



# **Monitorar portas de rede**

## **ONTAP 9**

NetApp  
February 12, 2026

# Índice

Monitorar portas de rede .....	1
Monitore a integridade das portas de rede ONTAP .....	1
Monitore a acessibilidade das portas de rede ONTAP .....	2
Saiba mais sobre o uso de portas na rede ONTAP .....	6
Tráfego de entrada .....	6
Tráfego de saída .....	7
Saiba mais sobre as portas internas do ONTAP .....	9

# Monitorar portas de rede

## Monitore a integridade das portas de rede ONTAP

O gerenciamento ONTAP de portas de rede inclui monitoramento automático de integridade e um conjunto de monitores de integridade para ajudá-lo a identificar portas de rede que podem não ser adequadas para hospedar LIFs.

### Sobre esta tarefa

Se um monitor de integridade determinar que uma porta de rede não está saudável, ele avisa os administradores por meio de uma mensagem EMS ou marca a porta como degradada. O ONTAP evita hospedar LIFs em portas de rede degradadas se houver destinos de failover alternativos saudáveis para esse LIF. Uma porta pode se degradar devido a um evento de falha suave, como flapping de link (links que saltam rapidamente entre cima e baixo) ou particionamento de rede:

- As portas de rede no IPspace do cluster são marcadas como degradadas quando apresentam flapping de link ou perda de acessibilidade da camada 2 (L2) a outras portas de rede no domínio de broadcast.
- As portas de rede em IPspaces que não sejam de cluster são marcadas como degradadas quando apresentam flapping de link.

Você deve estar ciente dos seguintes comportamentos de uma porta degradada:

- Uma porta degradada não pode ser incluída em uma VLAN ou em um grupo de interfaces.

Se uma porta membro de um grupo de interfaces for marcada como degradada, mas o grupo de interfaces ainda estiver marcado como saudável, LIFs podem ser hospedados nesse grupo de interfaces.

- Os LIFs são migrados automaticamente de portas degradadas para portas íntegras.
- Durante um evento de failover, uma porta degradada não é considerada como o destino de failover. Se não houver portas íntegras disponíveis, as portas degradadas hospedam LIFs de acordo com a política de failover normal.
- Não é possível criar, migrar ou reverter um LIF para uma porta degradada.

Pode modificar a `ignore-health-status` definição da porta de rede para `true`. Em seguida, você pode hospedar um LIF nas portas saudáveis.

### Passos

1. Inicie sessão no modo de privilégio avançado:

```
set -privilege advanced
```

2. Verifique quais monitores de integridade estão ativados para monitorar o estado da porta de rede:

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

O status de integridade de uma porta é determinado pelo valor dos monitores de integridade.

Os seguintes monitores de integridade estão disponíveis e ativados por padrão no ONTAP:

- Monitor de saúde com link flapping: Monitora o flapping do link

Se uma porta tiver um link batendo mais de uma vez em cinco minutos, essa porta será marcada como degradada.

- Monitor de integridade de acessibilidade L2: Monitora se todas as portas configuradas no mesmo domínio de broadcast têm acessibilidade L2

Esse monitor de integridade relata L2 problemas de acessibilidade em todos os IPspaces; no entanto, ele marca apenas as portas no IPspace do cluster como degradadas.

- Monitor CRC: Monitora as estatísticas de CRC nas portas

Este monitor de integridade não marca uma porta como degradada, mas gera uma mensagem EMS quando se observa uma taxa de falha de CRC muito alta.

Saiba mais sobre `network options port-health-monitor show` o ["Referência do comando ONTAP"](#)na .

3. Ative ou desative qualquer um dos monitores de integridade para um espaço IPspace conforme desejado usando o `network options port-health-monitor modify` comando.

Saiba mais sobre `network options port-health-monitor modify` o ["Referência do comando ONTAP"](#)na .

4. Veja a integridade detalhada de um porto:

```
network port show -health
```

O comando `output` exibe o status de integridade da porta, `ignore health status configuration` e lista dos motivos pelos quais a porta é marcada como degradada.

Um status de integridade da porta pode ser `healthy` ou `degraded`.

Se a `ignore health status configuration` for `true`, ela indica que o status de integridade da porta foi modificado de `degraded` para `healthy` pelo administrador.

Se a `ignore health status configuration` for `false`, o status de integridade da porta será determinado automaticamente pelo sistema.

Saiba mais sobre `network port show` o ["Referência do comando ONTAP"](#)na .

## Monitore a acessibilidade das portas de rede ONTAP

O monitoramento de acessibilidade é integrado ao ONTAP 9.8 e posterior. Use esse monitoramento para identificar quando a topologia de rede física não corresponde à configuração do ONTAP. Em alguns casos, o ONTAP pode reparar a acessibilidade da porta. Em outros casos, etapas adicionais são necessárias.

## Sobre esta tarefa

Use esses comandos para verificar, diagnosticar e reparar configurações incorretas de rede resultantes da configuração do ONTAP que não corresponde ao cabeamento físico ou à configuração do switch de rede.

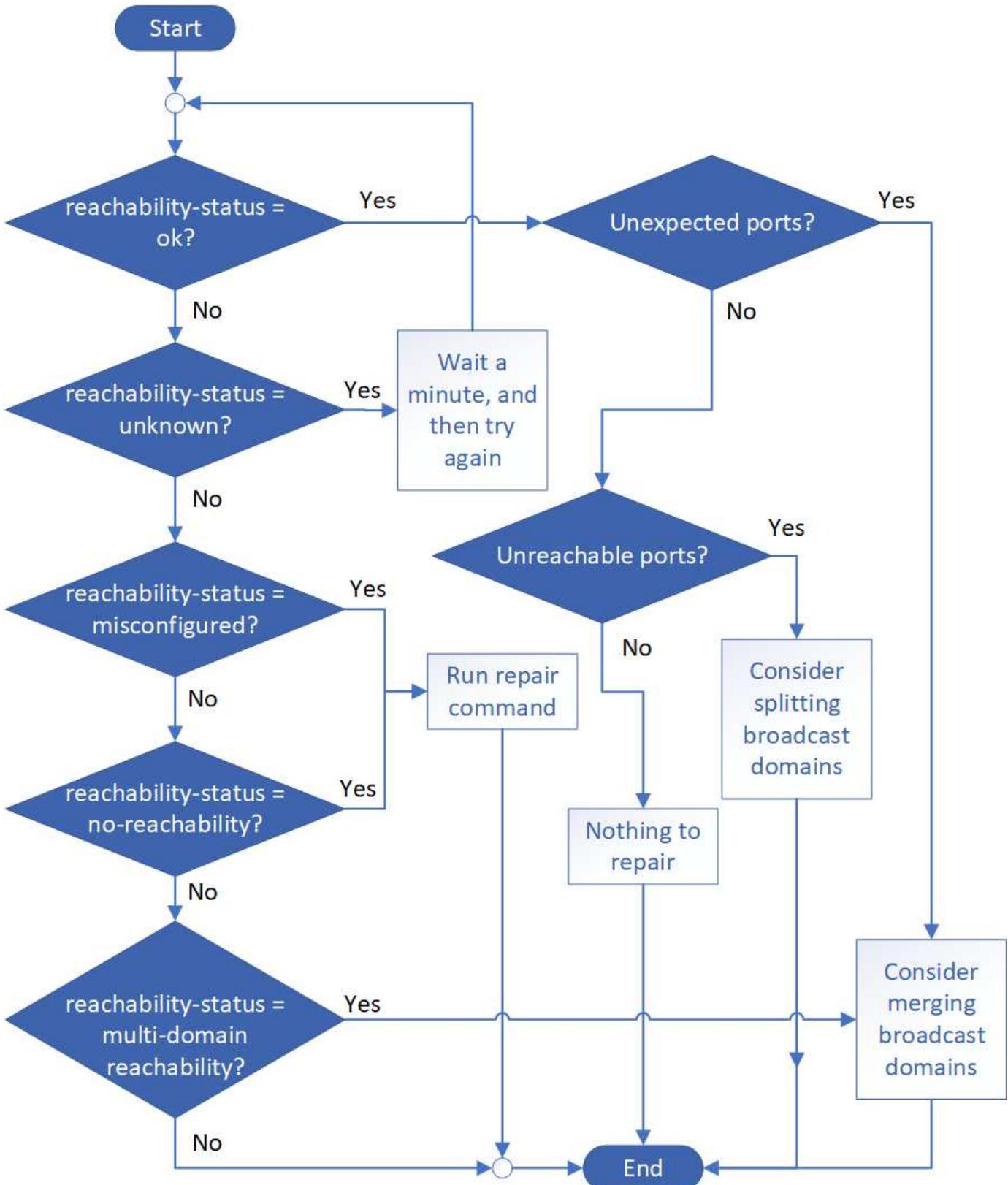
## Passo

1. Exibir acessibilidade da porta:

```
network port reachability show
```

Saiba mais sobre `network port reachability show` o "[Referência do comando ONTAP](#)" na .

2. Use a seguinte árvore de decisão e tabela para determinar a próxima etapa, se houver.



Status de acessibilidade	Descrição

ok	<p>A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído. Se o status de acessibilidade for "ok", mas houver "portas inesperadas", considere mesclar um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha <a href="#">portas inesperadas</a>.</p> <p>Se o status de acessibilidade for "ok", mas houver "portas inalcançáveis", considere dividir um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha <a href="#">portas inalcançáveis</a>.</p> <p>Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.</p>
Portas inesperadas	<p>A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast.</p> <p>Examine a conectividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast.</p> <p>Para obter mais informações, <a href="#">"Mesclar domínios de broadcast"</a>consulte .</p>
Portas inalcançáveis	<p>Se um único domínio de broadcast tiver sido particionado em dois conjuntos de acessibilidade diferentes, você poderá dividir um domínio de broadcast para sincronizar a configuração do ONTAP com a topologia de rede física.</p> <p>Normalmente, a lista de portas inalcançáveis define o conjunto de portas que devem ser divididas em outro domínio de broadcast depois de ter verificado que a configuração física e do switch é precisa.</p> <p>Para obter mais informações, <a href="#">"Dividir domínios de broadcast"</a>consulte .</p>
acessibilidade mal configurada	<p>A porta não tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, a porta tem acessibilidade da camada 2 para um domínio de broadcast diferente.</p> <p>Você pode reparar a acessibilidade da porta. Ao executar o seguinte comando, o sistema atribuirá a porta ao domínio de broadcast ao qual tem acessibilidade:</p> <pre>network port reachability repair -node -port</pre> <p>Para obter mais informações, <a href="#">"Acessibilidade da porta de reparo"</a>consulte .</p>
sem acessibilidade	<p>A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente.</p> <p>Você pode reparar a acessibilidade da porta. Quando você executa o seguinte comando, o sistema atribuirá a porta a um novo domínio de broadcast criado automaticamente no IPspace padrão:</p> <pre>network port reachability repair -node -port</pre> <p>Para obter mais informações, <a href="#">"Acessibilidade da porta de reparo"</a>consulte . Saiba mais sobre network port reachability repair o <a href="#">"Referência do comando ONTAP"</a>na .</p>

multidomínio-accessibilidade	<p>A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast.</p> <p>Examine a conectividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast.</p> <p>Para obter mais informações, consulte "<a href="#">Mesclar domínios de broadcast</a>" ou "<a href="#">Acessibilidade da porta de reparo</a>".</p>
desconhecido	<p>Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.</p>

Depois de reparar uma porta, você precisa verificar e resolver LIFs e VLANs deslocados. Se a porta fazia parte de um grupo de interfaces, você também precisa entender o que aconteceu com esse grupo de interfaces. Para obter mais informações, "[Acessibilidade da porta de reparo](#)" consulte .

## Saiba mais sobre o uso de portas na rede ONTAP

Várias portas conhecidas são reservadas para comunicações ONTAP com serviços específicos. Conflitos de porta ocorrem se um valor de porta no ambiente de rede de storage for o mesmo que o valor em uma porta ONTAP.

### Tráfego de entrada

O tráfego de entrada no storage ONTAP usa os seguintes protocolos e portas:

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância
TCP	22	Acesso de shell seguro ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nós
TCP	80	Acesso à página da Web ao endereço IP do LIF de gerenciamento de cluster
TCP/UDP	111	RPCBIND, chamada de procedimento remoto para NFS
UDP	123	NTP, protocolo de tempo de rede
TCP	135	MSRPC, chamada de procedimento remoto da Microsoft
TCP	139	NETBIOS-SSN, sessão de serviço NetBIOS para CIFS
TCP/UDP	161-162	SNMP, protocolo simples de gerenciamento de rede
TCP	443	Acesso seguro à página da Web ao endereço IP do LIF de gerenciamento de cluster

TCP	445	MS Active Domain Services, Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP/UDP	635	Montagem NFS para interagir com um sistema de arquivos remoto como se fosse local
TCP	749	Kerberos
UDP	953	Daemon de nomes
TCP/UDP	2049	Daemon do servidor NFS
TCP	2050	NRV, protocolo de volume remoto NetApp
TCP	3260	Acesso iSCSI através do iSCSI data LIF
TCP/UDP	4045	Daemon de bloqueio NFS
TCP/UDP	4046	Monitor de status da rede para NFS
UDP	4049	Rquotad RPC NFS
UDP	4444	KRB524, Kerberos 524
UDP	5353	DNS multicast
TCP	10000	Backup usando protocolo de gerenciamento de dados de rede (NDMP)
TCP	11104	Peering de cluster, gerenciamento bidirecional de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Peering de cluster, transferência bidirecional de dados SnapMirror usando LIFs entre clusters
SSL/TLS	30000	Aceita conexões de controle seguras NDMP entre o DMA e o servidor NDMP por meio de soquetes seguros (SSL/TLS). Os scanners de segurança podem relatar uma vulnerabilidade na porta 30000.

## Tráfego de saída

O tráfego de saída no seu armazenamento ONTAP pode ser configurado usando regras básicas ou avançadas, dependendo das necessidades da empresa.

### Regras básicas de saída

Todas as portas podem ser usadas para todo o tráfego de saída através dos protocolos ICMP, TCP e UDP.

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Todo o tráfego de saída
Todos os TCP	Tudo	Todo o tráfego de saída
Todos os UDP	Tudo	Todo o tráfego de saída

## Regras de saída avançadas

Se você precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo ONTAP.

### Ative Directory

Protocolo	Porta	Fonte	Destino	Finalidade
TCP	88	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS, iSCSI)	Floresta do ative Directory	Autenticação Kerberos V.
UDP	137	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	Serviço de nomes NetBIOS
UDP	138	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	Serviço de datagrama NetBIOS
TCP	139	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	Sessão de serviço NetBIOS
TCP	389	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	LDAP
UDP	389	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	LDAP
TCP	445	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	464	LIF de gerenciamento de nós, LIF de dados (NFS, CIFS)	Floresta do ative Directory	Alterar e definir a senha Kerberos V (SET_CHANGE)
UDP	464	LIF de gerenciamento de nós, Data LIF (NFS, CIFS)	Floresta do ative Directory	Administração de chaves Kerberos
TCP	749	LIF de gerenciamento de nós, Data LIF (NFS, CIFS)	Floresta do ative Directory	Alterar e definir a senha Kerberos V (RPCSEC_GSS)

### AutoSupport

Protocolo	Porta	Fonte	Destino	Finalidade
TCP	80	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)

### SNMP

Protocolo	Porta	Fonte	Destino	Finalidade
TCP/UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP

## SnapMirror

Protocolo	Porta	Fonte	Destino	Finalidade
TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror

## Outros serviços

Protocolo	Porta	Fonte	Destino	Finalidade
TCP	25	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport
UDP	53	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
UDP	67	LIF de gerenciamento de nós	DHCP	Servidor DHCP
UDP	68	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
UDP	514	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog
TCP	5010	LIF entre clusters	Ponto de extremidade de backup ou ponto de extremidade de restauração	Fazer backup e restaurar operações para o recurso Backup to S3
TCP	18600 a 18699	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP

## Saiba mais sobre as portas internas do ONTAP

A tabela a seguir lista as portas que o ONTAP usa internamente e suas funções. O ONTAP usa essas portas para diversas funções, como estabelecer comunicação LIF intracluster.

Esta lista não é exaustiva e pode variar em diferentes ambientes.

Porta/protocolo	Componente/função
514	Syslog
900	RPC de cluster do NetApp
902	RPC de cluster do NetApp
904	RPC de cluster do NetApp
905	RPC de cluster do NetApp
910	RPC de cluster do NetApp

911	RPC de cluster do NetApp
913	RPC de cluster do NetApp
914	RPC de cluster do NetApp
915	RPC de cluster do NetApp
918	RPC de cluster do NetApp
920	RPC de cluster do NetApp
921	RPC de cluster do NetApp
924	RPC de cluster do NetApp
925	RPC de cluster do NetApp
927	RPC de cluster do NetApp
928	RPC de cluster do NetApp
929	RPC de cluster do NetApp
930	Serviços de kernel e funções de gerenciamento (KSMF)
931	RPC de cluster do NetApp
932	RPC de cluster do NetApp
933	RPC de cluster do NetApp
934	RPC de cluster do NetApp
935	RPC de cluster do NetApp
936	RPC de cluster do NetApp
937	RPC de cluster do NetApp
939	RPC de cluster do NetApp
940	RPC de cluster do NetApp
951	RPC de cluster do NetApp
954	RPC de cluster do NetApp
955	RPC de cluster do NetApp
956	RPC de cluster do NetApp
958	RPC de cluster do NetApp
961	RPC de cluster do NetApp
963	RPC de cluster do NetApp
964	RPC de cluster do NetApp
966	RPC de cluster do NetApp
967	RPC de cluster do NetApp
975	Key Management Interoperability Protocol (KMIP)
982	RPC de cluster do NetApp

983	RPC de cluster do NetApp
5125	Porta de controle alternativa para disco
5133	Porta de controle alternativa para disco
5144	Porta de controle alternativa para disco
65502	Escopo do nó SSH
65503	Compartilhamento de LIF
7700	Gerenciador de Sessões de Cluster (CSM)
7810	RPC de cluster do NetApp
7811	RPC de cluster do NetApp
7812	RPC de cluster do NetApp
7813	RPC de cluster do NetApp
7814	RPC de cluster do NetApp
7815	RPC de cluster do NetApp
7816	RPC de cluster do NetApp
7817	RPC de cluster do NetApp
7818	RPC de cluster do NetApp
7819	RPC de cluster do NetApp
7820	RPC de cluster do NetApp
7821	RPC de cluster do NetApp
7822	RPC de cluster do NetApp
7823	RPC de cluster do NetApp
7824	RPC de cluster do NetApp
7835-7839 e 7845-7849	Portas TCP para comunicação intracluster
8023	Escopo do nó TELNET
8443	Porta NAS ONTAP S3 para Amazon FSx
8514	RSH do âmbito do nó
9877	Porta do cliente KMIP (somente host local interno)
10006	Porta TCP para comunicação de interconexão HA

## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

**ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.**

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

**LEGENDA DE DIREITOS LIMITADOS:** o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.