Monitorar portas de rede

ONTAP 9

NetApp
January 17, 2025

Índice

Monitorar portas de rede

Monitore a integridade das portas de rede

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.

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.
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` configuração 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` configuração for `true`, ela indica que o status de integridade da porta foi modificado de `degraded` para `healthy` pelo administrador.

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

Monitorar a acessibilidade das portas de rede (ONTAP 9.8 e posterior)

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

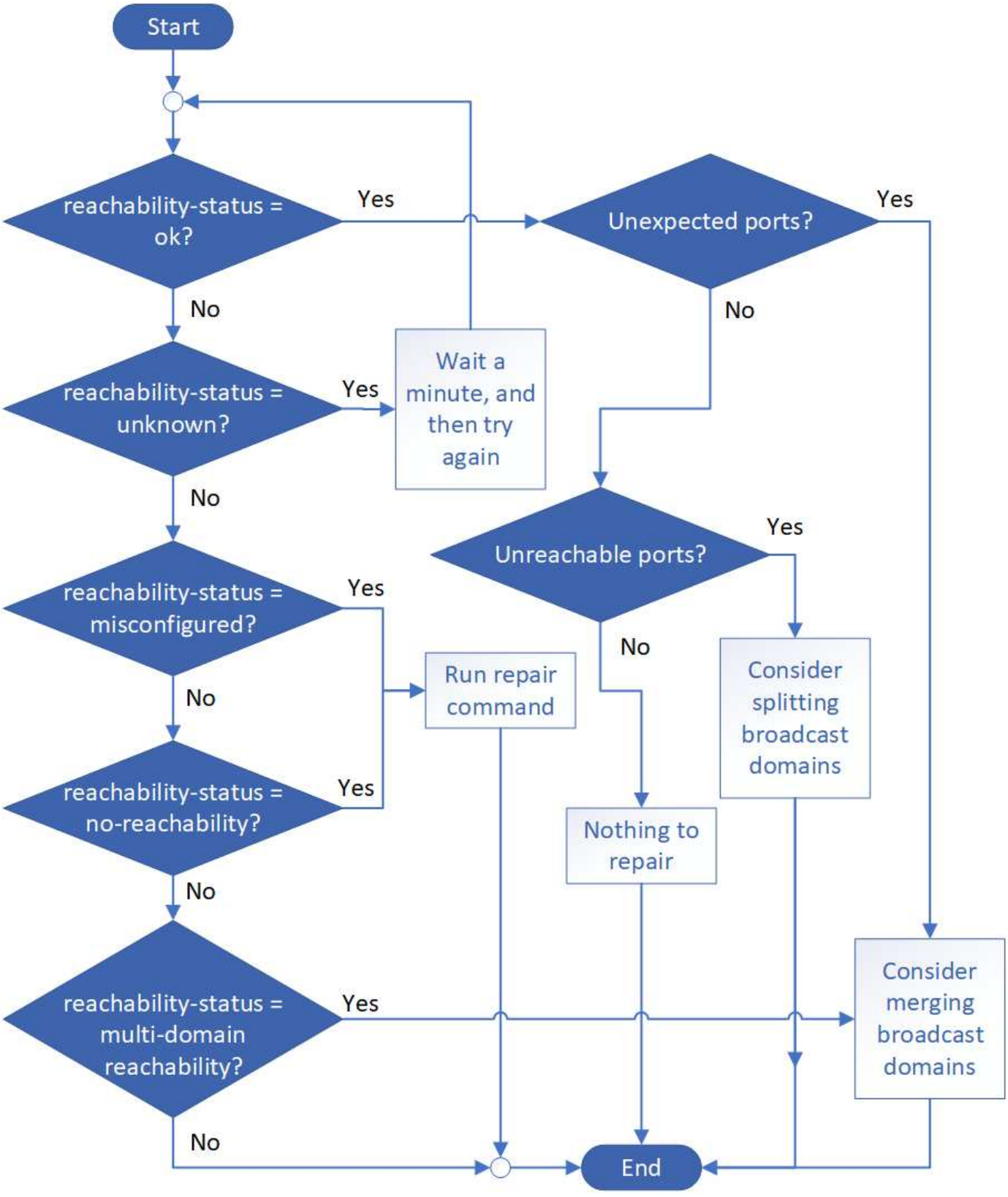
Use esses comandos para verificar, diagnosticar e reparar configurações incorretas de rede resultantes da configuração do ONTAP que não corresponde ao cabeamento físico ou à configuração do switch de rede.

Passo

1. Exibir acessibilidade da porta:

```
network port reachability show
```

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



Status de acessibilidade	Descrição
ok	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 *portas inesperadas*. 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 *portas inalcançáveis*. Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.
Portas inesperadas	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. Examine a conetividade 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. Para obter mais informações, "Mesclar domínios de broadcast"consulte .
Portas inalcançáveis	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. 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. Para obter mais informações, "Dividir domínios de broadcast"consulte .
acessibilidade mal configurada	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. 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: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

sem acessibilidade	A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente. 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: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .
multidomínio-acessibilidade	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. Examine a conetividade 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. Para obter mais informações, consulte "Mesclar domínios de broadcast" ou "Acessibilidade da porta de reparo".
desconhecido	Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.

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 .

Visão geral das portas ONTAP

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

A tabela a seguir lista as portas TCP e UDP usadas pelo ONTAP.

Serviço	Porta/protocolo	Descrição
ssh	22/TCP	Login de shell seguro
telnet	23/TCP	Início de sessão remoto
DNS	53/TCP	Carregue o DNS balanceado
http	80/TCP	Protocolo de transferência de texto Hyper
rpcbind	111/TCP	Chamada de procedimento remoto
rpcbind	111/UDP	Chamada de procedimento remoto
ntp	123/UDP	Protocolo de hora de rede
msrpc	135/UDP	MSRPC

netbios-ssn	139/TCP	Sessão de serviço NetBIOS
snmp	161/UDP	Protocolo de gerenciamento de rede simples
https	443/TCP	HTTP em TLS
microsoft-ds	445/TCP	Microsoft-ds
montagem	635/TCP	Montagem em NFS
montagem	635/UDP	Suporte NFS
nomeado	953/UDP	Daemon de nomes
nfs	2049/UDP	Daemon do servidor NFS
nfs	2049/TCP	Daemon do servidor NFS
nrv	2050/TCP	Protocolo de volume remoto da NetApp
iscsi	3260/TCP	Porta de destino iSCSI
lockd	4045/TCP	Daemon de bloqueio NFS
lockd	4045/UDP	Daemon de bloqueio NFS
NSM	4046/TCP	Monitor de estado da rede
NSM	4046/UDP	Monitor de estado da rede
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS - protocolo binário de escuta
https	8443/TCP	Ferramenta GUI 7MTT através de https
ndmp	10000/TCP	Protocolo de gerenciamento de dados de rede
Peering de clusters	11104/TCP	Peering de cluster, bidirecional
Peering de cluster, bidirecional	11105/TCP	Peering de clusters
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	aceite as ligações de controlo através de tomadas seguras
porta de testemunhas cifs	40001/TCP	porta de testemunhas cifs
tls	50000/TCP	Segurança da camada de transporte
iscsi	65200/TCP	Porta de ISCSI

Portas internas do ONTAP

A tabela a seguir lista as portas TCP e UDP que são usadas internamente pelo ONTAP. Essas portas são usadas para estabelecer comunicação LIF entre clusters:

Porta/protocolo	Descrição
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
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
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
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
8023	Escopo do nó TELNET
8514	RSH do âmbito do nó
9877	Porta do cliente KMIP (somente host local interno)

Informações sobre direitos autorais

Informações sobre marcas comerciais