



# **Gestione della rete**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommario

Gestione della rete .....	1
Inizia subito .....	1
Componenti di rete .....	5
Flusso di lavoro di failover del percorso NAS (ONTAP 9,8 e versioni successive) .....	10
Flusso di lavoro di failover del percorso NAS (ONTAP 9,7 e versioni precedenti) .....	18
Porte di rete .....	30
IPspaces .....	56
Domini di broadcast .....	63
Gruppi e policy di failover .....	85
Subnet (solo amministratori del cluster) .....	89
Creare SVM .....	97
Interfacce logiche (LIF) .....	104
Bilanciamento dei carichi di rete .....	134
Risoluzione del nome host .....	143
Proteggere la rete .....	146
Contrassegno QoS (solo amministratori del cluster) .....	161
Gestione SNMP (solo amministratori cluster) .....	163
Gestire il routing in una SVM .....	174
Visualizzare le informazioni di rete .....	179

# Gestione della rete

## Inizia subito

### Panoramica sulla gestione della rete

Puoi utilizzare le seguenti informazioni per eseguire un'amministrazione di base della rete di storage usando System Manager o l'interfaccia CLI. È possibile configurare le porte di rete fisiche e virtuali (VLAN e gruppi di interfacce), creare LIF utilizzando IPv4 e IPv6, gestire i servizi di routing e risoluzione degli host nei cluster, utilizzare il bilanciamento del carico per ottimizzare il traffico di rete e monitorare un cluster utilizzando SNMP.

Se non diversamente specificato, le procedure CLI si applicano a tutte le versioni di ONTAP 9.

Per comprendere l'impatto delle funzionalità di rete disponibili in ogni versione di ONTAP 9, vedere la ["Note di rilascio di ONTAP"](#).

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per visualizzare un grafico che mostra i componenti e la configurazione della rete. A partire da ONTAP 9.12, è possibile visualizzare l'associazione di LIF e subnet nella griglia delle interfacce di rete. Se si utilizza Gestione sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), vedere ["Gestione della rete"](#).

La nuova funzionalità di visualizzazione della rete consente agli utenti di visualizzare il percorso delle connessioni di rete tra host, porte, SVM, volumi e così via in un'interfaccia grafica.

Il grafico viene visualizzato quando si seleziona **rete > Panoramica** o quando si seleziona ➔ Dalla sezione **Network** della dashboard.

La figura mostra le seguenti categorie di componenti:


- Host
- Porte di storage
- Interfacce di rete
- VM di storage
- Componenti per l'accesso ai dati

Ogni sezione mostra ulteriori dettagli che è possibile spostare il mouse o selezionare per eseguire attività di configurazione e gestione della rete.

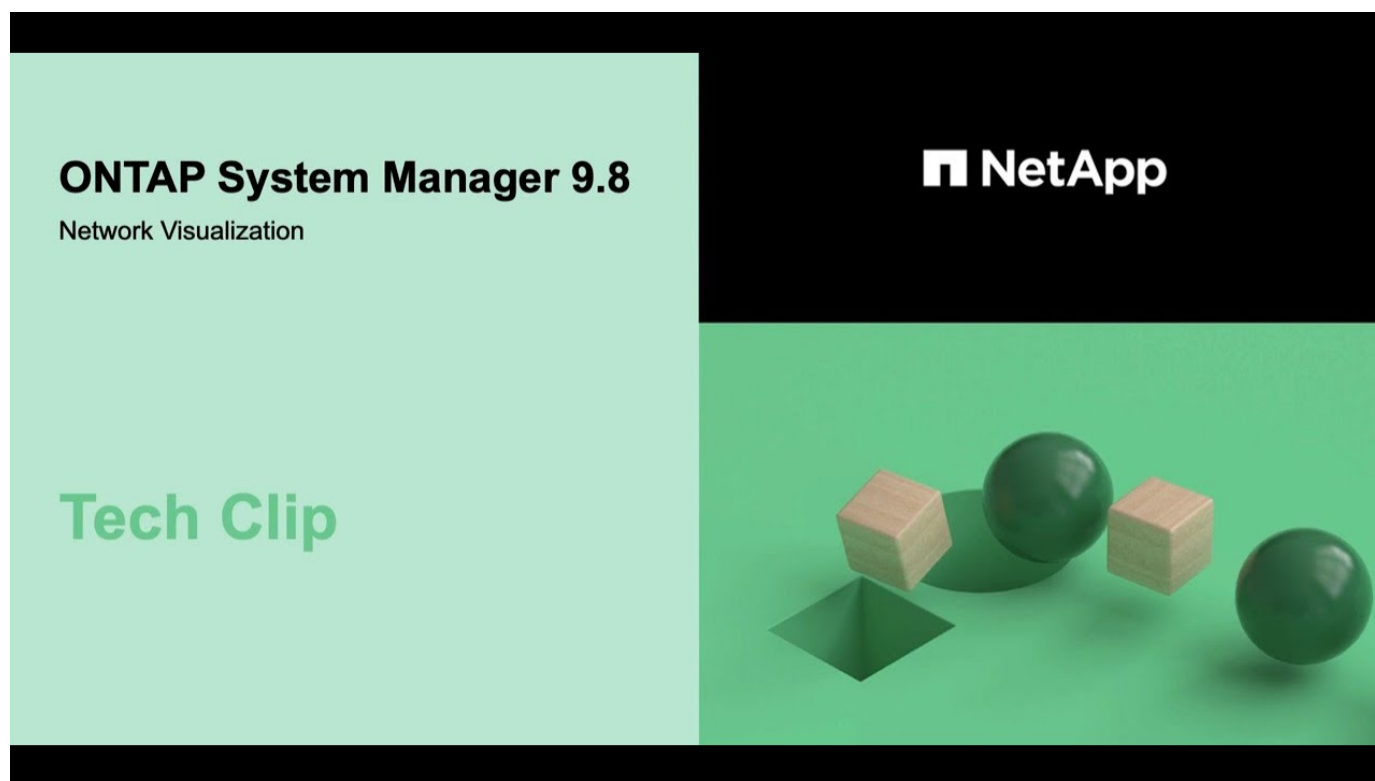
### Esempi

Di seguito sono riportati alcuni esempi dei diversi modi in cui è possibile interagire con la grafica per visualizzare i dettagli di ciascun componente o avviare azioni per gestire la rete:

- Fare clic su un host per visualizzarne la configurazione: Porte, interfacce di rete, VM di storage e componenti di accesso ai dati associati.
- Passare il mouse sul numero di volumi in una VM di storage per selezionare un volume e visualizzarne i dettagli.
- Selezionare un'interfaccia iSCSI per visualizzarne le prestazioni nell'ultima settimana.

- Fare clic su  accanto a un componente per avviare azioni per modificare tale componente.
- Determinare rapidamente dove potrebbero verificarsi problemi nella rete, indicato da una "X" accanto ai componenti non funzionanti.

## Video System Manager Network Visualization



### Verificare la configurazione di rete in seguito a un aggiornamento ONTAP da ONTAP 9,7x o versione precedente

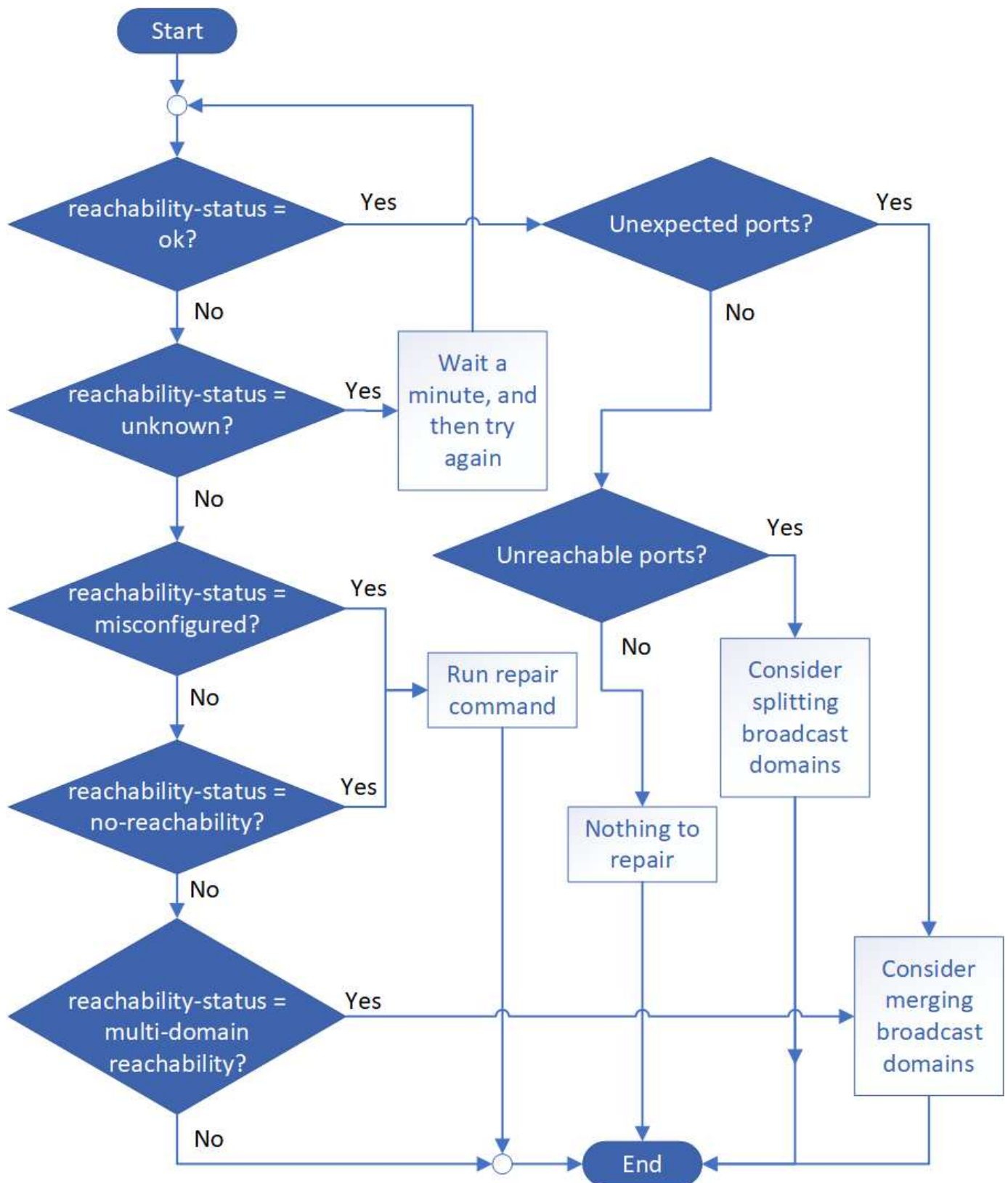
Dopo aver eseguito l'aggiornamento da ONTAP 9,7x o versione precedente a ONTAP 9,8 o versione successiva, è necessario verificare la configurazione di rete. Dopo l'aggiornamento, ONTAP monitora automaticamente la raggiungibilità di livello 2.

#### Fase

1. Verificare che ogni porta sia raggiungibile dal proprio dominio di trasmissione previsto:

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

L'output del comando contiene i risultati di raggiungibilità. Utilizzare il seguente albero decisionale e la seguente tabella per comprendere i risultati di raggiungibilità (stato di raggiungibilità) e determinare cosa, se necessario, fare in seguito.



stato di raggiungibilità	Descrizione
--------------------------	-------------

ok	<p>La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato.</p> <p>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, vedere <a href="#">"Unire i domini di broadcast"</a>.</p> <p>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, vedere <a href="#">"Suddividere i domini di broadcast"</a>.</p> <p>Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.</p>
riconfigurazione non corretta	<p>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.</p> <p>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:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
nessuna raggiungibilità	<p>La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente.</p> <p>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:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
raggiungibilità multi-dominio	<p>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.</p> <p>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.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a> oppure <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
sconosciuto	<p>Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.</p>

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"](#).

## Componenti di rete

### Panoramica dei componenti di rete di un cluster

Prima di configurare il cluster, è necessario acquisire familiarità con i componenti di rete di un cluster. La configurazione dei componenti fisici di rete di un cluster in componenti logici offre la flessibilità e la funzionalità multi-tenancy di ONTAP.

I vari componenti di rete in un cluster sono i seguenti:

- Porte fisiche

Le schede di interfaccia di rete (NIC) e gli host bus adapter (HBA) forniscono connessioni fisiche (Ethernet e Fibre Channel) da ciascun nodo alle reti fisiche (reti di gestione e dati).

Per i requisiti del sito, le informazioni sullo switch, il cablaggio delle porte e il cablaggio delle porte integrate del controller, consultare la Hardware Universe all'indirizzo ["hwu.netapp.com"](http://hwu.netapp.com).

- Porte logiche

Le Virtual Local Area Network (VLAN) e i gruppi di interfacce costituiscono le porte logiche. I gruppi di interfacce trattano diverse porte fisiche come una singola porta, mentre le VLAN suddividono una porta fisica in più porte separate.

- IPspaces

È possibile utilizzare un IPspace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

- Domini di broadcast

Un dominio di broadcast risiede in un IPspace e contiene un gruppo di porte di rete, potenzialmente provenienti da molti nodi del cluster, appartenenti alla stessa rete Layer 2. Le porte del gruppo vengono utilizzate in una SVM per il traffico dati.

- Subnet

Una subnet viene creata all'interno di un dominio di broadcast e contiene un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Questo pool di indirizzi IP semplifica l'allocazione degli indirizzi IP durante la creazione di LIF.

- Interfacce logiche

Un'interfaccia logica (LIF) è un indirizzo IP o un nome di porta universale (WWPN) associato a una porta. È associato ad attributi come gruppi di failover, regole di failover e regole firewall. Una LIF comunica attraverso la rete attraverso la porta (fisica o logica) alla quale è attualmente associata.

I diversi tipi di LIF in un cluster sono LIF di dati, LIF di gestione con ambito cluster, LIF di gestione con ambito nodo, LIF di intercluster e LIF di cluster. La proprietà delle LIF dipende dalla SVM in cui risiede la LIF. Le LIF dei dati sono di proprietà delle SVM dei dati, le LIF di gestione con ambito del nodo, la gestione con ambito del cluster e le LIF tra cluster sono di proprietà delle SVM amministrative e le LIF del cluster

sono di proprietà delle SVM del cluster.

- Zone DNS

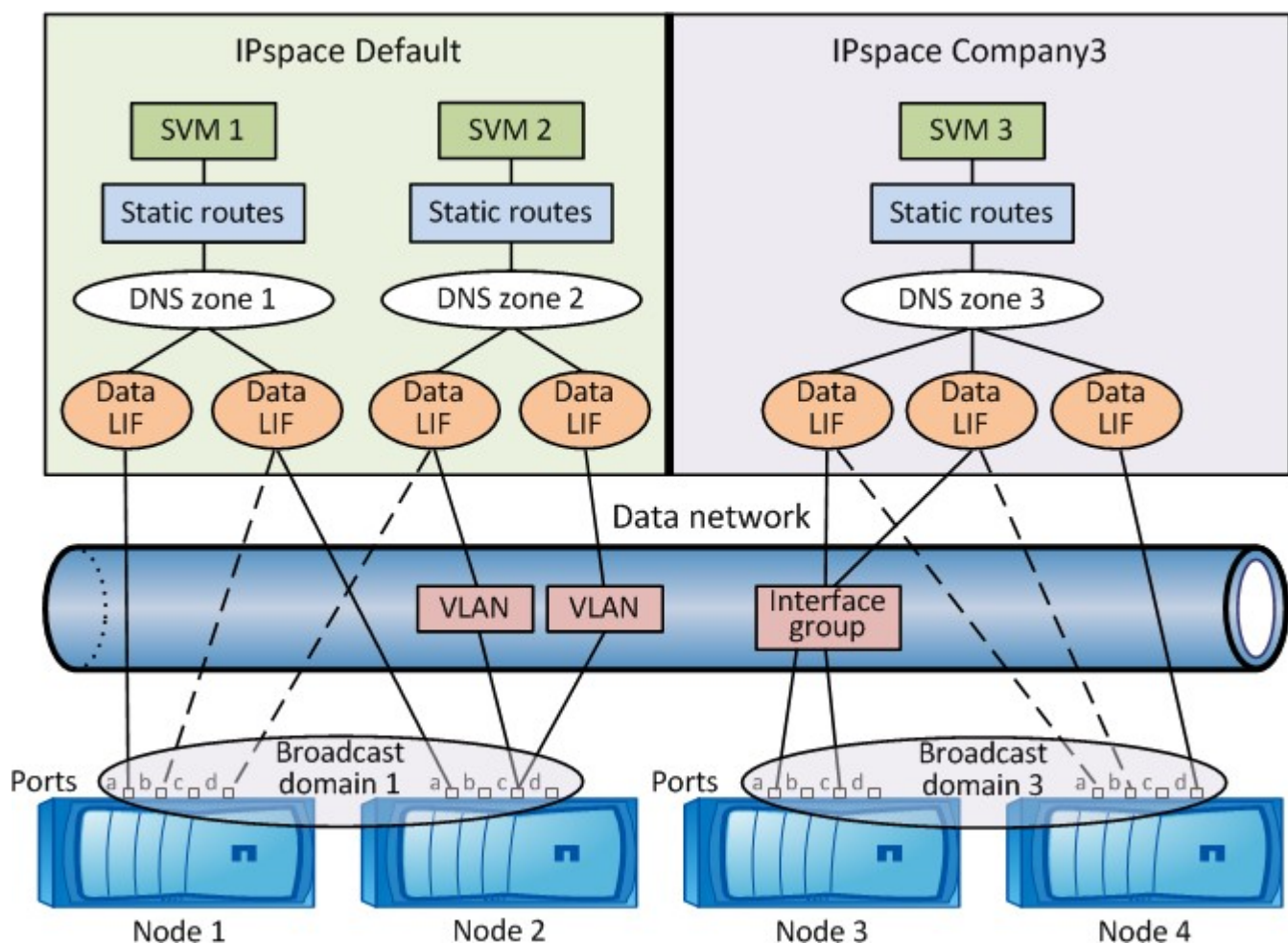
È possibile specificare la zona DNS durante la creazione della LIF, fornendo un nome per la LIF da esportare attraverso il server DNS del cluster. Più LIF possono condividere lo stesso nome, consentendo alla funzione di bilanciamento del carico DNS di distribuire gli indirizzi IP per il nome in base al carico.

Le SVM possono avere più zone DNS.

- Routing

Ogni SVM è autosufficiente per quanto riguarda il networking. Una SVM possiede LIF e route che possono raggiungere ciascuno dei server esterni configurati.

La seguente figura illustra come i diversi componenti di rete sono associati in un cluster a quattro nodi:



## Linee guida per il cablaggio di rete

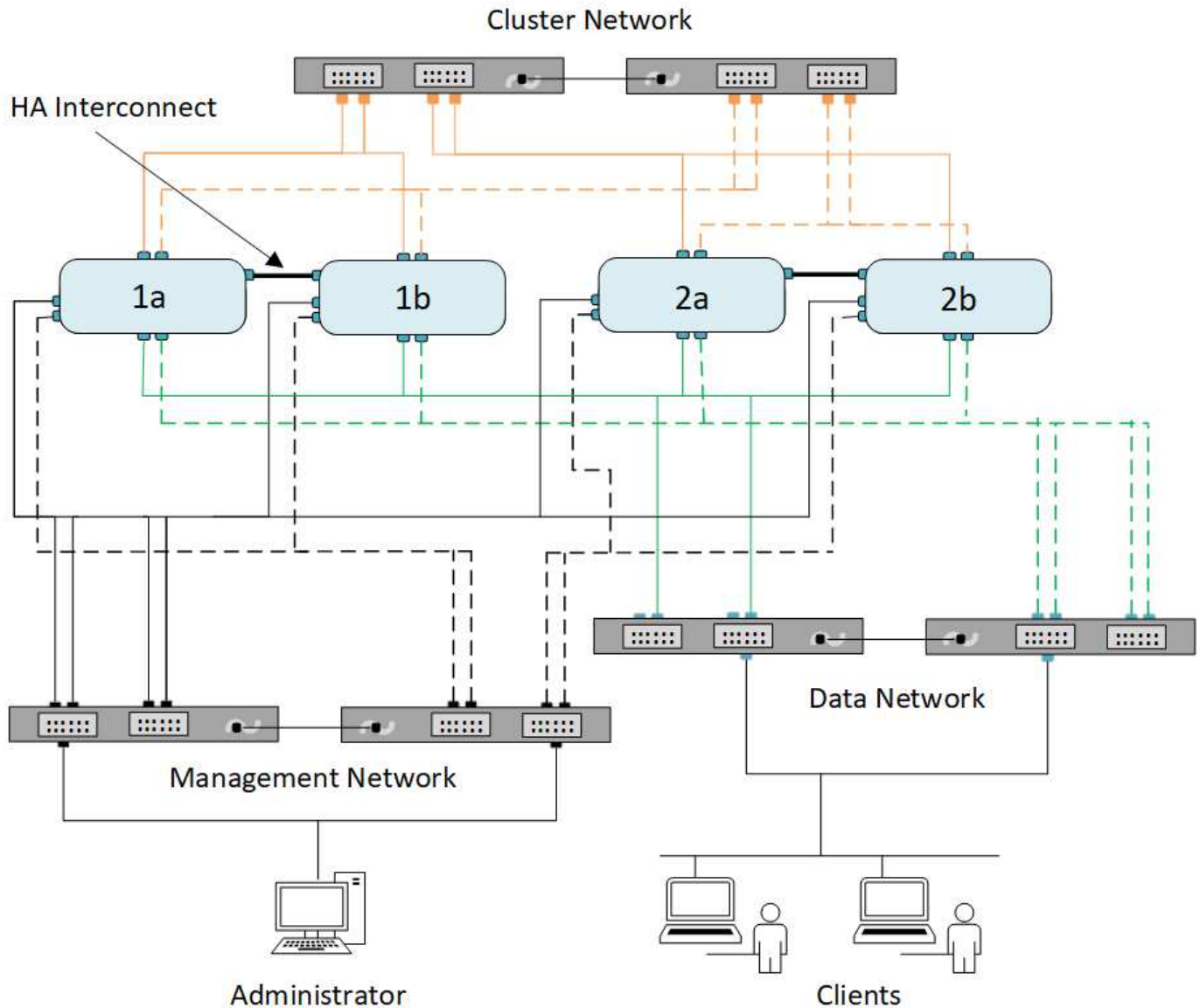
Le Best practice per il cablaggio di rete separano il traffico nelle seguenti reti: Cluster, gestione e dati.

È necessario collegare un cluster in modo che il traffico del cluster si trovi su una rete separata da tutto il traffico. È una pratica facoltativa, ma consigliata, che prevede la separazione del traffico di gestione della rete dai dati e dal traffico intracluster. Mantenendo reti separate, è possibile ottenere performance migliori, facilità di



amministrazione e maggiore sicurezza e accesso di gestione ai nodi.

Il seguente diagramma illustra il cablaggio di rete di un cluster ha a quattro nodi che include tre reti separate:



Per il cablaggio delle connessioni di rete, seguire alcune linee guida:

- Ciascun nodo deve essere connesso a tre reti distinte.

Una rete è per la gestione, una per l'accesso ai dati e una per la comunicazione intracluster. Le reti di gestione e dati possono essere separate in modo logico.

- È possibile disporre di più connessioni di rete dati a ciascun nodo per migliorare il flusso di traffico (dati) del client.
- Un cluster può essere creato senza connessioni di rete dati, ma deve includere una connessione di interconnessione del cluster.
- Devono essere sempre presenti due o più connessioni cluster per ciascun nodo.

Per ulteriori informazioni sul cablaggio di rete, consultare ["Centro di documentazione dei sistemi AFF e FAS"](#) e

## Relazione tra domini di broadcast, gruppi di failover e policy di failover

I domini di broadcast, i gruppi di failover e le policy di failover lavorano insieme per determinare quale porta assume il controllo in caso di guasto del nodo o della porta su cui è configurato un LIF.

Un dominio di broadcast elenca tutte le porte raggiungibili nella stessa rete Ethernet Layer 2. Un pacchetto di trasmissione Ethernet inviato da una delle porte viene visto da tutte le altre porte nel dominio di trasmissione. Questa caratteristica di raggiungibilità comune di un dominio di broadcast è importante per i LIF perché se un LIF dovesse eseguire il failover su qualsiasi altra porta del dominio di broadcast, potrebbe comunque raggiungere tutti gli host locali e remoti raggiungibili dalla porta originale.

I gruppi di failover definiscono le porte all'interno di un dominio di broadcast che forniscono una copertura di failover LIF reciproca. Ogni dominio di broadcast dispone di un gruppo di failover che include tutte le porte. Questo gruppo di failover contenente tutte le porte nel dominio di broadcast è il gruppo di failover predefinito e consigliato per LIF. È possibile creare gruppi di failover con sottoinsiemi più piccoli definiti, ad esempio un gruppo di failover di porte con la stessa velocità di collegamento all'interno di un dominio di broadcast.

Una policy di failover determina il modo in cui una LIF utilizza le porte di un gruppo di failover quando un nodo o una porta non funziona. Considerare la policy di failover come un tipo di filtro applicato a un gruppo di failover. Le destinazioni di failover per una LIF (l'insieme di porte a cui una LIF può eseguire il failover) vengono determinate applicando la policy di failover della LIF al gruppo di failover della LIF nel dominio di broadcast.

È possibile visualizzare le destinazioni di failover per una LIF utilizzando il seguente comando CLI:

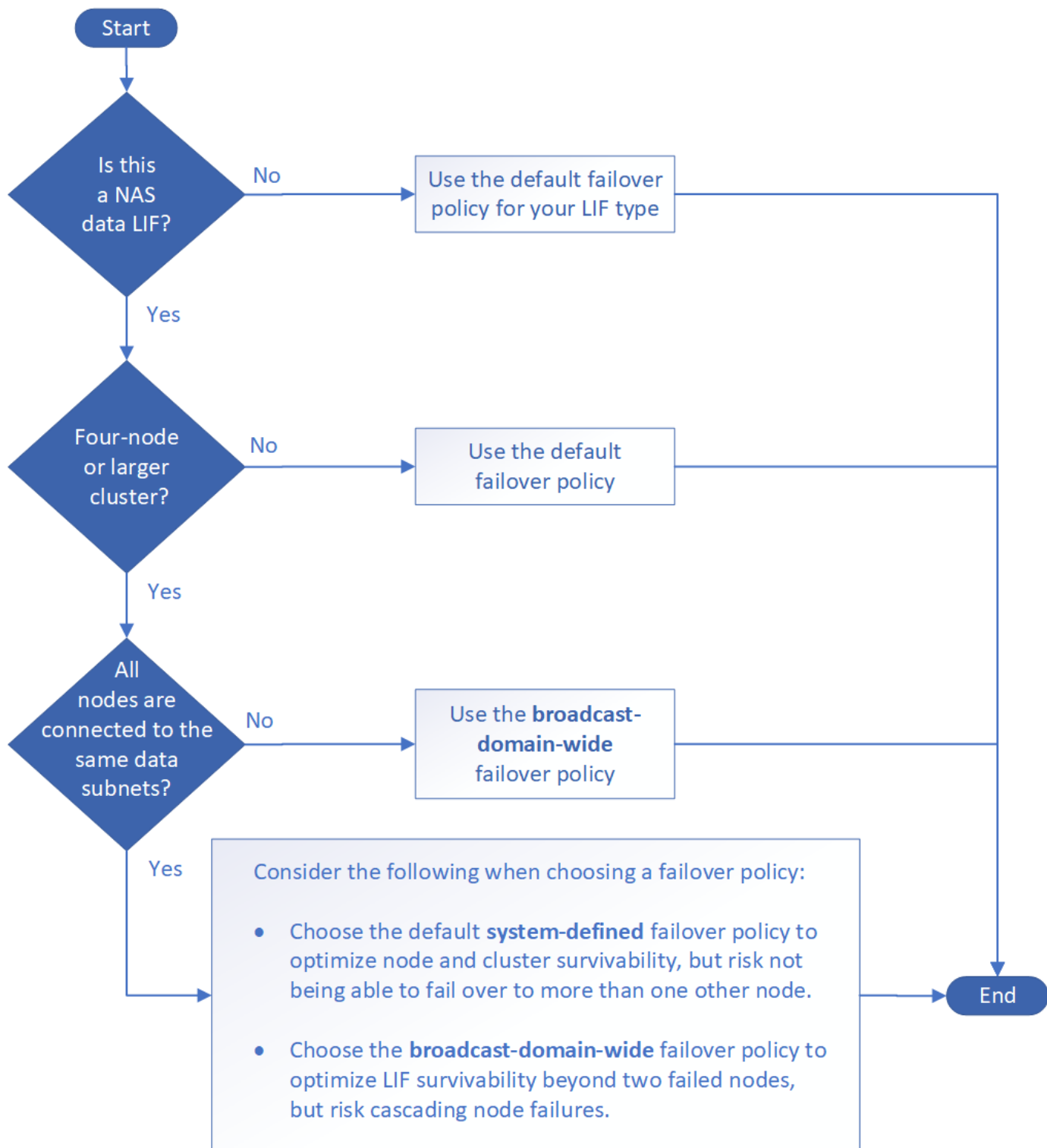
```
network interface show -failover
```

NetApp consiglia vivamente di utilizzare la policy di failover predefinita per il tipo di LIF.

### Decidere quale policy di failover LIF utilizzare

Decidere se utilizzare la policy di failover predefinita consigliata o se modificarla in base al tipo e all'ambiente LIF in uso.

#### Albero decisionale delle policy di failover



#### Policy di failover predefinite per tipo LIF

Tipo LIF	Policy di failover predefinita	Descrizione
LIF BGP	disattivato	LIF non esegue il failover su un'altra porta.
LIF del cluster	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.

LIF. Gestione cluster	broadcast-domain-wide	LIF esegue il failover su porte nello stesso dominio di broadcast, su qualsiasi nodo del cluster.
LIF di intercluster	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.
LIF dati NAS	definito dal sistema	LIF esegue il failover su un altro nodo che non è il partner ha.
LIF di gestione dei nodi	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.
LIF dati SAN	disattivato	LIF non esegue il failover su un'altra porta.

Il criterio di failover "sfo-partner-only" non è un criterio predefinito, ma può essere utilizzato quando si desidera che LIF esegue il failover su una porta solo sul nodo principale o sul partner SFO.

## Flusso di lavoro di failover del percorso NAS (ONTAP 9,8 e versioni successive)

### Informazioni sul failover del percorso NAS (ONTAP 9,8 e versioni successive)

Questo flusso di lavoro guida l'utente attraverso le fasi di configurazione della rete per impostare il failover del percorso NAS per ONTAP 9.8 e versioni successive. Questo flusso di lavoro presuppone quanto segue:

- Si desidera utilizzare le Best practice di failover del percorso NAS in un flusso di lavoro che semplifica la configurazione di rete.
- Si desidera utilizzare la CLI, non System Manager.
- Si sta configurando la rete su un nuovo sistema che esegue ONTAP 9.8 o versione successiva.

Se si esegue una versione di ONTAP precedente alla 9.8, è necessario utilizzare la seguente procedura di failover del percorso NAS per ONTAP da 9.0 a 9.7:

- ["Workflow di failover del percorso NAS ONTAP 9.0-9.7"](#)

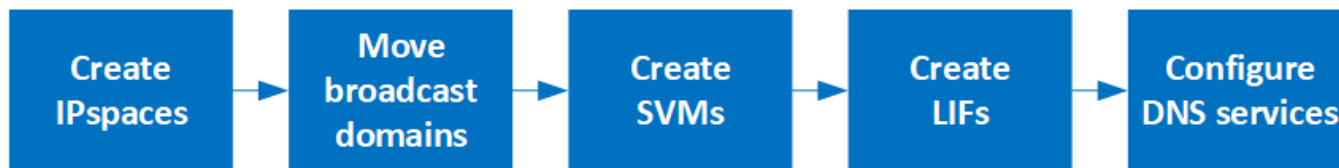
Se si desidera ottenere dettagli sulla gestione della rete, è necessario utilizzare il materiale di riferimento per la gestione della rete:

- [Panoramica sulla gestione della rete](#)

### Flusso di lavoro (ONTAP 9,8 e versioni successive)

Se hai già familiarità con i concetti di base del networking, potresti risparmiare tempo nell'impostazione della rete esaminando questo flusso di lavoro pratico per la configurazione del failover del percorso NAS.

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. Per gestire il failover del percorso, è possibile fare affidamento sulle impostazioni predefinite di ONTAP.



Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore di collegamento). Invece, la tecnologia multipathing sull'host trasferisce il traffico a un LIF diverso. Per ulteriori informazioni, vedere ["Amministrazione SAN"](#).

1

### "Completare il foglio di lavoro"

Utilizzare il foglio di lavoro per pianificare il failover del percorso NAS.

2

### "Creare IPspaces"

Crea uno spazio di indirizzi IP distinto per ciascuna SVM in un cluster.

3

### "Spostare i domini di broadcast negli IPspaces"

Spostare i domini di broadcast in IPspace.

4

### "Creare SVM"

Creazione di SVM per fornire dati ai client.

5

### "Creare LIF"

Creare LIF sulle porte che servono per accedere ai dati.

6

### "Configurare i servizi DNS per la SVM"

Configurare i servizi DNS per la SVM prima di creare un server NFS o SMB.

## Foglio di lavoro per la configurazione del failover del percorso NAS (ONTAP 9,8 e versioni successive)

Completare tutte le sezioni del foglio di lavoro prima di configurare il failover del percorso NAS.

### Configurazione di IPspace

È possibile utilizzare un IPspace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------

IPSpace name (Nome IPSpace): Identificativo univoco di IPSpace.	Sì	
---	----	--

### Configurazione del dominio di trasmissione

Un dominio di trasmissione raggruppa le porte che appartengono alla stessa rete Layer 2 e imposta la MTU per le porte del dominio di trasmissione.

I domini di broadcast vengono assegnati a un IPSpace. Un IPSpace può contenere uno o più domini di broadcast.



La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Per ogni dominio di broadcast creato da ONTAP, viene creato anche un gruppo di failover con lo stesso nome che contiene tutte le porte nel dominio di broadcast.

Informazioni	Necessario?	I tuoi valori
<p>IPSpace name (Nome IPSpace): L'IPSpace a cui è assegnato il dominio di trasmissione.</p> <p>Questo IPSpace deve esistere.</p>	Sì	
<p>Broadcast domain name (Nome dominio di trasmissione): Il nome del dominio di trasmissione.</p> <p>Questo nome deve essere univoco in IPSpace.</p>	Sì	
<p>MTU il valore massimo dell'unità di trasmissione per il dominio di trasmissione, generalmente impostato su <b>1500</b> o <b>9000</b>.</p> <p>Il valore MTU viene applicato a tutte le porte nel dominio di trasmissione e a tutte le porte che vengono successivamente aggiunte al dominio di trasmissione.</p> <p>Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete. Tenere presente che la MTU non deve superare i 1500 byte per la gestione della porta e0M e il traffico del processore di servizio.</p>	Sì	

<p>Porte le porte vengono assegnate ai domini di trasmissione in base alla raggiungibilità. Una volta completata l'assegnazione delle porte, verificare la raggiungibilità eseguendo il <code>network port reachability show</code> comando.</p> <p>Queste porte possono essere porte fisiche, VLAN o gruppi di interfacce.</p>	Sì	
---	----	--

## Configurazione della subnet

Una subnet contiene pool di indirizzi IP e un gateway predefinito che può essere assegnato alle LIF utilizzate dalle SVM che risiedono nell'IPSpace.

- Quando si crea una LIF su una SVM, è possibile specificare il nome della subnet invece di fornire un indirizzo IP e una subnet.
- Poiché una subnet può essere configurata con un gateway predefinito, non è necessario creare il gateway predefinito in una fase separata durante la creazione di una SVM.
- Un dominio di broadcast può contenere una o più subnet.
- È possibile configurare le LIF SVM presenti su sottoreti diverse associando più di una subnet al dominio di trasmissione di IPspace.
- Ogni subnet deve contenere indirizzi IP che non si sovrappongono agli indirizzi IP assegnati ad altre subnet dello stesso IPspace.
- È possibile assegnare indirizzi IP specifici alle LIF dei dati SVM e creare un gateway predefinito per la SVM invece di utilizzare una subnet.

Informazioni	Necessario?	I tuoi valori
<p>IPSpace name (Nome IPspace): L'IPspace a cui verrà assegnata la subnet.</p> <p>Questo IPspace deve esistere.</p>	Sì	
<p>Subnet name (Nome subnet): Il nome della subnet.</p> <p>Questo nome deve essere univoco in IPspace.</p>	Sì	
<p>Broadcast domain name (Nome dominio di trasmissione): Il dominio di trasmissione a cui verrà assegnata la subnet.</p> <p>Questo dominio di trasmissione deve risiedere nell'IPspace specificato.</p>	Sì	
<p>Subnet name e mask la subnet e la maschera in cui risiedono gli indirizzi IP.</p>	Sì	

<p>Gateway (Gateway): È possibile specificare un gateway predefinito per la subnet.</p> <p>Se non si assegna un gateway durante la creazione della subnet, è possibile assegnarne uno in un secondo momento.</p>	No	
<p>Intervalli di indirizzi IP è possibile specificare un intervallo di indirizzi IP o indirizzi IP specifici.</p> <p>Ad esempio, è possibile specificare un intervallo come:</p> <p>192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145</p> <p>Se non si specifica un intervallo di indirizzi IP, l'intero intervallo di indirizzi IP nella subnet specificata sarà disponibile per l'assegnazione ai file LIF.</p>	No	
<p>Force update of LIF associations (forza aggiornamento delle associazioni LIF): Specifica se forzare l'aggiornamento delle associazioni LIF esistenti.</p> <p>Per impostazione predefinita, la creazione della subnet non riesce se le interfacce del service processor o di rete utilizzano gli indirizzi IP degli intervalli forniti.</p> <p>L'utilizzo di questo parametro consente di associare qualsiasi interfaccia indirizzata manualmente alla subnet e di eseguire correttamente il comando.</p>	No	

## Configurazione SVM

Utilizzate le SVM per fornire dati a client e host.

I valori registrati servono per la creazione di una SVM di dati predefinita. Se si sta creando una SVM di origine MetroCluster, consultare ["Guida all'installazione e alla configurazione di Fabric-Attached MetroCluster"](#) o il ["Guida all'installazione e alla configurazione di Stretch MetroCluster"](#).

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Nome di dominio completo (FQDN) dell'SVM. Questo nome deve essere univoco per tutti i campionati di cluster.	Sì	
Root volume name (Nome volume root): Il nome del volume root SVM.	Sì	



Aggregate name (Nome aggregato): Il nome dell'aggregato che contiene il volume root SVM. Questo aggregato deve esistere.	Sì	
Security Style (stile di sicurezza): Lo stile di sicurezza per il volume root SVM. I valori possibili sono <b>ntfs</b> , <b>unix</b> e <b>misto</b> .	Sì	
IPSpace name (Nome IPspace): L'IPspace a cui è assegnata la SVM. Questo IPspace deve esistere.	No	
Lingua SVM impostazione della lingua predefinita da utilizzare per SVM e i relativi volumi. Se non si specifica una lingua predefinita, la lingua SVM predefinita viene impostata su <b>C.UTF-8</b> . L'impostazione della lingua SVM determina il set di caratteri utilizzato per visualizzare i nomi dei file e i dati di tutti i volumi NAS nella SVM. È possibile modificare la lingua dopo la creazione di SVM.	No	

## Configurazione LIF

Una SVM fornisce i dati ai client e agli host attraverso una o più interfacce logiche di rete (LIF).

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Il nome della SVM per la LIF.	Sì	
LIF name (Nome LIF): Il nome della LIF. È possibile assegnare più LIF di dati per nodo ed è possibile assegnare LIF a qualsiasi nodo del cluster, a condizione che il nodo disponga di porte dati disponibili. Per garantire la ridondanza, è necessario creare almeno due LIF di dati per ciascuna subnet di dati e assegnare le LIF assegnate a una determinata subnet a porte home su nodi diversi. <b>Importante:</b> se si configura un server SMB per ospitare Hyper-V o SQL Server su SMB per soluzioni operative senza interruzioni, SVM deve disporre di almeno una LIF di dati su ogni nodo del cluster.	Sì	
Politica di servizio Politica di servizio per LIF. La politica di servizio definisce quali servizi di rete possono utilizzare la LIF. I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema.	Sì	

Protocolli consentiti i LIF basati su IP non richiedono protocolli consentiti, utilizzare invece la riga della policy di servizio. Specificare i protocolli consentiti per LE LIF SAN sulle porte FibreChannel. Questi sono i protocolli che possono utilizzare tale LIF. I protocolli che utilizzano la LIF non possono essere modificati dopo la creazione della LIF. Specificare tutti i protocolli quando si configura la LIF.	No	
Nodo home il nodo a cui la LIF restituisce quando la LIF viene riportata alla porta home. È necessario registrare un nodo principale per ciascun LIF di dati.	Sì	
La porta principale o il dominio di broadcast hanno scelto una delle seguenti opzioni: <b>Port</b> (porta): Specificare la porta a cui l'interfaccia logica restituisce quando la LIF viene riportata alla porta home. Questa operazione viene eseguita solo per il primo LIF nella subnet di un IPspace, altrimenti non è necessaria. <b>Broadcast Domain</b> (dominio di trasmissione): Specificare il dominio di trasmissione e il sistema selezionerà la porta appropriata a cui l'interfaccia logica restituisce quando LIF viene riportato alla porta home.	Sì	
Subnet name (Nome subnet): La subnet da assegnare alla SVM. Tutti i dati LIF utilizzati per creare connessioni SMB continuamente disponibili ai server applicazioni devono trovarsi sulla stessa sottorete.	Sì (se si utilizza una subnet)	

## Configurazione DNS

È necessario configurare il DNS sulla SVM prima di creare un server NFS o SMB.

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Il nome della SVM su cui si desidera creare un server NFS o SMB.	Sì	
DNS domain name (Nome dominio DNS): Elenco di nomi di dominio da aggiungere a un nome host durante l'esecuzione della risoluzione dei nomi da host a IP. Elencare prima il dominio locale, seguito dai nomi di dominio per i quali vengono eseguite più spesso query DNS.	Sì	

Indirizzi IP dei server DNS elenco degli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server NFS o SMB. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server SMB farà parte. Il record SRV viene utilizzato per associare il nome di un servizio al nome del computer DNS di un server che offre tale servizio. La creazione del server SMB non riesce se ONTAP non riesce a ottenere i record di posizione del servizio tramite query DNS locali. Il modo più semplice per garantire che ONTAP possa individuare i record SRV di Active Directory consiste nel configurare i server DNS integrati come server DNS di SVM. È possibile utilizzare server DNS non integrati in Active Directory, a condizione che l'amministratore DNS abbia aggiunto manualmente i record SRV alla zona DNS che contiene informazioni sui controller di dominio Active Directory. Per informazioni sui record SRV integrati in Active Directory, vedere l'argomento <a href="#">"Come funziona il supporto DNS per Active Directory su Microsoft TechNet"</a> .	Sì	
--	----	--

## Configurazione DNS dinamica

Prima di poter utilizzare il DNS dinamico per aggiungere automaticamente le voci DNS ai server DNS integrati in Active Directory, è necessario configurare il DNS dinamico (DDNS) su SVM.

I record DNS vengono creati per ogni LIF di dati sulla SVM. Creando più LIFS di dati su SVM, è possibile bilanciare il carico delle connessioni client agli indirizzi IP dei dati assegnati. Il carico DNS bilancia le connessioni effettuate utilizzando il nome host con gli indirizzi IP assegnati in modo round-robin.

Informazioni	Necessario?	I tuoi valori
Nome SVM la SVM su cui si desidera creare un server NFS o SMB.	Sì	
Se utilizzare DDNS specifica se utilizzare DDNS. I server DNS configurati su SVM devono supportare DDNS. Per impostazione predefinita, il DDNS è disattivato.	Sì	

Se utilizzare DDNS sicuro DDNS sicuro è supportato solo con DNS integrato in Active Directory. Se il DNS integrato in Active Directory consente solo aggiornamenti DDNS sicuri, il valore di questo parametro deve essere true. Per impostazione predefinita, il DDNS sicuro è disattivato. È possibile attivare il DDNS sicuro solo dopo la creazione di un server SMB o di un account Active Directory per SVM.	No	
FQDN del dominio DNS l'FQDN del dominio DNS. È necessario utilizzare lo stesso nome di dominio configurato per i servizi dei nomi DNS su SVM.	No	

## Flusso di lavoro di failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

### Configurazione del failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

Questo flusso di lavoro guida l'utente attraverso le fasi di configurazione della rete per impostare il failover del percorso NAS per ONTAP 9.0 - 9.7. Questo flusso di lavoro presuppone quanto segue:

- Si desidera utilizzare le Best practice di failover del percorso NAS che semplificano la configurazione di rete.
- Si desidera utilizzare la CLI, non System Manager.
- Si sta configurando la rete su un nuovo sistema che esegue ONTAP da 9.0 a 9.7.

Se si esegue una versione di ONTAP successiva alla 9.7, è necessario utilizzare la procedura di failover del percorso NAS per ONTAP 9.8 o versione successiva:

- [Workflow di failover del percorso NAS di ONTAP 9.8 e versioni successive](#)

Per ulteriori informazioni sui componenti di rete e sulla gestione, è necessario utilizzare il materiale di riferimento per la gestione della rete:

- [Panoramica sulla gestione della rete](#)

### Flusso di lavoro (ONTAP 9,7 e versioni precedenti)

Se hai già familiarità con i concetti di base del networking, potresti risparmiare tempo nell'impostazione della rete esaminando questo flusso di lavoro pratico per la configurazione del failover del percorso NAS.

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. Se la rete è piatta, è possibile utilizzare le impostazioni predefinite di ONTAP per gestire il failover del percorso. In caso contrario, è necessario configurare il failover del percorso seguendo i passaggi di questo flusso di lavoro.



Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore di collegamento). Invece, la tecnologia multipathing sull'host trasferisce il traffico a un LIF diverso. Per ulteriori informazioni, vedere ["Amministrazione SAN"](#).

**1****"Completare il foglio di lavoro"**

Utilizzare il foglio di lavoro per pianificare il failover del percorso NAS.

**2****"Creare IPspaces"**

Crea uno spazio di indirizzi IP distinto per ciascuna SVM in un cluster.

**3****"Creare domini di broadcast"**

Creare domini di broadcast.

**4****"Creare sottoreti"**

Creare subnet.

**5****"Creare SVM"**

Creazione di SVM per fornire dati ai client.

**6****"Creare LIF"**

Creare LIF sulle porte che servono per accedere ai dati.

**7****"Configurare i servizi DNS per la SVM"**

Configurare i servizi DNS per la SVM prima di creare un server NFS o SMB.

## Foglio di lavoro per la configurazione del failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

Completare tutte le sezioni del foglio di lavoro prima di configurare il failover del percorso NAS.

### Configurazione di IPSpace

È possibile utilizzare un IPSpace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------

Nome IPSpace	Sì	
<ul style="list-style-type: none"> <li>• Il nome di IPSpace.</li> <li>• Il nome deve essere univoco nel cluster.</li> </ul>		

## Configurazione del dominio di trasmissione


Un dominio di trasmissione raggruppa le porte che appartengono alla stessa rete Layer 2 e imposta la MTU per le porte del dominio di trasmissione.

I domini di broadcast vengono assegnati a un IPSpace. Un IPSpace può contenere uno o più domini di broadcast.



La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Quando si crea un dominio di broadcast, ONTAP crea automaticamente un gruppo di failover con lo stesso nome. Il gruppo di failover contiene tutte le porte assegnate al dominio di trasmissione.

Informazioni	Necessario?	I tuoi valori
Nome IPSpace	Sì	
<ul style="list-style-type: none"> <li>• L'IPSpace a cui è assegnato il dominio di trasmissione.</li> <li>• IPSpace deve esistere.</li> </ul>		
Nome di dominio di trasmissione	Sì	
<ul style="list-style-type: none"> <li>• Il nome del dominio di trasmissione.</li> <li>• Questo nome deve essere univoco in IPSpace.</li> </ul>		

<p>MTU</p> <ul style="list-style-type: none"> <li>• MTU del dominio di trasmissione.</li> <li>• Generalmente impostato su <b>1500</b> o <b>9000</b>.</li> <li>• Il valore MTU viene applicato a tutte le porte nel dominio di trasmissione e a tutte le porte che vengono successivamente aggiunte al dominio di trasmissione.</li> </ul> <div>  <p>Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete. Tenere presente che la MTU non deve superare i 1500 byte per la gestione della porta e0M e il traffico del processore di servizio.</p> </div>	<p>Sì</p>	
<p>Porte</p> <ul style="list-style-type: none"> <li>• Le porte di rete da aggiungere al dominio di trasmissione.</li> <li>• Le porte assegnate al dominio di trasmissione possono essere porte fisiche, VLAN o gruppi di interfacce (ifgroup).</li> <li>• Se una porta si trova in un altro dominio di trasmissione, deve essere rimossa prima di poter essere aggiunta al dominio di trasmissione.</li> <li>• Le porte vengono assegnate specificando sia il nome del nodo che la porta, ad esempio node1:e0d.</li> </ul>	<p>Sì</p>	

## Configurazione della subnet

Una subnet contiene pool di indirizzi IP e un gateway predefinito che può essere assegnato alle LIF utilizzate dalle SVM che risiedono nell'IPSpace.

- Quando si crea una LIF su una SVM, è possibile specificare il nome della subnet invece di fornire un indirizzo IP e una subnet.



- Poiché una subnet può essere configurata con un gateway predefinito, non è necessario creare il gateway predefinito in una fase separata durante la creazione di una SVM.
- Un dominio di broadcast può contenere una o più subnet. È possibile configurare le LIF SVM presenti su sottoreti diverse associando più di una subnet al dominio di trasmissione di IPspace.
- Ogni subnet deve contenere indirizzi IP che non si sovrappongono agli indirizzi IP assegnati ad altre subnet dello stesso IPspace.
- È possibile assegnare indirizzi IP specifici alle LIF dei dati SVM e creare un gateway predefinito per la SVM invece di utilizzare una subnet.

Informazioni	Necessario?	I tuoi valori
<b>Nome IPspace</b> <ul style="list-style-type: none"> <li>• L'IPspace a cui verrà assegnata la subnet.</li> <li>• IPspace deve esistere.</li> </ul>	Sì	
<b>Nome della subnet</b> <ul style="list-style-type: none"> <li>• Il nome della subnet.</li> <li>• Il nome deve essere univoco in IPspace.</li> </ul>	Sì	
<b>Nome di dominio di trasmissione</b> <ul style="list-style-type: none"> <li>• Il dominio di trasmissione a cui verrà assegnata la subnet.</li> <li>• Il dominio di trasmissione deve risiedere nell'IPspace specificato.</li> </ul>	Sì	
<b>Subnet name e mask</b> <ul style="list-style-type: none"> <li>• Subnet e maschera in cui risiedono gli indirizzi IP.</li> </ul>	Sì	
<b>Gateway</b> <ul style="list-style-type: none"> <li>• È possibile specificare un gateway predefinito per la subnet.</li> <li>• Se non si assegna un gateway quando si crea la subnet, è possibile assegnarne uno in qualsiasi momento.</li> </ul>	No	

<p>Intervalli di indirizzi IP</p> <ul style="list-style-type: none"> <li>• È possibile specificare un intervallo di indirizzi IP o indirizzi IP specifici. Ad esempio, è possibile specificare un intervallo come: 192.168.1.1– 192.168.1.100, 192.168.1.112, 192.168.1.145</li> <li>• Se non si specifica un intervallo di indirizzi IP, l'intero intervallo di indirizzi IP nella subnet specificata sarà disponibile per l'assegnazione ai file LIF.</li> </ul>	No	
<p>Forzare l'aggiornamento delle associazioni LIF</p> <ul style="list-style-type: none"> <li>• Specifica se forzare l'aggiornamento delle associazioni LIF esistenti.</li> <li>• Per impostazione predefinita, la creazione della subnet non riesce se le interfacce del service processor o di rete utilizzano gli indirizzi IP degli intervalli forniti.</li> <li>• L'utilizzo di questo parametro consente di associare qualsiasi interfaccia indirizzata manualmente alla subnet e di eseguire correttamente il comando.</li> </ul>	No	

## Configurazione SVM

Utilizzate le SVM per fornire dati a client e host.

I valori registrati servono per la creazione di una SVM di dati predefinita. Se si sta creando una SVM di origine MetroCluster, consultare ["Installare un MetroCluster collegato al fabric"](#) o il ["Installare un MetroCluster stretch"](#).

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------


<p>Nome SVM</p> <ul style="list-style-type: none"> <li>• Il nome della SVM.</li> <li>• È necessario utilizzare un nome di dominio completo (FQDN) per garantire nomi SVM univoci nei vari campionati di cluster.</li> </ul>	Sì	
<p>Nome del volume root</p> <ul style="list-style-type: none"> <li>• Il nome del volume root SVM.</li> </ul>	Sì	
<p>Nome dell'aggregato</p> <ul style="list-style-type: none"> <li>• Il nome dell'aggregato che contiene il volume root SVM.</li> <li>• Questo aggregato deve esistere.</li> </ul>	Sì	
<p>Stile di sicurezza</p> <ul style="list-style-type: none"> <li>• Lo stile di sicurezza per il volume root SVM.</li> <li>• I valori possibili sono <b>ntfs</b>, <b>unix</b> e <b>misto</b>.</li> </ul>	Sì	
<p>Nome IPSpace</p> <ul style="list-style-type: none"> <li>• L'IPSpace a cui è assegnata la SVM.</li> <li>• Questo IPSpace deve esistere.</li> </ul>	No	

<p>Impostazione della lingua SVM</p> <ul style="list-style-type: none"> <li>• La lingua predefinita da utilizzare per SVM e i relativi volumi.</li> <li>• Se non si specifica una lingua predefinita, la lingua SVM predefinita viene impostata su <b>C.UTF-8</b>.</li> <li>• L'impostazione della lingua SVM determina il set di caratteri utilizzato per visualizzare i nomi dei file e i dati di tutti i volumi NAS nella SVM. È possibile modificare la lingua dopo la creazione di SVM.</li> </ul>	No	
---	----	--

## Configurazione LIF

Una SVM fornisce i dati ai client e agli host attraverso una o più interfacce logiche di rete (LIF).

Informazioni	Necessario?	I tuoi valori
<p>Nome SVM</p> <ul style="list-style-type: none"> <li>• Il nome della SVM per la LIF.</li> </ul>	Sì	
<p>Nome LIF</p> <ul style="list-style-type: none"> <li>• Il nome del LIF.</li> <li>• È possibile assegnare più LIF di dati per nodo ed è possibile assegnare LIF a qualsiasi nodo del cluster, a condizione che il nodo disponga di porte dati disponibili.</li> <li>• Per garantire la ridondanza, è necessario creare almeno due LIF di dati per ciascuna subnet di dati e assegnare le LIF assegnate a una determinata subnet a porte home su nodi diversi. <b>Importante:</b> se si configura un server SMB per ospitare Hyper-V o SQL Server su SMB per soluzioni operative senza interruzioni, SVM deve disporre di almeno una LIF di dati su ogni nodo del cluster.</li> </ul>	Sì	

<p>Ruolo LIF</p> <ul style="list-style-type: none"> <li>• Il ruolo della LIF.</li> <li>• Ai file LIF dei dati viene assegnato il ruolo dei dati.</li> </ul>	<p>Sì, estratto da ONTAP 9.6</p>	<p>dati</p>
<p>Politica di servizio</p> <p>Politica di servizio per LIF. La politica di servizio definisce quali servizi di rete possono utilizzare la LIF. I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema.</p>	<p>Sì, a partire da ONTAP 9.6</p>	
<p>Protocolli consentiti</p> <ul style="list-style-type: none"> <li>• I protocolli che possono utilizzare LIF.</li> <li>• Per impostazione predefinita, SMB, NFS e FlexCache sono consentiti. Il protocollo FlexCache consente di utilizzare un volume come volume di origine per un volume FlexCache su un sistema che esegue Data ONTAP in modalità 7.</li> </ul> <div>  <p>I protocolli che utilizzano la LIF non possono essere modificati dopo la creazione della LIF. Specificare tutti i protocolli quando si configura la LIF.</p> </div>	<p>No</p>	
<p>Nodo principale</p> <ul style="list-style-type: none"> <li>• Il nodo a cui la LIF restituisce quando la LIF viene riportata alla porta home.</li> <li>• È necessario registrare un nodo principale per ciascun LIF di dati.</li> </ul>	<p>Sì</p>	

Porta home o dominio di broadcast  <ul style="list-style-type: none"> <li>• La porta a cui l'interfaccia logica ritorna quando la LIF viene riportata alla porta home.</li> <li>• È necessario registrare una porta home per ciascun LIF di dati.</li> </ul>	Sì	
Nome della subnet  <ul style="list-style-type: none"> <li>• Subnet da assegnare alla SVM.</li> <li>• Tutti i dati LIF utilizzati per creare connessioni SMB continuamente disponibili ai server applicazioni devono trovarsi sulla stessa sottorete.</li> </ul>	Sì (se si utilizza una subnet)	

## Configurazione DNS

È necessario configurare il DNS sulla SVM prima di creare un server NFS o SMB.

Informazioni	Necessario?	I tuoi valori
Nome SVM  <ul style="list-style-type: none"> <li>• Il nome della SVM su cui si desidera creare un server NFS o SMB.</li> </ul>	Sì	
Nome di dominio DNS  <ul style="list-style-type: none"> <li>• Un elenco di nomi di dominio da aggiungere a un nome host quando si esegue la risoluzione dei nomi da host a IP.</li> <li>• Elencare prima il dominio locale, seguito dai nomi di dominio per i quali vengono eseguite più spesso query DNS.</li> </ul>	Sì	

<p>Indirizzi IP dei server DNS</p> <ul style="list-style-type: none"> <li>• Elenco di indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server NFS o SMB.</li> <li>• I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server SMB farà parte. Il record SRV viene utilizzato per associare il nome di un servizio al nome del computer DNS di un server che offre tale servizio. La creazione del server SMB non riesce se ONTAP non riesce a ottenere i record di posizione del servizio tramite query DNS locali. Il modo più semplice per garantire che ONTAP possa individuare i record SRV di Active Directory consiste nel configurare i server DNS integrati come server DNS di SVM. È possibile utilizzare server DNS non integrati in Active Directory, a condizione che l'amministratore DNS abbia aggiunto manualmente i record SRV alla zona DNS che contiene informazioni sui controller di dominio Active Directory.</li> <li>• Per informazioni sui record SRV integrati in Active Directory, vedere l'argomento <a href="#">"Come funziona il supporto DNS per Active Directory su Microsoft TechNet"</a>.</li> </ul>	<p>Sì</p>	
---	-----------	--

## Configurazione DNS dinamica

Prima di poter utilizzare il DNS dinamico per aggiungere automaticamente le voci DNS ai server DNS integrati in Active Directory, è necessario configurare il DNS dinamico (DDNS) su SVM.

I record DNS vengono creati per ogni LIF di dati sulla SVM. Creando più LIFS di dati su SVM, è possibile bilanciare il carico delle connessioni client agli indirizzi IP dei dati assegnati. Il carico DNS bilancia le

connessioni effettuate utilizzando il nome host con gli indirizzi IP assegnati in modo round-robin.

Informazioni	Necessario?	I tuoi valori
<b>Nome SVM</b> <ul style="list-style-type: none"><li>• SVM su cui si desidera creare un server NFS o SMB.</li></ul>	Sì	
<b>Se utilizzare DDNS</b> <ul style="list-style-type: none"><li>• Specifica se utilizzare DDNS.</li><li>• I server DNS configurati su SVM devono supportare DDNS. Per impostazione predefinita, il DDNS è disattivato.</li></ul>	Sì	
<b>Se utilizzare DDNS sicuro</b> <ul style="list-style-type: none"><li>• Il DDNS sicuro è supportato solo con il DNS integrato in Active Directory.</li><li>• Se il DNS integrato in Active Directory consente solo aggiornamenti DDNS sicuri, il valore di questo parametro deve essere true.</li><li>• Per impostazione predefinita, il DDNS sicuro è disattivato.</li><li>• È possibile attivare il DDNS sicuro solo dopo la creazione di un server SMB o di un account Active Directory per SVM.</li></ul>	No	
<b>FQDN del dominio DNS</b> <ul style="list-style-type: none"><li>• L'FQDN del dominio DNS.</li><li>• È necessario utilizzare lo stesso nome di dominio configurato per i servizi dei nomi DNS su SVM.</li></ul>	No	

## Porte di rete

### Configurare le porte di rete

Le porte sono porte fisiche (NIC) o virtualizzate, ad esempio gruppi di interfacce o VLAN.



Le Virtual Local Area Network (VLAN) e i gruppi di interfacce costituiscono le porte virtuali. I gruppi di interfacce trattano diverse porte fisiche come una singola porta, mentre le VLAN suddividono una porta fisica in più porte logiche separate.

- **Porte fisiche:** Le LIF possono essere configurate direttamente su porte fisiche.
- **Interface group (Gruppo di interfacce):** Aggregato di porte contenente due o più porte fisiche che fungono da singola porta di linea. Un gruppo di interfacce può essere monomodale, multimodale o multimodale dinamica.
- **VLAN:** Porta logica che riceve e invia traffico con tag VLAN (standard IEEE 802.1Q). Le caratteristiche della porta VLAN includono l'ID VLAN della porta. Le porte fisiche sottostanti o del gruppo di interfacce sono considerate porte di trunk VLAN e le porte dello switch connesso devono essere configurate per collegare gli ID VLAN.

La porta fisica sottostante o le porte del gruppo di interfacce per una porta VLAN possono continuare a ospitare le LIF, che trasmettono e ricevono traffico senza tag.

- **Virtual IP (VIP) port (porta IP virtuale):** Porta logica utilizzata come porta home per un LIF VIP. Le porte VIP vengono create automaticamente dal sistema e supportano solo un numero limitato di operazioni. Le porte VIP sono supportate a partire da ONTAP 9.5.

La convenzione di denominazione delle porte è *enumberletter*:

- Il primo carattere descrive il tipo di porta. "E" rappresenta Ethernet.
- Il secondo carattere indica lo slot numerato in cui si trova l'adattatore porta.
- Il terzo carattere indica la posizione della porta su un adattatore multiporta. "a" indica la prima porta, "b" la seconda porta e così via.

Ad esempio, e0b Indica che una porta Ethernet è la seconda porta sulla scheda madre del nodo.

Le VLAN devono essere denominate utilizzando la sintassi `port_name-vlan-id`.

`port_name` specifica la porta fisica o il gruppo di interfacce.

`vlan-id` Specifica l'identificazione della VLAN sulla rete. Ad esempio, e1c-80 È un nome VLAN valido.

## Configurare le porte di rete

### Combina le porte fisiche per creare gruppi di interfacce

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.

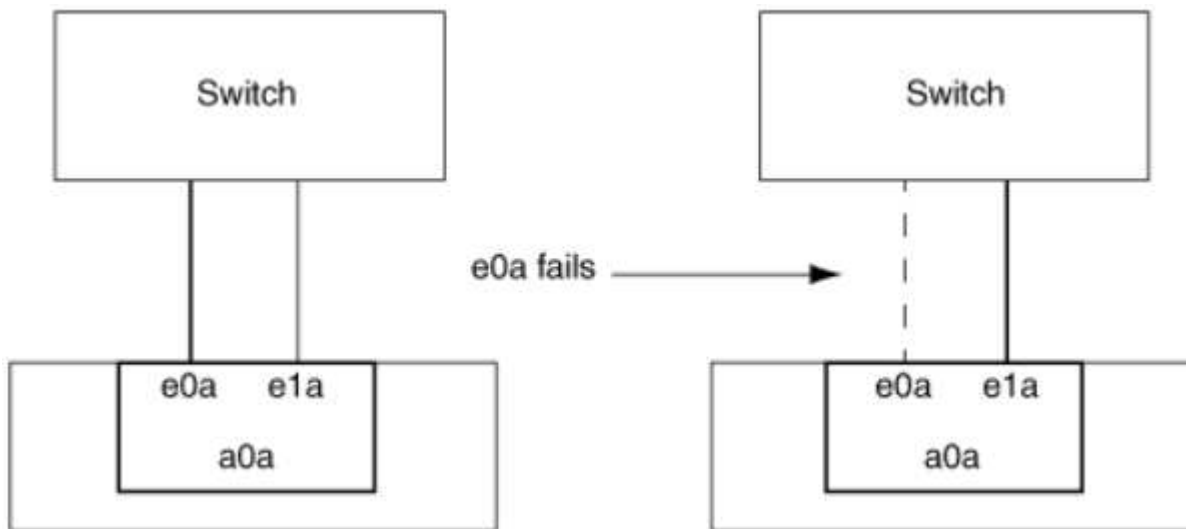
## Caratteristiche dei gruppi di interfacce single-mode

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

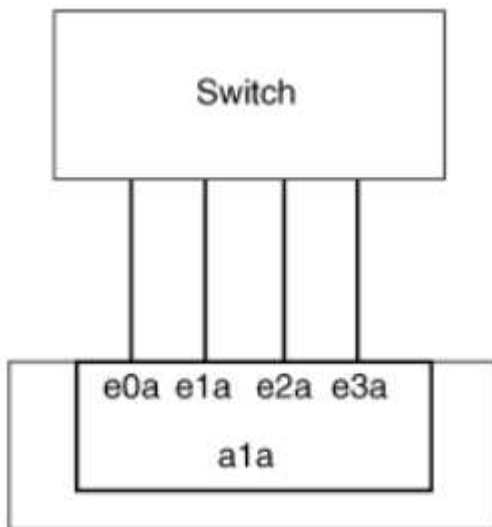
L'implementazione del gruppo di interfacce statiche multimodali in ONTAP è conforme allo standard IEEE 802.3ad (statico). Qualsiasi switch che supporti gli aggregati, ma non dispone di uno scambio di pacchetti di controllo per la configurazione di un aggregato, può essere utilizzato con gruppi di interfacce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

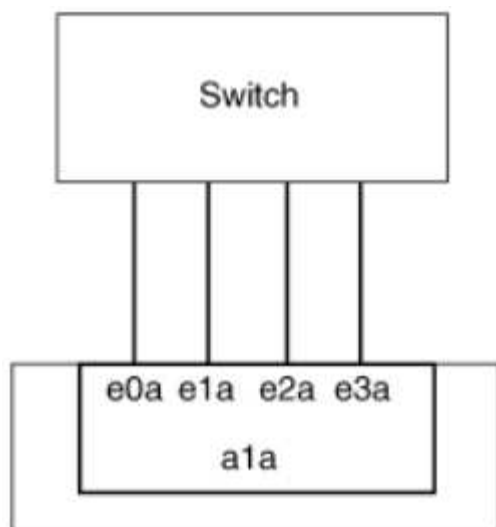
L'algoritmo di bilanciamento del carico ONTAP determina la porta membro da utilizzare per trasmettere il traffico in uscita e non controlla la modalità di ricezione dei frame in entrata. Lo switch determina il membro (singola porta fisica) del proprio gruppo di canali di porte da utilizzare per la trasmissione, 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 multimodali siano utilizzate in modo uguale 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 uniforme sulle porte di rete di un gruppo di interfacce multimodali.

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.

The screenshot shows the 'Add Link Aggregation Group' configuration page in the ONTAP System Manager. The left sidebar contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE (Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas, Storage VMs, Tiers), NETWORK (Overview, Ethernet Ports, FC Ports), EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER (Overview, Settings, Disks). The main content area is titled 'Add Link Aggregation Group' and includes a close button (X). The configuration fields are: 'NODE' (dropdown menu showing 'sti47-vsrm-ucs521e'), 'BROADCAST DOMAIN' (dropdown menu showing 'Automatically select broadcast domain (Recommended)' with a red arrow pointing to a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'), 'PORTS TO INCLUDE' (checkboxes for 'e0e' and 'e0f'), 'MODE' (radio buttons for 'Single' (selected), 'Multiple', and 'LACP'), and 'LOAD DISTRIBUTION' (radio buttons for 'IP based' (selected), 'MAC based', and 'Port').

#### CLI

## Utilizzare la CLI per creare un gruppo di interfacce

Per un elenco completo delle restrizioni di configurazione applicabili ai gruppi di interfacce delle porte, vedere `network port ifgrp add-port` pagina man.

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.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

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
```

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

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.

### 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
```

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.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

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

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

## Configurare VLAN 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 9.13.1 e 9.14.1, le porte senza tag non utilizzate da interfacce logiche (LIF) e prive di connettività VLAN nativa sullo switch connesso vengono contrassegnate come degradate. Ciò consente di identificare le porte non utilizzate e non indica un'interruzione. Le VLAN native consentono il traffico non tagged sulla porta base ifgrp, come le trasmissioni ONTAP CFM. Configurare VLAN native sullo switch per impedire il blocco del traffico non tagged.

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`.

#### 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.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

## 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
```

## Modificare gli attributi delle porte di rete

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
```

## Converti le porte NIC da 40 GbE in più porte da 10 GbE per la connettività da 10 GbE

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.



## Rimozione di una scheda di rete dal nodo (ONTAP 9,8 e versioni successive)

Questo argomento è valido per ONTAP 9,8 e versioni successive. Potrebbe essere necessario rimuovere una scheda NIC difettosa dal relativo slot o spostarla in un altro slot per scopi di manutenzione.

### Fasi

1. Spegnerne 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.

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` o usare il `displaced-interface restore` comando.

## Rimozione di una scheda di rete dal nodo (ONTAP 9,7 o versione precedente)

Questo argomento riguarda ONTAP 9.7 o versioni precedenti. Potrebbe essere

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

### Prima di iniziare

- Tutte le LIF ospitate sulle porte NIC devono essere state migrate o eliminate.
- Nessuna delle porte NIC può essere la porta principale di qualsiasi LIF.
- Per eliminare le porte da una scheda NIC, è necessario disporre di privilegi avanzati.

### Fasi

1. Eliminare le porte dalla scheda NIC:

```
network port delete
```

2. Verificare che le porte siano state eliminate:

```
network port show
```

3. Ripetere il passaggio 1 se l'output del comando di visualizzazione della porta di rete mostra ancora la porta eliminata.

### Monitorare le porte di rete

#### Monitorare lo stato delle porte di rete

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.

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

#### **Monitorare la raggiungibilità delle porte di rete (ONTAP 9.8 e versioni successive)**

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**

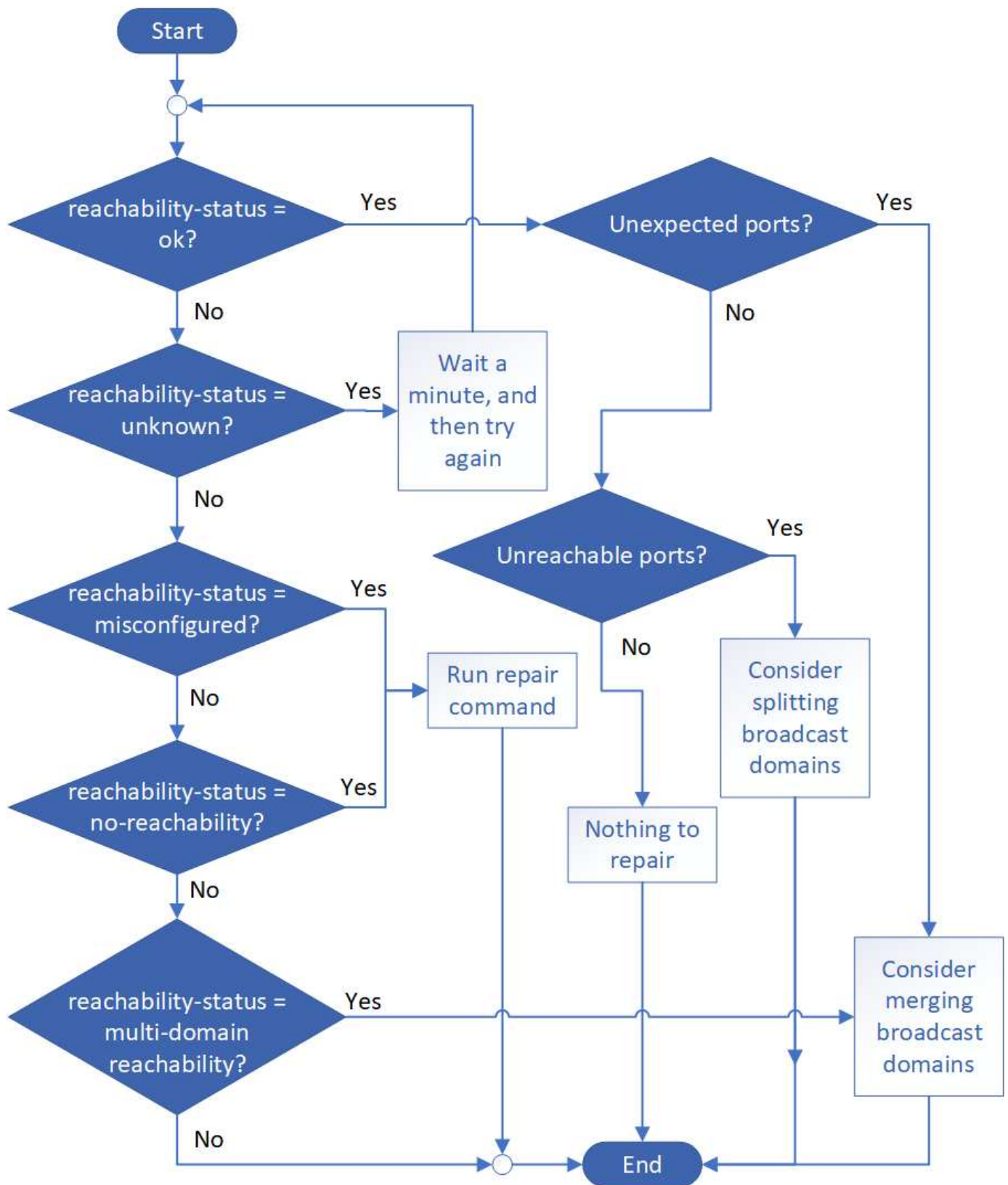
Utilizzare questi comandi per verificare, diagnosticare e riparare le configurazioni errate della rete derivanti dalla configurazione ONTAP che non corrisponde al cablaggio fisico o alla configurazione dello switch di rete.

#### **Fase**

1. Visualizzazione della raggiungibilità delle porte:

```
network port reachability show
```

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



Stato di raggiungibilità	Descrizione
--------------------------	-------------

ok	<p>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 <i>Unexpected ports</i>.</p> <p>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 <i>Unreachable ports</i> riportata di seguito.</p> <p>Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.</p>
Porte impreviste	<p>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.</p> <p>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.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a>.</p>
Porte non raggiungibili	<p>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.</p> <p>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.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Suddividere i domini di broadcast"</a>.</p>
riconfigurazione non corretta	<p>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.</p> <p>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:</p> <p>`network port reachability repair -node -port` Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
nessuna raggiungibilità	<p>La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente.</p> <p>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:</p> <p>`network port reachability repair -node -port` Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>

raggiungibilità multi-dominio	<p>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.</p> <p>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.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a> oppure <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
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"](#).

#### Panoramica delle porte ONTAP

Alcune porte note sono riservate per le comunicazioni ONTAP con servizi specifici. I conflitti di porta si verificano se il valore di una porta nell'ambiente di rete dello storage è lo stesso della porta ONTAP.

La seguente tabella elenca le porte TCP e UDP utilizzate da ONTAP.

Servizio	Porta/protocollo	Descrizione
ssh	22/TCP	Login shell sicuro
telnet	23/TCP	Accesso remoto
DNS	53/TCP	DNS con bilanciamento del carico
http	80/TCP	Hyper Text Transfer Protocol
rpcbind	111/TCP	Chiamata di procedura remota
rpcbind	111/UDP	Chiamata di procedura remota
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC
netbios-sn	139/TCP	Sessione del servizio NetBIOS
snmp	161/UDP	Protocollo di gestione di rete semplice
https	443/TCP	HTTP su TLS
microsoft-ds	445/TCP	Microsoft-ds
montare	635/TCP	Montaggio NFS
montare	635/UDP	Montaggio NFS
con nome	953/UDP	Nome daemon

nfs	2049/UDP	Daemon del server NFS
nfs	2049/TCP	Daemon del server NFS
nrv	2050/TCP	Protocollo NetApp Remote Volume
iscsi	3260/TCP	Porta di destinazione iSCSI
blocco	4045/TCP	Daemon di blocco NFS
blocco	4045/UDP	Daemon di blocco NFS
NSM	4046/TCP	Network Status Monitor (Monitor di stato della rete)
NSM	4046/UDP	Network Status Monitor (Monitor di stato della rete)
rquotad	4049/UDP	Protocollo NFS rquotad
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS - protocollo binario di ascolto
https	8443/TCP	7MTT GUI Tool tramite https
ndmp	10000/TCP	Network Data Management Protocol
Peering dei cluster	11104/TCP	Peering dei cluster, bidirezionale
Peering dei cluster, bidirezionale	11105/TCP	Peering dei cluster
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	accetta connessioni di controllo su prese sicure
porta del testimone cifs	40001/TCP	porta del testimone cifs
tls	50000/TCP	Sicurezza del livello di trasporto
iscsi	65200/TCP	Porta iSCSI

#### Porte interne ONTAP

La tabella seguente elenca le porte TCP e UDP utilizzate internamente da ONTAP. Queste porte vengono utilizzate per stabilire una comunicazione LIF intracluster:

Porta/protocollo	Descrizione
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
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
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
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
8023	Ambito del nodo TELNET
8514	Scope del nodo RSH
9877	Porta client KMIP (solo host locale interno)

## IPspaces

### Configurare la panoramica degli IPspace

Gli IPspaces consentono di configurare un singolo cluster ONTAP in modo che i client possano accedervi da più di un dominio di rete separato a livello amministrativo, anche se questi client utilizzano lo stesso intervallo di subnet di indirizzi IP. Ciò consente la separazione del traffico client per la privacy e la sicurezza.

Un IPspace definisce uno spazio di indirizzi IP distinto in cui risiedono le macchine virtuali di storage (SVM). Le porte e gli indirizzi IP definiti per un IPspace sono applicabili solo all'interno di tale IPspace. Viene mantenuta una tabella di routing distinta per ogni SVM all'interno di un IPspace; pertanto, non si verifica alcun routing del traffico cross-SVM o cross-IPspace.



Gli IPspaces supportano indirizzi IPv4 e IPv6 nei rispettivi domini di routing.

Se si gestisce lo storage per una singola organizzazione, non è necessario configurare gli IPspaces. Se si gestisce lo storage per più aziende su un singolo cluster ONTAP e si è certi che nessuno dei clienti dispone di

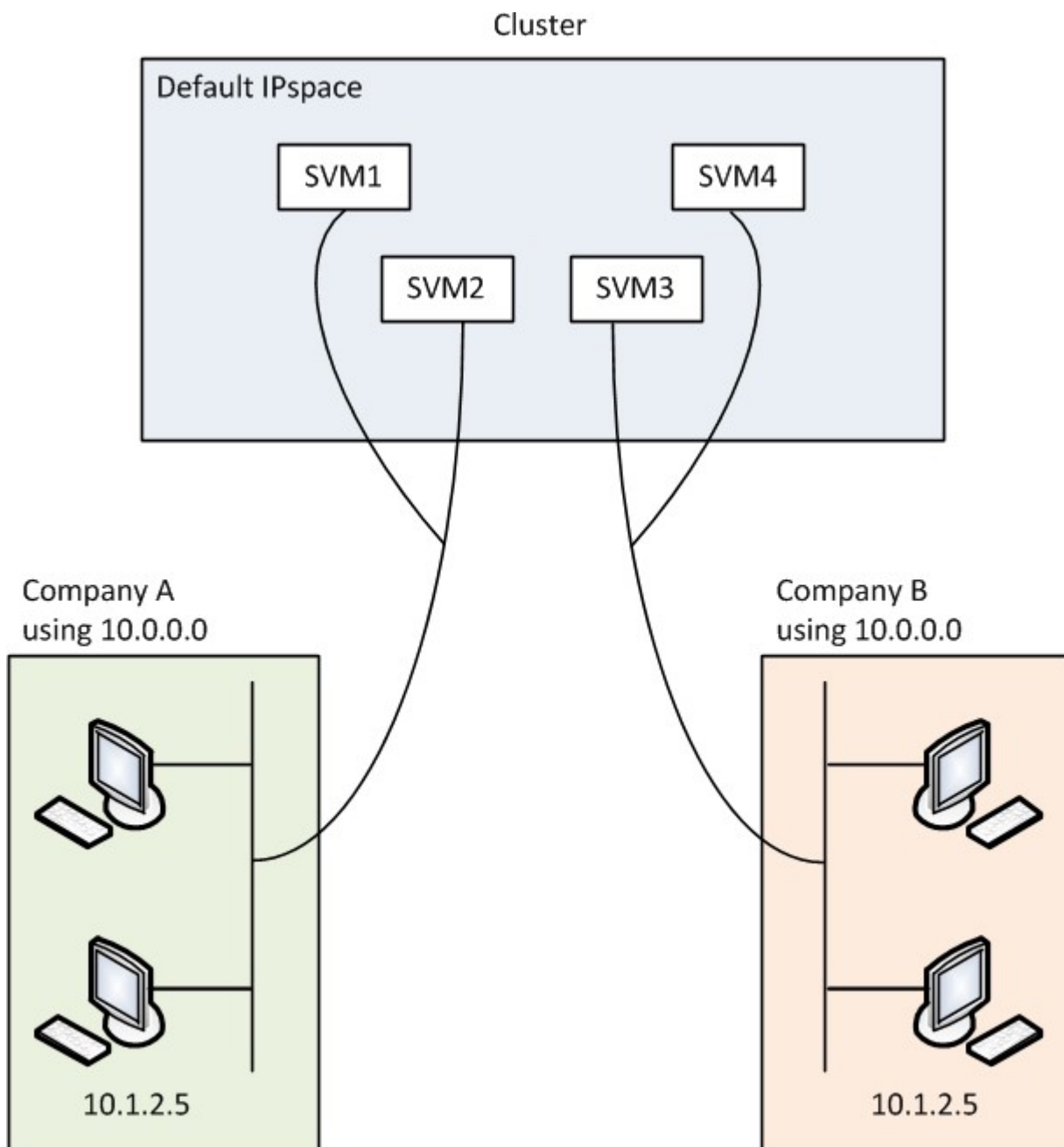
configurazioni di rete in conflitto, non è necessario utilizzare gli IPspaces. In molti casi, l'utilizzo di macchine virtuali di storage (SVM), con le proprie tabelle di routing IP distinte, può essere utilizzato per separare configurazioni di rete uniche invece di utilizzare gli spazi IPspace.

### Esempio di utilizzo di IPspaces

Un'applicazione comune per l'utilizzo di IPspaces è quando un provider di servizi di storage (SSP) deve connettere i clienti delle aziende A e B a un cluster ONTAP in loco e entrambe le aziende utilizzano gli stessi intervalli di indirizzi IP privati.

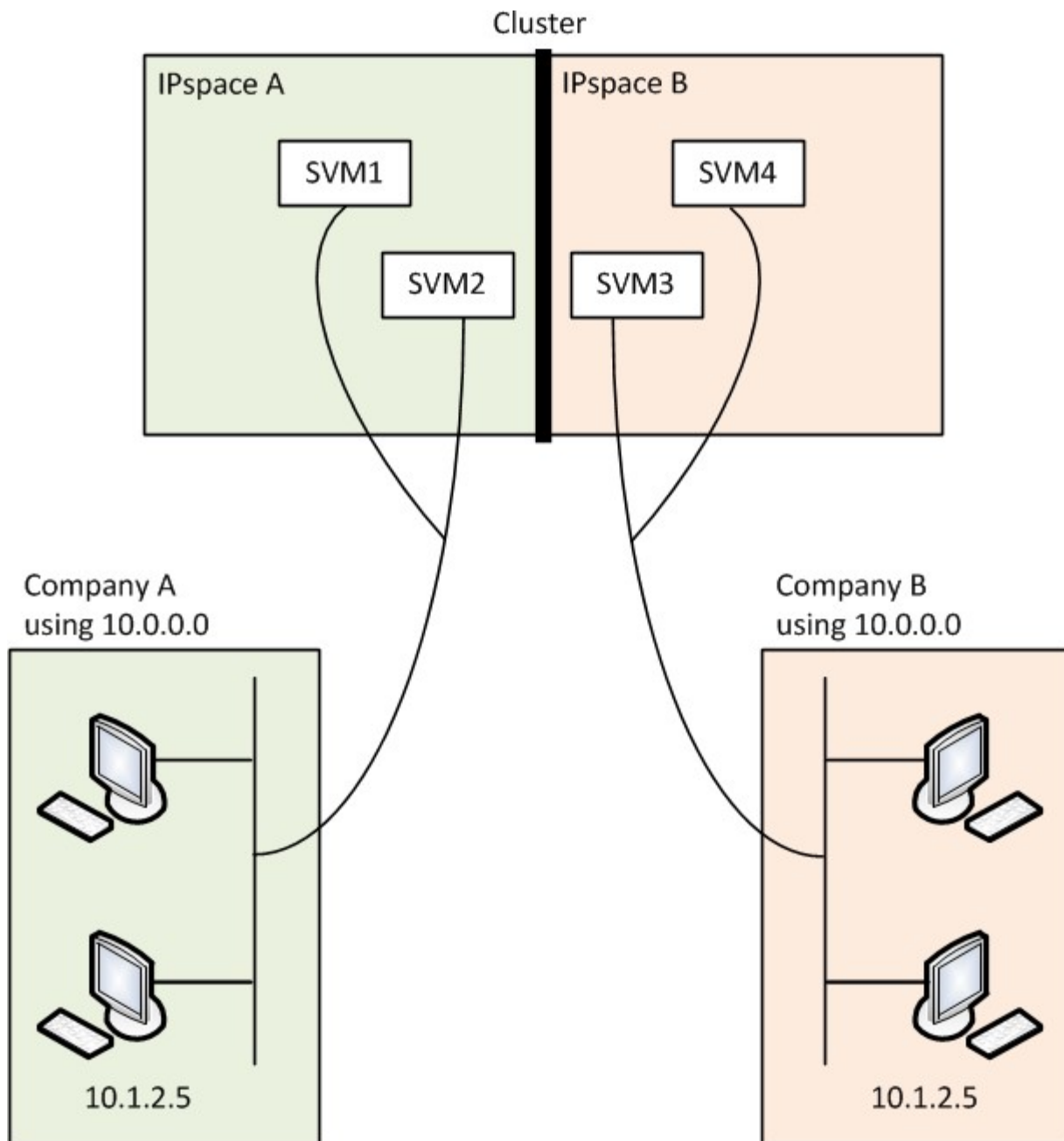
SSP crea SVM sul cluster per ciascun cliente e fornisce un percorso di rete dedicato da due SVM alla rete dell'azienda A e dalle altre due SVM alla rete dell'azienda B.

Questo tipo di implementazione viene illustrato nella figura seguente e funziona se entrambe le aziende utilizzano intervalli di indirizzi IP non privati. Tuttavia, l'illustrazione mostra entrambe le aziende che utilizzano gli stessi intervalli di indirizzi IP privati, causando problemi.



Entrambe le aziende utilizzano la subnet dell'indirizzo IP privato 10.0.0.0, causando i seguenti problemi:

- Le SVM nel cluster nella posizione SSP presentano indirizzi IP in conflitto se entrambe le aziende decidono di utilizzare lo stesso indirizzo IP per le rispettive SVM.
- Anche se le due aziende concordano sull'utilizzo di indirizzi IP diversi per le proprie SVM, possono insorgere problemi.
- Ad esempio, se un client nella rete Di A ha lo stesso indirizzo IP di un client nella rete di B, i pacchetti destinati a un client nello spazio degli indirizzi Di A potrebbero essere instradati a un client nello spazio degli indirizzi di B e viceversa.
- Se le due società decidono di utilizzare spazi di indirizzi che si escludono a vicenda (Ad esempio, A utilizza 10.0.0.0 con una maschera di rete di 255.128.0.0 e B utilizza 10.128.0.0 con una maschera di rete di 255.128.0.0), L'SSP deve configurare percorsi statici sul cluster per instradare il traffico in modo appropriato alle reti Di A e B.
- Questa soluzione non è scalabile (a causa di percorsi statici) né sicura (il traffico broadcast viene inviato a tutte le interfacce del cluster).per superare questi problemi, SSP definisce due spazi IPsul cluster, uno per ciascuna azienda. Poiché non viene instradato alcun traffico multiIPSpace, i dati di ciascuna azienda vengono instradati in modo sicuro alla rispettiva rete anche se tutte le SVM sono configurate nello spazio degli indirizzi 10.0.0.0, come mostrato nella seguente illustrazione:



Inoltre, gli indirizzi IP a cui si fa riferimento dai vari file di configurazione, ad esempio `/etc/hosts` file, il `/etc/hosts.equiv` file, e. the `/etc/rc` Sono relativi a tale IPspace. Pertanto, gli IPspaces consentono a SSP di configurare lo stesso indirizzo IP per i dati di configurazione e autenticazione per più SVM, senza conflitti.

### Proprietà standard di IPspaces

Gli IPspaces speciali vengono creati per impostazione predefinita al momento della creazione del cluster. Inoltre, vengono create speciali macchine virtuali di storage (SVM) per ogni IPspace.

Due IPspaces vengono creati automaticamente quando il cluster viene inizializzato:

- IPspace "predefinito"

IPspace è un container per porte, subnet e SVM che servono dati. Se la configurazione non richiede spazi IP separati per i client, è possibile creare tutti gli SVM in questo spazio IPspace. Questo IPspace contiene

anche le porte di gestione del cluster e dei nodi.

- IPSpace "cluster"

Questo IPSpace contiene tutte le porte del cluster di tutti i nodi del cluster. Viene creato automaticamente al momento della creazione del cluster. Fornisce connettività alla rete interna del cluster privato. Man mano che altri nodi si uniscono al cluster, le porte del cluster da tali nodi vengono aggiunte all'IPSpace "Cluster".

Esiste una SVM di "sistema" per ogni IPSpace. Quando si crea un IPSpace, viene creata una SVM di sistema predefinita con lo stesso nome:

- La SVM di sistema per l'IPSpace "Cluster" trasporta il traffico del cluster tra i nodi di un cluster sulla rete interna del cluster privato.

È gestito dall'amministratore del cluster e ha il nome "Cluster".

- La SVM di sistema per l'IPSpace "predefinito" trasporta il traffico di gestione per il cluster e i nodi, incluso il traffico tra cluster.

Viene gestito dall'amministratore del cluster e utilizza lo stesso nome del cluster.

- La SVM di sistema per un IPSpace personalizzato creato trasporta il traffico di gestione per tale SVM.

Viene gestito dall'amministratore del cluster e utilizza lo stesso nome di IPSpace.

Una o più SVM per client possono esistere in un IPSpace. Ogni SVM client dispone di volumi e configurazioni dati propri e viene amministrato indipendentemente dalle altre SVM.

## Creare IPspaces

Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono le macchine virtuali di storage (SVM). È possibile creare spazi IP quando è necessario che le SVM dispongano di storage, amministrazione e routing sicuri. È possibile utilizzare un IPSpace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

### A proposito di questa attività

Esiste un limite di 512 IPspaces a livello di cluster. Il limite a livello di cluster è ridotto a 256 IPSpace per i cluster che contengono nodi con 6 GB di RAM. Consulta il Hardware Universe per determinare se sono applicati limiti aggiuntivi alla tua piattaforma.

["NetApp Hardware Universe"](#)



Un nome IPSpace non può essere "tutto" perché "tutto" è un nome riservato al sistema.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fase

1. Creare un IPSpace:

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

ipspace\_name È il nome dell'IPSpace che si desidera creare. Il seguente comando crea IPSpace ipspace1 su un cluster:

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

## 2. Visualizzare gli IPSpace:

```
network ipspace show
```

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

Viene creato IPSpace, insieme alla SVM di sistema per IPSpace. Il sistema SVM trasporta il traffico di gestione.

### Al termine

Se si crea un IPSpace in un cluster con una configurazione MetroCluster, gli oggetti IPSpace devono essere replicati manualmente nei cluster partner. Qualsiasi SVM creata e assegnata a un IPSpace prima della replica di IPSpace non verrà replicata nei cluster partner.

I domini di broadcast vengono creati automaticamente in IPSpace "Default" e possono essere spostati tra gli IPspaces utilizzando il seguente comando:

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

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1", utilizzare il seguente comando:

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

## Visualizzare gli IPspaces

È possibile visualizzare l'elenco degli IPspace presenti in un cluster ed è possibile visualizzare le macchine virtuali di storage (SVM), i domini di trasmissione e le porte assegnati a ciascun IPSpace.

### Fase

Visualizzare gli IPspaces e le SVM in un cluster:

```
network ipspace show [-ipspacename ipspacename]
```

Il seguente comando visualizza tutti gli IPspaces, le SVM e i domini di broadcast nel cluster:

```
network ipspace show
IPspace          Vserver List          Broadcast Domains
-----
Cluster
Default          Cluster              Cluster
                  vs1, cluster-1        Default
ipspacel1        vs3, vs4, ipspacel1   bcast1
```

Il seguente comando visualizza i nodi e le porte che fanno parte di IPSpace ipspacel1:

```
network ipspace show -ipspacename ipspacel1
IPspace name: ipspacel1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspacel1
```

## Eliminare un IPSpace

Se non è più necessario un IPSpace, è possibile eliminarlo.

### Prima di iniziare

Non devono essere presenti domini di broadcast, interfacce di rete o SVM associati all'IPSpace che si desidera eliminare.

Gli IPspace "Default" e "Cluster" definiti dal sistema non possono essere cancellati.

### Fase

Eliminazione di un IPSpace:

```
network ipspace delete -ipspacename ipspacename
```

Il seguente comando elimina IPSpace ipspacel1 dal cluster:

```
network ipspace delete -ipspacename ipspacel1
```



# Domini di broadcast

## Dominio di broadcast (ONTAP 9,8 e versioni successive)

### Panoramica del dominio di trasmissione (ONTAP 9,8 e versioni successive)

I domini di broadcast sono destinati a raggruppare le porte di rete che appartengono alla stessa rete Layer 2. Le porte del gruppo possono quindi essere utilizzate da una macchina virtuale di storage (SVM) per il traffico di dati o di gestione.

Un dominio di broadcast risiede in un IPSpace. Durante l'inizializzazione del cluster, il sistema crea due domini di broadcast predefiniti:

- Il dominio di trasmissione "predefinito" contiene le porte che si trovano nello spazio IPSpace "predefinito".

Queste porte vengono utilizzate principalmente per la gestione dei dati. Anche le porte di gestione del cluster e dei nodi si trovano in questo dominio di broadcast.

- Il dominio di trasmissione "Cluster" contiene le porte che si trovano nell'IPSpace "Cluster".

Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster di tutti i nodi del cluster.

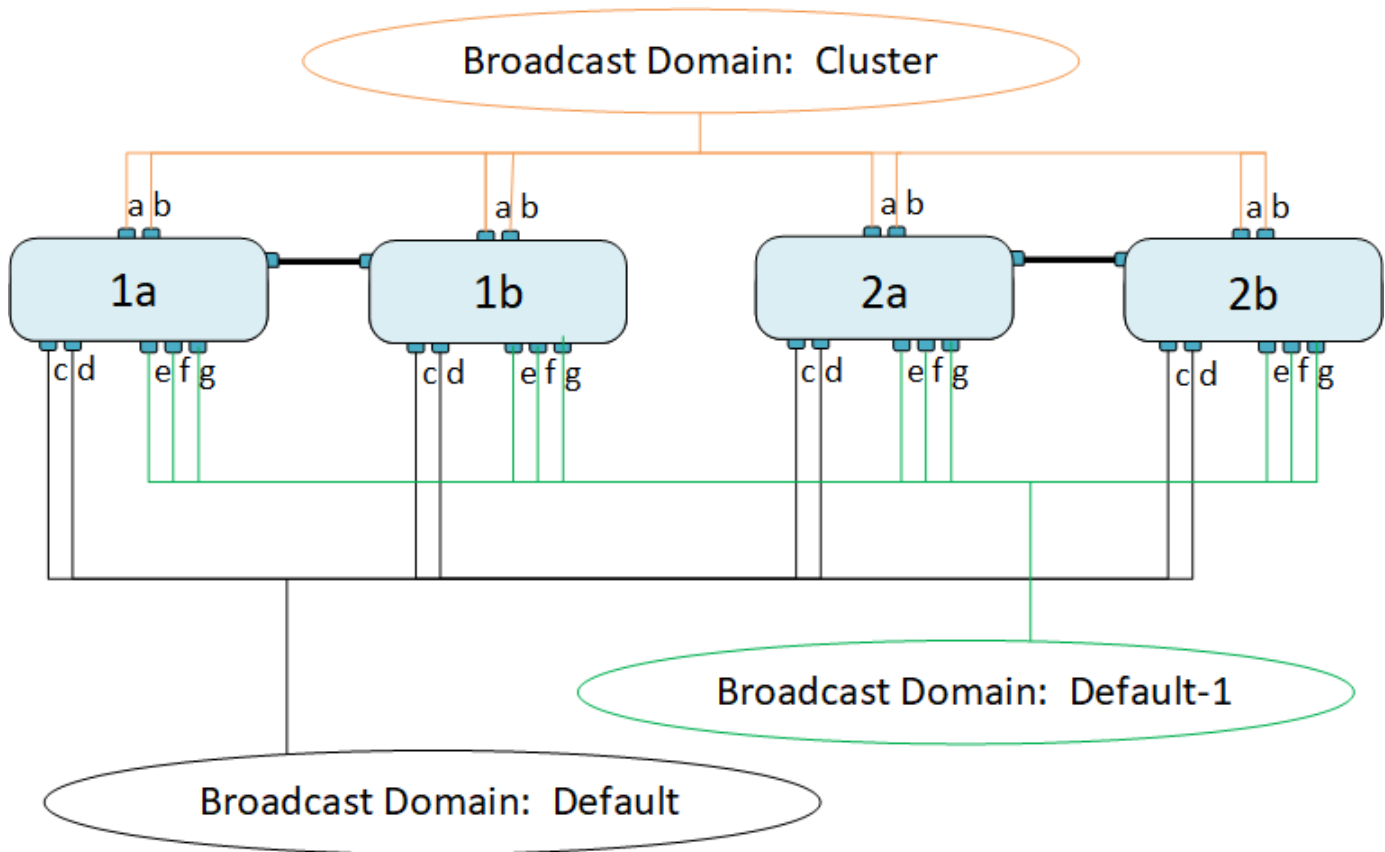
Se necessario, il sistema crea ulteriori domini di broadcast nell'IPSpace predefinito. Il dominio di trasmissione "predefinito" contiene la porta home della LIF di gestione, oltre a tutte le altre porte che hanno la capacità di raggiungere tale porta di livello 2. I domini di broadcast aggiuntivi sono denominati "Default-1", "Default-2" e così via.

### Esempio di utilizzo di domini di broadcast

Un dominio di broadcast è un insieme di porte di rete nello stesso IPSpace che ha anche la raggiungibilità di livello 2 l'una rispetto all'altra, incluse generalmente le porte di molti nodi del cluster.

L'illustrazione mostra le porte assegnate a tre domini di broadcast in un cluster a quattro nodi:

- Il dominio di broadcast "Cluster" viene creato automaticamente durante l'inizializzazione del cluster e contiene le porte a e b di ciascun nodo del cluster.
- Il dominio broadcast "Default" viene creato automaticamente anche durante l'inizializzazione del cluster e contiene le porte c e d di ciascun nodo del cluster.
- Il sistema crea automaticamente eventuali domini di broadcast aggiuntivi durante l'inizializzazione del cluster in base alla raggiungibilità della rete di livello 2. Questi domini di broadcast aggiuntivi sono denominati Default-1, Default-2 e così via.



Viene creato automaticamente un gruppo di failover con lo stesso nome e con le stesse porte di rete di ciascuno dei domini di trasmissione. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover.

### Aggiungere un dominio di broadcast

I domini di broadcast raggruppano le porte di rete nel cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM.

A partire da ONTAP 9.8, i domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. A partire da ONTAP 9.12.0, oltre ai domini di broadcast creati automaticamente, è possibile aggiungere manualmente un dominio di broadcast in Gestore di sistema.

### Prima di iniziare

Le porte che si desidera aggiungere al dominio di trasmissione non devono appartenere a un altro dominio di trasmissione. Se le porte che si desidera utilizzare appartengono a un altro dominio di trasmissione, ma non sono utilizzate, rimuoverle dal dominio di trasmissione originale.

### A proposito di questa attività

- Tutti i nomi di dominio di trasmissione devono essere univoci all'interno di un IPspace.
- Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di aggregazione di collegamenti/gruppi di interfacce (LAG/ifgrps).
- Se le porte che si desidera utilizzare appartengono a un altro dominio di broadcast, ma non sono utilizzate, rimuoverle dal dominio di broadcast esistente prima di aggiungerle al nuovo dominio.
- L'MTU (Maximum Transmission Unit) delle porte aggiunte a un dominio di broadcast viene aggiornato al valore MTU impostato nel dominio di broadcast.

- Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.
- Se non si specifica un nome IPspace, il dominio di trasmissione viene creato nell'IPspace "predefinito".

Per semplificare la configurazione del sistema, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte.

## System Manager

### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Fare clic su **+ Add**
3. Assegnare un nome al dominio di trasmissione.
4. Impostare la MTU.
5. Selezionare IPspace.
6. Salvare il dominio di trasmissione.

È possibile modificare o eliminare un dominio di trasmissione dopo averlo aggiunto.

### CLI

In ONTAP 9.7 o versioni precedenti, è possibile creare manualmente un dominio di broadcast.

Se si utilizza ONTAP 9,8 e versioni successive, i domini di broadcast vengono creati automaticamente in base alla raggiungibilità del livello 2. Per ulteriori informazioni, vedere ["Riparare la raggiungibilità delle porte"](#).

### Fasi

1. Visualizzare le porte non attualmente assegnate a un dominio di trasmissione:

```
network port show
```

Se il display è grande, utilizzare `network port show -broadcast-domain` per visualizzare solo le porte non assegnate.

2. Creare un dominio di broadcast:

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

a. `broadcast_domain_name` è il nome del dominio di trasmissione che si desidera creare.

b. `mtu_value` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.

Questo valore viene applicato a tutte le porte aggiunte a questo dominio di trasmissione.

c. `ipspace_name` È il nome dell'IPspace a cui verrà aggiunto questo dominio di trasmissione.

L'IPspace "predefinito" viene utilizzato a meno che non si specifichi un valore per questo parametro.

d. `ports_list` è l'elenco delle porte che verranno aggiunte al dominio di trasmissione.

Le porte vengono aggiunte nel formato `node_name:port_number`, ad esempio, `node1:e0c`.

3. Verificare che il dominio di trasmissione sia stato creato come desiderato:

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

### Esempio

Il seguente comando crea il dominio di trasmissione bcast1 nell'IPSpace predefinito, imposta la MTU su 1500 e aggiunge quattro porte:

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

### Al termine

È possibile definire il pool di indirizzi IP che saranno disponibili nel dominio di trasmissione creando una subnet oppure assegnare SVM e interfacce a IPSpace in questo momento. Per ulteriori informazioni, vedere ["Peering di cluster e SVM"](#).

Se è necessario modificare il nome di un dominio di trasmissione esistente, utilizzare `network port broadcast-domain rename` comando.

## Aggiunta o rimozione di porte da un dominio di broadcast (ONTAP 9,8 e versioni successive)

I domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. Non è necessario rimuovere manualmente le porte dai domini di broadcast.

Se la raggiungibilità della porta di rete è cambiata, tramite la connettività fisica della rete o la configurazione dello switch, e una porta di rete appartiene a un dominio di trasmissione diverso, consultare il seguente argomento:


["Riparare la raggiungibilità delle porte"](#)

## System Manager

A partire da ONTAP 9.14.1, è possibile utilizzare System Manager per riassegnare le porte Ethernet nei domini di broadcast. Si consiglia di assegnare ogni porta Ethernet a un dominio di broadcast. Pertanto, se si annulla l'assegnazione di una porta Ethernet a un dominio di broadcast, è necessario riassegnarla a un dominio di broadcast diverso.

### Fasi

Per riassegnare le porte Ethernet, attenersi alla seguente procedura:

1. Selezionare **rete > Panoramica**.
2. Nella sezione **Domini di trasmissione**, selezionare  accanto al nome di dominio.
3. Nel menu a discesa, selezionare **Modifica**.
4. Nella pagina **Modifica dominio di trasmissione**, deselezionare le porte Ethernet che si desidera riassegnare a un altro dominio.
5. Per ogni porta deselezionata viene visualizzata la finestra **Riassegna porta Ethernet**. Selezionare il dominio di notifica a cui si desidera riassegnare la porta, quindi selezionare **Riassegna**.
6. Selezionare tutte le porte che si desidera assegnare al dominio di broadcast corrente e salvare le modifiche.

### CLI

Se la raggiungibilità della porta di rete è cambiata, tramite la connettività fisica della rete o la configurazione dello switch, e una porta di rete appartiene a un dominio di trasmissione diverso, consultare il seguente argomento:

#### "Riparare la raggiungibilità delle porte"

In alternativa, è possibile aggiungere o rimuovere manualmente le porte dai domini di broadcast utilizzando `network port broadcast-domain add-ports` o il `network port broadcast-domain remove-ports` comando.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Le porte che si intende aggiungere a un dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.
- Le porte che già appartengono a un gruppo di interfacce non possono essere aggiunte singolarmente a un dominio di trasmissione.

### A proposito di questa attività

Quando si aggiungono e rimuovono le porte di rete, si applicano le seguenti regole:

Quando si aggiungono porte...	Durante la rimozione delle porte...
Le porte possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).	N/A.
Le porte vengono aggiunte al gruppo di failover definito dal sistema del dominio di trasmissione.	Le porte vengono rimosse da tutti i gruppi di failover nel dominio di trasmissione.
La MTU delle porte viene aggiornata al valore MTU impostato nel dominio di trasmissione.	L'MTU delle porte non cambia.

L'IPSpace delle porte viene aggiornato al valore IPspace del dominio di trasmissione.

Le porte vengono spostate in IPspace predefinito senza attributi di dominio di trasmissione.



Se si rimuove l'ultima porta membro di un gruppo di interfacce utilizzando `network port ifgrp remove-port` determina la rimozione della porta del gruppo di interfacce dal dominio di trasmissione, in quanto non è consentita una porta vuota del gruppo di interfacce in un dominio di trasmissione.

## Fasi

1. Consente di visualizzare le porte attualmente assegnate o non assegnate a un dominio di trasmissione utilizzando `network port show` comando.
2. Aggiungere o rimuovere le porte di rete dal dominio di trasmissione:

Se si desidera...	Utilizzare...
Aggiungere porte a un dominio di broadcast	<code>network port broadcast-domain add-ports</code>
Rimuovere le porte da un dominio di broadcast	<code>network port broadcast-domain remove-ports</code>

3. Verificare che le porte siano state aggiunte o rimosse dal dominio di trasmissione:

```
network port show
```

Per ulteriori informazioni su questi comandi, vedere ["Comandi di ONTAP 9"](#).

## Esempi di aggiunta e rimozione di porte

Il seguente comando aggiunge la porta e0g sul cluster di nodi 1-01 e la porta e0g sul cluster di nodi 1-02 al dominio di trasmissione bcast1 nell'IPspace predefinito:

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

Il seguente comando aggiunge due porte del cluster al dominio di trasmissione Cluster nell'IPspace del cluster:

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

Il seguente comando rimuove la porta e0e sul cluster di nodi 1-01 dal dominio di broadcast cast1 nell'IPspace predefinito:

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

## Spostamento dei domini di broadcast in IPspace (ONTAP 9,8 e versioni successive)

Spostare i domini di broadcast creati dal sistema in base alla raggiungibilità del livello 2

negli IPspaces creati.

Prima di spostare il dominio di trasmissione, è necessario verificare la raggiungibilità delle porte nei domini di trasmissione.

La scansione automatica delle porte può determinare quali porte possono raggiungere l'una con l'altra e posizionarle nello stesso dominio di trasmissione, ma questa scansione non è in grado di determinare l'IPSpace appropriato. Se il dominio di trasmissione appartiene a un IPSpace non predefinito, è necessario spostarlo manualmente seguendo la procedura descritta in questa sezione.

### Prima di iniziare

I domini di broadcast vengono configurati automaticamente come parte delle operazioni di creazione e Unione del cluster. ONTAP definisce il dominio di broadcast "predefinito" come l'insieme di porte con connettività di livello 2 alla porta home dell'interfaccia di gestione sul primo nodo creato nel cluster. Se necessario, vengono creati altri domini di broadcast denominati **Default-1**, **Default-2** e così via.

Quando un nodo si unisce a un cluster esistente, le relative porte di rete si uniscono automaticamente ai domini di broadcast esistenti in base alla raggiungibilità del livello 2. Se non sono raggiungibili in un dominio di trasmissione esistente, le porte vengono inserite in uno o più nuovi domini di trasmissione.

### A proposito di questa attività

- Le porte con LIF del cluster vengono automaticamente inserite nell'IPSpace "Cluster".
- Le porte con raggiungibilità alla porta home della LIF di gestione dei nodi vengono inserite nel dominio broadcast "Default".
- Gli altri domini di broadcast vengono creati automaticamente da ONTAP come parte dell'operazione di creazione o Unione del cluster.
- Quando si aggiungono VLAN e gruppi di interfacce, queste vengono automaticamente inserite nel dominio di trasmissione appropriato circa un minuto dopo la loro creazione.

### Fasi

1. Verificare la raggiungibilità delle porte nei domini di trasmissione. ONTAP monitora automaticamente la raggiungibilità del Layer 2. Utilizzare il seguente comando per verificare che ogni porta sia stata aggiunta a un dominio di trasmissione e che sia "ok".

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

2. Se necessario, spostare i domini di broadcast in altri spazi IP:

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

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1":

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

### Spostamento dei domini di broadcast in IPSpace (ONTAP 9,8 e versioni successive)

Spostare i domini di broadcast creati dal sistema in base alla raggiungibilità del livello 2 negli IPspaces creati.

Prima di spostare il dominio di trasmissione, è necessario verificare la raggiungibilità delle porte nei domini di trasmissione.



La scansione automatica delle porte può determinare quali porte possono raggiungere l'una con l'altra e posizzarle nello stesso dominio di trasmissione, ma questa scansione non è in grado di determinare l'IPSpace appropriato. Se il dominio di trasmissione appartiene a un IPSpace non predefinito, è necessario spostarlo manualmente seguendo la procedura descritta in questa sezione.

### Prima di iniziare

I domini di broadcast vengono configurati automaticamente come parte delle operazioni di creazione e Unione del cluster. ONTAP definisce il dominio di broadcast "predefinito" come l'insieme di porte con connettività di livello 2 alla porta home dell'interfaccia di gestione sul primo nodo creato nel cluster. Se necessario, vengono creati altri domini di broadcast denominati **Default-1**, **Default-2** e così via.

Quando un nodo si unisce a un cluster esistente, le relative porte di rete si uniscono automaticamente ai domini di broadcast esistenti in base alla raggiungibilità del livello 2. Se non sono raggiungibili in un dominio di trasmissione esistente, le porte vengono inserite in uno o più nuovi domini di trasmissione.

### A proposito di questa attività

- Le porte con LIF del cluster vengono automaticamente inserite nell'IPSpace "Cluster".
- Le porte con raggiungibilità alla porta home della LIF di gestione dei nodi vengono inserite nel dominio broadcast "Default".
- Gli altri domini di broadcast vengono creati automaticamente da ONTAP come parte dell'operazione di creazione o Unione del cluster.
- Quando si aggiungono VLAN e gruppi di interfacce, queste vengono automaticamente inserite nel dominio di trasmissione appropriato circa un minuto dopo la loro creazione.

### Fasi

1. Verificare la raggiungibilità delle porte nei domini di trasmissione. ONTAP monitora automaticamente la raggiungibilità del Layer 2. Utilizzare il seguente comando per verificare che ogni porta sia stata aggiunta a un dominio di trasmissione e che sia "ok".

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

2. Se necessario, spostare i domini di broadcast in altri spazi IP:

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

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1":

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

### Suddivisione dei domini di broadcast (ONTAP 9,8 e versioni successive)

Se la raggiungibilità delle porte di rete è cambiata, attraverso la connettività fisica della rete o la configurazione dello switch, Inoltre, un gruppo di porte di rete precedentemente configurate in 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 di rete fisica.

Per determinare se un dominio di broadcast della porta di rete è suddiviso in più set di raggiungibilità, utilizzare `network port reachability show -details` Controllare e prestare attenzione a quali porte non sono dotate di connettività l'una con l'altra ("Porte irraggiungibili"). 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.

### Fase

Suddividere un dominio di broadcast in due domini di broadcast:

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

- `ipspace_name` è il nome dell'ipspace in cui risiede il dominio di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà suddiviso.
- `-new-broadcast-domain` è il nome del nuovo dominio di trasmissione che verrà creato.
- `-ports` è il nome del nodo e la porta da aggiungere al nuovo dominio di trasmissione.

### Unione di domini di broadcast (ONTAP 9,8 e versioni successive)

Se la raggiungibilità delle porte di rete è cambiata, attraverso la connettività fisica della rete o la configurazione dello switch, e due gruppi di porte di rete precedentemente configurati in più domini di broadcast ora condividono la raggiungibilità, è possibile utilizzare l'Unione di due domini di broadcast per sincronizzare la configurazione ONTAP con la topologia fisica della rete.

Per determinare se più domini di broadcast appartengono a un set di raggiungibilità, utilizzare il comando "network port reachability show -details" e prestare attenzione a quali porte configurate in un altro dominio di broadcast hanno effettivamente la connettività l'una all'altra ("porte impreviste"). In genere, l'elenco delle porte impreviste definisce il set di porte che devono essere unite nel dominio di trasmissione dopo aver verificato che la configurazione fisica e quella dello switch sono accurate.

### Fase

Unire le porte da un dominio di broadcast in un dominio di broadcast esistente:

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

- `ipspace_name` è il nome dell'ipspace in cui risiedono i domini di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà unito.
- `-into-broadcast-domain` è il nome del dominio di trasmissione che riceverà porte aggiuntive.

### Modifica del valore MTU per le porte in un dominio di broadcast (ONTAP 9,8 e versioni successive)

È possibile modificare il valore MTU per un dominio di broadcast per modificare il valore MTU per tutte le porte in tale dominio di broadcast. Questa operazione può essere eseguita per supportare le modifiche della topologia apportate alla rete.

## Prima di iniziare

Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.

## A proposito di questa attività

La modifica del valore MTU causa una breve interruzione del traffico sulle porte interessate. Il sistema visualizza un prompt che richiede di rispondere con y per modificare la MTU.

## Fase

Modificare il valore MTU per tutte le porte in un dominio di broadcast:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` è il nome del dominio di trasmissione.
- `mtu` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.
- `ipSPACE` È il nome dell'IPSpace in cui risiede il dominio di trasmissione. L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione. Il seguente comando modifica la MTU in 9000 per tutte le porte nel dominio di trasmissione `bcast1`:

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

## Visualizza domini di broadcast (ONTAP 9,8 e versioni successive)

È possibile visualizzare l'elenco dei domini di broadcast all'interno di ciascun IPSpace di un cluster. L'output mostra anche l'elenco delle porte e il valore MTU per ciascun dominio di broadcast.

## Fase

Visualizzare i domini di broadcast e le porte associate nel cluster:

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

Il seguente comando visualizza tutti i domini di trasmissione e le porte associate nel cluster:

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

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

Il seguente comando visualizza le porte nel dominio di trasmissione Default-1 che presentano uno stato di errore di aggiornamento, che indica che la porta non può essere aggiornata correttamente:

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

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

Per ulteriori informazioni, vedere ["Comandi di ONTAP 9"](#).

## Eliminare un dominio di trasmissione

Se non è più necessario un dominio di trasmissione, è possibile eliminarlo. In questo modo, le porte associate al dominio di trasmissione vengono spostate nello spazio IPspace "predefinito".

### Prima di iniziare

Non devono essere presenti subnet, interfacce di rete o SVM associate al dominio di trasmissione che si desidera eliminare.

## A proposito di questa attività

- Impossibile eliminare il dominio di trasmissione "Cluster" creato dal sistema.
- Tutti i gruppi di failover correlati al dominio di trasmissione vengono rimossi quando si elimina il dominio di trasmissione.


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

### System Manager

**A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare un dominio di trasmissione**

L'opzione di eliminazione non viene visualizzata quando il dominio di trasmissione contiene porte o è associato a una subnet.

### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Selezionare  > **Elimina** accanto al dominio di trasmissione che si desidera rimuovere.

### CLI

**Utilizzare la CLI per eliminare un dominio di trasmissione**

### Fase

Eliminazione di un dominio di broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipSPACE ipSPACE_name]
```

Il seguente comando elimina il dominio di trasmissione Default-1 in IPSPACE ipSPACE1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipSPACE
ipSPACE1
```

## Dominio di broadcast (ONTAP 9,7 e versioni precedenti)

### Panoramica del dominio di trasmissione (ONTAP 9,7 e versioni precedenti)

I domini di broadcast sono destinati a raggruppare le porte di rete che appartengono alla stessa rete Layer 2. Le porte del gruppo possono quindi essere utilizzate da una macchina virtuale di storage (SVM) per il traffico di dati o di gestione.

Un dominio di broadcast risiede in un IPSPACE. Durante l'inizializzazione del cluster, il sistema crea due domini di broadcast predefiniti:

- Il dominio di trasmissione predefinito contiene le porte che si trovano nello spazio IPSPACE predefinito. Queste porte vengono utilizzate principalmente per la gestione dei dati. Anche le porte di gestione del cluster e dei nodi si trovano in questo dominio di broadcast.
- Il dominio di broadcast del cluster contiene le porte che si trovano in Cluster IPSPACE. Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster di tutti i nodi del cluster.

Se sono stati creati IPspaces univoci per separare il traffico client, è necessario creare un dominio di broadcast in ciascuno di questi IPspaces.



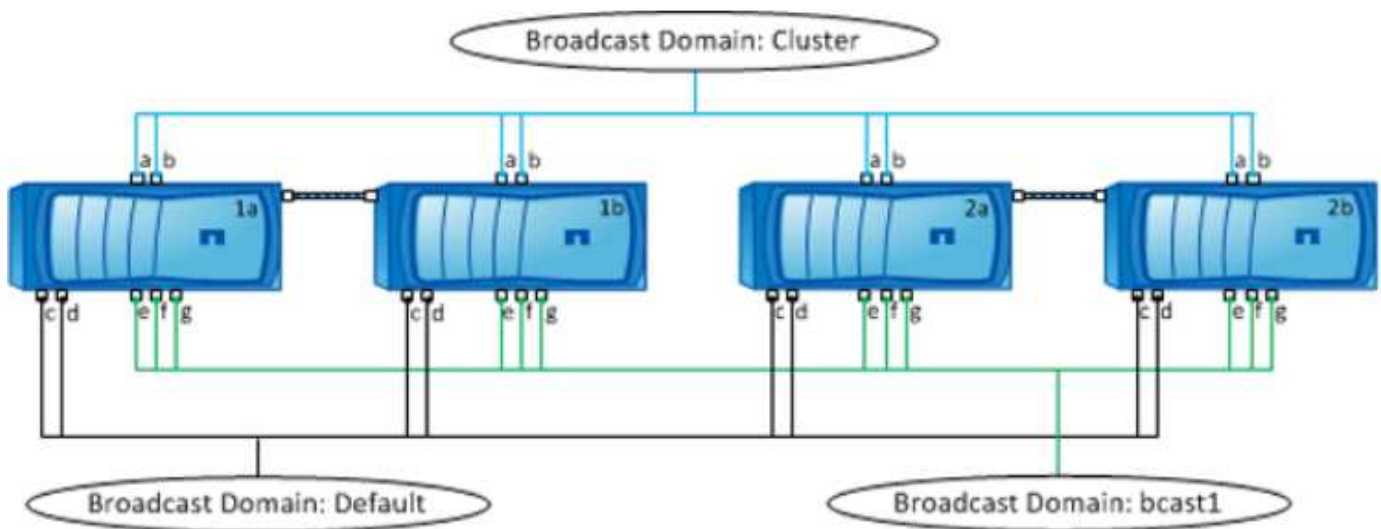
Creare un dominio di broadcast per raggruppare le porte di rete nel cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM.

#### Esempio di utilizzo di domini di broadcast

Un dominio di broadcast è un insieme di porte di rete nello stesso IPspace che ha anche la raggiungibilità di livello 2 l'una rispetto all'altra, incluse generalmente le porte di molti nodi del cluster.

L'illustrazione mostra le porte assegnate a tre domini di broadcast in un cluster a quattro nodi:

- Il dominio di broadcast del cluster viene creato automaticamente durante l'inizializzazione del cluster e contiene le porte a e b di ciascun nodo del cluster.
- Il dominio di broadcast predefinito viene creato automaticamente anche durante l'inizializzazione del cluster e contiene le porte c e d di ciascun nodo del cluster.
- Il dominio di broadcast bcast1 è stato creato manualmente e contiene le porte e, f e g di ciascun nodo del cluster. Questo dominio di broadcast è stato creato dall'amministratore di sistema specificamente per consentire a un nuovo client di accedere ai dati attraverso una nuova SVM.



Viene creato automaticamente un gruppo di failover con lo stesso nome e con le stesse porte di rete di ciascuno dei domini di trasmissione. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover.

#### Determinazione delle porte che possono essere utilizzate per un dominio di trasmissione (ONTAP 9,7 e versioni precedenti)

Prima di poter configurare un dominio di trasmissione da aggiungere al nuovo IPspace, è necessario determinare quali porte sono disponibili per il dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## A proposito di questa attività

- Le porte possono essere porte fisiche, VLAN o gruppi di interfacce (ifgroup).
- Le porte che si desidera aggiungere al nuovo dominio di trasmissione non possono essere assegnate a un dominio di trasmissione esistente.
- Se le porte che si desidera aggiungere al dominio di trasmissione si trovano già in un altro dominio di trasmissione (ad esempio, il dominio di trasmissione predefinito in IPSpace predefinito), è necessario rimuovere le porte da tale dominio di trasmissione prima di assegnarle al nuovo dominio di trasmissione.
- Le porte a cui sono assegnati LIF non possono essere rimosse da un dominio di broadcast.
- Poiché le LIF di gestione del cluster e dei nodi sono assegnate al dominio di broadcast predefinito in IPSpace predefinito, le porte assegnate a queste LIF non possono essere rimosse dal dominio di broadcast predefinito.

## Fasi

1. Determinare le assegnazioni correnti delle porte.

```
network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	----	-----	-----	-----	----	-----
node1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
node2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

In questo esempio, l'output del comando fornisce le seguenti informazioni:

- Porte e0c, e0d, e0e, e0f, e. e0g Su ciascun nodo vengono assegnati al dominio di broadcast predefinito.
  - Queste porte sono potenzialmente disponibili per l'utilizzo nel dominio di trasmissione dell'IPSpace che si desidera creare.
2. Determinare quali porte nel dominio di broadcast predefinito sono assegnate alle interfacce LIF e quindi non possono essere spostate in un nuovo dominio di broadcast.

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster						
	node1_clus1	up/up	10.0.2.40/24	node1	e0a	true
	node1_clus2	up/up	10.0.2.41/24	node1	e0b	true
	node2_clus1	up/up	10.0.2.42/24	node2	e0a	true
	node2_clus2	up/up	10.0.2.43/24	node2	e0b	true
cluster1						
	cluster_mgmt	up/up	10.0.1.41/24	node1	e0c	true
	node1_mgmt	up/up	10.0.1.42/24	node1	e0c	true
	node2_mgmt	up/up	10.0.1.43/24	node2	e0c	true

Nell'esempio seguente, l'output del comando fornisce le seguenti informazioni:

- Le porte del nodo vengono assegnate alla porta e0c. Su ciascun nodo e il nodo principale della LIF amministrativa del cluster è attivo e0c acceso node1.
- Porte e0d, e0e, e0f, e. e0g. Su ogni nodo non sono presenti LIF e possono essere rimossi dal dominio di broadcast predefinito e quindi aggiunti a un nuovo dominio di broadcast per il nuovo IPspace.

### Creare un dominio di trasmissione (ONTAP 9.7 e versioni precedenti)

In ONTAP 9.7 e versioni precedenti, si crea un dominio di broadcast per raggruppare le porte di rete del cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM. È necessario creare un dominio di trasmissione per un IPspace personalizzato. Le SVM create in IPspace utilizzano le porte nel dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

A partire da ONTAP 9.8, i domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. Se si utilizza ONTAP 9.8 o versione successiva, questa procedura non è necessaria.

In ONTAP 9.7 e versioni precedenti, le porte che si intende aggiungere al dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.

#### A proposito di questa attività

La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Quando si crea un dominio di broadcast, ONTAP crea automaticamente un gruppo di failover con lo stesso nome. Il gruppo di failover contiene tutte le porte assegnate al dominio di trasmissione.

- Tutti i nomi di dominio di trasmissione devono essere univoci all'interno di un IPspace.



- Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).
- Se le porte che si desidera utilizzare appartengono a un altro dominio di trasmissione, ma non sono utilizzate, utilizzare `network port broadcast-domain remove-ports` per rimuovere le porte dal dominio di trasmissione esistente.
- Le MTU delle porte aggiunte a un dominio di trasmissione vengono aggiornate al valore MTU impostato nel dominio di trasmissione.
- Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.
- Se non si specifica un nome IPspace, il dominio di trasmissione viene creato nell'IPspace "predefinito".

Per semplificare la configurazione del sistema, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte.

## Fasi

1. Visualizzare le porte non attualmente assegnate a un dominio di trasmissione:

```
network port show
```

Se il display è grande, utilizzare `network port show -broadcast-domain` per visualizzare solo le porte non assegnate.

2. Creare un dominio di broadcast:

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

◦ *broadcast\_domain\_name* è il nome del dominio di trasmissione che si desidera creare.

◦ *mtu\_value* È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.

Questo valore viene applicato a tutte le porte aggiunte a questo dominio di trasmissione.

◦ *ipspace\_name* È il nome dell'IPspace a cui verrà aggiunto questo dominio di trasmissione.

L'IPspace "predefinito" viene utilizzato a meno che non si specifichi un valore per questo parametro.

◦ *ports\_list* è l'elenco delle porte che verranno aggiunte al dominio di trasmissione.

Le porte vengono aggiunte nel formato *node\_name:port\_number*, ad esempio, `node1:e0c`.

3. Verificare che il dominio di trasmissione sia stato creato come desiderato:

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

## Esempio

Il seguente comando crea il dominio di trasmissione `bcast1` nell'IPspace predefinito, imposta la MTU su 1500 e aggiunge quattro porte:

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

## Al termine

È possibile definire il pool di indirizzi IP che saranno disponibili nel dominio di trasmissione creando una subnet oppure assegnare SVM e interfacce a IPspace in questo momento. Per ulteriori informazioni, vedere ["Peering di cluster e SVM"](#).

Se è necessario modificare il nome di un dominio di trasmissione esistente, utilizzare `network port broadcast-domain rename` comando.

### Aggiunta o rimozione di porte da un dominio di trasmissione (ONTAP 9,7 e versioni precedenti)

È possibile aggiungere porte di rete durante la creazione iniziale di un dominio di trasmissione oppure aggiungere o rimuovere porte da un dominio di trasmissione già esistente. Ciò consente di utilizzare in modo efficiente tutte le porte del cluster.

Se le porte che si desidera aggiungere al nuovo dominio di trasmissione si trovano già in un altro dominio di trasmissione, è necessario rimuovere le porte da tale dominio di trasmissione prima di assegnarle al nuovo dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

#### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Le porte che si intende aggiungere a un dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.
- Le porte che già appartengono a un gruppo di interfacce non possono essere aggiunte singolarmente a un dominio di trasmissione.

#### A proposito di questa attività

Quando si aggiungono e rimuovono le porte di rete, si applicano le seguenti regole:

Quando si aggiungono porte...	Durante la rimozione delle porte...
Le porte possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).	N/A.
Le porte vengono aggiunte al gruppo di failover definito dal sistema del dominio di trasmissione.	Le porte vengono rimosse da tutti i gruppi di failover nel dominio di trasmissione.
La MTU delle porte viene aggiornata al valore MTU impostato nel dominio di trasmissione.	L'MTU delle porte non cambia.
L'IPspace delle porte viene aggiornato al valore IPspace del dominio di trasmissione.	Le porte vengono spostate in IPspace predefinito senza attributi di dominio di trasmissione.



Se si rimuove l'ultima porta membro di un gruppo di interfacce utilizzando `network port ifgrp remove-port` determina la rimozione della porta del gruppo di interfacce dal dominio di trasmissione, in quanto non è consentita una porta vuota del gruppo di interfacce in un dominio di trasmissione.

#### Fasi

1. Consente di visualizzare le porte attualmente assegnate o non assegnate a un dominio di trasmissione utilizzando `network port show` comando.

## 2. Aggiungere o rimuovere le porte di rete dal dominio di trasmissione:

Se si desidera...	Utilizzare...
Aggiungere porte a un dominio di broadcast	<code>network port broadcast-domain add-ports</code>
Rimuovere le porte da un dominio di broadcast	<code>network port broadcast-domain remove-ports</code>

## 3. Verificare che le porte siano state aggiunte o rimosse dal dominio di trasmissione:

```
network port show
```

Per ulteriori informazioni su questi comandi, vedere ["Comandi di ONTAP 9"](#).

### Esempi di aggiunta e rimozione di porte

Il seguente comando aggiunge la porta e0g sul cluster di nodi 1-01 e la porta e0g sul cluster di nodi 1-02 al dominio di trasmissione bcast1 nell'IPSpace predefinito:

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

Il seguente comando aggiunge due porte del cluster al dominio di trasmissione Cluster nell'IPSpace del cluster:

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

Il seguente comando rimuove la porta e0e sul cluster di nodi 1-01 dal dominio di broadcast cast1 nell'IPSpace predefinito:

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

### Suddivisione dei domini di broadcast (ONTAP 9.7 o versioni precedenti)

È possibile modificare un dominio di broadcast esistente suddividendolo in due domini di broadcast diversi, con ciascun dominio di broadcast contenente alcune delle porte originali assegnate al dominio di broadcast originale.

#### A proposito di questa attività

- Se le porte si trovano in un gruppo di failover, è necessario suddividere tutte le porte di un gruppo di failover.
- Se alle porte sono associati LIF, i LIF non possono far parte degli intervalli di una subnet.

#### Fase

Suddividere un dominio di broadcast in due domini di broadcast:

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

- `ipspace_name` È il nome dell'IPSpace in cui risiede il dominio di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà suddiviso.
- `-new-broadcast-domain` è il nome del nuovo dominio di trasmissione che verrà creato.
- `-ports` è il nome del nodo e la porta da aggiungere al nuovo dominio di trasmissione.

### Unione di domini di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile spostare tutte le porte da un dominio di broadcast a un dominio di broadcast esistente utilizzando il comando `merge`.

Questa operazione riduce i passaggi necessari per rimuovere tutte le porte da un dominio di trasmissione e aggiungerle a un dominio di trasmissione esistente.

#### Fase

Unire le porte da un dominio di broadcast in un dominio di broadcast esistente:

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

- `ipspace_name` È il nome dell'IPSpace in cui risiedono i domini di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà unito.
- `-into-broadcast-domain` è il nome del dominio di trasmissione che riceverà porte aggiuntive.

#### Esempio

Il seguente esempio unisce il dominio di trasmissione `bd-data1` al dominio di trasmissione `bd-data2`:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

### Modifica del valore MTU per le porte in un dominio di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile modificare il valore MTU per un dominio di broadcast per modificare il valore MTU per tutte le porte in tale dominio di broadcast. Questa operazione può essere eseguita per supportare le modifiche della topologia apportate alla rete.

#### Prima di iniziare

Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.

#### A proposito di questa attività

La modifica del valore MTU causa una breve interruzione del traffico sulle porte interessate. Il sistema visualizza un prompt che richiede di rispondere con y per modificare la MTU.

### Fase

Modificare il valore MTU per tutte le porte in un dominio di broadcast:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` è il nome del dominio di trasmissione.
- `mtu` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.
- `ipSPACE` È il nome dell'IPSpace in cui risiede il dominio di trasmissione. L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione. Il seguente comando modifica la MTU in 9000 per tutte le porte nel dominio di trasmissione `bcast1`:

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

### Visualizzazione dei domini di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile visualizzare l'elenco dei domini di broadcast all'interno di ciascun IPSpace di un cluster. L'output mostra anche l'elenco delle porte e il valore MTU per ciascun dominio di broadcast.

### Fase

Visualizzare i domini di broadcast e le porte associate nel cluster:

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

Il seguente comando visualizza tutti i domini di trasmissione e le porte associate nel cluster:

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

IPspace	Broadcast			Update
Name	Domain Name	MTU	Port List	Status Details
-----	-----	-----	-----	-----
Cluster	Cluster	9000		
			cluster-1-01:e0a	complete
			cluster-1-01:e0b	complete
			cluster-1-02:e0a	complete
			cluster-1-02:e0b	complete
Default	Default	1500		
			cluster-1-01:e0c	complete
			cluster-1-01:e0d	complete
			cluster-1-02:e0c	complete
			cluster-1-02:e0d	complete
	bcast1	1500		
			cluster-1-01:e0e	complete
			cluster-1-01:e0f	complete
			cluster-1-01:e0g	complete
			cluster-1-02:e0e	complete
			cluster-1-02:e0f	complete
			cluster-1-02:e0g	complete

Il seguente comando visualizza le porte nel dominio di trasmissione bcast1 che presentano uno stato di errore di aggiornamento, che indica che la porta non può essere aggiornata correttamente:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error
```

IPspace	Broadcast			Update
Name	Domain Name	MTU	Port List	Status Details
-----	-----	-----	-----	-----
Default	bcast1	1500		
			cluster-1-02:e0g	error

Per ulteriori informazioni, vedere ["Comandi di ONTAP 9"](#).

## Eliminare un dominio di trasmissione

Se non è più necessario un dominio di trasmissione, è possibile eliminarlo. In questo modo, le porte associate al dominio di trasmissione vengono spostate nello spazio IPspace "predefinito".

### Prima di iniziare

Non devono essere presenti subnet, interfacce di rete o SVM associate al dominio di trasmissione che si desidera eliminare.

### A proposito di questa attività

- Impossibile eliminare il dominio di trasmissione "Cluster" creato dal sistema.
- Tutti i gruppi di failover correlati al dominio di trasmissione vengono rimossi quando si elimina il dominio di trasmissione.


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

#### System Manager

**A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare un dominio di trasmissione**

L'opzione di eliminazione non viene visualizzata quando il dominio di trasmissione contiene porte o è associato a una subnet.

#### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Selezionare  > **Elimina** accanto al dominio di trasmissione che si desidera rimuovere.

#### CLI

**Utilizzare la CLI per eliminare un dominio di trasmissione**

#### Fase

Eliminazione di un dominio di broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipSPACE ipSPACE_name]
```

Il seguente comando elimina il dominio di trasmissione Default-1 in IPSPACE ipSPACE1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipSPACE
ipSPACE1
```

## Gruppi e policy di failover

### Panoramica sul failover LIF

Il failover LIF si riferisce alla migrazione automatica di una LIF a una porta di rete diversa in risposta a un errore di collegamento sulla porta corrente della LIF. Si tratta di un componente chiave per fornire alta disponibilità per le connessioni alle SVM. La configurazione del failover LIF comporta la creazione di un gruppo di failover, la modifica della LIF per l'utilizzo del gruppo di failover e la specifica di una policy di failover.

Un gruppo di failover contiene un set di porte di rete (porte fisiche, VLAN e gruppi di interfacce) da uno o più nodi in un cluster. Le porte di rete presenti nel gruppo di failover definiscono le destinazioni di failover disponibili per LIF. A un gruppo di failover possono essere assegnate le LIF di gestione del cluster, dei nodi, dell'intercluster e dei dati NAS.



Quando una LIF viene configurata senza una destinazione di failover valida, si verifica un'interruzione quando la LIF tenta di eseguire il failover. È possibile utilizzare il comando "network interface show -failover" per verificare la configurazione del failover.

Quando si crea un dominio di broadcast, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte di rete. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover. Questo è un'efficienza per gli amministratori che non desiderano gestire i propri gruppi di failover.

## Creare un gruppo di failover

Si crea un gruppo di failover di porte di rete in modo che una LIF possa migrare automaticamente a una porta diversa se si verifica un errore di collegamento sulla porta corrente della LIF. Questo consente al sistema di reindirizzare il traffico di rete ad altre porte disponibili nel cluster.

### A proposito di questa attività

Si utilizza `network interface failover-groups create` per creare il gruppo e aggiungere le porte al gruppo.

- Le porte aggiunte a un gruppo di failover possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).
- Tutte le porte aggiunte al gruppo di failover devono appartenere allo stesso dominio di broadcast.
- Una singola porta può risiedere in più gruppi di failover.
- Se si dispone di LIF in diverse VLAN o domini di broadcast, è necessario configurare i gruppi di failover per ogni VLAN o dominio di broadcast.
- I gruppi di failover non si applicano negli ambienti SAN iSCSI o FC.

### Fase

Creare un gruppo di failover:

```
network interface failover-groups create -vserver vs1 -failover-group failover_group_name -targets ports_list
```

- `vs1` È il nome della SVM che può utilizzare il gruppo di failover.
- `failover_group_name` è il nome del gruppo di failover che si desidera creare.
- `ports_list` è l'elenco delle porte che verranno aggiunte al gruppo di failover. Le porte vengono aggiunte nel formato `node_name>:port_number`, ad esempio `node1:e0c`.

Il seguente comando crea il gruppo di failover fg3 per SVM vs3 e aggiunge due porte:

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

### Al termine

- Ora che il gruppo di failover è stato creato, è necessario applicare il gruppo di failover a una LIF.



- L'applicazione di un gruppo di failover che non fornisce una destinazione di failover valida per una LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

## Configurare le impostazioni di failover su una LIF

È possibile configurare una LIF per il failover su un gruppo specifico di porte di rete applicando una policy di failover e un gruppo di failover alla LIF. È anche possibile disattivare il failover di una LIF su un'altra porta.

### A proposito di questa attività

- Quando viene creato un LIF, il failover LIF viene attivato per impostazione predefinita e l'elenco delle porte di destinazione disponibili viene determinato dal gruppo di failover predefinito e dalla policy di failover basata sul tipo LIF e sulla policy di servizio.

A partire da 9.5, è possibile specificare una politica di servizio per la LIF che definisce quali servizi di rete possono utilizzare la LIF. Alcuni servizi di rete impongono restrizioni di failover su una LIF.



Se la policy di servizio di una LIF viene modificata in modo da limitare ulteriormente il failover, la policy di failover della LIF viene aggiornata automaticamente dal sistema.

- È possibile modificare il comportamento di failover dei LIF specificando i valori per i parametri `-failover-group` e `-failover-policy` nel comando di modifica dell'interfaccia di rete.
- La modifica di una LIF che non ha una destinazione di failover valida per la LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

- A partire da ONTAP 9.11.1, sulle piattaforme ASA (All-Flash SAN Array), il failover LIF iSCSI viene abilitato automaticamente alle LIF iSCSI appena create sulle macchine virtuali storage appena create.

Inoltre, è possibile "[Abilitazione manuale del failover iSCSI LIF su LIF iSCSI pre-esistenti](#)", Ovvero le LIF create prima dell'aggiornamento a ONTAP 9.11.1 o versioni successive.

- L'elenco seguente descrive come l'impostazione `-failover-policy` influenza le porte di destinazione selezionate dal gruppo di failover:



Per il failover LIF iSCSI, solo le policy di failover `local-only`, `sfo-partner-only` e `disabled` sono supportati.

- `broadcast-domain-wide` Si applica a tutte le porte su tutti i nodi del gruppo di failover.
- `system-defined` Si applica solo a quelle porte sul nodo home di LIF e a un altro nodo del cluster, in genere un partner non SFO, se esistente.
- `local-only` Si applica solo a quelle porte sul nodo home di LIF.
- `sfo-partner-only` Si applica solo a quelle porte sul nodo principale della LIF e al suo partner SFO.
- `disabled` Indica che la LIF non è configurata per il failover.

## Fase

Configurare le impostazioni di failover per un'interfaccia esistente:

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

## Esempi di configurazione delle impostazioni di failover e disattivazione del failover

Il seguente comando imposta il criterio di failover su broadcast-domain-wide e utilizza le porte del gruppo di failover fg3 come destinazioni di failover per i dati LIF 1 su SVM vs3:

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

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

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

Il seguente comando disattiva il failover per LIF data1 su SVM vs3:

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

## Comandi per la gestione di policy e gruppi di failover

È possibile utilizzare `network interface failover-groups` comandi per gestire i gruppi di failover. Si utilizza `network interface modify` Comando per gestire i gruppi di failover e le policy di failover applicate a una LIF.

Se si desidera...	Utilizzare questo comando...
Aggiungere porte di rete a un gruppo di failover	<code>network interface failover-groups add-targets</code>
Rimuovere le porte di rete da un gruppo di failover	<code>network interface failover-groups remove-targets</code>
Modificare le porte di rete in un gruppo di failover	<code>network interface failover-groups modify</code>
Visualizza i gruppi di failover correnti	<code>network interface failover-groups show</code>

Configurare il failover su una LIF	<code>network interface modify -failover -group -failover-policy</code>
Visualizzare il gruppo di failover e la policy di failover utilizzati da ciascun LIF	<code>network interface show -fields failover-group, failover-policy</code>
Rinominare un gruppo di failover	<code>network interface failover-groups rename</code>
Eliminare un gruppo di failover	<code>network interface failover-groups delete</code>



La modifica di un gruppo di failover in modo che non fornisca una destinazione di failover valida per qualsiasi LIF nel cluster può causare un'interruzione quando un LIF tenta di eseguire il failover.

Per ulteriori informazioni, consultare le pagine man del `network interface failover-groups` e `network interface modify` comandi.

## Subnet (solo amministratori del cluster)

### Panoramica subnet

Le subnet consentono di allocare blocchi o pool specifici di indirizzi IP per la configurazione di rete ONTAP. In questo modo è possibile creare file LIF più facilmente specificando un nome di subnet invece di specificare i valori dell'indirizzo IP e della maschera di rete.

Una subnet viene creata all'interno di un dominio di trasmissione e contiene un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Gli indirizzi IP in una subnet vengono allocati alle porte nel dominio di trasmissione quando vengono create le LIF. Una volta rimossi i file LIF, gli indirizzi IP vengono restituiti al pool di subnet e sono disponibili per i file LIF futuri.

Si consiglia di utilizzare le subnet perché semplificano notevolmente la gestione degli indirizzi IP e semplificano la creazione di LIF. Inoltre, se si specifica un gateway durante la definizione di una subnet, una route predefinita a tale gateway viene aggiunta automaticamente alla SVM quando viene creata una LIF utilizzando tale subnet.

### Creare una subnet

È possibile creare una subnet per allocare blocchi specifici di indirizzi IPv4 o IPv6 da utilizzare in seguito quando si creano LIF per SVM.

In questo modo è possibile creare LIF più facilmente specificando un nome di subnet invece di dover specificare i valori dell'indirizzo IP e della maschera di rete per ciascun LIF.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Il dominio di trasmissione e l'IPSpace in cui si intende aggiungere la subnet devono già esistere.

#### **A proposito di questa attività**

- Tutti i nomi di subnet devono essere univoci all'interno di un IPSpace.
- Quando si aggiungono intervalli di indirizzi IP a una subnet, assicurarsi che non vi siano indirizzi IP sovrapposti nella rete in modo che sottoreti o host diversi non tentino di utilizzare lo stesso indirizzo IP.
- Se si specifica un gateway durante la definizione di una subnet, un percorso predefinito per tale gateway viene aggiunto automaticamente alla SVM quando viene creata una LIF utilizzando tale subnet. Se non si utilizzano sottoreti o se non si specifica un gateway durante la definizione di una subnet, è necessario utilizzare `route create` Comando per aggiungere manualmente un percorso alla SVM.

#### **Procedura**

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

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestore di sistema per creare una subnet.

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Fare clic su **+ Add** per creare una subnet.
3. Assegnare un nome alla subnet.
4. Specificare l'indirizzo IP della subnet.
5. Impostare la subnet mask.
6. Definire l'intervallo di indirizzi IP che compongono la subnet.
7. Se utile, specificare un gateway.
8. Selezionare il dominio di trasmissione a cui appartiene la subnet.
9. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

Utilizzare la CLI per creare una subnet.

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

- `subnet_name` è il nome della subnet di livello 3 che si desidera creare.

Il nome può essere una stringa di testo come "Mgmt" o un valore IP di subnet specifico come 192.0.2.0/24.

- `broadcast_domain_name` è il nome del dominio di trasmissione in cui risiede la subnet.
- `ipspace_name` È il nome dell'IPSpace di cui fa parte il dominio di trasmissione.

L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione.

- `subnet_address` È l'indirizzo IP e la maschera della subnet, ad esempio 192.0.2.0/24.
- `gateway_address` è il gateway per il percorso predefinito della subnet, ad esempio 192.0.2.1.
- `ip_address_list` Indica l'elenco o l'intervallo di indirizzi IP che verranno assegnati alla subnet.

Gli indirizzi IP possono essere singoli, un intervallo di indirizzi IP o una combinazione in un elenco separato da virgole.

- Il valore `true` può essere impostato per `-force-update-lif-associations` opzione.

Questo comando non riesce se un processore di servizio o un'interfaccia di rete sta attualmente utilizzando gli indirizzi IP nell'intervallo specificato. Impostando questo valore su `true`, tutte le interfacce indirizzate manualmente vengono associate alla subnet corrente e il comando viene eseguito correttamente.

Il seguente comando crea la subnet `sub1` nel dominio di trasmissione `Default-1` nell'IPSpace predefinito. Aggiunge un indirizzo IP e una maschera della subnet IPv4, il gateway e un intervallo di indirizzi IP:

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

Il seguente comando crea la subnet `sub2` nel dominio di trasmissione predefinito in IPSpace "Default". Aggiunge una serie di indirizzi IPv6:

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

#### Al termine

È possibile assegnare le SVM e le interfacce a un IPSpace utilizzando gli indirizzi nella subnet.

Se è necessario modificare il nome di una subnet esistente, utilizzare `network subnet rename` comando.

## Aggiungere o rimuovere indirizzi IP da una subnet


È possibile aggiungere indirizzi IP durante la creazione iniziale di una subnet oppure aggiungere indirizzi IP a una subnet già esistente. È inoltre possibile rimuovere gli indirizzi IP da una subnet esistente. In questo modo è possibile allocare solo gli indirizzi IP richiesti per le SVM.

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

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per aggiungere o rimuovere indirizzi IP da o verso una subnet

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare  > **Modifica** accanto alla subnet che si desidera modificare.
3. Aggiungere o rimuovere indirizzi IP.
4. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
`An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

Utilizzare la CLI per aggiungere o rimuovere indirizzi IP da o verso una subnet

#### A proposito di questa attività

Quando si aggiungono indirizzi IP, viene visualizzato un errore se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP dell'intervallo aggiunto. Se si desidera associare qualsiasi interfaccia indirizzata manualmente alla subnet corrente, è possibile impostare `-force-update-lif-associations` opzione a `true`.

Quando si rimuovono gli indirizzi IP, viene visualizzato un messaggio di errore se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP da rimuovere. Se si desidera che le interfacce continuino a utilizzare gli indirizzi IP dopo che sono state rimosse dalla subnet, è possibile impostare `-force-update-lif-associations` opzione a `true`.

### Fase

Aggiungere o rimuovere indirizzi IP da una subnet:

Se si desidera...	Utilizzare questo comando...
Aggiungere indirizzi IP a una subnet	<code>subnet add-range</code> di rete
Rimuovere gli indirizzi IP da una subnet	<code>remove-ranges subnet</code> di rete

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Il seguente comando aggiunge gli indirizzi IP da 192.0.2.82 a 192.0.2.85 alla subnet sub1:

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

Il seguente comando rimuove l'indirizzo IP 198.51.100.9 dalla subnet sub3:

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

Se l'intervallo corrente include da 1 a 10 e da 20 a 40 e si desidera aggiungere da 11 a 19 e da 41 a 50 (consentendo in pratica da 1 a 50), è possibile sovrapporre l'intervallo di indirizzi esistente utilizzando il comando seguente. Questo comando aggiunge solo i nuovi indirizzi e non influisce sugli indirizzi esistenti:

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

## Modificare le proprietà della subnet

È possibile modificare l'indirizzo di sottorete e il valore della maschera, l'indirizzo del gateway o l'intervallo di indirizzi IP in una subnet esistente.

### A proposito di questa attività

- Quando si modificano gli indirizzi IP, è necessario assicurarsi che non vi siano indirizzi IP sovrapposti nella rete in modo che sottoreti o host diversi non tentino di utilizzare lo stesso indirizzo IP.
- Se si aggiunge o si modifica l'indirizzo IP del gateway, il gateway modificato viene applicato alle nuove SVM quando in esse viene creata una LIF utilizzando la subnet. Se il percorso non esiste già, viene creato un percorso predefinito per il gateway SVM. Potrebbe essere necessario aggiungere manualmente un nuovo percorso alla SVM quando si modifica l'indirizzo IP del gateway.

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



## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione di sistema per modificare le proprietà della subnet

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare **> Modifica** accanto alla subnet che si desidera modificare.
3. Apportare modifiche.
4. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

#### Utilizzare la CLI per modificare le proprietà della subnet

#### Fase

Modificare le proprietà della subnet:

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

- `subnet_name` è il nome della subnet che si desidera modificare.
- `ipspace` È il nome dell'IPSpace in cui risiede la subnet.
- `subnet` è il nuovo indirizzo e la nuova maschera della subnet, se applicabile; ad esempio, 192.0.2.0/24.
- `gateway` è il nuovo gateway della subnet, se applicabile; ad esempio, 192.0.2.1. L'immissione di "" rimuove la voce del gateway.
- `ip_ranges` È il nuovo elenco, o intervallo, di indirizzi IP che verranno allocati alla subnet, se applicabile. Gli indirizzi IP possono essere singoli indirizzi, un intervallo o indirizzi IP o una combinazione in un elenco separato da virgole. L'intervallo specificato qui sostituisce gli indirizzi IP esistenti.
- `force-update-lif-associations` È necessario quando si modifica l'intervallo di indirizzi IP. È possibile impostare il valore su **true** per questa opzione quando si modifica l'intervallo di indirizzi IP. Questo comando non riesce se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP nell'intervallo specificato. Impostando questo valore su **true**, qualsiasi interfaccia indirizzata manualmente viene associata alla subnet corrente e il comando viene eseguito correttamente.

Il seguente comando modifica l'indirizzo IP del gateway della subnet sub3:

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

## Visualizzare le subnet

È possibile visualizzare l'elenco degli indirizzi IP allocati a ciascuna subnet all'interno di un IPspace. L'output mostra anche il numero totale di indirizzi IP disponibili in ciascuna subnet e il numero di indirizzi attualmente utilizzati.

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

### System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per visualizzare le subnet

#### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Visualizzare l'elenco delle subnet.

### CLI

Utilizzare la CLI per visualizzare le subnet

#### Fase

Visualizzare l'elenco delle subnet e gli intervalli di indirizzi IP associati utilizzati in tali subnet:

```
network subnet show
```

Il seguente comando visualizza le subnet e le proprietà della subnet:

```
network subnet show

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

## Eliminare una subnet

Se non è più necessaria una subnet e si desidera disallocare gli indirizzi IP assegnati alla

subnet, è possibile eliminarla.

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

### System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare una subnet

#### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare **⋮ > Elimina** accanto alla subnet che si desidera rimuovere.
3. Salvare le modifiche.

### CLI

#### Utilizzare la CLI per eliminare una subnet

##### A proposito di questa attività

Se un processore di servizio o un'interfaccia di rete sta attualmente utilizzando indirizzi IP compresi negli intervalli specificati, viene visualizzato un messaggio di errore. Se si desidera che le interfacce continuino a utilizzare gli indirizzi IP anche dopo l'eliminazione della subnet, è possibile impostare l'opzione `-force-update-lif-associations` su `true` per rimuovere l'associazione della subnet con i LIF.

#### Fase

Per eliminare una subnet:

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

Il seguente comando elimina la subnet sub1 in IPspace ipspace1:

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

## Creare SVM

È necessario creare una SVM per fornire i dati ai client.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario conoscere lo stile di sicurezza del volume root SVM.

Se si intende implementare una soluzione Hyper-V o SQL Server su SMB su questa SVM, è necessario utilizzare lo stile di protezione NTFS per il volume root. I volumi che contengono file Hyper-V o file di database SQL devono essere impostati sulla protezione NTFS al momento della creazione. Impostando lo stile di protezione del volume root su NTFS, si garantisce di non creare inavvertitamente volumi di dati UNIX o misti di tipo sicurezza.

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

## System Manager

È possibile utilizzare System Manager per creare una VM di storage.

### Fasi

1. Selezionare **Storage VM**.
2. Fare clic su **+ Add** Per creare una VM di storage.
3. Assegnare un nome alla VM di storage.
4. Selezionare il protocollo di accesso:
  - SMB/CIFS, NFS
  - iSCSI
  - FC
  - NVMe
  - i. Se si seleziona **Enable SMB/CIFS** (attiva SMB/CIFS\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Nome amministratore	Specificare il nome utente dell'amministratore per la VM di storage SMB/CIFS.
Password	Specificare la password dell'amministratore per la VM di storage SMB/CIFS.
Nome server	Specificare il nome del server per la VM di storage SMB/CIFS.
Dominio Active Directory	Specificare il dominio Active Directory per fornire l'autenticazione dell'utente per la VM di storage SMB/CIFS.
Unità organizzativa	Specificare l'unità organizzativa all'interno del dominio Active Directory associato al server SMB/CIFS. "CN=Computers" è il valore predefinito che può essere modificato.
Crittografa i dati durante l'accesso alle condivisioni nella VM di storage	Selezionare questa casella di controllo per crittografare i dati utilizzando SMB 3.0 per impedire l'accesso non autorizzato ai file sulle condivisioni nella VM di storage SMB/CIFS.
Domini	Aggiungere, rimuovere o riordinare i domini elencati per la VM di storage SMB/CIFS.
Server dei nomi	Aggiungere, rimuovere o riordinare i server dei nomi per la VM di storage SMB/CIFS.

Lingua predefinita	Specifica l'impostazione di codifica della lingua predefinita per la VM di storage e i relativi volumi. Utilizzare la CLI per modificare le impostazioni dei singoli volumi all'interno di una VM di storage.
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NFS** (attiva NFS), completare la seguente configurazione:

O casella di controllo	Descrizione
Allow NFS client access (Consenti accesso client NFS)	Selezionare questa casella di controllo quando tutti i volumi creati sulla VM di storage NFS devono utilizzare il percorso del volume root "/" per il montaggio e il passaggio. Aggiungere regole al criterio di esportazione "predefinito" per consentire un mount traversal ininterrotto.

Regole	<p>Fare clic su <b>+ Add</b> per creare regole.</p> <ul style="list-style-type: none"> <li>• Client Specification (specifica client): Specificare i nomi host, gli indirizzi IP, i netgroup o i domini.</li> <li>• Access Protocols (protocolli di accesso): Selezionare una combinazione delle seguenti opzioni: <ul style="list-style-type: none"> <li>◦ SMB/CIFS</li> <li>◦ FlexCache</li> <li>◦ NFS <ul style="list-style-type: none"> <li>▪ NFSv3</li> <li>▪ NFSv4</li> </ul> </li> </ul> </li> <li>• Access Details (Dettagli di accesso): Per ciascun tipo di utente, specificare il livello di accesso, di sola lettura, di lettura/scrittura o di superutente. I tipi di utente includono: <ul style="list-style-type: none"> <li>◦ Tutto</li> <li>◦ Tutti (come utente anonimo)</li> <li>◦ UNIX</li> <li>◦ Kerberos 5</li> <li>◦ Kerberos 5i</li> <li>◦ Kerberos 5p</li> <li>◦ NTLM</li> </ul> </li> </ul> <p>Salvare la regola.</p>
Lingua predefinita	<p>Specifica l'impostazione di codifica della lingua predefinita per la VM di storage e i relativi volumi. Utilizzare la CLI per modificare le impostazioni dei singoli volumi all'interno di una VM di storage.</p>
Interfaccia di rete	<p>Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b>. Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b>. È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.</p>

Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.
----------------------------------	---

1. Se si seleziona **Enable iSCSI** (attiva iSCSI\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable FC** (attiva FC\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Configurare le porte FC	Selezionare le interfacce di rete sui nodi che si desidera includere nella VM di storage. Si consigliano due interfacce di rete per nodo.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NVMe/FC** (attiva NVMe/FC\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Configurare le porte FC	Selezionare le interfacce di rete sui nodi che si desidera includere nella VM di storage. Si consigliano due interfacce di rete per nodo.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NVMe/TCP** (attiva NVMe/TCP\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Salvare le modifiche.

## CLI

Utilizzare l'interfaccia utente di ONTAP per creare una subnet.

## Fasi

1. Determinare quali aggregati sono candidati per contenere il volume root SVM.

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

È necessario scegliere un aggregato con almeno 1 GB di spazio libero per contenere il volume root. Se si intende configurare l'auditing NAS su SVM, è necessario disporre di almeno 3 GB di spazio libero aggiuntivo sull'aggregato root, con lo spazio extra utilizzato per creare il volume di staging di



auditing quando l'auditing è attivato.



Se il controllo NAS è già abilitato su una SVM esistente, il volume di staging dell'aggregato viene creato immediatamente dopo il completamento della creazione dell'aggregato.

2. Registrare il nome dell'aggregato su cui si desidera creare il volume root SVM.
3. Se si prevede di specificare una lingua quando si crea la SVM e non si conosce il valore da utilizzare, identificare e registrare il valore della lingua che si desidera specificare:

```
vserver create -language ?
```

4. Se si prevede di specificare una policy Snapshot quando si crea la SVM e non si conosce il nome della policy, elencare le policy disponibili e identificare e registrare il nome della policy Snapshot che si desidera utilizzare:

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

5. Se si prevede di specificare un criterio di quota quando si crea la SVM e non si conosce il nome del criterio, elencare i criteri disponibili e identificare e registrare il nome del criterio di quota che si desidera utilizzare:

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

6. Creare una SVM:

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

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

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

7. Verificare che la configurazione SVM sia corretta.

```
vserver show -vserver vs1
```

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

In questo esempio, il comando crea la SVM denominata "vs1" in IPspace "ipspace1". Il volume root è denominato "vs1\_root" e viene creato su aggr3 con lo stile di sicurezza NTFS.



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

## Interfacce logiche (LIF)

### Panoramica della LIF

#### Panoramica sulla configurazione delle LIF

Una LIF (interfaccia logica) rappresenta un punto di accesso di rete a un nodo del cluster. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.

Un amministratore del cluster può creare, visualizzare, modificare, migrare, ripristinare, Oppure eliminare i LIF. Un amministratore di SVM può visualizzare solo le LIF associate a SVM.

Un LIF è un indirizzo IP o WWPN con caratteristiche associate, ad esempio una policy di servizio, una porta home, un nodo home, un elenco di porte a cui eseguire il failover e una policy firewall. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

Le LIF possono essere ospitate sulle seguenti porte:

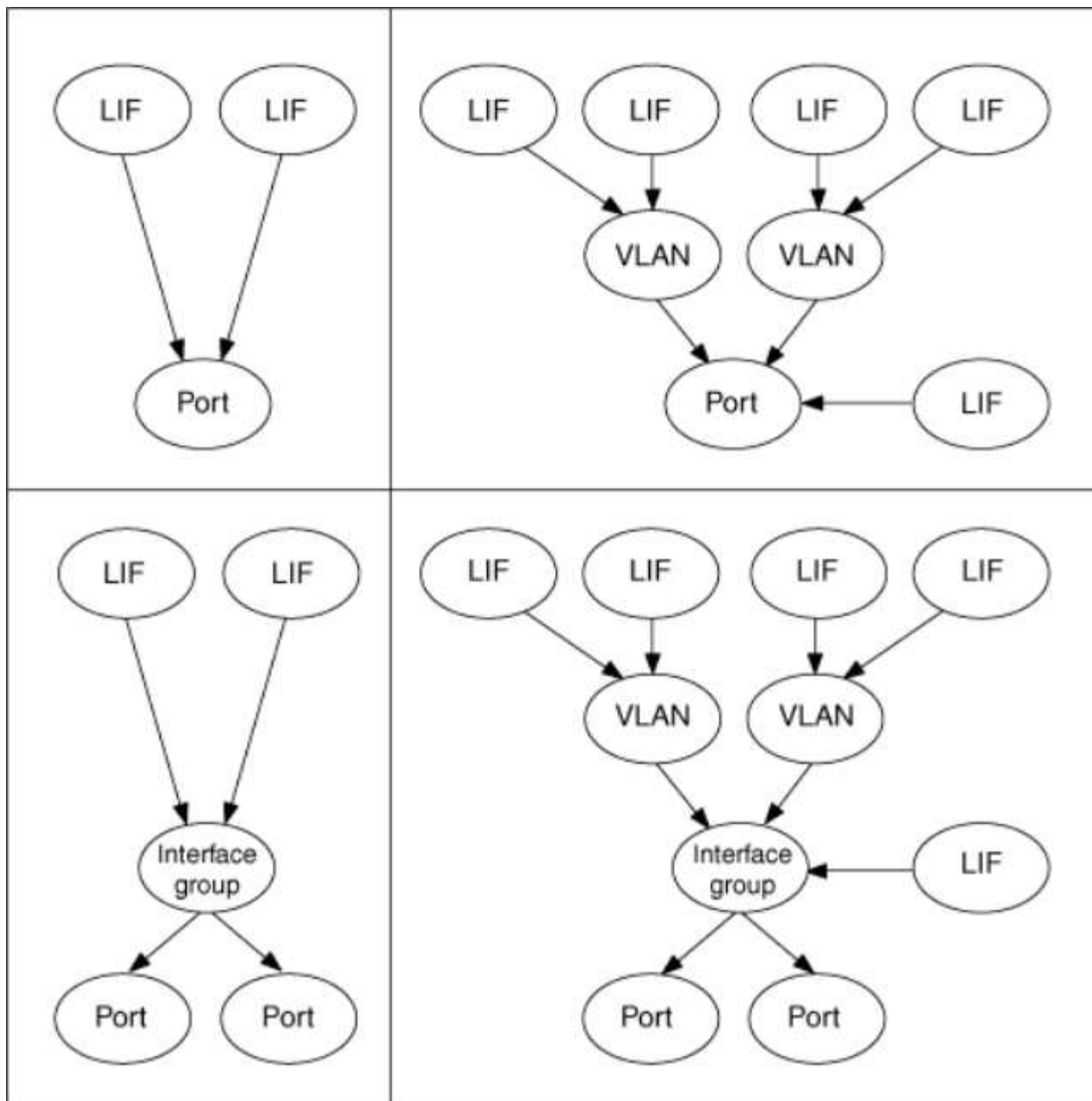
- Porte fisiche che non fanno parte di gruppi di interfacce
- Gruppi di interfacce
- VLAN
- Porte fisiche o gruppi di interfacce che ospitano VLAN
- Porte VIP (Virtual IP)

A partire da ONTAP 9.5, le LIF VIP sono supportate e sono ospitate su porte VIP.

Durante la configurazione di protocolli SAN come FC su un LIF, questo verrà associato a un WWPN.

["Amministrazione SAN"](#)

La seguente figura illustra la gerarchia di porte in un sistema ONTAP:



#### Failover e sconto della LIF

Un failover LIF si verifica quando una LIF passa dal nodo home o dalla porta al nodo partner ha o alla porta. Il failover di una LIF può essere attivato automaticamente da ONTAP o manualmente dall'amministratore del cluster per determinati eventi, come un collegamento Ethernet fisico inattivo o un nodo che abbandona il quorum del database replicato (RDB). Quando si verifica un failover della LIF, ONTAP continua a lavorare normalmente sul nodo partner fino alla risoluzione della causa del failover. Quando il nodo home o la porta torna in salute, la LIF viene riportata dal partner di ha al nodo home o alla porta. Questa inversione è chiamata sconto.

Per il failover e il giveback della LIF, le porte di ciascun nodo devono appartenere allo stesso dominio di broadcast. Per verificare che le porte rilevanti su ciascun nodo appartengano allo stesso dominio di broadcast, vedere quanto segue:

- ONTAP 9,8 e versioni successive: ["Riparare la raggiungibilità delle porte"](#)
- ONTAP 9.7 e versioni precedenti: ["Aggiungere o rimuovere porte da un dominio di broadcast"](#)

Per le LIF con failover LIF abilitato (automaticamente o manualmente) si applica quanto segue:

- Per le LIF che utilizzano una policy di servizio dati, puoi controllare le restrizioni delle policy di failover:
  - ONTAP 9,6 e versioni successive: ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#)
  - ONTAP 9,5 e versioni precedenti: ["Ruoli LIF in ONTAP 9.5 e versioni precedenti"](#)
- L'autorevert dei LIF avviene quando l'autorevert è impostato su `true` E quando la porta home della LIF è in buone condizioni e in grado di ospitare la LIF.
- In un takeover pianificato o non pianificato del nodo, la LIF sul nodo preso in consegna, esegue il failover nel partner di ha. La porta su cui si verifica il failover di LIF è determinata da VIF Manager.
- Una volta completato il failover, la LIF funziona normalmente.
- Al momento di eseguire un giveback, la LIF torna al nodo home e alla porta, se l'opzione di indirizzamento automatico è impostata su `true`.
- Quando un collegamento ethernet si interrompe su una porta che ospita una o più LIF, VIF Manager esegue la migrazione delle LIF dalla porta inattiva a una porta diversa nello stesso dominio di trasmissione. La nuova porta potrebbe trovarsi nello stesso nodo o nel suo partner ha. Dopo il ripristino del collegamento e se l'opzione di ripristino automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.
- Quando un nodo abbandona il quorum del database replicato (RDB), il VIF Manager migra le LIF dal nodo fuori quorum al partner ha. Dopo che il nodo torna al quorum e se l'opzione di revert automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.

### Compatibilità LIF con i tipi di porta

Le LIF possono avere caratteristiche diverse per supportare diversi tipi di porta.



Quando le LIF di intercluster e di gestione sono configurate nella stessa subnet, il traffico di gestione potrebbe essere bloccato da un firewall esterno e le connessioni AutoSupport e NTP potrebbero non funzionare. È possibile ripristinare il sistema eseguendo `network interface modify -vserver vservice name -lif intercluster LIF -status-admin up|down` Comando per attivare/disattivare la LIF dell'intercluster. Tuttavia, è necessario impostare la LIF di intercluster e la LIF di gestione in diverse subnet per evitare questo problema.

LIF	Descrizione
LIF dati	LIF associata a una macchina virtuale di storage (SVM) e utilizzata per comunicare con i client. Su una porta è possibile disporre di più LIF di dati. Queste interfacce possono migrare o eseguire il failover in tutto il cluster. È possibile modificare una LIF dei dati per fungere da LIF di gestione SVM modificando la relativa policy firewall in mgmt. Le sessioni stabilite per i server NIS, LDAP, Active Directory, WINS e DNS utilizzano le LIF dei dati.

LIF del cluster	LIF utilizzata per trasportare il traffico intracluster tra i nodi di un cluster. Le LIF del cluster devono sempre essere create sulle porte del cluster. Le LIF del cluster possono eseguire il failover tra le porte del cluster sullo stesso nodo, ma non possono essere migrate o sottoposte a failover su un nodo remoto. Quando un nuovo nodo si unisce a un cluster, gli indirizzi IP vengono generati automaticamente. Tuttavia, se si desidera assegnare manualmente gli indirizzi IP alle LIF del cluster, è necessario assicurarsi che i nuovi indirizzi IP si trovino nello stesso intervallo di subnet delle LIF del cluster esistenti.
LIF gestione cluster	LIF che fornisce un'unica interfaccia di gestione per l'intero cluster. Una LIF di gestione del cluster può eseguire il failover su qualsiasi nodo del cluster. Non è possibile eseguire il failover sulle porte del cluster o dell'intercluster
LIF intercluster	Una LIF utilizzata per la comunicazione tra cluster, il backup e la replica. È necessario creare una LIF intercluster su ciascun nodo del cluster prima di stabilire una relazione di peering del cluster. Queste LIF possono eseguire il failover solo sulle porte dello stesso nodo. Non è possibile eseguire la migrazione o il failover su un altro nodo del cluster.
LIF di gestione dei nodi	LIF che fornisce un indirizzo IP dedicato per la gestione di un nodo specifico in un cluster. Le LIF di gestione dei nodi vengono create al momento della creazione o dell'adesione al cluster. Queste LIF vengono utilizzate per la manutenzione del sistema, ad esempio quando un nodo diventa inaccessibile dal cluster.
LIF. VIP	Per LIF VIP si intende qualsiasi LIF di dati creata su una porta VIP. Per ulteriori informazioni, vedere <a href="#">"Configurare i LIF VIP (Virtual IP)"</a> .

### LIF e policy di servizio (ONTAP 9,6 e versioni successive)

È possibile assegnare policy di servizio (invece di ruoli LIF o policy firewall) alle LIF che determinano il tipo di traffico supportato per le LIF. Le policy di servizio definiscono una raccolta di servizi di rete supportati da una LIF. ONTAP offre una serie di policy di servizio integrate che possono essere associate a una LIF.

È possibile visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

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

Le funzioni non associate a un servizio specifico utilizzeranno un comportamento definito dal sistema per selezionare le LIF per le connessioni in uscita.

### Policy di servizio per SVM di sistema

La SVM amministrativa e qualsiasi SVM di sistema contengono policy di servizio che possono essere utilizzate per le LIF in tale SVM, incluse le LIF di gestione e intercluster. Questi criteri vengono creati automaticamente dal sistema quando viene creato un IPspace.

Nella tabella seguente sono elencati i criteri integrati per i LIF nelle SVM di sistema a partire da ONTAP 9.12.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

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

Policy	Servizi inclusi	Ruolo equivalente	Descrizione
--------	-----------------	-------------------	-------------

intercluster predefinito	intercluster-core, management-https	intercluster	Utilizzato da LIF che trasportano traffico intercluster. Nota: Service Intercluster-core è disponibile da ONTAP 9.5 con il nome net-intercluster service policy.
default-route-announce	gestione-bgp	-	Utilizzato da LIF con connessioni peer BGP. Nota: Disponibile da ONTAP 9.5 con il nome net-route-announce service policy.
gestione predefinita	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt, o cluster-mgmt	Utilizzare questa policy di gestione con ambito di sistema per creare LIF di gestione con ambito di nodo e cluster di proprietà di una SVM di sistema. Queste LIF possono essere utilizzate per le connessioni in uscita verso server DNS, ad, LDAP o NIS, nonché per alcune connessioni aggiuntive per supportare le applicazioni eseguite per conto dell'intero sistema. A partire da ONTAP 9.12.1, è possibile utilizzare <code>management-log-forwarding</code> Servizio per controllare quali LIF vengono utilizzati per inoltrare i registri di audit a un server syslog remoto.

La seguente tabella elenca i servizi che i file LIF possono utilizzare su un SVM di sistema a partire da ONTAP 9.11.1:

Servizio	Limiti di failover	Descrizione
core intercluster	solo nodo principale	Servizi di intercluster principali
core di gestione	-	Servizi di gestione principali
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Servizi per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione: autosupport	-	Servizi relativi alla pubblicazione dei payload AutoSupport
gestione-bgp	solo porta home	Servizi correlati alle interazioni peer BGP
backup-ndmp-control	-	Servizi per i controlli di backup NDMP

gestione-ems	-	Servizi per l'accesso alla messaggistica di gestione
client ntp di gestione	-	Introdotta in ONTAP 9.10.1. Servizi per l'accesso al client NTP.
management-ntp-server	-	Introdotta in ONTAP 9.11.1. Servizi per l'accesso alla gestione del server NTP
gestione-portmap	-	Servizi per la gestione di portmap
management-rsh-server	-	Servizi per la gestione dei server rsh
server-snmp-di-gestione	-	Servizi per la gestione del server SNMP
management-telnet-server	-	Servizi per la gestione dei server telnet
management-log-forwarding	-	Introdotta in ONTAP 9.12.1. Servizi per l'inoltro dei log di controllo

#### Policy di servizio per SVM di dati

Tutti i dati SVM contengono policy di servizio che possono essere utilizzate dai LIF in tale SVM.

Nella tabella seguente sono elencati i criteri integrati per le LIF nelle SVM di dati a partire da ONTAP 9.11.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

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

Policy	Servizi inclusi	Protocollo dati equivalente	Descrizione
gestione predefinita	management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nessuno	Utilizza questa policy di gestione con ambito SVM per creare LIF di gestione SVM di proprietà di una SVM di dati. Queste LIF possono essere utilizzate per fornire l'accesso SSH o HTTPS agli amministratori di SVM. Se necessario, questi LIF possono essere utilizzati per le connessioni in uscita a server DNS, ad, LDAP o NIS esterni.
blocchi-di-dati-predefiniti	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati SAN orientato a blocchi. A partire da ONTAP 9.10.1, la policy "default-data-block" è obsoleta. Utilizzare invece la policy di servizio "default-data-iscsi".



default-data-files	data-fpolicy-client, data-dns-server, data-flexcache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Utilizzare il criterio default-data-files per creare LIF NAS che supportino protocolli di dati basati su file. A volte è presente un solo LIF nella SVM, pertanto questo criterio consente di utilizzare la LIF per le connessioni in uscita a un server DNS, ad, LDAP o NIS esterno. È possibile rimuovere questi servizi da questa policy se si preferisce che queste connessioni utilizzino solo LIF di gestione.
default-data-iscsi	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati iSCSI.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Utilizzato da LIF che trasportano traffico dati NVMe/TCP.

La tabella seguente elenca i servizi che possono essere utilizzati su una SVM di dati insieme alle eventuali restrizioni imposte da ciascun servizio alla policy di failover di una LIF a partire da ONTAP 9.11.1:

Servizio	Restrizioni di failover	Descrizione
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Introdotta nei servizi ONTAP 9.10.1 per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione-portmap	-	Servizi per l'accesso alla gestione di portmap
server-snmp-di-gestione	-	Introdotta nei servizi ONTAP 9.10.1 per l'accesso alla gestione del server SNMP
core di dati	-	Servizi dati principali
nfs dati	-	Servizio dati NFS
cifs dei dati	-	Servizio dati CIFS
data-flexcache	-	Servizio dati FlexCache
iscsi dati	solo porta home	Servizio dati iSCSI
backup-ndmp-control	-	Introdotta in ONTAP 9.10.1 Backup NDMP controlla il servizio dati

server-dns-dati	-	Introdotta nel servizio dati del server DNS di ONTAP 9.10.1
data-fpolicy-client	-	Servizio dati delle policy di screening dei file
data-nvme-tcp	solo porta home	Introdotta nel servizio dati TCP NVMe di ONTAP 9.10.1
data-s3-server	-	Servizio dati server Simple Storage Service (S3)

È necessario conoscere il modo in cui le policy di servizio vengono assegnate alle LIF nelle SVM di dati:

- Se viene creata una SVM dati con un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando i servizi specificati.
- Se viene creata una SVM dati senza specificare un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando un elenco predefinito di servizi dati.

L'elenco dei servizi dati predefiniti include i servizi iSCSI, NFS, NVMe, SMB e FlexCache.

- Quando si crea una LIF con un elenco di protocolli dati, una politica di servizio equivalente ai protocolli dati specificati viene assegnata alla LIF.
- Se non esiste una politica di servizio equivalente, viene creata una politica di servizio personalizzata.
- Quando si crea una LIF senza una policy di servizio o un elenco di protocolli dati, la policy di servizio default-data-files viene assegnata alla LIF per impostazione predefinita.

### Servizio data-core

Il servizio data-core consente ai componenti che in precedenza utilizzavano le LIF con il ruolo dati di funzionare come previsto sui cluster che sono stati aggiornati per gestire le LIF utilizzando le policy di servizio invece dei ruoli LIF (che sono deprecati in ONTAP 9.6).

La specifica del data-core come servizio non apre alcuna porta nel firewall, ma il servizio deve essere incluso in qualsiasi politica di servizio in una SVM dati. Ad esempio, per impostazione predefinita, la politica di servizio file di dati predefiniti contiene i seguenti servizi:

- core di dati
- nfs dati
- cifs dei dati
- data-flexcache

Il servizio data-core deve essere incluso nella policy per garantire che tutte le applicazioni che utilizzano LIF funzionino come previsto, ma gli altri tre servizi possono essere rimossi, se lo si desidera.

### Servizio LIF lato client

A partire da ONTAP 9.10.1, ONTAP offre servizi LIF lato client per più applicazioni. Questi servizi consentono di controllare quali LIF vengono utilizzati per le connessioni in uscita per conto di ciascuna applicazione.

I seguenti nuovi servizi consentono agli amministratori di controllare quali LIF vengono utilizzati come indirizzi

di origine per determinate applicazioni.

Servizio	Restrizioni SVM	Descrizione
management-ad-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client Active Directory per le connessioni in uscita a un server ad esterno.
client-dns-di-gestione	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client DNS per le connessioni in uscita a un server DNS esterno.
management-ldap-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client LDAP per le connessioni in uscita a un server LDAP esterno.
management-nis-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client NIS per le connessioni in uscita a un server NIS esterno.
client ntp di gestione	solo sistema	A partire da ONTAP 9.10.1, ONTAP fornisce il servizio client NTP per le connessioni in uscita a un server NTP esterno.
data-fpolicy-client	solo dati	A partire da ONTAP 9.8, ONTAP fornisce il servizio client per le connessioni FPolicy in uscita.

Ciascuno dei nuovi servizi viene incluso automaticamente in alcune policy di servizio integrate, ma gli amministratori possono rimuoverli dalle policy integrate o aggiungerli a policy personalizzate per controllare quali LIF vengono utilizzate per le connessioni in uscita per conto di ciascuna applicazione.

### Ruoli LIF (ONTAP 9,5 e versioni precedenti)

Le LIF con ruoli diversi hanno caratteristiche diverse. Un ruolo LIF determina il tipo di traffico supportato dall'interfaccia, insieme alle regole di failover applicabili, alle restrizioni firewall in vigore, alla sicurezza, al bilanciamento del carico e al comportamento di routing per ogni LIF. Una LIF può avere uno dei seguenti ruoli: Cluster, gestione del cluster, dati, intercluster, gestione dei nodi, e undef (non definito). Il ruolo undef viene utilizzato per i LIF BGP.

A partire da ONTAP 9.6, i ruoli LIF sono deprecati. È necessario specificare le policy di servizio per le LIF anziché un ruolo. Non è necessario specificare un ruolo LIF quando si crea una LIF con una politica di servizio.

### Sicurezza LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster

Richiedere una subnet IP privata?	No	Sì	No	No	No
Hai bisogno di una rete sicura?	No	Sì	No	No	Sì
Policy firewall predefinita	Molto restrittivo	Aprire completamente	Medio	Medio	Molto restrittivo
Il firewall è personalizzabile?	Sì	No	Sì	Sì	Sì

#### Failover LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Comportamento predefinito	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF e su un nodo partner non SFO	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF	Qualsiasi porta dello stesso gruppo di failover	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF
È personalizzabile?	Sì	No	Sì	Sì	Sì

#### Routing LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Quando è necessario un percorso predefinito?	Quando i client o i controller di dominio si trovano su una subnet IP diversa	Mai	Quando uno dei tipi di traffico primari richiede l'accesso a una subnet IP diversa	Quando l'amministratore si connette da un'altra subnet IP	Quando altre LIF intercluster si trovano su una subnet IP diversa
Quando è necessario un instradamento statico a una specifica subnet IP?	Raro	Mai	Raro	Raro	Quando i nodi di un altro cluster hanno le proprie LIF di intercluster in sottoreti IP diverse

Quando è necessario un percorso host statico verso un server specifico?	Per fare in modo che uno dei tipi di traffico sia elencato nella LIF di gestione dei nodi, eseguire una LIF di dati piuttosto che una LIF di gestione dei nodi. Ciò richiede una modifica del firewall corrispondente.	Mai	Raro	Raro	Raro
---	--	-----	------	------	------

#### Ribilanciamento LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
DNS: Utilizzare come server DNS?	Sì	No	No	No	No
DNS: Esportare come zona?	Sì	No	No	No	No

#### Tipi di traffico primari LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Tipi di traffico primari	Server NFS, server CIFS, client NIS, Active Directory, LDAP, WINS, client e server DNS, iSCSI e server FC	Intracluster	Server SSH, server HTTPS, client NTP, SNMP, client AutoSupport, Client DNS, caricamento aggiornamenti software	Server SSH, server HTTPS	Replica tra cluster

## Gestire le LIF

### Configurare le policy di servizio LIF

È possibile configurare le policy di servizio LIF per identificare un singolo servizio o un elenco di servizi che utilizzeranno una LIF.

#### Creare una politica di servizio per le LIF

È possibile creare una politica di servizio per le LIF. È possibile assegnare una policy di servizio a una o più

LIF, consentendo così al LIF di trasportare il traffico per un singolo servizio o un elenco di servizi.

Per eseguire, sono necessari privilegi avanzati `network interface service-policy create` comando.

### A proposito di questa attività

I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema. La maggior parte dei casi di utilizzo è soddisfatta utilizzando una politica di servizio integrata piuttosto che creare una politica di servizio personalizzata.

Se necessario, è possibile modificare queste policy di servizio incorporate.

### Fasi

1. Visualizzare i servizi disponibili nel cluster:

```
network interface service show
```

I servizi rappresentano le applicazioni a cui si accede da una LIF e le applicazioni servite dal cluster. Ogni servizio include zero o più porte TCP e UDP su cui l'applicazione è in ascolto.

Sono disponibili i seguenti servizi di gestione e dati aggiuntivi:

```
cluster1::> network interface service show

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

2. Visualizzare le policy di servizio esistenti nel cluster:

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

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0

```
7 entries were displayed.
```

### 3. Creare una politica di servizio:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

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

- "nome\_servizio" specifica un elenco di servizi da includere nella policy.
- "IP\_address/mask" specifica l'elenco di subnet mask per gli indirizzi ai quali è consentito l'accesso ai servizi nella politica di servizio. Per impostazione predefinita, tutti i servizi specificati vengono aggiunti con un elenco di indirizzi consentiti predefinito di 0.0.0.0/0, che consente il traffico da tutte le subnet. Quando viene fornito un elenco di indirizzi non predefinito, i file LIF che utilizzano il criterio sono configurati per bloccare tutte le richieste con un indirizzo di origine che non corrisponde a nessuna delle maschere specificate.

Nell'esempio seguente viene illustrato come creare una policy del servizio dati, *svm1\_data\_policy*, per una SVM che include i servizi *NFS* e *SMB*:

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

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

Nell'esempio seguente viene illustrato come creare una policy di servizio tra cluster:

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

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

#### 4. Verificare che la politica di servizio sia stata creata.

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

Il seguente output mostra le policy di servizio disponibili:



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

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	intercluster1	intercluster-core: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	svm1_data_policy	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0

```
9 entries were displayed.
```

### Al termine

Assegnare la politica di servizio a una LIF al momento della creazione o modificando una LIF esistente.

## Assegnare una politica di servizio a una LIF

È possibile assegnare una politica di servizio a una LIF al momento della creazione della LIF o modificando la LIF. Una politica di servizio definisce l'elenco dei servizi che possono essere utilizzati con LIF.

### A proposito di questa attività

È possibile assegnare le policy di servizio per le LIF nelle SVM di amministrazione e dati.

### Fase

A seconda del momento in cui si desidera assegnare la politica di servizio a una LIF, eseguire una delle seguenti operazioni:

Se sei...	Assegnare la politica di servizio...
Creazione di una LIF	Interfaccia di rete create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifica di una LIF	modifica interfaccia di rete -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

Quando si specifica una politica di servizio per una LIF, non è necessario specificare il protocollo dati e il ruolo per la LIF. È supportata anche la creazione di LIF specificando il ruolo e i protocolli dati.



Una politica di servizio può essere utilizzata solo dalle LIF nella stessa SVM specificata durante la creazione della politica di servizio.

### Esempi

Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF per utilizzare la politica di servizio di gestione predefinita:

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

### Comandi per la gestione delle policy di servizio LIF

Utilizzare `network interface service-policy` Comandi per gestire le policy di servizio LIF.

### Prima di iniziare

La modifica della policy di servizio di una LIF in una relazione di SnapMirror attiva interrompe il programma di replica. Se si converte una LIF da intercluster a non intercluster (o viceversa), le modifiche non verranno replicate nel cluster sottoposto a peering. Per aggiornare il cluster peer dopo aver modificato la policy di servizio LIF, eseguire prima l' `snapmirror abort` operazione quindi [risincronizzazione della relazione di replica](#).

Se si desidera...	Utilizzare questo comando...
Creazione di una politica di servizio (sono richiesti privilegi avanzati)	<code>network interface service-policy create</code>

Se si desidera...	Utilizzare questo comando...
Aggiunta di una voce di servizio aggiuntiva a una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy add-service</code>
Clonare una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy clone</code>
Modifica di una voce di servizio in una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy modify-service</code>
Rimozione di una voce di servizio da una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy remove-service</code>
Rinominare una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy rename</code>
Eliminazione di una policy di servizio esistente (privilegi avanzati richiesti)	<code>network interface service-policy delete</code>
Ripristinare una policy di servizio integrata al suo stato originale (sono richiesti privilegi avanzati)	<code>network interface service-policy restore-defaults</code>
Visualizzare le policy di servizio esistenti	<code>network interface service-policy show</code>

### Creazione di una LIF (interfaccia di rete)

Una SVM fornisce i dati ai client attraverso una o più interfacce logiche di rete (LIF). Per accedere ai dati, è necessario creare LIF sulle porte che si desidera utilizzare. Una LIF (interfaccia di rete) è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

#### Best practice

Le porte dello switch connesse a ONTAP devono essere configurate come porte edge spanning-tree per ridurre i ritardi durante la migrazione LIF.

#### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- La porta di rete fisica o logica sottostante deve essere stata configurata con lo stato di attivazione amministrativa.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando System Manager o `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

### A proposito di questa attività

- Non è possibile assegnare protocolli NAS e SAN allo stesso LIF.

I protocolli supportati sono SMB, NFS, FlexCache, iSCSI e FC; iSCSI e FC non possono essere combinati con altri protocolli. Tuttavia, i protocolli SAN basati su NAS ed Ethernet possono essere presenti sulla stessa porta fisica.

- Non si consiglia di configurare le LIF che trasportano il traffico SMB in modo da ripristinare automaticamente i propri nodi domestici. Questo suggerimento è obbligatorio se il server SMB deve ospitare una soluzione per operazioni senza interruzioni con Hyper-V o SQL Server su SMB.
- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Tutti i servizi di mappatura dei nomi e risoluzione dei nomi host utilizzati da una SVM, come DNS, NIS, LDAP e Active Directory, Deve essere raggiungibile da almeno un LIF che gestisce il traffico dati della SVM.
- Una LIF che gestisce il traffico intracluster tra i nodi non deve trovarsi sulla stessa subnet di una LIF che gestisce il traffico di gestione o di una LIF che gestisce il traffico di dati.
- La creazione di una LIF che non dispone di una destinazione di failover valida genera un messaggio di avviso.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster:
  - System Manager: A partire da ONTAP 9.12.0, visualizzare il throughput nella griglia dell'interfaccia di rete.
  - CLI: Utilizzare `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

A partire da ONTAP 9.4, FC-NVMe è supportato. Se si sta creando una LIF FC-NVMe, tenere presente quanto segue:

- Il protocollo NVMe deve essere supportato dall'adattatore FC su cui viene creato il LIF.
- FC-NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare un LIF che gestisca il traffico di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.
- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- È possibile configurare un solo NVMe LIF che gestisce il traffico dati per SVM.
- Quando si crea un'interfaccia di rete con una subnet, ONTAP seleziona automaticamente un indirizzo IP disponibile dalla subnet selezionata e lo assegna all'interfaccia di rete. È possibile modificare la subnet se sono presenti più subnet, ma non è possibile modificare l'indirizzo IP.
- Quando si crea (aggiunge) una SVM per un'interfaccia di rete, non è possibile specificare un indirizzo IP compreso nell'intervallo di una subnet esistente. Viene visualizzato un errore di conflitto di subnet. Questo problema si verifica in altri flussi di lavoro per un'interfaccia di rete, come la creazione o la modifica di interfacce di rete tra cluster nelle impostazioni SVM o nelle impostazioni del cluster.

- A partire da ONTAP 9.10.1, la `network interface` I comandi CLI includono un `-rdma-protocols` Parametro per configurazioni NFS su RDMA. La creazione di interfacce di rete per configurazioni NFS su RDMA è supportata in Gestione sistemi a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere [Configurare LIFS per NFS su RDMA](#).
- A partire da ONTAP 9.11.1, il failover automatico iSCSI LIF è disponibile nelle piattaforme ASA (All-Flash SAN Array).

Il failover LIF iSCSI viene attivato automaticamente (il criterio di failover è impostato su `sfo-partner-only` e il valore di autorevert è impostato su `true`) Sulle LIF iSCSI appena create se non esistono LIF iSCSI nella SVM specificata o se tutte le LIF iSCSI esistenti nella SVM specificata sono già abilitate con il failover LIF iSCSI.

Se dopo aver eseguito l'aggiornamento a ONTAP 9.11.1 o versioni successive si dispone di LIF iSCSI esistenti in una SVM che non sono state abilitate con la funzione di failover LIF iSCSI e si creano nuove LIF iSCSI nella stessa SVM, le nuove LIF iSCSI assumono la stessa policy di failover (`disabled`) Delle LIF iSCSI esistenti in SVM.

#### ["Failover LIF iSCSI per piattaforme ASA"](#)

A partire da ONTAP 9.7, ONTAP sceglie automaticamente la porta home di un LIF, purché almeno un LIF esista già nella stessa sottorete di tale LIF. ONTAP sceglie una porta home nello stesso dominio di broadcast delle altre LIF della subnet. È comunque possibile specificare una porta home, ma non è più necessaria (a meno che non esistano file LIF in tale subnet nell'IPSpace specificato).

A partire da ONTAP 9.12.0, la procedura da seguire dipende dall'interfaccia in uso: Gestore di sistema o CLI:

## System Manager

### Utilizzare System Manager per aggiungere un'interfaccia di rete

#### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **+ Add**.
3. Selezionare uno dei seguenti ruoli di interfaccia:
  - a. Dati
  - b. Intercluster
  - c. Gestione SVM
4. Selezionare il protocollo:
  - a. SMB/CIFS E NFS
  - b. ISCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/TCP
5. Assegnare un nome al LIF o accettare il nome generato dalle selezioni precedenti.
6. Accettare il nodo home o utilizzare il menu a discesa per selezionarlo.
7. Se almeno una subnet è configurata nell'IPSpace dell'SVM selezionato, viene visualizzato il menu a discesa Subnet (sottorete).
  - a. Se si seleziona una subnet, selezionarla dall'elenco a discesa.
  - b. Se si procede senza una subnet, viene visualizzato il menu a discesa del dominio di trasmissione:
    - i. Specificare l'indirizzo IP. Se l'indirizzo IP è in uso, viene visualizzato un messaggio di avviso.
    - ii. Specificare una subnet mask.
8. Selezionare la porta home dal dominio di trasmissione, automaticamente (scelta consigliata) o selezionandola dal menu a discesa. Il controllo della porta Home viene visualizzato in base al dominio di trasmissione o alla selezione della subnet.
9. Salvare l'interfaccia di rete.

#### CLI

### Utilizzare la CLI per creare una LIF

#### Fasi

1. Determinare quali porte del dominio di trasmissione si desidera utilizzare per la LIF.

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

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

2. Verificare che la subnet che si desidera utilizzare per i file LIF contenga un numero sufficiente di indirizzi IP inutilizzati.

```
network subnet show -ipspace ipspace1
```

3. Creare una o più LIF sulle porte che si desidera utilizzare per accedere ai dati.

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

- **-home-node** È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

Puoi anche specificare se LIF deve ripristinare automaticamente il nodo home e la porta home con l'opzione `-auto-revert`.

- **-home-port** È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. La pagina [network route create](#) man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- **-auto-revert** Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `true` in base alle policy di gestione della rete nel proprio ambiente.
- **-service-policy** A partire da ONTAP 9.5, è possibile assegnare una politica di servizio per la LIF con `-service-policy` opzione. Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di

protocolli dati per la LIF. In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.

- ° -data-protocol Consente di creare una LIF che supporti i protocolli FCP o NVMe/FC. Questa opzione non è necessaria quando si crea un LIF IP.

4. **Opzionale:** Assegnare un indirizzo IPv6 nell'opzione -address:

- Utilizzare il comando `network ndp prefix show` per visualizzare l'elenco dei prefissi RA appresi sulle varie interfacce.

Il `network ndp prefix show` il comando è disponibile a livello di privilegio avanzato.

- Utilizzare il formato `prefix::id` Per costruire manualmente l'indirizzo IPv6.

`prefix` è il prefisso appreso sulle varie interfacce.

Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

5. Verificare che la configurazione dell'interfaccia LIF sia corretta.

```
network interface show -vserver vs1
```

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

6. Verificare che la configurazione del gruppo di failover sia quella desiderata.

```
network interface show -failover -vserver vs1
```

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

7. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	ping di rete



## Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

Il seguente comando crea una LIF NVMe/FC e specifica `nvme-fc` protocollo dati:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## Modificare una LIF

È possibile modificare una LIF modificando gli attributi, ad esempio il nodo principale o il nodo corrente, lo stato amministrativo, l'indirizzo IP, la netmask, la policy di failover, policy firewall e policy di servizio. È inoltre possibile modificare la famiglia di indirizzi di una LIF da IPv4 a IPv6.

### A proposito di questa attività

- Quando si modifica lo stato amministrativo di una LIF su inattivo, i blocchi NFSv4 in sospeso vengono mantenuti fino a quando lo stato amministrativo della LIF non viene riportato su UP.

Per evitare conflitti di blocco che possono verificarsi quando altri LIF tentano di accedere ai file bloccati, è necessario spostare i client NFSv4 su un LIF diverso prima di impostare lo stato amministrativo su inattivo.

- Non è possibile modificare i protocolli dati utilizzati da un FC LIF. Tuttavia, è possibile modificare i servizi assegnati a una politica di servizio o la politica di servizio assegnata a una LIF IP.

Per modificare i protocolli dati utilizzati da un LIF FC, è necessario eliminare e ricreare il LIF. Per apportare modifiche alla politica di servizio di un LIF IP, si verifica una breve interruzione durante l'esecuzione degli aggiornamenti.

- Non è possibile modificare il nodo principale o il nodo corrente di una LIF di gestione con ambito di nodo.

- Quando si utilizza una subnet per modificare l'indirizzo IP e il valore della maschera di rete per una LIF, viene assegnato un indirizzo IP dalla subnet specificata; se l'indirizzo IP precedente della LIF proviene da una subnet diversa, l'indirizzo IP viene restituito a tale subnet.
- Per modificare la famiglia di indirizzi di una LIF da IPv4 a IPv6, è necessario utilizzare la notazione con i due punti per l'indirizzo IPv6 e aggiungere un nuovo valore per `-netmask-length` parametro.
- Non è possibile modificare gli indirizzi IPv6 link-local configurati automaticamente.
- La modifica di una LIF che non ha una destinazione di failover valida per la LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

- A partire da ONTAP 9.5, è possibile modificare la politica di servizio associata a una LIF.

In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.

- A partire da ONTAP 9.11.1, il failover automatico di LIF iSCSI è disponibile sulle piattaforme ASA (All-Flash SAN Array).

Per le LIF iSCSI pre-esistenti, ovvero le LIF create prima dell'upgrade alla versione 9.11.1 o successiva, è possibile modificare il criterio di failover in ["Attiva il failover automatico della LIF iSCSI"](#).

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

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per modificare un'interfaccia di rete

### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **> Modifica** accanto all'interfaccia di rete che si desidera modificare.
3. Modificare una o più impostazioni dell'interfaccia di rete. Per ulteriori informazioni, vedere ["Creare una LIF"](#).
4. Salvare le modifiche.

### CLI

#### Utilizzare la CLI per modificare una LIF

### Fasi

1. Modificare gli attributi di una LIF utilizzando `network interface modify` comando.

Nell'esempio seguente viene illustrato come modificare l'indirizzo IP e la maschera di rete dei dati LIF 2 utilizzando un indirizzo IP e il valore della maschera di rete della subnet client1\_sub:

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

2. Verificare che gli indirizzi IP siano raggiungibili.

Se si utilizza...	Quindi utilizzare...
Indirizzi IPv4	<code>network ping</code>
Indirizzi IPv6	<code>network ping6</code>

## Migrare una LIF

Potrebbe essere necessario migrare un LIF a una porta diversa sullo stesso nodo o su un nodo diverso all'interno del cluster, se la porta è guasta o richiede manutenzione. La migrazione di un LIF è simile al failover LIF, ma la migrazione LIF è un'operazione manuale, mentre il failover LIF è la migrazione automatica di un LIF in risposta a un errore di collegamento sulla porta di rete corrente del LIF.

## Prima di iniziare

- È necessario che sia stato configurato un gruppo di failover per le LIF.
- Il nodo di destinazione e le porte devono essere operativi e devono poter accedere alla stessa rete della porta di origine.

## A proposito di questa attività

- I LIF BGP risiedono sulla porta home e non possono essere migrati su altri nodi o porte.
- Prima di rimuovere la scheda NIC dal nodo, è necessario migrare i file LIF ospitati sulle porte appartenenti a una scheda NIC in altre porte del cluster.
- È necessario eseguire il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.
- Una LIF con ambito di nodo, come LIF di gestione con ambito di nodo, LIF di cluster, LIF di intercluster, non può essere migrata a un nodo remoto.
- Quando si esegue la migrazione di un LIF NFSv4 tra nodi, si verifica un ritardo fino a 45 secondi prima che il LIF sia disponibile su una nuova porta.

Per risolvere questo problema, utilizzare NFSv4.1 dove non si verificano ritardi.

- Puoi migrare LIF iSCSI su piattaforme ASA (All-Flash SAN Array) che eseguono ONTAP 9.11.1 o versioni successive.

La migrazione delle LIF iSCSI è limitata alle porte sul nodo principale o sul partner ha.

- Se la tua piattaforma non è una piattaforma ASA (All-Flash SAN Array) che esegue ONTAP versione 9.11.1 o successiva, non puoi migrare le LIF iSCSI da un nodo a un altro nodo.

Per aggirare questa restrizione, è necessario creare una LIF iSCSI sul nodo di destinazione. Scopri di più ["Creazione di LIF iSCSI"](#).

- Se si desidera migrare una LIF (interfaccia di rete) per NFS su RDMA, assicurarsi che la porta di destinazione sia compatibile con RoCE. È necessario eseguire ONTAP 9.10.1 o versione successiva per migrare un file LIF con l'interfaccia CLI o ONTAP 9.12.1 per eseguire la migrazione utilizzando Gestione sistema. In System Manager, una volta selezionata la porta di destinazione compatibile con RoCE, selezionare la casella di controllo accanto a **Usa porte RoCE** per completare correttamente la migrazione. Scopri di più ["Configurazione di LIF per NFS su RDMA"](#).
- Le operazioni di offload delle copie VMware VAAI non vengono eseguite quando si esegue la migrazione della LIF di origine o di destinazione. Informazioni sulla funzione di off-load delle copie:
  - ["Ambienti NFS"](#)
  - ["Ambienti SAN"](#)

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

## System Manager

### Utilizzare System Manager per migrare un'interfaccia di rete

#### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **⋮ > Migrate** accanto all'interfaccia di rete che si desidera modificare.



Per una LIF iSCSI, nella finestra di dialogo **Migrate Interface**, selezionare il nodo di destinazione e la porta del partner ha.

Se vuoi migrare la LIF iSCSI in modo permanente, seleziona la casella di controllo. La LIF iSCSI deve essere offline prima di poter essere migrata in modo permanente. Inoltre, una volta migrata in modo permanente, una LIF iSCSI non può essere annullata. Non esiste alcuna opzione di revert.

3. Fare clic su **Migra**.
4. Salvare le modifiche.

#### CLI

### Utilizzare la CLI per migrare una LIF

#### Fase

A seconda che si desideri migrare una LIF specifica o tutte le LIF, eseguire l'azione appropriata:

Se si desidera eseguire la migrazione...	Immettere il seguente comando...
Una LIF specifica	<code>network interface migrate</code>
Tutte le LIF di gestione dei dati e dei cluster su un nodo	<code>network interface migrate-all</code>
Tutte le LIF di una porta	<code>network interface migrate-all -node &lt;node&gt; -port &lt;port&gt;</code>

Nell'esempio seguente viene illustrato come migrare un LIF denominato `datalif1` Su SVM `vs0` alla porta `e0d` acceso `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b  
-dest-port e0d
```

Nell'esempio seguente viene illustrato come migrare tutti i dati e le LIF di gestione del cluster dal nodo (locale) corrente:

```
network interface migrate-all -node local
```

**Ripristinare la porta home di un LIF**

È possibile ripristinare la porta home di un LIF dopo il failover o la migrazione a una porta diversa manualmente o automaticamente. Se la porta home di un LIF specifico non è disponibile, LIF rimane sulla porta corrente e non viene ripristinata.

**A proposito di questa attività**


- Se si porta la porta home di un LIF in stato attivo prima di impostare l'opzione di revert automatico, il LIF non viene restituito alla porta home.
- Il LIF non viene ripristinato automaticamente a meno che il valore dell'opzione "auto-revert" non sia impostato su true.
- È necessario assicurarsi che l'opzione "auto-revert" (indirizzamento automatico) sia attivata per ripristinare le porte home dei file LIF.

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

**System Manager**

**Utilizzare System Manager per ripristinare un'interfaccia di rete alla porta home**

**Fasi**

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare  **> Ripristina** accanto all'interfaccia di rete che si desidera modificare.
3. Selezionare **Ripristina** per ripristinare un'interfaccia di rete alla porta home.

**CLI**

**Utilizzare l'interfaccia CLI per ripristinare la porta LIF home**

**Fase**

Ripristinare manualmente o automaticamente la porta home di un LIF:

Se si desidera ripristinare la porta home di un LIF...	Quindi immettere il seguente comando...
Manualmente	<code>network interface revert -vserver vservice_name -lif lif_name</code>
Automaticamente	<code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code>

**ONTAP 9.8 e versioni successive: Ripristino da una LIF del cluster configurata in modo errato**

Non è possibile creare un cluster quando la rete del cluster è cablata a uno switch, ma non tutte le porte configurate in Cluster IPspace possono raggiungere le altre porte configurate in Cluster IPspace.

**A proposito di questa attività**

In un cluster con switch, se un'interfaccia di rete del cluster (LIF) è configurata sulla porta errata o se una porta del cluster è collegata alla rete errata, il `cluster create` il comando può non riuscire e visualizzare il seguente errore:

```
Not all local cluster ports have reachability to one another.  
Use the "network port reachability show -detail" command for more details.
```

I risultati di `network port show` Il comando potrebbe indicare che diverse porte vengono aggiunte a Cluster IPspace perché sono connesse a una porta configurata con una LIF del cluster. Tuttavia, i risultati di `network port reachability show -detail` il comando rivela quali porte non dispongono di connettività l'una con l'altra.

Per eseguire il ripristino da una LIF del cluster configurata su una porta non raggiungibile con le altre porte configurate con le LIF del cluster, attenersi alla seguente procedura:

#### Fasi

1. Ripristinare la porta home del LIF del cluster alla porta corretta:

```
network port modify -home-port
```

2. Rimuovere dal dominio di trasmissione del cluster le porte che non hanno LIF del cluster configurate:

```
network port broadcast-domain remove-ports
```

3. Creare il cluster:

```
cluster create
```

#### Risultato

Una volta completata la creazione del cluster, il sistema rileva la configurazione corretta e inserisce le porte nei domini di trasmissione corretti.

#### Eliminare una LIF

È possibile eliminare un'interfaccia di rete (LIF) non più richiesta.

#### Prima di iniziare

I LIF da eliminare non devono essere in uso.

#### Fasi

1. Contrassegnare i file LIF che si desidera eliminare come amministrativamente bassi utilizzando il seguente comando:

```
network interface modify -vserver vservice_name -lif lif_name -status  
-admin down
```

2. Utilizzare `network interface delete` Comando per eliminare una o tutte le LIF:

Se si desidera eliminare...	Immettere il comando ...
Una LIF specifica	<code>network interface delete -vserver vs1 -lif lif_name</code>
Tutte le LIF	<code>network interface delete -vserver vs1 -lif *</code>

Il seguente comando elimina LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilizzare `network interface show` Comando per confermare che la LIF è stata eliminata.

## Bilanciamento dei carichi di rete

### Panoramica della rete Balance

È possibile configurare il cluster per soddisfare le richieste dei client da LIF caricate in modo appropriato. Ciò comporta un utilizzo più bilanciato di LIF e porte, che a sua volta consente migliori performance del cluster.

Il bilanciamento del carico DNS consente di selezionare una LIF di dati opportunamente caricata e di bilanciare il traffico di rete dell'utente su tutte le porte disponibili (fisiche, gruppi di interfacce e VLAN).

Con il bilanciamento del carico DNS, i LIF sono associati alla zona di bilanciamento del carico di una SVM. Un server DNS a livello di sito è configurato per inoltrare tutte le richieste DNS e restituire il LIF meno caricato in base al traffico di rete e alla disponibilità delle risorse delle porte (utilizzo della CPU, throughput, connessioni aperte e così via). Il bilanciamento del carico DNS offre i seguenti vantaggi:

- Nuove connessioni client bilanciate tra le risorse disponibili.
- Non è richiesto alcun intervento manuale per decidere quali LIF utilizzare durante il montaggio di una specifica SVM.
- Il bilanciamento del carico DNS supporta NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 e S3.

### Come funziona il bilanciamento del carico DNS

I client montano una SVM specificando un indirizzo IP (associato a una LIF) o un nome host (associato a più indirizzi IP). Per impostazione predefinita, i LIF vengono selezionati dal server DNS a livello di sito in modo round-robin, che bilancia il carico di lavoro in tutte le LIF.

Il bilanciamento del carico round-robin può comportare l'overload di alcune LIF, pertanto è possibile utilizzare una zona di bilanciamento del carico DNS che gestisce la risoluzione del nome host in una SVM. L'utilizzo di una zona di bilanciamento del carico DNS garantisce un migliore bilanciamento delle nuove connessioni client tra le risorse disponibili, migliorando le performance del cluster.

Una zona di bilanciamento del carico DNS è un server DNS all'interno del cluster che valuta dinamicamente il



carico su tutte le LIF e restituisce una LIF caricata correttamente. In una zona di bilanciamento del carico, DNS assegna un peso (metrico), in base al carico, a ciascun LIF.

A ogni LIF viene assegnato un peso in base al carico della porta e all'utilizzo della CPU del nodo principale. Le LIF che si trovano su porte meno caricate hanno una maggiore probabilità di essere restituite in una query DNS. I pesi possono anche essere assegnati manualmente.

## Creare una zona di bilanciamento del carico DNS

È possibile creare una zona di bilanciamento del carico DNS per facilitare la selezione dinamica di una LIF in base al carico, ovvero al numero di client montati su una LIF. È possibile creare una zona di bilanciamento del carico durante la creazione di una LIF dati.

### Prima di iniziare

Il server di inoltro DNS sul server DNS del sito deve essere configurato per inoltrare tutte le richieste per la zona di bilanciamento del carico ai file LIF configurati.

L'articolo della Knowledge base ["Come impostare il bilanciamento del carico DNS in Cluster-Mode"](#) Sul sito del supporto NetApp sono disponibili ulteriori informazioni sulla configurazione del bilanciamento del carico DNS mediante l'inoltro condizionale.

### A proposito di questa attività

- Qualsiasi LIF di dati può rispondere alle query DNS per un nome di zona per il bilanciamento del carico DNS.
- Una zona di bilanciamento del carico DNS deve avere un nome univoco nel cluster e il nome della zona deve soddisfare i seguenti requisiti:
  - Non deve superare i 256 caratteri.
  - Deve includere almeno un periodo.
  - Il primo e l'ultimo carattere non devono essere un punto o altri caratteri speciali.
  - Non può includere spazi tra caratteri.
  - Ogni etichetta nel nome DNS non deve superare i 63 caratteri.

Un'etichetta è il testo che compare prima o dopo il periodo. Ad esempio, la zona DNS denominata storage.company.com ha tre etichette.

### Fase

Utilizzare `network interface create` con il `dns-zone` Opzione per creare una zona di bilanciamento del carico DNS.

Se la zona di bilanciamento del carico esiste già, la LIF viene aggiunta ad essa. Per ulteriori informazioni sul comando, vedere ["Comandi di ONTAP 9"](#).

Nell'esempio riportato di seguito viene illustrato come creare una zona di bilanciamento del carico DNS denominata storage.company.com durante la creazione della LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

## Aggiungere o rimuovere una LIF da una zona di bilanciamento del carico

È possibile aggiungere o rimuovere una LIF dalla zona di bilanciamento del carico DNS di una macchina virtuale (SVM). È inoltre possibile rimuovere tutti i file LIF contemporaneamente da una zona di bilanciamento del carico.

### Prima di iniziare

- Tutte le LIF in una zona di bilanciamento del carico devono appartenere alla stessa SVM.
- Una LIF può far parte di una sola zona di bilanciamento del carico DNS.
- Se le LIF appartengono a sottoreti diverse, devono essere stati impostati gruppi di failover per ciascuna sottorete.

### A proposito di questa attività

Una LIF che si trova nello stato di inattività amministrativa viene temporaneamente rimossa dalla zona di bilanciamento del carico DNS. Quando la LIF ritorna allo stato di amministrazione attiva, la LIF viene aggiunta automaticamente alla zona di bilanciamento del carico DNS.

### Fase

Aggiungere o rimuovere una LIF da una zona di bilanciamento del carico:

Se si desidera...	Inserisci...
Aggiungere una LIF	<code>network interface modify -vserver vs1 -lif lif1 -dns-zone zone1</code> Esempio: <code>`network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com`</code>
Rimuovere una singola LIF	<code>network interface modify -vserver vs1 -lif lif1 -dns-zone none</code> Esempio: <code>`network interface modify -vserver vs1 -lif data1 -dns-zone none`</code>
Rimuovere tutti i LIF	<code>`network interface modify -vserver vs1 -lif * -dns-zone none`</code> Esempio: <code>`network interface modify -vserver vs0 -lif * -dns-zone none`</code> È possibile rimuovere una SVM da una zona di bilanciamento del carico rimuovendo tutte le LIF presenti nella SVM da tale zona.

## Configurazione dei servizi DNS (ONTAP 9,8 e versioni successive)

È necessario configurare i servizi DNS per SVM prima di creare un server NFS o SMB. In genere, i server dei nomi DNS sono i server DNS integrati in Active Directory per il dominio a cui si aggiungerà il server NFS o SMB.

## A proposito di questa attività

I server DNS integrati in Active Directory contengono i record di posizione del servizio (SRV) per i server LDAP e dei controller di dominio. Se SVM non riesce a trovare i server LDAP e i controller di dominio di Active Directory, la configurazione del server NFS o SMB non riesce.

Le SVM utilizzano il database ns-switch dei servizi dei nomi host per determinare i servizi dei nomi da utilizzare e in quale ordine quando si cercano informazioni sugli host. I due name service supportati per il database host sono file e dns.

Prima di creare il server SMB, è necessario assicurarsi che il dns sia una delle origini.



Per visualizzare le statistiche per i servizi dei nomi DNS per il processo mgwd e il processo SecD, utilizzare l'interfaccia utente Statistics.

## Fasi

1. Determinare la configurazione corrente per il database dei servizi di nomi host. In questo esempio, il database del servizio nomi host utilizza le impostazioni predefinite.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Eseguire le seguenti operazioni, se necessario.

- a. Aggiungere il servizio nome DNS al database del servizio nome host nell'ordine desiderato oppure riordinare le origini.

In questo esempio, il database degli host è configurato per l'utilizzo di DNS e file locali in tale ordine.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verificare che la configurazione dei name service sia corretta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configurare i servizi DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



Il comando di creazione dns dei servizi vserver esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

4. Verificare che la configurazione DNS sia corretta e che il servizio sia attivato.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Convalidare lo stato dei server dei nomi.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configurare il DNS dinamico sulla SVM

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.

### Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

### A proposito di questa attività

Il nome di dominio completo (FQDN) specificato deve essere univoco:

Il nome di dominio completo (FQDN) specificato deve essere univoco:

- Per NFS, il valore specificato in `-vserver-fqdn` come parte di `vserver services name-service dns dynamic-update` Command diventa il nome FQDN registrato per i LIF.
- Per SMB, i valori specificati come nome NetBIOS del server CIFS e nome di dominio completo del server CIFS diventano FQDN registrato per i LIF. Non è configurabile in ONTAP. Nel seguente scenario, l'FQDN LIF è "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC. Per ulteriori informazioni, vedere ["RFC 1123"](#).

## Fasi

### 1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

### 2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Configurazione dei servizi DNS (ONTAP 9,7 e versioni precedenti)

È necessario configurare i servizi DNS per SVM prima di creare un server NFS o SMB. In genere, i server dei nomi DNS sono i server DNS integrati in Active Directory per il dominio a cui si aggiungerà il server NFS o SMB.

## A proposito di questa attività

I server DNS integrati in Active Directory contengono i record di posizione del servizio (SRV) per i server LDAP e dei controller di dominio. Se SVM non riesce a trovare i server LDAP e i controller di dominio di Active Directory, la configurazione del server NFS o SMB non riesce.

Le SVM utilizzano il database ns-switch dei servizi dei nomi host per determinare i servizi dei nomi da utilizzare e in quale ordine quando si cercano informazioni sugli host. I due name service supportati per il database host sono `files` e `dns`.

È necessario assicurarsi che `dns` È una delle origini prima di creare il server SMB.



Per visualizzare le statistiche per i servizi dei nomi DNS per il processo `mgwd` e il processo `SecD`, utilizzare l'interfaccia utente `Statistics`.

## Fasi

1. Determinare la configurazione corrente per `hosts` database name services.

In questo esempio, il database del servizio nomi host utilizza le impostazioni predefinite.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Eseguire le seguenti operazioni, se necessario.

- a. Aggiungere il servizio nome DNS al database del servizio nome host nell'ordine desiderato oppure riordinare le origini.

In questo esempio, il database degli host è configurato per l'utilizzo di DNS e file locali in tale ordine.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- a. Verificare che la configurazione dei name service sia corretta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configurare i servizi DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



I servizi `vserver name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

4. Verificare che la configurazione DNS sia corretta e che il servizio sia attivato.

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

##### 5. Convalidare lo stato dei server dei nomi.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configurare il DNS dinamico sulla SVM

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.

### Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

### A proposito di questa attività

Il nome di dominio completo (FQDN) specificato deve essere univoco:

- Per NFS, il valore specificato in `-vserver-fqdn` come parte di `vserver services name-service dns dynamic-update` Command diventa il nome FQDN registrato per i LIF.
- Per SMB, i valori specificati come nome NetBIOS del server CIFS e nome di dominio completo del server CIFS diventano FQDN registrato per i LIF. Non è configurabile in ONTAP. Nel seguente scenario, l'FQDN LIF è "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC. Per ulteriori informazioni, vedere ["RFC 1123"](#).

## Fasi

### 1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

### 2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Configurare i servizi DNS dinamici

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.



## Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

## A proposito di questa attività

L'FQDN specificato deve essere univoco.



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC.

## Fasi

1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name  
-is-enabled true [-use-secure {true|false} -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

# Risoluzione del nome host

## Panoramica sulla risoluzione dei nomi host

ONTAP deve essere in grado di convertire i nomi host in indirizzi IP numerici per fornire l'accesso ai client e ai servizi di accesso. È necessario configurare le macchine virtuali di storage (SVM) in modo che utilizzino i name service locali o esterni per risolvere le informazioni sugli host. ONTAP supporta la configurazione di un server DNS esterno o la configurazione del file host locale per la risoluzione dei nomi host.

Quando si utilizza un server DNS esterno, è possibile configurare il DNS dinamico (DDNS), che invia automaticamente informazioni DNS nuove o modificate dal sistema di storage al server DNS. Senza aggiornamenti DNS dinamici, è necessario aggiungere manualmente le informazioni DNS (nome DNS e indirizzo IP) ai server DNS identificati quando un nuovo sistema viene messo in linea o quando le informazioni DNS esistenti cambiano. Questo processo è lento e soggetto a errori. Durante il disaster recovery, la configurazione manuale può causare un lungo downtime.

## Configurare il DNS per la risoluzione del nome host

Il DNS viene utilizzato per accedere a fonti locali o remote per ottenere informazioni sull'host. È necessario configurare il DNS per accedere a una o a entrambe queste origini.

ONTAP deve essere in grado di cercare le informazioni dell'host per fornire un accesso appropriato ai client. È necessario configurare i name service per consentire a ONTAP di accedere ai servizi DNS locali o esterni per ottenere le informazioni sull'host.

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX.

### Configurazione di una SVM e di una LIF di dati per la risoluzione del nome host utilizzando un server DNS esterno

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host vengono risolti utilizzando server DNS esterni.

#### Prima di iniziare

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

#### A proposito di questa attività

Vedere [Configurare i servizi DNS dinamici](#) Per ulteriori informazioni sulla configurazione del DNS dinamico su SVM.

#### Fasi

1. Abilitare il DNS sulla SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



Il `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

2. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check`

comando.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Per informazioni sulle politiche di servizio relative al DNS, vedere ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#).

## Configurare la tabella Name Service Switch per la risoluzione dei nomi host

Per consentire a ONTAP di consultare il servizio di nomi locale o esterno per recuperare le informazioni sull'host, è necessario configurare correttamente la tabella degli switch del servizio di nomi.

### Prima di iniziare

È necessario decidere quale name service utilizzare per il mapping degli host nel proprio ambiente.

### Fasi

1. Aggiungere le voci necessarie alla tabella dei name service switch:

```
vserver services name-service ns-switch modify -vserver <vserver_name>  
-database <database_name> -source <source_names>
```

2. Verificare che la tabella name service switch contenga le voci previste nell'ordine desiderato:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

### Esempio

Nell'esempio seguente viene modificata una voce nella tabella degli switch del servizio nomi per SVM VS1 in modo da utilizzare prima il file hosts locale e poi un server DNS esterno per risolvere i nomi host:

```
vserver services name-service ns-switch modify -vserver vs1 -database  
hosts -sources files,dns
```

## Gestire la tabella degli host (solo amministratori del cluster)

Un amministratore del cluster può aggiungere, modificare, eliminare e visualizzare le voci del nome host nella tabella hosts della macchina virtuale di storage amministrativa (SVM). Un amministratore SVM può configurare le voci del nome host solo per la SVM

assegnata.

## Comandi per la gestione delle voci dei nomi host locali

È possibile utilizzare `vserver services name-service dns hosts` Per creare, modificare o eliminare le voci della tabella host DNS.

Quando si creano o modificano le voci del nome host DNS, è possibile specificare più indirizzi alias separati da virgole.

Se si desidera...	Utilizzare questo comando...
Creare un nome host DNS	<code>vserver services name-service dns hosts create</code>
Modificare una voce del nome host DNS	<code>vserver services name-service dns hosts modify</code>
Eliminare una voce del nome host DNS	<code>vserver services name-service dns hosts delete</code>

Per ulteriori informazioni, consultare ["Comandi di ONTAP 9"](#) per `vserver services name-service dns hosts` comandi.

## Proteggere la rete

### Configurare la sicurezza di rete utilizzando gli standard FIPS (Federal Information Processing Standards)

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare le crittografie deboli, ad esempio RC4, in ONTAP.

Per impostazione predefinita, SSL su ONTAP è impostato con la compliance FIPS disattivata e il protocollo SSL attivato con quanto segue:

- TLSv1.3 (a partire da ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Se si desidera che gli account amministratore accedano alle SVM con una chiave pubblica SSH, assicurarsi che l'algoritmo della chiave host sia supportato prima di attivare la modalità SSL FIPS.

**Nota:** il supporto dell'algoritmo della chiave host è stato modificato in ONTAP 9.11.1 e versioni successive.

Release di ONTAP	Tipi di chiave supportati	Tipi di chiave non supportati
9.11.1 e versioni successive	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Gli account di chiave pubblica SSH esistenti senza gli algoritmi di chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

Per ulteriori informazioni, vedere ["Abilitare gli account a chiave pubblica SSH"](#).

Per ulteriori informazioni sulla configurazione della modalità SSL FIPS, consultare `security config modify` pagina man.

## Abilitare FIPS

Si consiglia a tutti gli utenti sicuri di modificare la propria configurazione di sicurezza subito dopo l'installazione o l'aggiornamento del sistema. Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.



Quando FIPS è attivato, non è possibile installare o creare un certificato con una chiave RSA di lunghezza pari a 4096.

## Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Attiva FIPS:

```
security config modify -interface SSL -is-fips-enabled true
```

3. Quando viene richiesto di continuare, immettere `y`
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente uno ad uno ogni nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

## Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Disattiva FIPS

Se si esegue ancora una configurazione di sistema precedente e si desidera configurare ONTAP con compatibilità con le versioni precedenti, è possibile attivare SSLv3 solo quando FIPS è disattivato.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Disattivare FIPS digitando:

```
security config modify -interface SSL -is-fips-enabled false
```

3. Quando viene richiesto di continuare, immettere y.
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente ciascun nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

### Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Visualizza lo stato di conformità FIPS

È possibile verificare se l'intero cluster esegue le impostazioni di configurazione della protezione corrente.

### Fasi

1. Riavviare uno alla volta ciascun nodo del cluster.

Non riavviare tutti i nodi del cluster contemporaneamente. È necessario riavviare il sistema per assicurarsi che tutte le applicazioni del cluster eseguano la nuova configurazione di sicurezza e per tutte le modifiche apportate alla modalità FIPS on/off, ai protocolli e ai cifrari.

2. Visualizza lo stato di conformità corrente:

```
security config show
```

```
security config show
```

Cluster				Cluster
Security	Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready				
-----	-----	-----	-----	-----
-----				
SSL	false	TLsv1_2, TLsv1_1, TLsv1	ALL:!LOW:!aNULL: !EXP:!eNULL	yes

## Configurare la crittografia IP Security (IPsec) over wire

ONTAP utilizza IPsec (Internet Protocol Security) in modalità di trasporto per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito. IPsec offre la crittografia dei dati per tutto il traffico IP, inclusi i protocolli NFS, iSCSI e SMB.

A partire da ONTAP 9.12.1, il supporto IPsec del protocollo host front-end è disponibile nelle configurazioni MetroCluster IP e MetroCluster fabric-attached.

Il supporto di IPsec nei cluster MetroCluster è limitato al traffico host front-end e non è supportato dalle LIF intercluster MetroCluster.

A partire da ONTAP 9.10.1, è possibile utilizzare chiavi precondivise (PSK) o certificati per l'autenticazione con IPsec. In precedenza, solo gli PSK erano supportati con IPsec.

A partire da ONTAP 9.9.1, gli algoritmi di crittografia utilizzati da IPsec sono validati in FIPS 140-2. Gli algoritmi vengono generati dal modulo crittografico NetApp in ONTAP che riporta la convalida FIPS 140-2.

A partire da ONTAP 9.8, ONTAP supporta IPsec in modalità di trasporto.

Una volta configurato IPsec, il traffico di rete tra il client e ONTAP viene protetto con misure preventive per combattere gli attacchi di tipo play e man-in-the-middle (MITM).

Per NetApp SnapMirror e la crittografia del traffico di peering del cluster, la crittografia di peering del cluster (CPE) e la protezione TLS (Transport Layer Security) sono ancora consigliate su IPsec per garantire la sicurezza in transito via cavo. Questo perché TLS offre performance migliori rispetto a IPsec.

Mentre la funzionalità IPsec è attivata sul cluster, la rete richiede una voce del database dei criteri di protezione (SPD) che corrisponda al traffico da proteggere e che specifichi i dettagli di protezione (come la suite di crittografia e il metodo di autenticazione) prima che il traffico possa fluire. Su ciascun client è necessaria anche una voce SPD corrispondente.

## **Abilitare IPsec sul cluster**

È possibile attivare IPsec sul cluster per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito.

### **Fasi**

1. Scopri se IPsec è già attivato:

```
security ipsec config show
```

Se il risultato include `IPsec Enabled: false`, passare alla fase successiva.

2. Attiva IPsec:

```
security ipsec config modify -is-enabled true
```

3. Eseguire nuovamente il comando di rilevamento:

```
security ipsec config show
```

Il risultato ora include `IPsec Enabled: true`.

## **Preparare la creazione del criterio IPsec con l'autenticazione del certificato**

È possibile saltare questo passaggio se si utilizzano solo chiavi pre-condivise (PSK) per l'autenticazione e non si utilizza l'autenticazione del certificato.

Prima di creare un criterio IPsec che utilizza i certificati per l'autenticazione, è necessario verificare che siano soddisfatti i seguenti prerequisiti:



- Sia ONTAP che il client devono avere installato il certificato CA dell'altra parte in modo che i certificati dell'entità finale (ONTAP o client) siano verificabili da entrambe le parti
- Viene installato un certificato per il LIF ONTAP che partecipa al criterio



Le LIF ONTAP possono condividere i certificati. Non è richiesta una mappatura uno-a-uno tra certificati e LIF.

## Fasi

1. Installare tutti i certificati CA utilizzati durante l'autenticazione reciproca, incluse le CA lato ONTAP e lato client, nella gestione dei certificati ONTAP, a meno che non sia già installato (come nel caso di una CA root autofirmata di ONTAP).

### Comando di esempio

```
cluster::> security certificate install -vserver svm_name -type server-ca
-cert-name my_ca_cert
```

2. Per assicurarsi che la CA installata rientri nel percorso di ricerca della CA IPsec durante l'autenticazione, aggiungere le CA di gestione dei certificati ONTAP al modulo IPsec utilizzando `security ipsec ca-certificate add` comando.

### Comando di esempio

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
my_ca_cert
```

3. Creare e installare un certificato per l'utilizzo da parte della LIF ONTAP. La CA emittente di questo certificato deve essere già installata in ONTAP e aggiunta a IPsec.

### Comando di esempio

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

Per ulteriori informazioni sui certificati in ONTAP, vedere i comandi dei certificati di protezione nella documentazione di ONTAP 9 .

## Definizione del database dei criteri di protezione (SPD)

IPsec richiede una voce SPD prima di consentire il flusso del traffico sulla rete. Ciò vale sia che si utilizzi un PSK o un certificato per l'autenticazione.

## Fasi

1. Utilizzare `security ipsec policy create` comando a:
  - a. Selezionare l'indirizzo IP ONTAP o la subnet degli indirizzi IP per partecipare al trasporto IPsec.
  - b. Selezionare gli indirizzi IP del client che si connetteranno agli indirizzi IP ONTAP.



Il client deve supportare Internet Key Exchange versione 2 (IKEv2) con una chiave precondivisa (PSK).

- c. Opzionale. Selezionare i parametri di traffico a grana fine, ad esempio i protocolli di livello superiore (UDP, TCP, ICMP, ecc.) , i numeri delle porte locali e i numeri delle porte remote per proteggere il traffico. I parametri corrispondenti sono `protocols`, `local-ports` e `remote-ports`

rispettivamente.

Ignorare questo passaggio per proteggere tutto il traffico tra l'indirizzo IP ONTAP e l'indirizzo IP del client. La protezione di tutto il traffico è l'impostazione predefinita.

- d. Immettere PSK o Public-Key Infrastructure (PKI) per `auth-method` parametro per il metodo di autenticazione desiderato.
  - i. Se si immette una PSK, includere i parametri, quindi premere <enter> per visualizzare la richiesta di immissione e verifica della chiave precondivisa.



`local-identity` e `remote-identity` I parametri sono facoltativi se sia l'host che il client utilizzano il metodo `strongSwan` e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

- ii. Se si inserisce un'infrastruttura PKI, è necessario immettere anche il `cert-name`, `local-identity`, `remote-identity` parametri. Se l'identità del certificato lato remoto non è nota o se sono previste più identità client, inserire l'identità speciale `ANYTHING`.

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Il traffico IP non può passare tra il client e il server finché ONTAP e il client non hanno impostato i criteri IPSec corrispondenti e le credenziali di autenticazione (PSK o certificato) non sono installate su entrambi i lati. Per ulteriori informazioni, vedere la configurazione IPSec lato client.

### Utilizzare le identità IPsec

Per il metodo di autenticazione con chiave pre-condivisa, le identità locali e remote sono facoltative se host e client utilizzano il metodo di autenticazione con chiave `strongSwan` e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

Per il metodo di autenticazione PKI/certificato, le identità locali e remote sono obbligatorie. Le identità specificano l'identità certificata all'interno del certificato di ciascun lato e vengono utilizzate nel processo di verifica. Se l'identità remota è sconosciuta o se può essere costituita da diverse identità, utilizzare l'identità speciale `ANYTHING`.

### A proposito di questa attività

All'interno di ONTAP, le identità vengono specificate modificando la voce SPD o durante la creazione del criterio SPD. Il nome SPD può essere un indirizzo IP o un nome di identità in formato stringa.

### Fase

Per modificare un'impostazione di identità SPD esistente, utilizzare il seguente comando:

```
security ipsec policy modify
```

### Comando di esempio

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

### Configurazione di più client IPSec

Quando un numero limitato di client deve sfruttare IPSec, è sufficiente utilizzare una singola voce SPD per ciascun client. Tuttavia, quando centinaia o addirittura migliaia di client devono sfruttare IPSec, NetApp consiglia di utilizzare una configurazione con più client IPSec.

#### A proposito di questa attività

ONTAP supporta la connessione di più client su molte reti a un singolo indirizzo IP SVM con IPSec attivato. È possibile eseguire questa operazione utilizzando uno dei seguenti metodi:

- **Configurazione subnet**

Per consentire a tutti i client di una determinata subnet (ad esempio 192.168.134.0/24) di connettersi a un singolo indirizzo IP SVM utilizzando una singola voce di policy SPD, è necessario specificare `remote-ip-subnets` sotto forma di subnet. Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta.



Quando si utilizza una singola voce di criterio in una configurazione di subnet, i client IPSec in tale subnet condividono l'identità IPSec e la chiave precondivisa (PSK). Tuttavia, questo non è vero con l'autenticazione del certificato. Quando si utilizzano i certificati, ciascun client può utilizzare il proprio certificato univoco o un certificato condiviso per l'autenticazione. IPSec ONTAP verifica la validità del certificato in base alle CA installate nel relativo archivio di attendibilità locale. ONTAP supporta anche il controllo dell'elenco di revocche di certificati (CRL).

- **Consenti configurazione di tutti i client**

Per consentire a qualsiasi client, indipendentemente dall'indirizzo IP di origine, di connettersi all'indirizzo IP SVM abilitato a IPSec, utilizzare `0.0.0.0/0` carattere jolly quando si specifica `remote-ip-subnets` campo.

Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta. Per l'autenticazione del certificato, è possibile immettere `ANYTHING`.

Inoltre, quando `0.0.0.0/0` se si utilizza il carattere jolly, è necessario configurare un numero di porta locale o remota specifico da utilizzare. Ad esempio, `NFS port 2049`.

#### Fasi

a. Utilizzare uno dei seguenti comandi per configurare IPSec per più client.

i. Se si utilizza la **configurazione della subnet** per supportare più client IPSec:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

### Comando di esempio

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

- i. Se si utilizza l'opzione **Allow all clients Configuration** (Consenti configurazione di tutti i client) per supportare più client IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

### Comando di esempio

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

## Statistiche IPsec

Attraverso la negoziazione, è possibile stabilire un canale di sicurezza denominato SA (IKE Security Association) tra l'indirizzo IP di ONTAP SVM e l'indirizzo IP del client. I SAS IPsec vengono installati su entrambi gli endpoint per eseguire le operazioni di crittografia e decrittografia dei dati.

È possibile utilizzare i comandi delle statistiche per controllare lo stato di IPsec SAS e IKE SAS.

### Comandi di esempio

Comando di esempio IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Comando e output di esempio SA IPsec:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

Vserver	Policy Name	Local Address	Remote Address	Initiator-SPI	State
vs1	test34	192.168.134.34	192.168.134.44	c764f9ee020cec69	ESTABLISHED

Comando e output di esempio SA IPsec:

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipseca -node cluster1-node1
      Policy  Local          Remote          Inbound  Outbound
Vserver  Name    Address          Address          SPI      SPI
State
-----
-----
vs1      test34
          192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED
```

## Configurare le policy firewall per le LIF

La configurazione di un firewall migliora la sicurezza del cluster e impedisce l'accesso non autorizzato al sistema di storage. Per impostazione predefinita, il firewall integrato è configurato in modo da consentire l'accesso remoto a un set specifico di servizi IP per le LIF di dati, gestione e intercluster.

A partire da ONTAP 9.10.1:

- Le policy firewall sono obsolete e vengono sostituite dalle policy di servizio LIF. In precedenza, il firewall integrato era gestito tramite policy firewall. Questa funzionalità viene ora eseguita utilizzando una policy di servizio LIF.
- Tutti i criteri firewall sono vuoti e non aprono porte nel firewall sottostante. Tutte le porte devono invece essere aperte utilizzando una policy di servizio LIF.
- Non è richiesta alcuna azione dopo un aggiornamento alla versione 9.10.1 o successiva per passare dalle policy firewall alle policy di servizio LIF. Il sistema crea automaticamente policy di servizio LIF coerenti con le policy firewall in uso nella release precedente di ONTAP. Se si utilizzano script o altri strumenti che creano e gestiscono policy firewall personalizzate, potrebbe essere necessario aggiornare tali script per creare policy di servizio personalizzate.

Per ulteriori informazioni, vedere ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#).

Le policy firewall possono essere utilizzate per controllare l'accesso ai protocolli dei servizi di gestione come SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS o SNMP. Non è possibile impostare policy firewall per protocolli dati come NFS o SMB.

È possibile gestire il servizio firewall e le policy nei seguenti modi:

- Attivazione o disattivazione del servizio firewall
- Visualizzazione della configurazione corrente del servizio firewall
- Creazione di un nuovo criterio firewall con il nome del criterio e i servizi di rete specificati
- Applicazione di un criterio firewall a un'interfaccia logica
- Creazione di una nuova policy firewall che sia una copia esatta di una policy esistente

È possibile utilizzare questa opzione per creare una policy con caratteristiche simili all'interno della stessa

SVM o per copiare la policy su una SVM diversa.

- Visualizzazione di informazioni sui criteri firewall
- Modifica degli indirizzi IP e delle netmask utilizzati da una policy firewall
- Eliminazione di una policy firewall non utilizzata da una LIF

## Policy firewall e LIF

I criteri firewall LIF vengono utilizzati per limitare l'accesso al cluster su ogni LIF. È necessario comprendere in che modo la policy firewall predefinita influenza l'accesso al sistema su ciascun tipo di LIF e come è possibile personalizzare una policy firewall per aumentare o ridurre la sicurezza su una LIF.

Durante la configurazione di un LIF utilizzando `network interface create` oppure `network interface modify` il valore specificato per `-firewall-policy` Il parametro determina i protocolli di servizio e gli indirizzi IP ai quali è consentito l'accesso a LIF.

In molti casi è possibile accettare il valore predefinito del criterio firewall. In altri casi, potrebbe essere necessario limitare l'accesso a determinati indirizzi IP e a determinati protocolli dei servizi di gestione. I protocolli dei servizi di gestione disponibili includono SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS E SNMP.

Per impostazione predefinita, il criterio firewall per tutte le LIF del cluster è "" e non possono essere modificati.

La tabella seguente descrive i criteri firewall predefiniti assegnati a ciascun LIF, in base al ruolo (ONTAP 9.5 e versioni precedenti) o ai criteri di servizio (ONTAP 9.6 e versioni successive), quando si crea il LIF:

Policy del firewall	Protocolli di servizio predefiniti	Accesso predefinito	LIF applicati a.
gestione	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Gestione del cluster, gestione SVM e LIF di gestione dei nodi
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Le LIF dei dati che supportano anche l'accesso alla gestione SVM
intercluster	https, ndmp, ndmps	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i LIF intercluster
dati	dns, ndmp, ndmps, portmap	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i dati LIF

## Configurazione del servizio portmap

Il servizio portmap associa i servizi RPC alle porte su cui sono in ascolto.

Il servizio portmap era sempre accessibile in ONTAP 9.3 e versioni precedenti, è diventato configurabile in ONTAP 9.4 fino a ONTAP 9.6 e viene gestito automaticamente a partire da ONTAP 9.7.

- In ONTAP 9.3 e versioni precedenti, il servizio portmap (rpcbind) era sempre accessibile sulla porta 111 nelle configurazioni di rete che si basavano sul firewall ONTAP integrato anziché su un firewall di terze parti.
- Da ONTAP 9.4 a ONTAP 9.6, è possibile modificare i criteri del firewall per controllare se il servizio portmap è accessibile su specifiche LIF.
- A partire da ONTAP 9.7, il servizio firewall portmap viene eliminato. La porta portmap viene invece aperta automaticamente per tutti i LIF che supportano il servizio NFS.

## **Il servizio Portmap è configurabile nel firewall in ONTAP 9.4 fino a ONTAP 9.6.**

Il resto di questo argomento illustra come configurare il servizio firewall portmap per le versioni da ONTAP 9.4 a ONTAP 9.6.

A seconda della configurazione, potrebbe essere possibile non consentire l'accesso al servizio su specifici tipi di LIF, in genere LIF di gestione e di intercluster. In alcuni casi, potresti persino essere in grado di impedire l'accesso alle LIF dei dati.

### **Quale comportamento ci si può aspettare**

Il comportamento da ONTAP 9.4 a ONTAP 9.6 è progettato per fornire una transizione perfetta all'aggiornamento. Se si accede già al servizio portmap su specifici tipi di LIF, questo continuerà ad essere accessibile attraverso questi tipi di LIF. Come in ONTAP 9.3 e versioni precedenti, nella policy di firewall per il tipo di LIF è possibile specificare i servizi a cui accedere.

Tutti i nodi del cluster devono eseguire ONTAP 9.4 fino a ONTAP 9.6 per rendere effettivo il comportamento. Viene influenzato solo il traffico in entrata.

Le nuove regole sono le seguenti:

- All'aggiornamento alla versione 9.4 fino alla 9.6, ONTAP aggiunge il servizio portmap a tutte le policy firewall esistenti, predefinite o personalizzate.
- Quando si crea un nuovo cluster o un nuovo IPspace, ONTAP aggiunge il servizio portmap solo al criterio dati predefinito, non ai criteri di gestione predefiniti o di intercluster.
- È possibile aggiungere il servizio portmap alle policy predefinite o personalizzate in base alle necessità e rimuovere il servizio in base alle necessità.

### **Come aggiungere o rimuovere il servizio portmap**

Per aggiungere il servizio portmap a una policy SVM o del firewall del cluster (renderlo accessibile all'interno del firewall), immettere:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Per rimuovere il servizio portmap da una policy SVM o del firewall del cluster (rendendolo inaccessibile all'interno del firewall), immettere:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

È possibile utilizzare il comando di modifica dell'interfaccia di rete per applicare il criterio firewall a una LIF esistente. Per la sintassi completa dei comandi, vedere ["Comandi di ONTAP 9"](#).

## Creare una policy firewall e assegnarla a una LIF

I criteri firewall predefiniti vengono assegnati a ciascun LIF quando si crea il LIF. In molti casi, le impostazioni predefinite del firewall funzionano correttamente e non è necessario modificarle. Se si desidera modificare i servizi di rete o gli indirizzi IP che possono accedere a una LIF, è possibile creare una policy firewall personalizzata e assegnarla alla LIF.

### A proposito di questa attività

- Non è possibile creare un criterio firewall con `policy` nome `data`, `intercluster`, `cluster`, o `mgmt`.

Questi valori sono riservati ai criteri firewall definiti dal sistema.

- Non è possibile impostare o modificare un criterio firewall per le LIF del cluster.

Il criterio del firewall per le LIF del cluster è impostato su `0.0.0.0/0` per tutti i tipi di servizi.

- Se è necessario rimuovere un servizio da un criterio, è necessario eliminare il criterio firewall esistente e crearne uno nuovo.
- Se IPv6 è attivato nel cluster, è possibile creare policy firewall con indirizzi IPv6.

Dopo aver attivato IPv6, `data`, `intercluster`, e `mgmt` I criteri firewall includono `::/0`, il carattere jolly IPv6, nell'elenco degli indirizzi accettati.

- Quando si utilizza System Manager per configurare la funzionalità di protezione dei dati tra cluster, è necessario assicurarsi che gli indirizzi IP LIF tra cluster siano inclusi nell'elenco consentito e che il servizio HTTPS sia consentito sia per le LIF tra cluster che per i firewall di proprietà dell'azienda.

Per impostazione predefinita, il `intercluster` La policy firewall consente l'accesso da tutti gli indirizzi IP (`0.0.0.0/0`, o `::/0` per IPv6) e abilita i servizi HTTPS, NDMP e NDMPs. Se si modifica questo criterio predefinito o si crea un criterio firewall personalizzato per le LIF tra cluster, è necessario aggiungere ciascun indirizzo IP LIF tra cluster all'elenco consentito e attivare il servizio HTTPS.

- A partire da ONTAP 9.6, i servizi firewall HTTPS e SSH non sono supportati.

In ONTAP 9.6, il `management-https` e `management-ssh` I servizi LIF sono disponibili per l'accesso alla gestione HTTPS e SSH.

### Fasi

1. Creare una policy firewall che sarà disponibile per i LIF su una SVM specifica:

```
system services firewall policy create -vserver vservice_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

È possibile utilizzare questo comando più volte per aggiungere più di un servizio di rete e un elenco di indirizzi IP consentiti per ciascun servizio nella policy del firewall.

2. Verificare che il criterio sia stato aggiunto correttamente utilizzando `system services firewall policy show` comando.
3. Applicare il criterio firewall a una LIF:

```
network interface modify -vserver vservice_name -lif lif_name -firewall-policy
policy_name
```



4. Verificare che il criterio sia stato aggiunto correttamente alla LIF utilizzando `network interface show -fields firewall-policy` comando.

#### **Esempio di creazione e applicazione di un criterio firewall a una LIF**

Il seguente comando crea una policy firewall denominata `data_http` che abilita l'accesso ai protocolli HTTP e HTTPS dagli indirizzi IP sulla subnet 10.10, applica tale policy alla LIF denominata `data1` su SVM `vs1`, quindi mostra tutte le policy firewall sul cluster:

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster-1			
	data		
		dns	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	intercluster		
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	mgmt		
		dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
vs1			
	data_http		
		http	10.10.0.0/16
		https	10.10.0.0/16

```
network interface modify -vserver vs1 -lif data1 -firewall-policy  
data_http
```

```
network interface show -fields firewall-policy
```

vserver	lif	firewall-policy
-----	-----	-----
Cluster	node1_clus_1	
Cluster	node1_clus_2	
Cluster	node2_clus_1	
Cluster	node2_clus_2	
cluster-1	cluster_mgmt	mgmt
cluster-1	node1_mgmt1	mgmt
cluster-1	node2_mgmt1	mgmt
vs1	data1	data_http
vs3	data2	data

## Comandi per la gestione del servizio firewall e delle policy

È possibile utilizzare `system services firewall` comandi per la gestione del servizio firewall, il `system services firewall policy` comandi per la gestione delle policy firewall e di `network interface modify` Comando per gestire le impostazioni del firewall per le LIF.

Se si desidera...	Utilizzare questo comando...
Attiva o disattiva il servizio firewall	<code>system services firewall modify</code>
Visualizza la configurazione corrente per il servizio firewall	<code>system services firewall show</code>
Creare una policy firewall o aggiungere un servizio a una policy firewall esistente	<code>system services firewall policy create</code>
Applicare un criterio firewall a una LIF	<code>network interface modify -lif lifname -firewall-policy</code>
Modificare gli indirizzi IP e le netmask associate a un criterio firewall	<code>system services firewall policy modify</code>
Visualizza informazioni sui criteri firewall	<code>system services firewall policy show</code>
Creare una nuova policy firewall che sia una copia esatta di una policy esistente	<code>system services firewall policy clone</code>
Eliminare una policy firewall non utilizzata da una LIF	<code>system services firewall policy delete</code>

Per ulteriori informazioni, consultare le pagine man del `system services firewall`, `system services firewall policy`, e `network interface modify` comandi in ["Comandi di ONTAP 9"](#).

## Contrassegno QoS (solo amministratori del cluster)

### Panoramica sulla QoS

Il contrassegno della qualità del servizio (QoS) di rete consente di assegnare priorità a diversi tipi di traffico in base alle condizioni della rete per utilizzare in modo efficace le risorse di rete. È possibile impostare il valore DSCP (differentiate Services code point) dei pacchetti IP in uscita per i tipi di traffico supportati per IPspace.

### Marcatura DSCP per la conformità UC

È possibile attivare il contrassegno DSCP (differentiate Services code point) sul traffico dei pacchetti IP in uscita (in uscita) per un determinato protocollo con un codice DSCP predefinito o fornito dall'utente. Il contrassegno DSCP è un meccanismo per la classificazione e la gestione del traffico di rete ed è un

componente della conformità UC (Unified Capability).

La marcatura DSCP (nota anche come *marcatura QoS* o *marcatura della qualità del servizio*) viene attivata fornendo un valore IPspace, protocollo e DSCP. I protocolli su cui è possibile applicare il contrassegno DSCP sono NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet e SNMP.

Se non si fornisce un valore DSCP quando si attiva la marcatura DSCP per un determinato protocollo, viene utilizzato un valore predefinito:

- Il valore predefinito per il traffico/protocolli dati è 0x0A (10).
- Il valore predefinito per i protocolli di controllo/traffico è 0x30 (48).

## Modificare i valori di marcatura QoS

È possibile modificare i valori di marcatura della qualità del servizio (QoS) per diversi protocolli, per ciascun IPspace.

### Prima di iniziare

Tutti i nodi del cluster devono eseguire la stessa versione di ONTAP.

### Fase

Modificare i valori di marcatura QoS utilizzando `network qos-marking modify` comando.

- Il `-ipSpace` Parameter (parametro) specifica l'IPspace per cui la voce di marcatura QoS deve essere modificata.
- Il `-protocol` Parametro specifica il protocollo per cui la voce di marcatura QoS deve essere modificata. Il `network qos-marking modify` la pagina man descrive i possibili valori del protocollo.
- Il `-dscp` Il parametro specifica il valore DSCP (Differentiated Services Code Point). I valori possibili vanno da 0 a 63.
- Il `-is-enabled` Il parametro viene utilizzato per attivare o disattivare il contrassegno QoS per il protocollo specificato nell'IPspace fornito da `-ipSpace` parametro.

Il seguente comando attiva il contrassegno QoS per il protocollo NFS nell'IPspace predefinito:

```
network qos-marking modify -ipSpace Default -protocol NFS -is-enabled true
```

Il seguente comando imposta il valore DSCP su 20 per il protocollo NFS nell'IPspace predefinito:

```
network qos-marking modify -ipSpace Default -protocol NFS -dscp 20
```

## Visualizzare i valori di marcatura QoS

È possibile visualizzare i valori di marcatura QoS per diversi protocolli, per ciascun IPspace.

### Fase

Visualizzare i valori di marcatura QoS utilizzando `network qos-marking show` comando.

Il seguente comando visualizza il contrassegno QoS per tutti i protocolli nell'IPSpace predefinito:

```
network qos-marking show -ipspace Default
IPspace          Protocol          DSCP    Enabled?
-----
Default
                CIFS              10      false
                FTP              48      false
                HTTP-admin       48      false
                HTTP-filesrv     10      false
                NDMP             10      false
                NFS              10      true
                SNMP            48      false
                SSH              48      false
                SnapMirror       10      false
                Telnet          48      false
                iSCSI           10      false

11 entries were displayed.
```

## Gestione SNMP (solo amministratori cluster)

### Panoramica SNMP

È possibile configurare SNMP per monitorare le SVM nel cluster per evitare i problemi prima che si verifichino e per rispondere ai problemi in caso di verificarsi. La gestione di SNMP implica la configurazione degli utenti SNMP e la configurazione delle destinazioni SNMP traphost (workstation di gestione) per tutti gli eventi SNMP. SNMP è disattivato per impostazione predefinita nei file LIF dei dati.

È possibile creare e gestire utenti SNMP di sola lettura nella SVM dei dati. Le LIF dei dati devono essere configurate per ricevere richieste SNMP su SVM.

Le workstation o i manager di gestione della rete SNMP possono richiedere informazioni all'agente SNMP SVM. L'agente SNMP raccoglie le informazioni e le inoltra ai gestori SNMP. L'agente SNMP genera inoltre notifiche trap ogni volta che si verificano eventi specifici. L'agente SNMP sulla SVM dispone di privilegi di sola lettura; non può essere utilizzato per operazioni impostate o per intraprendere un'azione correttiva in risposta a una trap. ONTAP fornisce un agente SNMP compatibile con le versioni SNMP v1, v2c e v3. SNMPv3 offre sicurezza avanzata utilizzando passphrase e crittografia.

Per ulteriori informazioni sul supporto SNMP nei sistemi ONTAP, vedere ["TR-4220: Supporto SNMP in Data ONTAP"](#).

### Panoramica MIB

Un MIB (Management Information base) è un file di testo che descrive oggetti e trap SNMP.

I MIB descrivono la struttura dei dati di gestione del sistema di storage e utilizzano uno spazio dei nomi gerarchico contenente OID (Object Identifier). Ogni OID identifica una variabile che può essere letta utilizzando

## SNMP.

Poiché i MIB non sono file di configurazione e ONTAP non legge questi file, la funzionalità SNMP non viene influenzata dai MIB. ONTAP fornisce il seguente file MIB:

- Una MIB personalizzata di NetApp (`netapp.mib`)

ONTAP supporta i MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), che mostrano sia i dati IPv4 che IPv6.

ONTAP fornisce inoltre un breve riferimento incrociato tra gli OID (Object Identifier) e i nomi brevi degli oggetti in `traps.dat` file.



Le versioni più recenti dei MIB e dei file `traps.dat` di ONTAP sono disponibili sul sito del supporto NetApp. Tuttavia, le versioni di questi file sul sito di supporto non corrispondono necessariamente alle funzionalità SNMP della versione di ONTAP in uso. Questi file vengono forniti per agevolare la valutazione delle funzionalità SNMP nella versione più recente di ONTAP.

## Trap SNMP

I trap SNMP acquisiscono le informazioni di monitoraggio del sistema inviate come notifica asincrona dall'agente SNMP al gestore SNMP.

Esistono tre tipi di trap SNMP: Standard, incorporato e definito dall'utente. I trap definiti dall'utente non sono supportati in ONTAP.

È possibile utilizzare una trap per controllare periodicamente le soglie operative o gli errori definiti nella MIB. Se viene raggiunta una soglia o viene rilevato un errore, l'agente SNMP invia un messaggio (trap) ai traphost che li avvisano dell'evento.



ONTAP supporta i trap SNMPv1 e, avviando ONTAP 9.1, i trap SNMPv3. ONTAP non supporta i trap SNMPv2c e informa.

## Trap SNMP standard

Questi trap sono definiti in RFC 1215. ONTAP supporta cinque trap SNMP standard: Coldstart, warmStart, linkGiù, linkup e AuthenticationFailure.



Il trap AuthenticationFailure è disattivato per impostazione predefinita. È necessario utilizzare `system snmp authtrap` per attivare il trap. Per ulteriori informazioni, consulta le pagine man: "[Comandi di ONTAP 9](#)"

## Trap SNMP integrati

I trap integrati sono predefiniti in ONTAP e vengono inviati automaticamente alle stazioni di gestione di rete presenti nell'elenco degli host trapezoidali in caso di evento. Questi trap, come `diskFailedShutdown`, `cpuTooBusy` e `volumeNearlyFull`, sono definiti nel MIB personalizzato.

Ogni trap integrato è identificato da un codice trap univoco.

## Creare una community SNMP e assegnarla a una LIF

È possibile creare una community SNMP che funga da meccanismo di autenticazione tra la stazione di gestione e la macchina virtuale di storage (SVM) quando si utilizzano SNMPv1 e SNMPv2c.

Creando community SNMP in una SVM di dati, è possibile eseguire comandi come `snmpwalk` e `snmpget` Sulle LIF dei dati.

### A proposito di questa attività

- Nelle nuove installazioni di ONTAP, SNMPv1 e SNMPv2c sono disattivati per impostazione predefinita.

SNMPv1 e SNMPv2c vengono attivati dopo la creazione di una community SNMP.

- ONTAP supporta le community di sola lettura.
- Per impostazione predefinita, il servizio SNMP è impostato su per il criterio firewall "dati" assegnato alle LIF dati `deny`.

È necessario creare un nuovo criterio firewall con il servizio SNMP impostato su `allow` Quando si crea un utente SNMP per un SVM dati.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- È possibile creare community SNMP per gli utenti SNMPv1 e SNMPv2c sia per SVM admin che per SVM dati.
- Poiché una SVM non fa parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

### Fasi

1. Creare una community SNMP utilizzando `system snmp community add` comando. Il seguente comando mostra come creare una community SNMP nel cluster SVM di amministrazione-1:

```
system snmp community add -type ro -community-name comty1 -vserver  
cluster-1
```

Il seguente comando mostra come creare una community SNMP nei dati SVM vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verificare che le community siano state create utilizzando il comando di visualizzazione della community `snmp` di sistema.

Il seguente comando mostra le due community create per SNMPv1 e SNMPv2c:

```

system snmp community show
cluster-1
rocomty1
vs1
rocomty2

```

3. Verificare se SNMP è consentito come servizio nella policy firewall "dati" utilizzando `system services firewall policy show` comando.

Il seguente comando indica che il servizio snmp non è consentito nella policy firewall "dati" predefinita (il servizio snmp è consentito solo nella policy firewall "mgmt"):

```

system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster-1
  data
    dns      0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
cluster-1
  intercluster
    https    0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
cluster-1
  mgmt
    dns      0.0.0.0/0
    http     0.0.0.0/0
    https    0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
    ntp      0.0.0.0/0
    snmp     0.0.0.0/0
    ssh      0.0.0.0/0

```

4. Creare un nuovo criterio firewall che consenta l'accesso tramite snmp utilizzando `system services firewall policy create` comando.

I seguenti comandi creano una nuova policy di firewall dati denominata "data1" che consente snmp



```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

Vserver	Policy	Service	Allowed
-----			
cluster-1			
	mgmt		
		snmp	0.0.0.0/0
vs1			
	data1		
		snmp	0.0.0.0/0

5. Applicare il criterio firewall a una LIF dati utilizzando il comando `network interface modify` (modifica interfaccia di rete) con il parametro `-firewall-policy`.

Il seguente comando assegna il nuovo criterio firewall "data1" a "datalif1" LIF:

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

## Configurare gli utenti SNMPv3 in un cluster

SNMPv3 è un protocollo sicuro rispetto a SNMPv1 e SNMPv2c. Per utilizzare SNMPv3, è necessario configurare un utente SNMPv3 per eseguire le utility SNMP dal gestore SNMP.

### Fase

Utilizzare il "comando di creazione dell'accesso di sicurezza" per creare un utente SNMPv3.

Viene richiesto di fornire le seguenti informazioni:

- Engine ID (ID motore): Il valore predefinito e raccomandato è l'ID motore locale
- Protocollo di autenticazione
- Password di autenticazione
- Protocollo di privacy
- Password del protocollo di privacy

### Risultato

L'utente SNMPv3 può accedere dal gestore SNMP utilizzando il nome utente e la password ed eseguire i comandi dell'utility SNMP.

### Parametri di sicurezza SNMPv3

SNMPv3 include una funzionalità di autenticazione che, quando selezionata, richiede agli utenti di inserire i

propri nomi, un protocollo di autenticazione, una chiave di autenticazione e il livello di sicurezza desiderato quando si richiama un comando.

Nella tabella seguente sono elencati i parametri di protezione di SNMPv3 :

Parametro	Opzione della riga di comando	Descrizione
ID motore	-E EngineID	ID motore dell'agente SNMP. Il valore predefinito è EngineID locale (consigliato).
SecurityName	-U Nome	Il nome utente non deve superare i 32 caratteri.
AuthProtocol	-A {none	MD5
SHA	SHA-256}	Il tipo di autenticazione può essere None, MD5, SHA o SHA-256.
Chiave authkey	-UNA PASSPHRASE	Passphrase con un minimo di otto caratteri.
Livello di sicurezza	-L {authNoPriv	AuthPriv
noAuthNoPriv}	Il livello di protezione può essere autenticazione, Nessuna privacy, autenticazione, privacy o nessuna autenticazione, Nessuna privacy.	PrivProtocol
-x { none	des	aes128}
Il protocollo di privacy può essere NONE, des o aes128	PrivPassword	-X password

### Esempi di diversi livelli di sicurezza

Questo esempio mostra come un utente SNMPv3 creato con diversi livelli di sicurezza può utilizzare i comandi lato client SNMP, ad esempio `snmpwalk`, per eseguire query sugli oggetti del cluster.

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.



È necessario utilizzare `snmpwalk` 5.3.1 o versione successiva quando il protocollo di autenticazione è SHA.

### Livello di sicurezza: Authprim

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza `authprim`.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Modalità FIPS

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Livello di sicurezza: AuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza autNoPriv.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

## Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy. Di conseguenza, non è possibile configurare un utente authNoPrivat SNMPv3 in modalità FIPS.

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Livello di sicurezza: NoAuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza noAuthNoPrimv.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

## Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy.

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Configurare i traphost per ricevere notifiche SNMP

È possibile configurare il traphost (gestore SNMP) in modo che riceva notifiche (PDU trap SNMP) quando vengono generati trap SNMP nel cluster. È possibile specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del traphost SNMP.

### Prima di iniziare

- I trap SNMP e SNMP devono essere attivati sul cluster.



I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.
- IPv6 deve essere attivato sul cluster per configurare i traphost SNMP utilizzando gli indirizzi IPv6.
- Per ONTAP 9.1 e versioni successive, è necessario specificare l'autenticazione di un modello di sicurezza basato sull'utente (USM) e le credenziali di privacy predefiniti durante la creazione di traphost.

### Fase

Aggiunta di un host SNMP traphost:

```
system snmp traphost add
```



I trap possono essere inviati solo quando almeno una stazione di gestione SNMP è specificata come host trapotato.

Il seguente comando aggiunge un nuovo host trapezoidale SNMPv3 denominato yyy.example.com con un utente USM noto:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

Il seguente comando aggiunge un host trapezoidale utilizzando l'indirizzo IPv6 dell'host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

## Comandi per la gestione di SNMP

È possibile utilizzare `system snmp` Comandi per gestire SNMP, trap e traphost. È possibile utilizzare `security` Comandi per gestire gli utenti SNMP per SVM. È possibile utilizzare `event` Comandi per gestire gli eventi relativi ai trap SNMP.

### Comandi per la configurazione di SNMP

Se si desidera...	Utilizzare questo comando...
Abilitare SNMP sul cluster	<pre>options -option-name snmp.enable -option-value on</pre> <p>Il servizio SNMP deve essere consentito in base alla policy firewall di gestione (mgmt). È possibile verificare se SNMP è consentito utilizzando il comando <code>show</code> del criterio firewall dei servizi di sistema.</p>
Disattivare SNMP sul cluster	<pre>options -option-name snmp.enable -option-value off</pre>

### Comandi per la gestione degli utenti SNMP v1, v2c e v3

Se si desidera...	Utilizzare questo comando...
Configurare gli utenti SNMP	<pre>security login create</pre>
Visualizzare gli utenti SNMP	<pre>security snmpusers and security login show -application snmp</pre>
Eliminare gli utenti SNMP	<pre>security login delete</pre>
Modificare il nome del ruolo di controllo dell'accesso di un metodo di accesso per gli utenti SNMP	<pre>security login modify</pre>

### Comandi per fornire informazioni di contatto e posizione

Se si desidera...	Utilizzare questo comando...
Visualizzare o modificare i dettagli di contatto del cluster	<pre>system snmp contact</pre>
Visualizzare o modificare i dettagli della posizione del cluster	<pre>system snmp location</pre>

## Comandi per la gestione delle community SNMP

Se si desidera...	Utilizzare questo comando...
Aggiungere una community di sola lettura (ro) per una SVM o per tutte le SVM nel cluster	<code>system snmp community add</code>
Eliminare una community o tutte le community	<code>system snmp community delete</code>
Visualizza l'elenco di tutte le community	<code>system snmp community show</code>

Poiché le SVM non fanno parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

## Comando per la visualizzazione dei valori delle opzioni SNMP

Se si desidera...	Utilizzare questo comando...
Visualizza i valori correnti di tutte le opzioni SNMP, inclusi il contatto del cluster, la posizione del contatto, se il cluster è configurato per l'invio di trap, l'elenco dei traphost, l'elenco delle community e il tipo di controllo degli accessi	<code>system snmp show</code>

## Comandi per la gestione di trap SNMP e traphosts

Se si desidera...	Utilizzare questo comando...
Abilitare i trap SNMP inviati dal cluster	<code>system snmp init -init 1</code>
Disattiva i trap SNMP inviati dal cluster	<code>system snmp init -init 0</code>
Aggiungere un host trapotato che riceve notifiche SNMP per eventi specifici nel cluster	<code>system snmp traphost add</code>
Eliminare un host trapezoidale	<code>system snmp traphost delete</code>
Visualizza l'elenco di traphosts	<code>system snmp traphost show</code>

## Comandi per la gestione degli eventi relativi ai trap SNMP

Se si desidera...	Utilizzare questo comando...
-------------------	------------------------------

Visualizza gli eventi per i quali vengono generati i trap SNMP (integrati)	<pre>event route show</pre> <p>Utilizzare <code>-snmp-support true</code> Parametro per visualizzare solo gli eventi relativi a SNMP.</p> <p>Utilizzare <code>instance -messagename &lt;message&gt;</code> parametro per visualizzare una descrizione dettagliata del motivo per cui si è verificato un evento e di eventuali azioni correttive.</p> <p>Il routing di singoli eventi trap SNMP a destinazioni host trapotate specifiche non è supportato. Tutti gli eventi trap SNMP vengono inviati a tutte le destinazioni dell'host trapotato.</p>
Visualizza un elenco di record della cronologia delle trap SNMP, che sono notifiche di eventi inviate alle trap SNMP	<pre>event snmphistory show</pre>
Eliminare un record di cronologia trap SNMP	<pre>event snmphistory delete</pre>

Per ulteriori informazioni su `system snmp`, `security`, e. event comandi, vedere le pagine man: ["Comandi di ONTAP 9"](#)

## Gestire il routing in una SVM

### Panoramica dell'instradamento delle SVM

La tabella di routing per una SVM determina il percorso di rete utilizzato dalla SVM per comunicare con una destinazione. È importante comprendere il funzionamento delle tabelle di routing in modo da prevenire i problemi di rete prima che si verifichino.

Le regole di routing sono le seguenti:

- ONTAP instrada il traffico sul percorso più specifico disponibile.
- ONTAP instrada il traffico su un percorso di gateway predefinito (con 0 bit di netmask) come ultima risorsa, quando non sono disponibili percorsi più specifici.

Nel caso di percorsi con la stessa destinazione, netmask e metrica, non vi è alcuna garanzia che il sistema utilizzi lo stesso percorso dopo un riavvio o un aggiornamento. Questo è un problema soprattutto se sono stati configurati più percorsi predefiniti.

Si consiglia di configurare un percorso predefinito solo per una SVM. Per evitare interruzioni, assicurarsi che il percorso predefinito sia in grado di raggiungere qualsiasi indirizzo di rete non raggiungibile da un percorso più specifico. Per ulteriori informazioni, consulta l'articolo della Knowledge base ["SU134: L'accesso alla rete potrebbe essere interrotto da una configurazione di routing errata in Clustered ONTAP"](#)



## Creare un percorso statico

È possibile creare percorsi statici all'interno di una macchina virtuale di storage (SVM) per controllare il modo in cui i LIF utilizzano la rete per il traffico in uscita.

Quando si crea una voce di percorso associata a una SVM, la route viene utilizzata da tutte le LIF di proprietà della SVM specificata e che si trovano sulla stessa sottorete del gateway.

### Fase

Utilizzare `network route create` per creare un percorso.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

## Abilitare il routing multipath

Se più percorsi hanno la stessa metrica per una destinazione, viene selezionato solo uno dei percorsi per il traffico in uscita. Ciò comporta la mancata utilizzo di altri percorsi per l'invio del traffico in uscita. È possibile abilitare il routing multipath per il bilanciamento del carico e utilizzare tutti i percorsi disponibili.

### Fasi

1. Accedere al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Abilita routing multipath:

```
network options multipath-routing modify -is-enabled true
```

Il routing multipath è abilitato per tutti i nodi nel cluster.

```
network options multipath-routing modify -is-enabled true
```

## Eliminare un percorso statico

È possibile eliminare un percorso statico non necessario da una SVM (Storage Virtual Machine).

### Fase

Utilizzare `network route delete` comando per eliminare un percorso statico.

Per ulteriori informazioni su questo comando, vedere `network route` pagina man: ["Comandi di ONTAP 9"](#).

Nell'esempio seguente viene eliminata una route statica associata a SVM vs0 con un gateway 10.63.0.1 e un indirizzo IP di destinazione 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

## Visualizzare le informazioni di routing

È possibile visualizzare informazioni sulla configurazione di routing per ogni SVM nel cluster. In questo modo è possibile diagnosticare i problemi di routing che comportano problemi di connettività tra applicazioni o servizi client e una LIF su un nodo del cluster.

### Fasi

1. Utilizzare `network route show` Comando per visualizzare i percorsi all'interno di una o più SVM. L'esempio seguente mostra un percorso configurato in SVM vs0:

```
network route show
(network route show)
Vserver          Destination      Gateway          Metric
-----
vs0
                0.0.0.0/0      172.17.178.1    20
```

2. Utilizzare `network route show-lifs` Comando per visualizzare l'associazione di route e LIF all'interno di una o più SVM.

L'esempio seguente mostra i file LIF con route di proprietà di vs0 SVM:

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        172.17.178.1    cluster_mgmt,
                  LIF-b-01_mgmt1,
                  LIF-b-02_mgmt1
```

3. Utilizzare `network route active-entry show` Comando per visualizzare i percorsi installati su uno o più nodi, SVM, subnet o percorsi con destinazioni specifiche.

L'esempio seguente mostra tutti i percorsi installati su una SVM specifica:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
```

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
127.0.0.1	127.0.0.1	lo	10	UHS
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-1

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
127.0.0.1	127.0.0.1	lo	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
-----	-----	-----	-----	-----
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC
fd20:8b1e:b255:814e::1	link#4	e0d	0	UHL

11 entries were displayed.

## Rimuovere i percorsi dinamici dalle tabelle di routing

Quando si ricevono i reindirizzamenti ICMP per IPv4 e IPv6, i percorsi dinamici vengono aggiunti alla tabella di routing. Per impostazione predefinita, i percorsi dinamici vengono rimossi dopo 300 secondi. Se si desidera mantenere percorsi dinamici per un periodo di tempo diverso, è possibile modificare il valore di timeout.

### A proposito di questa attività

È possibile impostare il valore di timeout da 0 a 65,535 secondi. Se si imposta il valore su 0, i percorsi non scadono mai. La rimozione di percorsi dinamici impedisce la perdita di connettività causata dalla persistenza di percorsi non validi.

### Fasi

1. Visualizza il valore di timeout corrente.

◦ Per IPv4:

```
network tuning icmp show
```

◦ Per IPv6:

```
network tuning icmp6 show
```

2. Modificare il valore di timeout.

◦ Per IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout  
timeout_value
```

◦ Per IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout  
timeout_value
```

3. Verificare che il valore di timeout sia stato modificato correttamente.

◦ Per IPv4:

```
network tuning icmp show
```

◦ Per IPv6:

```
network tuning icmp6 show
```

# Visualizzare le informazioni di rete

## Visualizzare la panoramica delle informazioni di rete

Utilizzando la CLI, puoi visualizzare informazioni relative a porte, LIF, percorsi, regole di failover, gruppi di failover, regole firewall, DNS, NIS e connessioni. A partire da ONTAP 9,8, è anche possibile scaricare i dati visualizzati in Gestione sistema relativi alla rete.

Queste informazioni possono essere utili in situazioni come la riconfigurazione delle impostazioni di rete o la risoluzione dei problemi del cluster.

Gli amministratori del cluster possono visualizzare tutte le informazioni di rete disponibili. Gli amministratori di SVM possono visualizzare solo le informazioni relative alle SVM assegnate.

In System Manager, quando si visualizzano le informazioni in una vista *List*, è possibile fare clic su **Download** e l'elenco degli oggetti visualizzati viene scaricato.

- L'elenco viene scaricato in formato CSV (comma-separated values).
- Vengono scaricati solo i dati nelle colonne visibili.
- Il nome del file CSV viene formattato con il nome dell'oggetto e l'indicazione dell'ora.

## Visualizza le informazioni sulla porta di rete

È possibile visualizzare informazioni su una porta specifica o su tutte le porte di tutti i nodi del cluster.

### A proposito di questa attività

Vengono visualizzate le seguenti informazioni:

- Nome del nodo
- Nome della porta
- Nome IPspace
- Nome di dominio di trasmissione
- Stato del collegamento (verso l'alto o verso il basso)
- Impostazione MTU
- Impostazione della velocità della porta e stato operativo (1 Gigabit o 10 Gigabit al secondo)
- Impostazione della negoziazione automatica (vero o falso)
- Modalità duplex e stato operativo (metà o pieno)
- Il gruppo di interfaccia della porta, se applicabile
- Le informazioni del tag VLAN della porta, se applicabile
- Lo stato di salute della porta (stato di salute o degradato)
- Motivi per cui una porta viene contrassegnata come degradata

Se i dati di un campo non sono disponibili (ad esempio, il duplex operativo e la velocità di una porta inattiva non sarebbero disponibili), il valore del campo viene elencato come –.

Fase

Visualizzare le informazioni sulla porta di rete utilizzando `network port show` comando.

È possibile visualizzare informazioni dettagliate per ciascuna porta specificando `-instance` o ottenere informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

```
network port show
Node: node1

Ignore
Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  degraded
false
e0d      Default      Default      up    1500  auto/1000  degraded
true
Node: node2

Ignore
Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  healthy
false
e0d      Default      Default      up    1500  auto/1000  healthy
false
8 entries were displayed.
```

## Visualizzazione delle informazioni su una VLAN (solo amministratori del cluster)

È possibile visualizzare informazioni su una VLAN specifica o su tutte le VLAN del cluster.

### A proposito di questa attività

È possibile visualizzare informazioni dettagliate per ciascuna VLAN specificando `-instance` parametro. È possibile visualizzare informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

### Fase

Visualizzare le informazioni sulle VLAN utilizzando `network port vlan show` comando. Il seguente comando visualizza le informazioni su tutte le VLAN nel cluster:

```
network port vlan show
```

Node	VLAN Name	Port	Network VLAN ID	Network MAC Address
cluster-1-01				
	a0a-10	a0a	10	02:a0:98:06:10:b2
	a0a-20	a0a	20	02:a0:98:06:10:b2
	a0a-30	a0a	30	02:a0:98:06:10:b2
	a0a-40	a0a	40	02:a0:98:06:10:b2
	a0a-50	a0a	50	02:a0:98:06:10:b2
cluster-1-02				
	a0a-10	a0a	10	02:a0:98:06:10:ca
	a0a-20	a0a	20	02:a0:98:06:10:ca
	a0a-30	a0a	30	02:a0:98:06:10:ca
	a0a-40	a0a	40	02:a0:98:06:10:ca
	a0a-50	a0a	50	02:a0:98:06:10:ca

## Visualizza informazioni sul gruppo di interfacce (solo amministratori del cluster)

È possibile visualizzare informazioni su un gruppo di interfacce per determinarne la configurazione.

### A proposito di questa attività

Vengono visualizzate le seguenti informazioni:

- Nodo su cui si trova il gruppo di interfacce
- Elenco delle porte di rete incluse nel gruppo di interfacce
- Nome del gruppo di interfacce
- Funzione di distribuzione (MAC, IP, porta o sequenziale)
- Indirizzo MAC (Media Access Control) del gruppo di interfacce
- Stato di attività della porta, ovvero se tutte le porte aggregate sono attive (partecipazione completa), se alcune sono attive (partecipazione parziale) o se nessuna è attiva

## Fase

Visualizzare le informazioni sui gruppi di interfacce utilizzando `network port ifgrp show` comando.

È possibile visualizzare informazioni dettagliate per ciascun nodo specificando `-instance` parametro. È possibile visualizzare informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

Il seguente comando visualizza le informazioni relative a tutti i gruppi di interfacce nel cluster:

```
network port ifgrp show
```

Node	Port IfGrp	Distribution Function	MAC Address	Active Ports	Ports
cluster-1-01	a0a	ip	02:a0:98:06:10:b2	full	e7a, e7b
cluster-1-02	a0a	sequential	02:a0:98:06:10:ca	full	e7a, e7b
cluster-1-03	a0a	port	02:a0:98:08:5b:66	full	e7a, e7b
cluster-1-04	a0a	mac	02:a0:98:08:61:4e	full	e7a, e7b

Il seguente comando visualizza informazioni dettagliate sul gruppo di interfacce per un singolo nodo:

```
network port ifgrp show -instance -node cluster-1-01
```

```
Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
Create Policy: multimode
MAC Address: 02:a0:98:06:10:b2
Port Participation: full
Network Ports: e7a, e7b
Up Ports: e7a, e7b
Down Ports: -
```

## Visualizzare le informazioni LIF

È possibile visualizzare informazioni dettagliate su una LIF per determinarne la configurazione.

È inoltre possibile visualizzare queste informazioni per diagnosticare i problemi LIF di base, ad esempio la ricerca di indirizzi IP duplicati o la verifica dell'appartenenza della porta di rete alla subnet corretta. Gli amministratori delle macchine virtuali di storage (SVM) possono visualizzare solo le informazioni relative alle LIF associate a SVM.

### A proposito di questa attività



Vengono visualizzate le seguenti informazioni:

- Indirizzo IP associato al LIF
- Stato amministrativo della LIF
- Stato operativo del LIF

Lo stato operativo delle LIF dei dati è determinato dallo stato delle SVM a cui sono associate le LIF dei dati. Quando la SVM viene arrestata, lo stato operativo della LIF diventa inattivo. Quando SVM viene riavviato, lo stato operativo diventa up

- E la porta su cui risiede LIF

Se i dati di un campo non sono disponibili (ad esempio, se non sono presenti informazioni estese sullo stato), il valore del campo viene elencato come –.

### **Fase**

Visualizzare le informazioni LIF utilizzando il comando show dell'interfaccia di rete.

È possibile visualizzare informazioni dettagliate per ciascun LIF specificando il parametro -instance oppure ottenere informazioni specifiche specificando i nomi dei campi utilizzando il parametro -fields.

Il seguente comando visualizza informazioni generali su tutte le LIF in un cluster:

# network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
example					
	lif1	up/up	192.0.2.129/22	node-01	e0d
false					
node	cluster_mgmt	up/up	192.0.2.3/20	node-02	e0c
false					
node-01	clus1	up/up	192.0.2.65/18	node-01	e0a
true					
	clus2	up/up	192.0.2.66/18	node-01	e0b
true					
	mgmt1	up/up	192.0.2.1/20	node-01	e0c
true					
node-02	clus1	up/up	192.0.2.67/18	node-02	e0a
true					
	clus2	up/up	192.0.2.68/18	node-02	e0b
true					
	mgmt2	up/up	192.0.2.2/20	node-02	e0d
true					
vs1	d1	up/up	192.0.2.130/21	node-01	e0d
false					
	d2	up/up	192.0.2.131/21	node-01	e0d
true					
	data3	up/up	192.0.2.132/20	node-02	e0c
true					

Il seguente comando mostra informazioni dettagliate su una singola LIF:

```
network interface show -lif data1 -instance

Vserver Name: vs1
Logical Interface Name: data1
Role: data
Data Protocol: nfs,cifs
Home Node: node-01
Home Port: e0c
Current Node: node-03
Current Port: e0c
Operational Status: up
Extended Status: -
Is Home: false
Network Address: 192.0.2.128
Netmask: 255.255.192.0
Bits in the Netmask: 18
IPv4 Link Local: -
Subnet Name: -
Administrative Status: up
Failover Policy: local-only
Firewall Policy: data
Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
Failover Group Name: Default
FCP WWPN: -
Address family: ipv4
Comment: -
IPspace of LIF: Default
```

Visualizzare le informazioni di routing

È possibile visualizzare informazioni sui percorsi all'interno di una SVM.

Fase

A seconda del tipo di informazioni di routing che si desidera visualizzare, immettere il comando appropriato:

Per visualizzare informazioni su...	Inserisci...
Percorsi statici, per SVM	network route show
LIF su ogni percorso, per SVM	network route show-lifs

È possibile visualizzare informazioni dettagliate per ciascun percorso specificando `-instance` parametro. Il seguente comando visualizza i percorsi statici all'interno delle SVM nel cluster 1:

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
0.0.0.0/0        10.63.0.1       10
cluster-1
0.0.0.0/0        198.51.9.1      10
vs1
0.0.0.0/0        192.0.2.1       20
vs3
0.0.0.0/0        192.0.2.1       20
```

Il seguente comando visualizza l'associazione di route statiche e interfacce logiche (LIFF) in tutte le SVM nel cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1       -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1      cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data2_1, data2_2
```

## Visualizzare le voci della tabella degli host DNS (solo amministratori del cluster)

Le voci della tabella host DNS associano i nomi host agli indirizzi IP. È possibile visualizzare i nomi host, gli alias e l'indirizzo IP a cui mappano tutte le SVM in un cluster.

## Fase

Visualizzare le voci del nome host per tutte le SVM utilizzando il comando `show` degli host dns dei servizi vserver.

Nell'esempio seguente vengono visualizzate le voci della tabella host:

```
vserver services name-service dns hosts show
Vserver      Address      Hostname      Aliases
-----
cluster-1
10.72.219.36  lnx219-36    -
vs1
10.72.219.37  lnx219-37    lnx219-37.example.com
```

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host vengono risolti utilizzando server DNS esterni.

## Visualizzare le configurazioni del dominio DNS

È possibile visualizzare la configurazione del dominio DNS di una o più macchine virtuali di storage (SVM) nel cluster per verificare che sia configurata correttamente.

## Fase

Visualizzazione delle configurazioni del dominio DNS mediante `vserver services name-service dns show` comando.

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
Vserver      State      Domains      Name
-----
cluster-1    enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs1          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs2          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs3          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
```

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1
      Vserver: vs1
      Domains: xyz.company.com
      Name Servers: 192.56.0.129, 192.56.0.130
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

## Visualizzare le informazioni sui gruppi di failover

È possibile visualizzare informazioni sui gruppi di failover, tra cui l'elenco di nodi e porte in ciascun gruppo di failover, se il failover è attivato o disattivato e il tipo di policy di failover che viene applicata a ciascuna LIF.

### Fasi

1. Visualizzare le porte di destinazione per ciascun gruppo di failover utilizzando `network interface failover-groups show` comando.

Il seguente comando visualizza le informazioni su tutti i gruppi di failover su un cluster a due nodi:

```
network interface failover-groups show
```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster1-01:e0a, cluster1-01:e0b, cluster1-02:e0a, cluster1-02:e0b
vs1	Default	cluster1-01:e0c, cluster1-01:e0d, cluster1-01:e0e, cluster1-02:e0c, cluster1-02:e0d, cluster1-02:e0e

2. Visualizzare le porte di destinazione e il dominio di trasmissione per uno specifico gruppo di failover utilizzando `network interface failover-groups show` comando.

Il seguente comando visualizza informazioni dettagliate sui dati del gruppo di failover 12 per SVM vs4:

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. Visualizzare le impostazioni di failover utilizzate da tutti i file LIF utilizzando `network interface show` comando.

Il seguente comando visualizza il criterio di failover e il gruppo di failover utilizzati da ciascun LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver    lif                failover-policy    failover-group
-----
Cluster    cluster1-01_clus_1    local-only         Cluster
Cluster    cluster1-01_clus_2    local-only         Cluster
Cluster    cluster1-02_clus_1    local-only         Cluster
Cluster    cluster1-02_clus_2    local-only         Cluster
cluster1    cluster_mgmt          broadcast-domain-wide Default
cluster1    cluster1-01_mgmt1     local-only         Default
cluster1    cluster1-02_mgmt1     local-only         Default
vs1         data1                 disabled           Default
vs3         data2                 system-defined     group2
```

## Visualizzare le destinazioni di failover LIF

Potrebbe essere necessario controllare se i criteri di failover e i gruppi di failover di una LIF sono configurati correttamente. Per evitare una configurazione errata delle regole di failover, è possibile visualizzare le destinazioni di failover per una singola LIF o per tutte le LIF.

### A proposito di questa attività

La visualizzazione delle destinazioni di failover LIF consente di verificare quanto segue:

- Se le LIF sono configurate con il gruppo di failover e la policy di failover corretti
- Se l'elenco risultante di porte di destinazione di failover è appropriato per ogni LIF
- Se la destinazione di failover di una LIF dati non è una porta di gestione (e0M)

### Fase

Visualizzare le destinazioni di failover di una LIF utilizzando `failover` opzione di `network interface`

show comando.

Il seguente comando visualizza le informazioni sulle destinazioni di failover per tutte le LIF in un cluster a due nodi. Il Failover Targets Riga mostra l'elenco (con priorità) delle combinazioni nodo-porta per un dato LIF.

```
network interface show -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
Cluster				
	node1_clus1	node1:e0a	local-only	Cluster
		Failover Targets: node1:e0a, node1:e0b		
	node1_clus2	node1:e0b	local-only	Cluster
		Failover Targets: node1:e0b, node1:e0a		
	node2_clus1	node2:e0a	local-only	Cluster
		Failover Targets: node2:e0a, node2:e0b		
	node2_clus2	node2:e0b	local-only	Cluster
		Failover Targets: node2:e0b, node2:e0a		
cluster1				
	cluster_mgmt	node1:e0c	broadcast-domain-wide	Default
		Failover Targets: node1:e0c, node1:e0d, node2:e0c, node2:e0d		
	node1_mgmt1	node1:e0c	local-only	Default
		Failover Targets: node1:e0c, node1:e0d		
	node2_mgmt1	node2:e0c	local-only	Default
		Failover Targets: node2:e0c, node2:e0d		
vs1				
	data1	node1:e0e	system-defined	bcast1
		Failover Targets: node1:e0e, node1:e0f, node2:e0e, node2:e0f		

## Visualizzare i LIF in una zona di bilanciamento del carico

È possibile verificare se una zona di bilanciamento del carico è configurata correttamente visualizzando tutte le LIF ad essa associate. È inoltre possibile visualizzare la zona di



bilanciamento del carico di una LIF specifica o le zone di bilanciamento del carico per tutte le LIF.

Fase

Visualizzare i LIF e i dettagli del bilanciamento del carico desiderati utilizzando uno dei seguenti comandi

Per visualizzare...	Inserisci...
LIF in una particolare zona di bilanciamento del carico	<code>network interface show -dns-zone zone_name</code>  <code>zone_name</code> specifica il nome della zona di bilanciamento del carico.
La zona di bilanciamento del carico di una LIF specifica	<code>network interface show -lif lif_name -fields dns-zone</code>
Le zone di bilanciamento del carico di tutte le LIF	<code>network interface show -fields dns-zone</code>

Esempi di visualizzazione delle zone di bilanciamento del carico per le LIF

Il seguente comando visualizza i dettagli di tutte le LIF nella zona di bilanciamento del carico `storage.company.com` per SVM `vs0`:

```
net int show -vserver vs0 -dns-zone storage.company.com
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	lif3	up/up	10.98.226.225/20	ndeux-11	e0c	true
	lif4	up/up	10.98.224.23/20	ndeux-21	e0c	true
	lif5	up/up	10.98.239.65/20	ndeux-11	e0c	true
	lif6	up/up	10.98.239.66/20	ndeux-11	e0c	true
	lif7	up/up	10.98.239.63/20	ndeux-21	e0c	true
	lif8	up/up	10.98.239.64/20	ndeux-21	e0c	true

Il seguente comando visualizza i dettagli della zona DNS dei dati LIF 3:

```
network interface show -lif data3 -fields dns-zone
```

Vserver	lif	dns-zone
vs0	data3	storage.company.com

Il seguente comando visualizza l'elenco di tutte le LIF del cluster e delle relative zone DNS:

```
network interface show -fields dns-zone
Vserver    lif          dns-zone
-----
cluster    cluster_mgmt none
ndeux-21   clus1        none
ndeux-21   clus2        none
ndeux-21   mgmt1        none
vs0        data1         storage.company.com
vs0        data2         storage.company.com
```

## Visualizzare le connessioni del cluster

È possibile visualizzare tutte le connessioni attive nel cluster o un numero di connessioni attive sul nodo in base al client, all'interfaccia logica, al protocollo o al servizio. È inoltre possibile visualizzare tutte le connessioni in ascolto nel cluster.

### Visualizza le connessioni attive per client (solo amministratori del cluster)

È possibile visualizzare le connessioni attive per client per verificare il nodo utilizzato da un client specifico e per visualizzare eventuali squilibri tra i conteggi dei client per nodo.

#### A proposito di questa attività

Il numero di connessioni attive per client è utile nei seguenti scenari:

- Ricerca di un nodo occupato o sovraccarico.
- Determinare il motivo per cui l'accesso di un determinato client a un volume è lento.

È possibile visualizzare i dettagli sul nodo a cui il client sta accedendo e confrontarlo con il nodo su cui risiede il volume. Se l'accesso al volume richiede l'attraversamento della rete del cluster, i client potrebbero riscontrare una riduzione delle performance a causa dell'accesso remoto al volume su un nodo remoto oversubsd.

- Verificare che tutti i nodi siano utilizzati allo stesso modo per l'accesso ai dati.
- Ricerca di client con un numero inaspettatamente elevato di connessioni.
- Verificare se alcuni client dispongono di connessioni a un nodo.

#### Fase

Visualizzare il numero delle connessioni attive per client su un nodo utilizzando `network connections active show-clients` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster        192.10.2.124            5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster        192.10.2.123            4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster        192.10.2.122            4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster        192.10.2.121            4

```

### Visualizzazione delle connessioni attive in base al protocollo (solo amministratori del cluster)

È possibile visualizzare un numero di connessioni attive in base al protocollo (TCP o UDP) su un nodo per confrontare l'utilizzo dei protocolli all'interno del cluster.

#### A proposito di questa attività

Il numero di connessioni attive per protocollo è utile nei seguenti scenari:

- Individuazione dei client UDP che perdono la connessione.

Se un nodo si trova vicino al limite di connessione, i client UDP sono i primi a essere ignorati.

- Verificare che non vengano utilizzati altri protocolli.

#### Fase

Visualizzare il numero delle connessioni attive in base al protocollo su un nodo utilizzando `network connections active show-protocols` comando.

Per ulteriori informazioni su questo comando, vedere la pagina `man`.

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
      vs0      UDP      19
      Cluster  TCP      11
node1
      vs0      UDP      17
      Cluster  TCP       8
node2
      vs1      UDP      14
      Cluster  TCP      10
node3
      vs1      UDP      18
      Cluster  TCP       4

```

### Visualizzazione delle connessioni attive per servizio (solo amministratori del cluster)

È possibile visualizzare un numero di connessioni attive in base al tipo di servizio (ad esempio, per NFS, SMB, mount e così via) per ciascun nodo di un cluster. Ciò è utile per confrontare l'utilizzo dei servizi all'interno del cluster, che consente di determinare il carico di lavoro primario di un nodo.

#### A proposito di questa attività

Il numero di connessioni attive per servizio è utile nei seguenti scenari:

- Verifica dell'utilizzo di tutti i nodi per i servizi appropriati e del corretto funzionamento del bilanciamento del carico per tale servizio.
- Verificare che non vengano utilizzati altri servizi. Visualizzare il numero delle connessioni attive per servizio su un nodo utilizzando `network connections active show-services` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-services
Node      Vserver Name      Service      Count
-----
node0
    vs0          mount          3
    vs0          nfs            14
    vs0          nlm_v4         4
    vs0          cifs_srv       3
    vs0          port_map       18
    vs0          rclopcp        27
    Cluster      ctlopcp        60
node1
    vs0          cifs_srv       3
    vs0          rclopcp        16
    Cluster      ctlopcp        60
node2
    vs1          rclopcp        13
    Cluster      ctlopcp        60
node3
    vs1          cifs_srv       1
    vs1          rclopcp        17
    Cluster      ctlopcp        60

```

### Visualizza le connessioni attive per LIF su un nodo e SVM

È possibile visualizzare un numero di connessioni attive per ciascuna LIF, per nodo e SVM (Storage Virtual Machine), per visualizzare gli squilibri di connessione tra le LIF all'interno del cluster.

#### A proposito di questa attività

Il numero di connessioni attive per LIF è utile nei seguenti scenari:

- Trovare un LIF sovraccarico confrontando il numero di connessioni su ciascun LIF.
- Verifica del corretto funzionamento del bilanciamento del carico DNS per tutti i file LIF dei dati.
- Confrontando il numero di connessioni con le varie SVM per individuare le SVM più utilizzate.

#### Fase

Visualizzare un numero di connessioni attive per ciascun LIF in base a SVM e nodo utilizzando `network connections active show-lifs` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    Cluster    node0_clus_1    6
    Cluster    node0_clus_2    5
node1
    vs0        datalif2        3
    Cluster    node1_clus_1    3
    Cluster    node1_clus_2    5
node2
    vs1        datalif2        1
    Cluster    node2_clus_1    5
    Cluster    node2_clus_2    3
node3
    vs1        datalif1        1
    Cluster    node3_clus_1    2
    Cluster    node3_clus_2    2

```

## Visualizzare le connessioni attive in un cluster

È possibile visualizzare informazioni sulle connessioni attive in un cluster per visualizzare LIF, porta, host remoto, servizio, macchine virtuali di storage (SVM) e protocollo utilizzati dalle singole connessioni.

### A proposito di questa attività

La visualizzazione delle connessioni attive in un cluster è utile nei seguenti scenari:

- Verificare che i singoli client utilizzino il protocollo e il servizio corretti sul nodo corretto.
- Se un client ha problemi ad accedere ai dati utilizzando una determinata combinazione di nodo, protocollo e servizio, è possibile utilizzare questo comando per trovare un client simile per la configurazione o il confronto delle tracce dei pacchetti.

### Fase

Visualizzare le connessioni attive in un cluster utilizzando `network connections active show` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

Il seguente comando mostra le connessioni attive sul nodo node1:

```
network connections active show -node node1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
Cluster	node1_clus_1:50297	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:13387	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:8340	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:42766	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:36119	192.0.2.250:7700	TCP/ctlopcp
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs3	data2:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map
vs3	data2:111	host1.aa.com:12017	UDP/port-map

Il seguente comando mostra le connessioni attive su SVM vs1:

```
network connections active show -vserver vs1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map

## Visualizzare le connessioni in ascolto in un cluster

È possibile visualizzare le informazioni relative alle connessioni in ascolto in un cluster per visualizzare le LIF e le porte che accettano le connessioni per un determinato protocollo e servizio.

### A proposito di questa attività

La visualizzazione delle connessioni in ascolto in un cluster è utile nei seguenti scenari:

- Verificare che il protocollo o il servizio desiderato sia in ascolto su una LIF se le connessioni del client a tale LIF non riescono in modo coerente.
- Verifica dell'apertura di un listener UDP/rclopcp in ogni LIF del cluster in caso di errore dell'accesso remoto ai dati di un volume su un nodo tramite LIF su un altro nodo.
- Verifica dell'apertura di un listener UDP/rclopcp in ogni LIF del cluster se i trasferimenti SnapMirror tra due nodi nello stesso cluster non funzionano.
- Verifica dell'apertura di un listener TCP/ctlopcp in ogni LIF di intercluster se i trasferimenti SnapMirror tra due nodi in cluster diversi non riescono.

### Fase

Visualizzare le connessioni in ascolto per nodo utilizzando `network connections listening show` comando.

```

network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700              TCP/ctlopcp
vs1               data1:4049                    UDP/unknown
vs1               data1:111                     TCP/port-map
vs1               data1:111                     UDP/port-map
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:2049                    TCP/nfs
vs1               data1:2049                    UDP/nfs
vs1               data1:635                     TCP/mount
vs1               data1:635                     UDP/mount
Cluster           node0_clus_2:7700              TCP/ctlopcp

```

## Comandi per la diagnosi dei problemi di rete

È possibile diagnosticare i problemi sulla rete utilizzando comandi come `ping`, `traceroute`, `ndp`, e `tcpdump`. È inoltre possibile utilizzare comandi come `ping6` e `traceroute6` Per diagnosticare i problemi IPv6.

Se si desidera...	Immettere questo comando...
Verificare se il nodo può raggiungere altri host sulla rete	<code>network ping</code>
Verificare se il nodo può raggiungere altri host sulla rete IPv6	<code>network ping6</code>
Tracciare il percorso che i pacchetti IPv4 portano a un nodo di rete	<code>network traceroute</code>
Tracciare il percorso che i pacchetti IPv6 portano a un nodo di rete	<code>network traceroute6</code>
Gestire il protocollo NDP (Neighbor Discovery Protocol)	<code>network ndp</code>
Visualizza le statistiche relative ai pacchetti ricevuti e inviati su un'interfaccia di rete specifica o su tutte le interfacce di rete	<code>run -node <i>node_name</i> ifstat</code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Visualizza le informazioni sui dispositivi vicini rilevati da ciascun nodo e porta del cluster, inclusi il tipo di dispositivo remoto e la piattaforma del dispositivo	<code>network device-discovery show</code>



Visualizzare i CDP vicini al nodo (ONTAP supporta solo annunci CDPv1)	<code>run -node <i>node_name</i> cdpd show-neighbors</code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Tracciare i pacchetti inviati e ricevuti nella rete	<code>network tcpdump start -node <i>node-name</i> -port <i>port_name</i></code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Misurare la latenza e il throughput tra nodi intercluster o intracluster	<code>`network test -path -source-node <i>source_nodename</i> local -destination-cluster <i>destination_clustername</i> -destination-node <i>destination_nodename</i> -session -type <i>Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</i></code> Per ulteriori informazioni, consultare <a href="#">"Gestione delle performance"</a> .

Per ulteriori informazioni su questi comandi, consulta le pagine man appropriate: ["Comandi di ONTAP 9"](#)

## Visualizzare la connettività di rete con i protocolli di rilevamento neighbor

### Visualizzare la connettività di rete con i protocolli di rilevamento neighbor

In un data center, è possibile utilizzare i protocolli neighbor Discovery per visualizzare la connettività di rete tra una coppia di sistemi fisici o virtuali e le relative interfacce di rete. ONTAP supporta due protocolli di rilevamento neighbor: Protocollo di rilevamento Cisco (CDP) e protocollo di rilevamento link Layer (LLDP).

I protocolli neighbor Discovery consentono di rilevare e visualizzare automaticamente informazioni sui dispositivi abilitati al protocollo collegati direttamente in una rete. Ogni dispositivo comunica informazioni di identificazione, funzionalità e connettività. Queste informazioni vengono trasmesse in frame Ethernet a un indirizzo MAC multicast e vengono ricevute da tutti i dispositivi abilitati per il protocollo vicini.

Affinché due dispositivi diventino vicini, ciascuno deve avere un protocollo abilitato e configurato correttamente. La funzionalità del protocollo di rilevamento è limitata alle reti direttamente connesse. I dispositivi adiacenti possono includere dispositivi abilitati al protocollo, come switch, router, bridge e così via. ONTAP supporta due protocolli di rilevamento neighbor, che possono essere utilizzati singolarmente o insieme.

### Cisco Discovery Protocol (CDP)

CDP è un protocollo di link Layer proprietario sviluppato da Cisco Systems. È attivato per impostazione predefinita in ONTAP per le porte del cluster, ma deve essere attivato esplicitamente per le porte dati.

### Link Layer Discovery Protocol (LLDP)

LLDP è un protocollo indipendente dal vendor specificato nel documento standard IEEE 802.1AB. Deve essere attivato esplicitamente per tutte le porte.

### Utilizzare CDP per rilevare la connettività di rete

L'utilizzo di CDP per rilevare la connettività di rete consiste nell'esaminare le considerazioni di implementazione, abilitarla sulle porte dati, visualizzare i dispositivi adiacenti e regolare i valori di configurazione CDP in base alle necessità. CDP è attivato per impostazione predefinita sulle porte del cluster.

Per poter visualizzare le informazioni relative ai dispositivi adiacenti, è necessario abilitare il protocollo CDP anche su switch e router.

Release di ONTAP	Descrizione
9.10.1 e versioni precedenti	Il CDP viene utilizzato anche dal monitor di stato dello switch del cluster per rilevare automaticamente gli switch del cluster e della rete di gestione.
9.11.1 e versioni successive	Il CDP viene utilizzato anche dal monitor di stato dello switch del cluster per rilevare automaticamente gli switch di cluster, storage e rete di gestione.

### Informazioni correlate

["Amministrazione del sistema"](#)

### Considerazioni sull'utilizzo di CDP

Per impostazione predefinita, i dispositivi compatibili con CDP inviano annunci CDPv2. I dispositivi conformi a CDP inviano annunci CDPv1 solo quando ricevono annunci CDPv1. ONTAP supporta solo CDPv1. Pertanto, quando un nodo ONTAP invia annunci CDPv1, i dispositivi adiacenti conformi a CDP restituiscono annunci CDPv1.

Prima di attivare CDP su un nodo, è necessario prendere in considerazione le seguenti informazioni:

- CDP è supportato per tutte le porte.
- Gli annunci CDP vengono inviati e ricevuti dalle porte in stato attivo.
- Per inviare e ricevere annunci CDP, è necessario attivare CDP sia sui dispositivi trasmittenti che su quelli riceventi.
- Gli annunci CDP vengono inviati a intervalli regolari ed è possibile configurare l'intervallo di tempo.
- Quando gli indirizzi IP vengono modificati per un LIF, il nodo invia le informazioni aggiornate nel successivo annuncio CDP.
- ONTAP 9.10.1 e versioni precedenti:
  - CDP è sempre attivato sulle porte del cluster.
  - CDP è disattivato, per impostazione predefinita, su tutte le porte non cluster.
- ONTAP 9.11.1 e versioni successive:
  - CDP è sempre abilitato sulle porte del cluster e dello storage.
  - CDP è disattivato, per impostazione predefinita, su tutte le porte non cluster e non storage.



A volte, quando i LIF vengono modificati sul nodo, le informazioni CDP non vengono aggiornate sul lato del dispositivo ricevente (ad esempio, uno switch). In caso di problemi di questo tipo, configurare l'interfaccia di rete del nodo sullo stato inattivo e quindi su.

- Solo gli indirizzi IPv4 vengono pubblicizzati negli annunci CDP.
- Per le porte di rete fisiche con VLAN, vengono annunciate tutte le LIF configurate sulle VLAN su tale porta.
- Per le porte fisiche che fanno parte di un gruppo di interfacce, tutti gli indirizzi IP configurati su quel gruppo di interfacce vengono annunciati su ciascuna porta fisica.
- Per un gruppo di interfacce che ospita VLAN, tutte le LIF configurate sul gruppo di interfacce e le VLAN vengono pubblicizzate su ciascuna porta di rete.

- Poiché i pacchetti CDP sono limitati a non più di 1500 byte, sulle porte configurate con un elevato numero di LIF è possibile che sullo switch adiacente venga riportato solo un sottoinsieme di questi indirizzi IP.

### Attiva o disattiva CDP

Per rilevare e inviare annunci pubblicitari a dispositivi adiacenti conformi a CDP, è necessario attivare CDP su ciascun nodo del cluster.

Per impostazione predefinita in ONTAP 9.10.1 e versioni precedenti, CDP è attivato su tutte le porte cluster di un nodo e disattivato su tutte le porte non cluster di un nodo.

Per impostazione predefinita, in ONTAP 9.11.1 e versioni successive, CDP viene attivato su tutte le porte di cluster e storage di un nodo e disattivato su tutte le porte non di cluster e non di storage di un nodo.

### A proposito di questa attività

Il `cdpd.enable` L'opzione controlla se CDP è attivato o disattivato sulle porte di un nodo:

- Per ONTAP 9.10.1 e versioni precedenti, ON attiva CDP su porte non cluster.
- Per ONTAP 9.11.1 e versioni successive, on attiva CDP su porte non cluster e non storage.
- Per ONTAP 9.10.1 e versioni precedenti, Off disattiva il CDP sulle porte non cluster; non è possibile disattivare il CDP sulle porte cluster.
- Per ONTAP 9.11.1 e versioni successive, Off disattiva il CDP sulle porte non cluster e non storage; non è possibile disattivare il CDP sulle porte cluster.

Quando CDP è disattivato su una porta collegata a un dispositivo conforme a CDP, il traffico di rete potrebbe non essere ottimizzato.

### Fasi

1. Visualizza l'impostazione CDP corrente per un nodo o per tutti i nodi di un cluster:

Per visualizzare l'impostazione CDP di...	Inserisci...
Un nodo	<code>run - node &lt;node_name&gt; options cdpd.enable</code>
Tutti i nodi di un cluster	<code>options cdpd.enable</code>

2. Abilitare o disabilitare CDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per attivare o disattivare CDP on...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.enable {on or off}</code>
Tutti i nodi di un cluster	<code>options cdpd.enable {on or off}</code>

### Visualizzare le informazioni CDP neighbor

È possibile visualizzare informazioni sui dispositivi vicini collegati a ciascuna porta dei nodi del cluster, a

condizione che la porta sia collegata a un dispositivo conforme a CDP. È possibile utilizzare `network device-discovery show -protocol cdp` per visualizzare le informazioni sui vicini.

### A proposito di questa attività

In ONTAP 9.10.1 e versioni precedenti, poiché CDP è sempre abilitato per le porte del cluster, le informazioni CDP neighbor vengono sempre visualizzate per tali porte. Il CDP deve essere attivato sulle porte non del cluster per visualizzare le informazioni sulle porte vicine.

In ONTAP 9.11.1 e versioni successive, poiché CDP è sempre abilitato per le porte del cluster e dello storage, le informazioni relative alle porte CDP adiacenti vengono sempre visualizzate per tali porte. Il CDP deve essere attivato sulle porte non cluster e non storage per visualizzare le informazioni sulle porte vicine.

### Fase

Visualizza informazioni su tutti i dispositivi compatibili con CDP collegati alle porte di un nodo del cluster:

```
network device-discovery show -node node -protocol cdp
```

Il seguente comando mostra i vicini collegati alle porte sul nodo sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local   Discovered
Protocol      Port    Device (LLDP: ChassisID)  Interface      Platform
-----
sti2650-212/cdp
              e0M     RTP-LF810-510K37.gdl.eng.netapp.com (SAL1942R8JS)
                                   Ethernet1/14    N9K-
C93120TX
              e0a     CS:RTP-CS01-510K35        0/8            CN1610
              e0b     CS:RTP-CS01-510K36        0/8            CN1610
              e0c     RTP-LF350-510K34.gdl.eng.netapp.com (FDO21521S76)
                                   Ethernet1/21    N9K-
C93180YC-FX
              e0d     RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/22    N9K-
C93180YC-FX
              e0e     RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/23    N9K-
C93180YC-FX
              e0f     RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/24    N9K-
C93180YC-FX
```

L'output elenca i dispositivi Cisco collegati a ciascuna porta del nodo specificato.

## Configurare il tempo di attesa per i messaggi CDP

Il tempo di attesa è il periodo di tempo durante il quale gli annunci CDP vengono memorizzati nella cache nelle periferiche compatibili con CDP adiacenti. Il tempo di attesa viene pubblicizzato in ciascun pacchetto CDPv1 e viene aggiornato ogni volta che un pacchetto CDPv1 viene ricevuto da un nodo.

- Il valore di `cdpd.holdtime` L'opzione deve essere impostata sullo stesso valore su entrambi i nodi di una coppia ha.
- Il valore predefinito del tempo di attesa è 180 secondi, ma è possibile immettere valori compresi tra 10 secondi e 255 secondi.
- Se un indirizzo IP viene rimosso prima della scadenza del tempo di attesa, le informazioni CDP vengono memorizzate nella cache fino alla scadenza del tempo di attesa.

### Fasi

1. Visualizza il tempo di attesa CDP corrente per un nodo o per tutti i nodi di un cluster:

Per visualizzare il tempo di attesa di...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.holdtime</code>
Tutti i nodi di un cluster	<code>options cdpd.holdtime</code>

2. Configurare il tempo di attesa CDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per impostare il tempo di attesa su...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.holdtime holdtime</code>
Tutti i nodi di un cluster	<code>options cdpd.holdtime holdtime</code>

## Impostare l'intervallo per l'invio di annunci CDP

Gli annunci CDP vengono inviati ai vicini CDP a intervalli periodici. È possibile aumentare o ridurre l'intervallo per l'invio di annunci CDP in base al traffico di rete e alle modifiche della topologia di rete.

- Il valore di `cdpd.interval` L'opzione deve essere impostata sullo stesso valore su entrambi i nodi di una coppia ha.
- L'intervallo predefinito è 60 secondi, ma è possibile immettere un valore compreso tra 5 secondi e 900 secondi.

### Fasi

1. Visualizza l'intervallo di tempo corrente per l'annuncio CDP per un nodo o per tutti i nodi di un cluster:

Per visualizzare l'intervallo per...	Inserisci...
--------------------------------------	--------------

Un nodo	<code>run -node node_name options cdpd.interval</code>
Tutti i nodi di un cluster	<code>options cdpd.interval</code>

2. Configurare l'intervallo per l'invio di annunci CDP per tutte le porte di un nodo o per tutte le porte di tutti i nodi di un cluster:

Per impostare l'intervallo per...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.interval interval</code>
Tutti i nodi di un cluster	<code>options cdpd.interval interval</code>

### Visualizzare o cancellare le statistiche CDP

È possibile visualizzare le statistiche CDP per il cluster e le porte non del cluster su ciascun nodo per rilevare potenziali problemi di connettività di rete. Le statistiche CDP sono cumulative rispetto all'ultima cancellazione.

#### A proposito di questa attività

In ONTAP 9.10.1 e versioni precedenti, poiché CDP è sempre abilitato per le porte, le statistiche CDP vengono sempre visualizzate per il traffico su tali porte. Il CDP deve essere attivato sulle porte per visualizzare le statistiche relative a tali porte.

In ONTAP 9.11.1 e versioni successive, poiché CDP è sempre abilitato per le porte di cluster e storage, le statistiche CDP vengono sempre visualizzate per il traffico su tali porte. Il CDP deve essere attivato su porte non cluster o non storage per visualizzare le statistiche relative a tali porte.

#### Fase

Visualizzare o cancellare le statistiche CDP correnti per tutte le porte su un nodo:

Se si desidera...	Inserisci...
Visualizzare le statistiche CDP	<code>run -node node_name cdpd show-stats</code>
Cancellare le statistiche CDP	<code>run -node node_name cdpd zero-stats</code>

### Esempio di visualizzazione e cancellazione delle statistiche

Il comando seguente mostra le statistiche CDP prima che vengano cancellate. L'output visualizza il numero totale di pacchetti inviati e ricevuti dall'ultima cancellazione delle statistiche.

```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	9116	Csum Errors:	0	Unsupported Vers:	4561
Invalid length:	0	Malformed:	0	Mem alloc fails:	0
Missing TLVs:	0	Cache overflow:	0	Other errors:	0

#### TRANSMIT

Packets:	4557	Xmit fails:	0	No hostname:	0
Packet truncated:	0	Mem alloc fails:	0	Other errors:	0

#### OTHER

Init failures:	0
----------------	---

Il seguente comando cancella le statistiche CDP:

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	0	Csum Errors:	0	Unsupported Vers:	0
Invalid length:	0	Malformed:	0	Mem alloc fails:	0
Missing TLVs:	0	Cache overflow:	0	Other errors:	0

#### TRANSMIT

Packets:	0	Xmit fails:	0	No hostname:	0
Packet truncated:	0	Mem alloc fails:	0	Other errors:	0

#### OTHER

Init failures:	0
----------------	---

Una volta cancellate, le statistiche iniziano ad accumularsi dopo l'invio o la ricezione del successivo annuncio CDP.

### Utilizzare LLDP per rilevare la connettività di rete

L'utilizzo di LLDP per rilevare la connettività di rete consiste nell'esaminare le considerazioni di implementazione, abilitarla su tutte le porte, visualizzare i dispositivi adiacenti e regolare i valori di configurazione LLDP in base alle necessità.

LLDP deve essere abilitato anche su qualsiasi switch e router prima di poter visualizzare le informazioni sui dispositivi vicini.

ONTAP attualmente riporta le seguenti strutture TLV (Type-length-value Structures):

- ID chassis
- ID porta
- TTL (Time-to-Live)
- Nome del sistema

Il nome di sistema TLV non viene inviato sui dispositivi CNA.

Alcuni adattatori di rete convergenti (CNA), come l'adattatore X1143 e le porte integrate UTA2, contengono il supporto di offload per LLDP:

- L'offload LLDP viene utilizzato per il Data Center Bridging (DCB).
- Le informazioni visualizzate potrebbero differire tra il cluster e lo switch.

I dati relativi all'ID dello chassis e all'ID della porta visualizzati dallo switch potrebbero essere diversi per le porte CNA e non CNA.

Ad esempio:

- Per porte non CNA:
  - L'ID dello chassis è un indirizzo MAC fisso di una delle porte sul nodo
  - Port ID (ID porta) è il nome della porta corrispondente sul nodo
- Per le porte CNA:
  - ID chassis e ID porta sono gli indirizzi MAC delle rispettive porte sul nodo.

Tuttavia, i dati visualizzati dal cluster sono coerenti per questi tipi di porte.



La specifica LLDP definisce l'accesso alle informazioni raccolte tramite un MIB SNMP. Tuttavia, ONTAP attualmente non supporta il MIB LDP.

#### **Attiva o disattiva LLDP**

Per rilevare e inviare annunci pubblicitari ai dispositivi adiacenti conformi a LLDP, è necessario attivare LLDP su ciascun nodo del cluster. A partire da ONTAP 9.7, LLDP è attivato per impostazione predefinita su tutte le porte di un nodo.

#### **A proposito di questa attività**

Per ONTAP 9.10.1 e versioni precedenti, la `lldp.enable` L'opzione controlla se LLDP è attivato o disattivato sulle porte di un nodo:

- `on` Attiva LLDP su tutte le porte.
- `off` Disattiva LLDP su tutte le porte.

Per ONTAP 9.11.1 e versioni successive, la `lldp.enable` L'opzione controlla se LLDP è attivato o disattivato sulle porte non cluster e non storage di un nodo:

- `on` Attiva LLDP su tutte le porte non cluster e non storage.



- `off` Disattiva LLDP su tutte le porte non cluster e non storage.

## Fasi

1. Visualizza l'impostazione LLDP corrente per un nodo o per tutti i nodi di un cluster:
  - **Nodo singolo:** `run -node node_name options lldp.enable`
  - **All Node (tutti i nodi):** Opzioni `lldp.enable`
2. Attivare o disattivare LLDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per attivare o disattivare LLDP on...	Inserisci...
Un nodo	<code>`run -node node_name options lldp.enable {on</code>
<code>off}`</code>	Tutti i nodi di un cluster
<code>`options lldp.enable {on</code>	<code>off}`</code>

- **Nodo singolo:**

```
run -node node_name options lldp.enable {on|off}
```

- **Tutti i nodi:**

```
options lldp.enable {on|off}
```

## Visualizzare le informazioni LLDP neighbor

È possibile visualizzare informazioni sui dispositivi vicini collegati a ciascuna porta dei nodi del cluster, a condizione che la porta sia collegata a un dispositivo compatibile con LLDP. Il comando `network device-Discovery show` consente di visualizzare le informazioni sulle periferiche vicine.

## Fase

1. Visualizza informazioni su tutti i dispositivi compatibili con LLDP collegati alle porte di un nodo del cluster:

```
network device-discovery show -node node -protocol lldp
```

Il seguente comando mostra i vicini collegati alle porte sul nodo `cluster-1_01`. L'output elenca i dispositivi abilitati LLDP collegati a ciascuna porta del nodo specificato. Se il `-protocol` Viene omessa, l'output elenca anche i dispositivi abilitati per CDP.

```

network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local   Discovered
Protocol      Port    Device                      Interface      Platform
-----
cluster-1_01/lldp
                e2a      0013.c31e.5c60              GigabitEthernet1/36
                e2b      0013.c31e.5c60              GigabitEthernet1/35
                e2c      0013.c31e.5c60              GigabitEthernet1/34
                e2d      0013.c31e.5c60              GigabitEthernet1/33

```

### Regolare l'intervallo di trasmissione degli annunci LLDP

Gli annunci LLDP vengono inviati ai vicini LLDP a intervalli periodici. È possibile aumentare o ridurre l'intervallo di invio degli annunci LLDP in base al traffico di rete e alle modifiche della topologia di rete.

#### A proposito di questa attività

L'intervallo predefinito consigliato da IEEE è 30 secondi, ma è possibile immettere un valore compreso tra 5 secondi e 300 secondi.

#### Fasi

1. Visualizza l'intervallo di tempo di annuncio LLDP corrente per un nodo o per tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.interval
```

- Tutti i nodi:

```
options lldp.xmit.interval
```

2. Regolare l'intervallo per l'invio di annunci LLDP per tutte le porte di un nodo o per tutte le porte di tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- Tutti i nodi:

```
options lldp.xmit.interval <interval>
```

## Regola il valore del time-to-live per gli annunci LLDP

TTL (Time-to-Live) è il periodo di tempo per il quale gli annunci LLDP vengono memorizzati nella cache nei dispositivi compatibili con LLDP vicini. Il TTL viene pubblicizzato in ciascun pacchetto LLDP e viene aggiornato ogni volta che un pacchetto LLDP viene ricevuto da un nodo. TTL può essere modificato nei frame LLDP in uscita.

### A proposito di questa attività

- TTL è un valore calcolato, il prodotto dell'intervallo di trasmissione (`lldp.xmit.interval`) e il moltiplicatore hold (`lldp.xmit.hold`) più uno.
- Il valore predefinito del moltiplicatore Hold è 4, ma è possibile immettere valori compresi tra 1 e 100.
- Il TTL predefinito è quindi di 121 secondi, come consigliato da IEEE, ma regolando l'intervallo di trasmissione e i valori del moltiplicatore di mantenimento, è possibile specificare un valore per i frame in uscita da 6 secondi a 30001 secondi.
- Se un indirizzo IP viene rimosso prima della scadenza del TTL, le informazioni LLDP vengono memorizzate nella cache fino alla scadenza del TTL.

### Fasi

1. Visualizza il valore del moltiplicatore di mantenimento corrente per un nodo o per tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.hold
```

- Tutti i nodi:

```
options lldp.xmit.hold
```

2. Regolare il valore del moltiplicatore Hold su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- Tutti i nodi:

```
options lldp.xmit.hold <hold_value>
```

## Visualizzare o cancellare le statistiche LLDP

È possibile visualizzare le statistiche LLDP per il cluster e le porte non del cluster su ciascun nodo per rilevare potenziali problemi di connettività di rete. Le statistiche LLDP sono cumulative a partire dall'ultima cancellazione.

### A proposito di questa attività

Per ONTAP 9.10.1 e versioni precedenti, poiché LLDP è sempre abilitato per le porte del cluster, le statistiche LLDP vengono sempre visualizzate per il traffico su tali porte. LLDP deve essere attivato sulle porte non cluster per visualizzare le statistiche per tali porte.

Per ONTAP 9.11.1 e versioni successive, poiché LLDP è sempre abilitato per le porte di cluster e storage, le statistiche LLDP vengono sempre visualizzate per il traffico su tali porte. LLDP deve essere abilitato sulle porte non cluster e non storage per visualizzare le statistiche per tali porte.

## Fase

Visualizzare o cancellare le statistiche LLDP correnti per tutte le porte su un nodo:

Se si desidera...	Inserisci...
Visualizzare le statistiche LLDP	<code>run -node node_name lldp stats</code>
Cancellare le statistiche LLDP	<code>run -node node_name lldp stats -z</code>

## Mostra e cancella esempio di statistiche

Il comando seguente mostra le statistiche LLDP prima che vengano cancellate. L'output visualizza il numero totale di pacchetti inviati e ricevuti dall'ultima cancellazione delle statistiche.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
  Total frames:      190k | Accepted frames:   190k | Total drops:
0
TRANSMIT
  Total frames:      5195 | Total failures:      0
OTHER
  Stored entries:      64
```

Il seguente comando cancella le statistiche LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
  Total frames:      0 | Accepted frames:      0 | Total drops:
0
TRANSMIT
  Total frames:      0 | Total failures:      0
OTHER
  Stored entries:      64
```

Una volta cancellate, le statistiche iniziano ad accumularsi dopo l'invio o la ricezione del successivo annuncio LLDP.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.