



Monitorare le porte di rete

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/networking/monitor_the_health_of_network_ports.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Monitorare le porte di rete	1
Monitorare lo stato delle porte di rete ONTAP	1
Monitorare la raggiungibilità delle porte di rete ONTAP	2
Informazioni sull'utilizzo delle porte sulla rete ONTAP	6
Trafﬁco in entrata	6
Trafﬁco in uscita	7
Informazioni sulle porte interne di ONTAP	9

Monitorare le porte di rete

Monitorare lo stato delle porte di rete ONTAP

La gestione ONTAP delle porte di rete include il monitoraggio automatico dello stato di salute e un set di monitor per aiutare a identificare le porte di rete che potrebbero non essere adatte per l'hosting di LIF.

A proposito di questa attività

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

- Le porte di rete nell'IPSpace del cluster vengono contrassegnate come degradate quando si verificano lo sfracello 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 sfracello dei collegamenti.

È necessario conoscere i seguenti comportamenti di una porta danneggiata:

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

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

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

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

Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

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

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

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

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

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

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

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

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

- Monitor CRC: Monitora le statistiche CRC sulle porte

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

Ulteriori informazioni su `network options port-health-monitor show` nella "[Riferimento al comando ONTAP](#)".

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

Ulteriori informazioni su `network options port-health-monitor modify` nella "[Riferimento al comando ONTAP](#)".

4. Visualizzazione dello stato dettagliato di una porta:

```
network port show -health
```

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

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

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

Ulteriori informazioni su `network port show` nella "[Riferimento al comando ONTAP](#)".

Monitorare la raggiungibilità delle porte di rete ONTAP

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

A proposito di questa attività

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

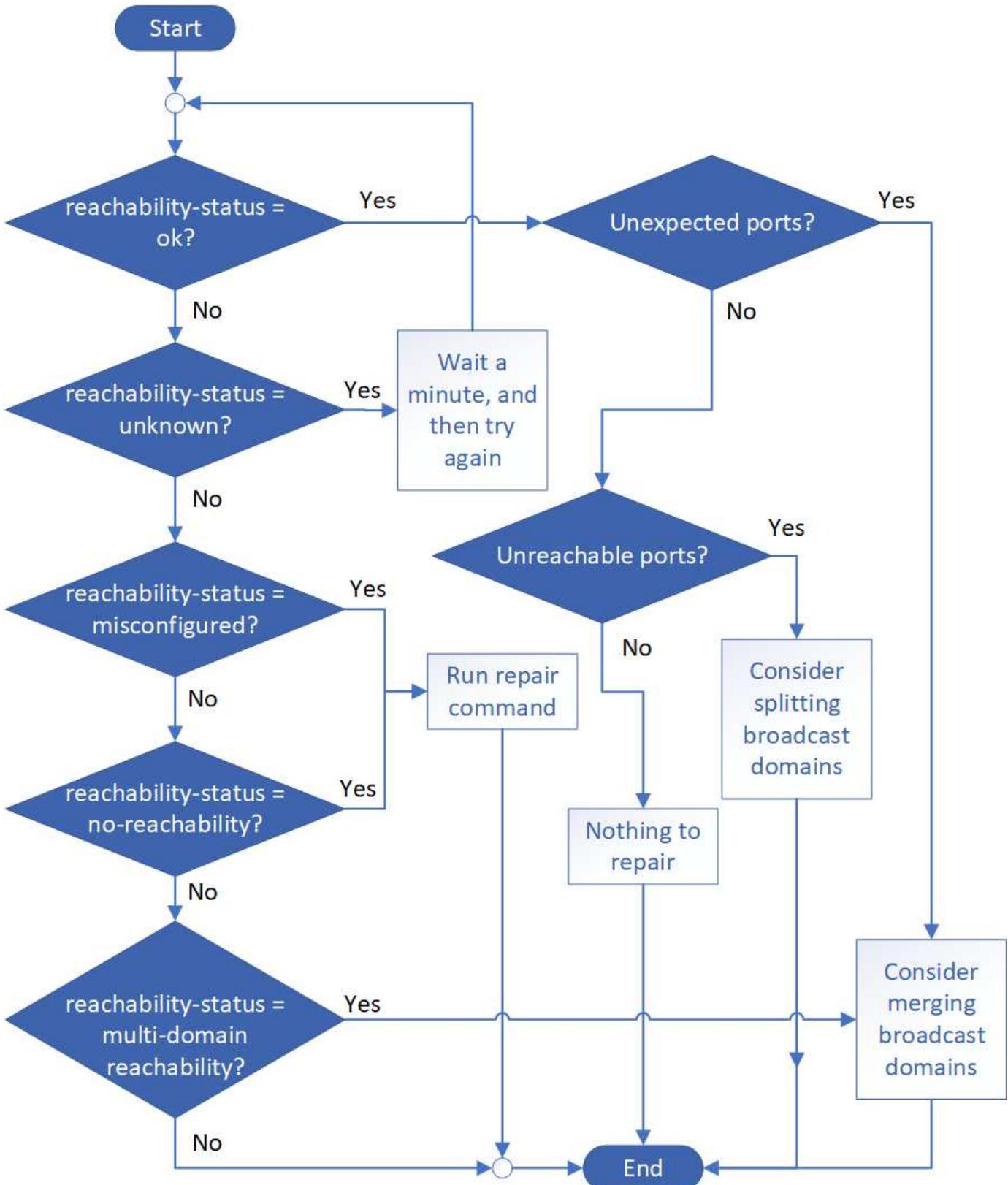
Fase

1. Visualizzazione della raggiungibilità delle porte:

```
network port reachability show
```

Ulteriori informazioni su network port reachability show nella "[Riferimento al comando ONTAP](#)".

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



Stato di raggiungibilità	Descrizione

ok	<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 "Unire i domini di broadcast".</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 "Suddividere i domini di broadcast".</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 "Riparare la raggiungibilità delle porte".</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><code>network port reachability repair -node -port</code> Per ulteriori informazioni, vedere "Riparare la raggiungibilità delle porte". Ulteriori informazioni su <code>network port reachability repair</code> nella "Riferimento al comando ONTAP".</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 "Unire i domini di broadcast" oppure "Riparare la raggiungibilità delle porte".</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](#)".

Informazioni sull'utilizzo delle porte sulla rete ONTAP

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

Traffico in entrata

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

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

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

Traffico in uscita

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

Regole di base in uscita

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

Protocollo	Porta	Scopo
------------	-------	-------

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

Regole avanzate in uscita

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

Active Directory

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

AutoSupport

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

SNMP

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

SnapMirror

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

Altri servizi

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

Informazioni sulle porte interne di ONTAP

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

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

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

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

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

Informazioni sul copyright

Copyright © 2026 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 COMMERCIALITÀ 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.