precedenza, i domini di broadcast venivano sempre selezionati automaticamente in base alla connettività di livello 2. Se si seleziona manualmente un dominio di trasmissione, viene visualizzato un avviso che indica che la selezione manuale di un dominio di trasmissione potrebbe causare la perdita di connettività.

Fasi

1. Selezionare **Network > Ethernet port > + VLAN**.
2. Selezionare il nodo dall'elenco a discesa.
3. Scegliere tra le seguenti opzioni:
   a. ONTAP (Seleziona dominio broadcast) per **selezionare automaticamente il dominio di broadcast (scelta consigliata)**.
   b. Per selezionare manualmente un dominio di trasmissione dall'elenco.
4. Selezionare le porte per la VLAN.
5. Specificare l'ID VLAN.
6. Salvare le modifiche.

CLI

Utilizzare la CLI per creare una VLAN

In alcuni casi, se si desidera creare la porta VLAN su una porta degradata senza correggere il problema hardware o la configurazione errata del software, è possibile impostare `-ignore-health-status` del parametro `network port modify` comando as `true`.

Ulteriori informazioni su `network port modify` nella "Riferimento al comando ONTAP".

Fasi

1. Utilizzare `network port vlan create` Per creare una VLAN.
2. Specificare il `vlan-name` o il `port` e. `vlan-id` Opzioni per la creazione di una VLAN. Il nome della VLAN è una combinazione del nome della porta (o del gruppo di interfacce) e dell'identificatore della VLAN dello switch di rete, con un trattino nel mezzo. Ad esempio, `e0c-24` e. `e1c-80` Sono nomi VLAN validi.

Nell'esempio seguente viene illustrato come creare una VLAN `e1c-80` collegato alla porta di rete `e1c` sul nodo `cluster-1-01`:

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

A partire da ONTAP 9.8, le VLAN vengono automaticamente collocate nei domini di trasmissione appropriati circa un minuto dopo la loro creazione. Se non si desidera che ONTAP esegua questa operazione e si preferisce inserire manualmente la VLAN in un dominio di trasmissione, specificare `-skip-broadcast-domain-placement` come parte di `vlan create` comando.

Ulteriori informazioni su `network port vlan create` nella "Riferimento al comando ONTAP".

Modificare una VLAN

È possibile modificare il dominio di trasmissione o disattivare una VLAN.

Utilizzare System Manager per modificare una VLAN

A partire da ONTAP 9.12.0, è possibile selezionare automaticamente il dominio di trasmissione o manualmente dall'elenco. In precedenza, i domini broadcast venivano sempre selezionati automaticamente in base alla connettività di livello 2. Se si seleziona manualmente un dominio di trasmissione, viene visualizzato un avviso che indica che la selezione manuale di un dominio di trasmissione potrebbe causare la perdita di connettività.

Fasi

1. Selezionare **Network > Ethernet port > VLAN**.
2. Selezionare l'icona di modifica.
3. Effettuare una delle seguenti operazioni:
   - Modificare il dominio di trasmissione selezionandone uno diverso dall'elenco.
   - Deselezionare la casella di controllo **Enabled**.
4. Salvare le modifiche.

Eliminare una VLAN

Potrebbe essere necessario eliminare una VLAN prima di rimuovere una NIC dal relativo slot. Quando si elimina una VLAN, questa viene automaticamente rimossa da tutte le regole e i gruppi di failover che la utilizzano.

Prima di iniziare

Assicurarsi che non vi siano LIF associati alla VLAN.

A proposito di questa attività

L'eliminazione dell'ultima VLAN da una porta potrebbe causare la disconnessione temporanea della rete dalla porta.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per eliminare una VLAN

Fasi

1. Selezionare **Network > Ethernet port > VLAN**.
2. Selezionare la VLAN che si desidera rimuovere.
3. Fare clic su **Delete** (Elimina).

CLI

Utilizzare la CLI per eliminare una VLAN

Fase

Utilizzare `network port vlan delete` Comando per eliminare una VLAN.

Nell'esempio seguente viene illustrato come eliminare la VLAN `e1c-80` dalla porta di rete `e1c` sul nodo `cluster-1-01`:

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

Ulteriori informazioni su `network port vlan delete` nella "Riferimento al comando ONTAP".

Modificare gli attributi delle porte di rete ONTAP

È possibile modificare le impostazioni di negoziazione automatica, duplex, controllo di flusso, velocità e stato di una porta di rete fisica.

Prima di iniziare

La porta che si desidera modificare non deve ospitare le LIF.

A proposito di questa attività

- Si sconsiglia di modificare le impostazioni amministrative delle interfacce di rete 100 GbE, 40 GbE, 10 GbE o 1 GbE.

  I valori impostati per la modalità duplex e la velocità della porta vengono definiti impostazioni amministrative. A seconda delle limitazioni di rete, le impostazioni amministrative possono differire dalle impostazioni operative (ovvero, la modalità duplex e la velocità effettivamente utilizzate dalla porta).

- Si sconsiglia di modificare le impostazioni amministrative delle porte fisiche sottostanti in un gruppo di interfacce.

  Il `-up-admin` parameter (disponibile a livello di privilegio avanzato) modifica le impostazioni amministrative della porta.

- Si sconsiglia di impostare `-up-admin` Impostazione amministrativa su false per tutte le porte su un nodo o per la porta che ospita l'ultimo LIF del cluster operativo su un nodo.
- Si sconsiglia di modificare le dimensioni MTU della porta di gestione, `e0M`.

- La dimensione MTU di una porta in un dominio di trasmissione non può essere modificata dal valore MTU impostato per il dominio di trasmissione.
- Le dimensioni MTU di una VLAN non possono superare il valore delle dimensioni MTU della porta di base.

Fasi

1. Modificare gli attributi di una porta di rete:

   `network port modify`

2. È possibile impostare `-ignore-health-status` campo su vero per specificare che il sistema può ignorare lo stato di integrità della porta di rete di una porta specificata.

   Lo stato di integrità della porta di rete viene modificato automaticamente da degradato a integro e questa porta può essere utilizzata per ospitare i file LIF. Impostare il controllo di flusso delle porte del cluster su `none`. Per impostazione predefinita, il controllo di flusso è impostato su `full`.

Il seguente comando disattiva il controllo di flusso sulla porta e0b impostando il controllo di flusso su NONE:

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

Ulteriori informazioni su `network port modify` nella "Riferimento al comando ONTAP".

Creare porte 10GbE per reti ONTAP convertendo 40GbE porte NIC

È possibile convertire le schede di interfaccia di rete (NIC) X1144A-R6 e X91440A-R6 40GbE per supportare quattro porte 10 GbE.

Se si connette una piattaforma hardware che supporta una di queste schede di rete a un cluster che supporta l'interconnessione del cluster a 10 GbE e le connessioni dati del cliente, la scheda di rete deve essere convertita per fornire le connessioni a 10 GbE necessarie.

Prima di iniziare

È necessario utilizzare un cavo breakout supportato.

A proposito di questa attività

Per un elenco completo delle piattaforme che supportano le schede di rete, vedere "Hardware Universe".

> Sulla scheda NIC X1144A-R6, è possibile convertire solo la porta A per supportare le quattro connessioni 10GbE. Una volta convertita la porta A, la porta e non è disponibile per l'uso.

Fasi

1. Accedere alla modalità di manutenzione.
2. Conversione della scheda di rete dal supporto da 40 GbE al supporto da 10 GbE.

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

3. Dopo aver utilizzato il comando convert, arrestare il nodo.
4. Installare o sostituire il cavo.
5. A seconda del modello hardware, utilizzare il SP (Service Processor) o BMC (Baseboard Management Controller) per spegnere e riaccendere il nodo in modo che la conversione sia effettiva.

Configurare le porte UTA X1143A-R6 per la rete ONTAP

Per impostazione predefinita, l'adattatore target unificato X1143A-R6 è configurato in modalità target FC, ma è possibile configurarne le porte come porte Ethernet e FCoE (CNA) da 10 GB o come porte di destinazione o iniziatore FC da 16 GB. Questo richiede diversi adattatori SFP+.

Se configurati per Ethernet e FCoE, gli adattatori X1143A-R6 supportano il traffico di destinazione simultaneo di NIC e FCoE sulla stessa porta 10-GBE. Se configurata per FC, ciascuna coppia di due porte che condivide lo stesso ASIC può essere configurata singolarmente per la destinazione FC o la modalità iniziatore FC. Ciò significa che un singolo adattatore X1143A-R6 può supportare la modalità di destinazione FC su una coppia a due porte e la modalità iniziatore FC su un'altra coppia a due porte. Le coppie di porte collegate allo stesso ASIC devono essere configurate nella stessa modalità.

In modalità FC, l'adattatore X1143A-R6 si comporta come qualsiasi dispositivo FC esistente con velocità fino a 16 Gbps. In modalità CNA, è possibile utilizzare l'adattatore X1143A-R6 per la condivisione simultanea del traffico NIC e FCoE sulla stessa porta 10 GbE. La modalità CNA supporta solo la modalità di destinazione FC per la funzione FCoE.

Per configurare l'adattatore di destinazione unificato (X1143A-R6), è necessario configurare le due porte adiacenti sullo stesso chip nella stessa modalità personality.

Fasi

1. Visualizzare la configurazione delle porte:

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

2. Configurare le porte in base alle esigenze per Fibre Channel (FC) o Converged Network Adapter (CNA):

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

3. Collegare i cavi appropriati per FC o Ethernet da 10 GB.
4. Verificare di avere installato il modulo SFP+ corretto:

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

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, in base al fabric FC a cui è collegato.

Convertire la porta UTA2 per l’utilizzo nella rete ONTAP

È possibile convertire la porta UTA2 da modalità Converged Network Adapter (CNA) a modalità Fibre Channel (FC) o viceversa.

È necessario modificare la personalità UTA2 dalla modalità CNA alla modalità FC quando è necessario modificare il supporto fisico che collega la porta alla rete o per supportare gli iniziatori FC e la destinazione.

Dalla modalità CNA alla modalità FC

Fasi

1. Portare l'adattatore offline:

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

2. Modificare la modalità della porta:

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

3. Riavviare il nodo, quindi portare l'adattatore in linea:

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

4. Avvisare l'amministratore o il gestore VIF di eliminare o rimuovere la porta, a seconda dei casi:
   - Se la porta viene utilizzata come porta principale di una LIF, fa parte di un gruppo di interfacce (ifgrp) o ospita VLAN, un amministratore deve eseguire le seguenti operazioni:
     - Spostare le LIF, rimuovere la porta da ifgrp o eliminare le VLAN, rispettivamente.
     - Eliminare manualmente la porta eseguendo il `network port delete` comando. Se il `network port delete` comando non riesce, l'amministratore dovrebbe risolvere gli errori, quindi eseguire nuovamente il comando.
   - Se la porta non viene utilizzata come porta home di un LIF, non è membro di un ifgrp e non ospita VLAN, il gestore VIF deve rimuovere la porta dai record al momento del riavvio. Se il gestore VIF non rimuove la porta, l'amministratore deve rimuoverla manualmente dopo il riavvio utilizzando il `network port delete` comando.

     Ulteriori informazioni su `network port delete` nella "Riferimento al comando ONTAP".

5. Verificare di avere installato il modulo SFP+ corretto:

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

   Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, prima di modificare la configurazione sul nodo.

Dalla modalità FC alla modalità CNA

Fasi

1. Portare l'adattatore offline:

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

2. Modificare la modalità della porta:

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

3. Riavviare il nodo
4. Verificare che sia installato il corretto SFP+.

   Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB.

Convertire i moduli ottici CNA/UTA2 per la rete ONTAP

È necessario modificare i moduli ottici sull'adattatore di destinazione unificato (CNA/UTA2) per supportare la modalità di personalità selezionata per l'adattatore.

Fasi

1. Verificare l'SFP+ corrente utilizzato nella scheda. Quindi, sostituire il modulo SFP+ corrente con il modulo SFP+ appropriato per il linguaggio preferito (FC o CNA).
2. Rimuovere i moduli ottici correnti dall'adattatore X1143A-R6.
3. Inserire i moduli corretti per l'ottica della modalità Personality (FC o CNA) preferita.
4. Verificare di avere installato il modulo SFP+ corretto:

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

   I moduli SFP+ supportati e i cavi in rame (Twinax) con marchio Cisco sono elencati nella "NetApp Hardware Universe".

Rimozione delle schede di rete dai nodi del cluster ONTAP

Potrebbe essere necessario rimuovere una scheda NIC difettosa dal relativo slot o spostarla in un altro slot per scopi di manutenzione.

> La procedura per la rimozione di una scheda di interfaccia di rete è diversa in ONTAP 9,7 e nelle versioni precedenti. Se è necessario rimuovere una scheda di rete da un nodo cluster ONTAP che esegue ONTAP 9,7 e versioni precedenti, consultare la procedura "Rimozione di una scheda di rete dal nodo (ONTAP 9,7 o versione precedente)".

Fasi

1. Spegnere il nodo.

2. Rimuovere fisicamente la scheda NIC dal relativo slot.
3. Accendere il nodo.
4. Verificare che la porta sia stata eliminata:

```
network port show
```

> ONTAP rimuove automaticamente la porta da qualsiasi gruppo di interfacce. Se la porta era l'unico membro di un gruppo di interfacce, il gruppo di interfacce viene cancellato. Ulteriori informazioni su `network port show` nella "Riferimento al comando ONTAP".

5. Se sulla porta sono configurate delle VLAN, queste vengono spostate. È possibile visualizzare le VLAN smontate utilizzando il seguente comando:

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

> Il `displaced-interface show`, `displaced-vlans show`, e. `displaced-vlans restore` i comandi sono univoci e non richiedono il nome completo del comando, che inizia con `cluster controller-replacement network`.

6. Queste VLAN vengono eliminate, ma possono essere ripristinate utilizzando il seguente comando:

```
displaced-vlans restore
```

7. Se sulla porta sono configurate delle LIF, ONTAP sceglie automaticamente nuove porte home per quelle LIF su un'altra porta nello stesso dominio di trasmissione. Se sullo stesso filer non viene trovata alcuna porta home adatta, tali LIF vengono considerati spostati. È possibile visualizzare i file LIF spostati utilizzando il seguente comando:

   `displaced-interface show`

8. Quando viene aggiunta una nuova porta al dominio di trasmissione sullo stesso nodo, le porte home per i file LIF vengono ripristinate automaticamente. In alternativa, è possibile impostare la porta home utilizzando `network interface modify -home-port -home-node or use the displaced-interface restore` comando.

Informazioni correlate

- "cluster controller-replacement network deplaced-interface delete"
- "modifica dell'interfaccia di rete"

Monitorare le porte di rete

Monitorare lo stato delle porte di rete ONTAP

La gestione ONTAP delle porte di rete include il monitoraggio automatico dello stato di salute e un set di monitor per aiutare a identificare le porte di rete che potrebbero non

essere adatte per l'hosting di LIF.

A proposito di questa attività

Se un monitor dello stato di salute determina che una porta di rete non è funzionante, avvisa gli amministratori tramite un messaggio EMS o contrassegna la porta come danneggiata. ONTAP evita l'hosting di LIF su porte di rete degradate se sono presenti destinazioni di failover alternative sane per tale LIF. Una porta può diventare degradata a causa di un errore di tipo soft, come ad esempio il link flapping (link che rimbalzano rapidamente tra up e down) o la partizione di rete:

- Le porte di rete nell'IPSpace del cluster vengono contrassegnate come degradate quando si verificano lo sfarfallio del collegamento o la perdita di raggiungibilità Layer 2 (L2) ad altre porte di rete nel dominio di trasmissione.
- Le porte di rete negli spazi IP non cluster vengono contrassegnate come degradate quando si verifica lo sfarfallio dei collegamenti.

È necessario conoscere i seguenti comportamenti di una porta danneggiata:

- Una porta degradata non può essere inclusa in una VLAN o in un gruppo di interfacce.

  Se una porta membro di un gruppo di interfacce è contrassegnata come degradata, ma il gruppo di interfacce è ancora contrassegnato come integro, i file LIF possono essere ospitati su quel gruppo di interfacce.

- Le LIF vengono migrate automaticamente dalle porte degradate alle porte integre.
- Durante un evento di failover, una porta degradata non viene considerata come destinazione di failover. Se non sono disponibili porte integre, le porte degradate ospitano le LIF in base alla normale policy di failover.
- Non è possibile creare, migrare o ripristinare una LIF su una porta degradata.

  È possibile modificare `ignore-health-status` impostazione della porta di rete su `true`. È quindi possibile ospitare una LIF sulle porte sane.

Fasi

1. Accedere alla modalità avanzata dei privilegi:

   ```
   set -privilege advanced
   ```

2. Controllare quali monitor di stato sono abilitati per il monitoraggio dello stato delle porte di rete:

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

   Lo stato di salute di una porta è determinato dal valore dei monitor di stato.

   I seguenti monitor di stato sono disponibili e abilitati per impostazione predefinita in ONTAP:

   - Monitor di stato link-flapping: Monitora il link flapping

     Se una porta presenta uno sfarfallio del collegamento più di una volta in cinque minuti, questa porta viene contrassegnata come degradata.

- L2 Reachability Health Monitor: Monitora se tutte le porte configurate nello stesso dominio di trasmissione hanno una raggiungibilità L2 l'una rispetto all'altra

  Questo monitor dello stato di salute segnala problemi di raggiungibilità L2 in tutti gli spazi IP; tuttavia, contrassegna solo le porte nell'IPSpace del cluster come degradate.

- Monitor CRC: Monitora le statistiche CRC sulle porte

  Questo monitor dello stato di salute non contrassegna una porta come degradata, ma genera un messaggio EMS quando si osserva un tasso di guasti CRC molto elevato.

Ulteriori informazioni su `network options port-health-monitor show` nella "Riferimento al comando ONTAP".

3. Attivare o disattivare i monitor di stato di un IPSpace come desiderato utilizzando `network options port-health-monitor modify` comando.

   Ulteriori informazioni su `network options port-health-monitor modify` nella "Riferimento al comando ONTAP".

4. Visualizzazione dello stato dettagliato di una porta:

```
network port show -health
```

L'output del comando visualizza lo stato di salute della porta, `ignore health status` impostazione ed elenco dei motivi per cui la porta è contrassegnata come degradata.

Lo stato di integrità della porta può essere `healthy` oppure `degraded`.

Se il `ignore health status` l'impostazione è `true`, indica che lo stato di salute della porta è stato modificato da `degraded` a. `healthy` dall'amministratore.

Se il `ignore health status` l'impostazione è `false`, lo stato delle porte viene determinato automaticamente dal sistema.

Ulteriori informazioni su `network port show` nella "Riferimento al comando ONTAP".

Monitorare la raggiungibilità delle porte di rete ONTAP

Il monitoraggio della raggiungibilità è integrato in ONTAP 9.8 e versioni successive. Utilizzare questo monitoraggio per identificare quando la topologia fisica della rete non corrisponde alla configurazione ONTAP. In alcuni casi, ONTAP può riparare la raggiungibilità delle porte. In altri casi, sono necessari ulteriori passaggi.

A proposito di questa attività

Utilizzare questi comandi per verificare, diagnosticare e riparare le configurazioni errate della rete derivanti dalla configurazione ONTAP che non corrisponde al cablaggio fisico o alla configurazione dello switch di rete.

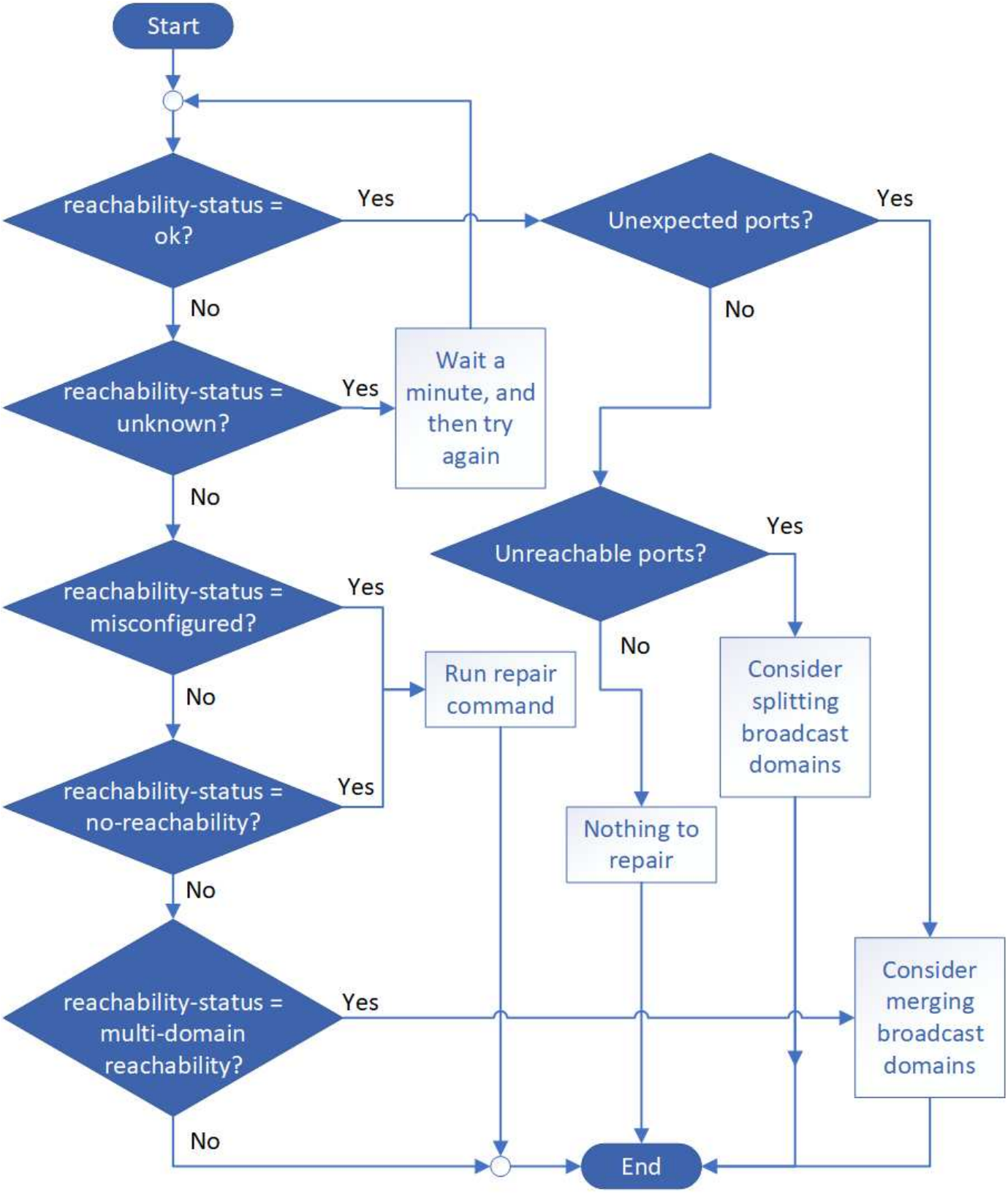
Fase

1. Visualizzazione della raggiungibilità delle porte:

```
network port reachability show
```

Ulteriori informazioni su `network port reachability show` nella "Riferimento al comando ONTAP".

2. Utilizzare la seguente struttura decisionale e la seguente tabella per determinare la fase successiva, se presente.



Stato di raggiungibilità	Descrizione

ok	La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato. Se lo stato di raggiungibilità è "ok", ma ci sono "porte impreviste", considerare la possibilità di unire uno o più domini di broadcast. Per ulteriori informazioni, consulta la seguente riga *Unexpected ports*. Se lo stato di raggiungibilità è "ok", ma ci sono "porte irraggiungibili", considerare la possibilità di suddividere uno o più domini di broadcast. Per ulteriori informazioni, consultare la riga *Unreachable ports* riportata di seguito. Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.
Porte impreviste	La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast. Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione. Per ulteriori informazioni, vedere "Unire i domini di broadcast".
Porte non raggiungibili	Se un singolo dominio di broadcast è stato suddiviso in due diversi set di raggiungibilità, è possibile suddividere un dominio di broadcast per sincronizzare la configurazione ONTAP con la topologia fisica della rete. In genere, l'elenco delle porte irraggiungibili definisce il set di porte che devono essere suddivise in un altro dominio di trasmissione dopo aver verificato che la configurazione fisica e quella dello switch sono accurate. Per ulteriori informazioni, vedere "Suddividere i domini di broadcast".
riconfigurazione non corretta	La porta non dispone di capacità di livello 2 rispetto al dominio di trasmissione assegnato; tuttavia, la porta dispone di capacità di livello 2 rispetto a un dominio di trasmissione diverso. È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta al dominio di trasmissione a cui è possibile accedere: `network port reachability repair -node -port`Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte".

nessuna raggiungibilità	La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente. È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta a un nuovo dominio di trasmissione creato automaticamente in IPSpace predefinito: `network port reachability repair -node -port` Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte". Ulteriori informazioni su `network port reachability repair` nella "Riferimento al comando ONTAP".
raggiungibilità multi-dominio	La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast. Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione. Per ulteriori informazioni, vedere "Unire i domini di broadcast" oppure "Riparare la raggiungibilità delle porte".
sconosciuto	Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.

Dopo aver riparato una porta, è necessario controllare e risolvere le LIF e le VLAN spostate. Se la porta faceva parte di un gruppo di interfacce, è necessario comprendere anche cosa è successo a quel gruppo di interfacce. Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte".

Informazioni sull'utilizzo delle porte sulla rete ONTAP

Diverse porte note sono riservate alle comunicazioni ONTAP con servizi specifici. I conflitti di porta si verificano se un valore di porta nell'ambiente di rete di archiviazione è uguale al valore di una porta ONTAP.

Traffico in entrata

Il traffico in entrata nello storage ONTAP utilizza i seguenti protocolli e porte:

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
TCP	22	Accesso sicuro alla shell all'indirizzo IP della LIF di gestione cluster o una LIF di gestione nodi
TCP	80	Accesso alla pagina web all'indirizzo IP della LIF di gestione cluster
TCP/UDP	111	RPCBIND, chiamata di procedura remota per NFS
UDP	123	NTP, protocollo orario di rete

TCP	135	MSRPC, chiamata di procedura remota Microsoft
TCP	139	NETBIOS-SSN, sessione di servizio NetBIOS per CIFS
TCP/UDP	161-162	SNMP, protocollo di gestione di rete semplice
TCP	443	Accesso sicuro alla pagina web all'indirizzo IP della LIF di gestione cluster
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS su TCP con framing NetBIOS
TCP/UDP	635	NFS mount per interagire con un file system remoto come se fosse locale
TCP	749	Kerberos
UDP	953	Nome daemon
TCP/UDP	2049	Daemon del server NFS
TCP	2050	NRV, protocollo volume remoto NetApp
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP/UDP	4045	Daemon di blocco NFS
TCP/UDP	4046	Network status monitor per NFS
UDP	4049	Rquotad RPC NFS
UDP	4444	KRB524, Kerberos 524
UDP	5353	DNS multicast
TCP	10000	Backup mediante Network Data Management Protocol (NDMP)
TCP	11104	Peering dei cluster, gestione bidirezionale delle sessioni di comunicazione intercluster per SnapMirror
TCP	11105	Peering del cluster, trasferimento di dati SnapMirror bidirezionale che utilizza intercluster LIF
SSL/TLS	30000	Accetta connessioni di controllo sicure NDMP tra il server DMA e NDMP tramite socket sicuri (SSL/TLS). Gli scanner di sicurezza possono segnalare una vulnerabilità sulla porta 30000.

Traffico in uscita

Il traffico in uscita nello storage ONTAP può essere impostato utilizzando regole di base o avanzate in base alle esigenze aziendali.

Regole di base in uscita

Tutte le porte possono essere utilizzate per tutto il traffico in uscita tramite i protocolli ICMP, TCP e UDP.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita

Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da ONTAP.

Active Directory

Protocollo	Porta	Origine	Destinazione	Scopo
TCP	88	Gestione dei nodi LIF, data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
UDP	137	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
UDP	138	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
TCP	139	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
TCP	389	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
UDP	389	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
TCP	445	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	464	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V (SET_CHANGE)
UDP	464	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
TCP	749	Gestione dei nodi LIF, data LIF (NFS, CIFS)	Insieme di strutture di Active Directory	Modificare e impostare la password Kerberos V (RPCSEC_GSS)

AutoSupport

Protocollo	Porta	Origine	Destinazione	Scopo
TCP	80	LIF di gestione dei nodi	support.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)

SNMP

Protocollo	Porta	Origine	Destinazione	Scopo
TCP/UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP

SnapMirror

Protocollo	Porta	Origine	Destinazione	Scopo
TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror

Altri servizi

Protocollo	Porta	Origine	Destinazione	Scopo
TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog
TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3
TCP	da 18600 a 18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP

Informazioni sulle porte interne di ONTAP

La tabella seguente elenca le porte utilizzate internamente da ONTAP e le relative funzioni. ONTAP utilizza queste porte per diverse funzioni, come ad esempio la comunicazione LIF intracluster.

Questo elenco non è esaustivo e potrebbe variare a seconda degli ambienti.

Porta/protocollo	Componente/funzione
514	Syslog
900	RPC cluster di NetApp

902	RPC cluster di NetApp
904	RPC cluster di NetApp
905	RPC cluster di NetApp
910	RPC cluster di NetApp
911	RPC cluster di NetApp
913	RPC cluster di NetApp
914	RPC cluster di NetApp
915	RPC cluster di NetApp
918	RPC cluster di NetApp
920	RPC cluster di NetApp
921	RPC cluster di NetApp
924	RPC cluster di NetApp
925	RPC cluster di NetApp
927	RPC cluster di NetApp
928	RPC cluster di NetApp
929	RPC cluster di NetApp
930	Servizi e funzioni di gestione del kernel (KSMF)
931	RPC cluster di NetApp
932	RPC cluster di NetApp
933	RPC cluster di NetApp
934	RPC cluster di NetApp
935	RPC cluster di NetApp
936	RPC cluster di NetApp
937	RPC cluster di NetApp
939	RPC cluster di NetApp
940	RPC cluster di NetApp
951	RPC cluster di NetApp
954	RPC cluster di NetApp
955	RPC cluster di NetApp
956	RPC cluster di NetApp
958	RPC cluster di NetApp
961	RPC cluster di NetApp
963	RPC cluster di NetApp
964	RPC cluster di NetApp

966	RPC cluster di NetApp
967	RPC cluster di NetApp
975	Protocollo KMIP (Key Management Interoperability Protocol)
982	RPC cluster di NetApp
983	RPC cluster di NetApp
5125	Porta di controllo alternativa per il disco
5133	Porta di controllo alternativa per il disco
5144	Porta di controllo alternativa per il disco
65502	SSH. Ambito nodo
65503	Condivisione LIF
7700	Gestione sessioni cluster (CSM)
7810	RPC cluster di NetApp
7811	RPC cluster di NetApp
7812	RPC cluster di NetApp
7813	RPC cluster di NetApp
7814	RPC cluster di NetApp
7815	RPC cluster di NetApp
7816	RPC cluster di NetApp
7817	RPC cluster di NetApp
7818	RPC cluster di NetApp
7819	RPC cluster di NetApp
7820	RPC cluster di NetApp
7821	RPC cluster di NetApp
7822	RPC cluster di NetApp
7823	RPC cluster di NetApp
7824	RPC cluster di NetApp
7835-7839 e 7845-7849	Porte TCP per la comunicazione intracluster
8023	Ambito del nodo TELNET
8443	Porta NAS ONTAP S3 per Amazon FSx
8514	Scope del nodo RSH
9877	Porta client KMIP (solo host locale interno)
10006	Porta TCP per la comunicazione di interconnessione HA

Informazioni sul copyright

Informazioni sul marchio commerciale