Portas de rede

ONTAP 9

NetApp
February 02, 2026

Índice

Portas de rede

Saiba mais sobre a configuração da porta de rede ONTAP

As portas são portas físicas (NICs) ou portas virtualizadas, como grupos de interfaces ou VLANs.

As redes de área local virtual (VLANs) e os grupos de interface constituem as portas virtuais. Os grupos de interface tratam várias portas físicas como uma única porta, enquanto as VLANs subdividem uma porta física em várias portas lógicas separadas.

- Portas físicas: LIFs podem ser configuradas diretamente em portas físicas.
- Grupo de interfaces: Um agregado de portas contendo duas ou mais portas físicas que atuam como uma única porta de tronco. Um grupo de interfaces pode ser multimodo, monomodo ou dinâmico.
- VLAN: Uma porta lógica que recebe e envia tráfego com tag VLAN (padrão IEEE 802,1Q.1ad). As caraterísticas da porta VLAN incluem o ID da VLAN para a porta. A porta física subjacente ou as portas do grupo de interfaces são consideradas portas de tronco VLAN, e as portas do switch conetado devem ser configuradas para ramificar os IDs de VLAN.

  A porta física subjacente ou as portas do grupo de interfaces para uma porta VLAN podem continuar hospedando LIFs, que transmitem e recebem tráfego não marcado.

- Porta IP virtual (VIP): Uma porta lógica que é usada como porta inicial para um LIF VIP. As portas VIP são criadas automaticamente pelo sistema e suportam apenas um número limitado de operações. As portas VIP são suportadas a partir do ONTAP 9.5.

A convenção de nomenclatura de portas é *enumberletter*:

- O primeiro caractere descreve o tipo de porta. "E" representa Ethernet.
- O segundo caractere indica o slot numerado no qual o adaptador de porta está localizado.
- O terceiro caractere indica a posição da porta em um adaptador multiporta. "a" indica a primeira porta, "b" indica a segunda porta, e assim por diante.

Por exemplo, `e0b` indica que uma porta Ethernet é a segunda porta na placa-mãe do nó.

As VLANs devem ser nomeadas usando a `port_name-vlan-id` sintaxe .

`port_name` especifica a porta física ou o grupo de interfaces.

`vlan-id` Especifica a identificação da VLAN na rede. Por exemplo, `e1c-80` é um nome de VLAN válido.

Configurar portas de rede

Combine portas físicas para criar grupos de interface do ONTAP

Um grupo de interface, também conhecido como Grupo de agregação de link (LAG), é criado combinando duas ou mais portas físicas no mesmo nó em uma única porta lógica. A porta lógica oferece maior resiliência, maior disponibilidade e compartilhamento de carga.

Tipos de grupo de interfaces

Três tipos de grupos de interface são suportados no sistema de armazenamento: Modo único, multimodo estático e multimodo dinâmico. Cada grupo de interfaces fornece diferentes níveis de tolerância a falhas. Os grupos de interface multimodo fornecem métodos para o tráfego de rede de balanceamento de carga.

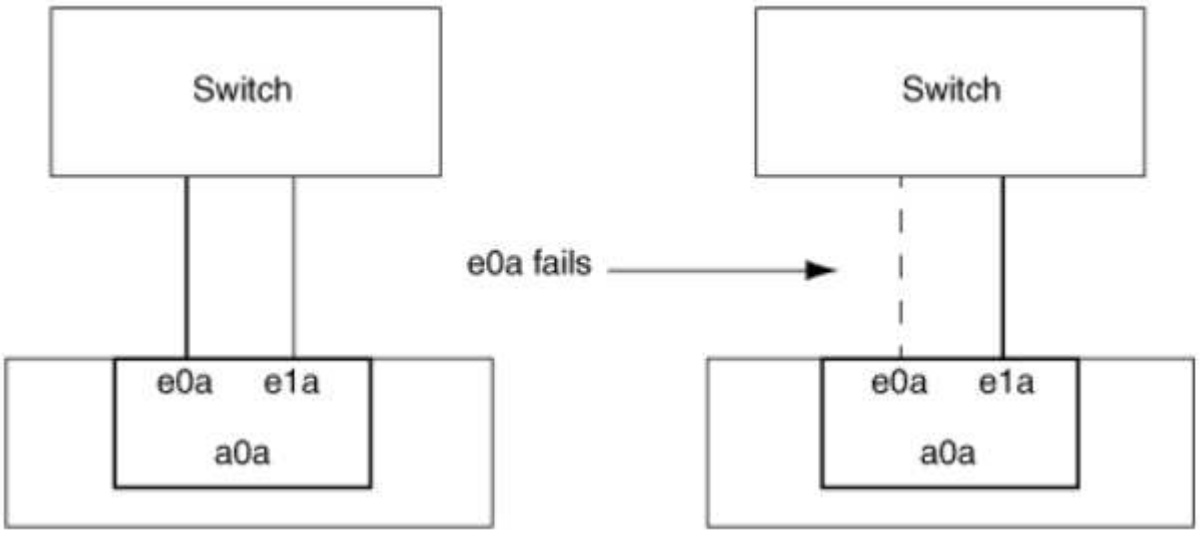
Caraterísticas dos grupos de interface monomodo

Em um grupo de interface de modo único, apenas uma das interfaces no grupo de interfaces está ativa. As outras interfaces estão em espera, prontas para assumir se a interface ativa falhar.

Caraterísticas de grupos de interface de modo único:

- Para failover, o cluster monitora o link ativo e controla o failover. Como o cluster monitora o link ativo, não há necessidade de configuração de switch.
- Pode haver mais de uma interface em espera em um grupo de interface de modo único.
- Se um grupo de interface de modo único abranger vários switches, você deve conetar os switches com um ISL (Inter-Switch Link).
- Para um grupo de interface de modo único, as portas do switch devem estar no mesmo domínio de broadcast.
- Os pacotes ARP de monitoramento de link, que têm um endereço de origem 0,0.0,0, são enviados pelas portas para verificar se as portas estão no mesmo domínio de broadcast.

A figura a seguir é um exemplo de um grupo de interface de modo único. Na figura, e0a e e1a fazem parte do grupo de interfaces monomodo a0a. Se a interface ativa, e0a, falhar, a interface standby e1a assume e mantém a conexão com o switch.



Para realizar a funcionalidade de modo único, a abordagem recomendada é usar grupos de failover. Ao usar um grupo de failover, a segunda porta ainda pode ser usada para outros LIFs e não precisa permanecer sem uso. Além disso, os grupos de failover podem abranger mais de duas portas e abranger portas em vários nós.

Caraterísticas de grupos de interface multimodo estático

A implementação do grupo de interfaces multimodo estático no ONTAP está em conformidade com a norma IEEE 802,3ad (estática). Qualquer switch que suporte agregados, mas não tenha troca de pacotes de controle

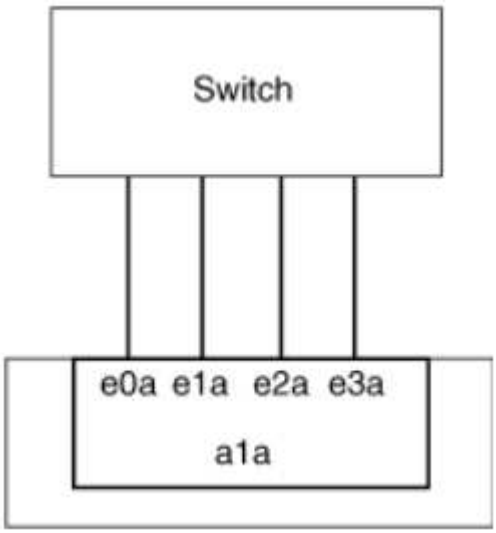
para configurar um agregado, pode ser usado com grupos de interface multimodo estático.

Os grupos de interface multimodo estático não estão em conformidade com a norma IEEE 802,3ad (dinâmica), também conhecida como Link Aggregation Control Protocol (LACP). O LACP é equivalente ao Protocolo de agregação de portas (PAgP), o protocolo de agregação de links proprietário da Cisco.

A seguir estão as caraterísticas de um grupo de interfaces multimodo estático:

- Todas as interfaces do grupo de interfaces estão ativas e compartilham um único endereço MAC.
  - Várias conexões individuais são distribuídas entre as interfaces no grupo de interfaces.
  - Cada conexão ou sessão usa uma interface dentro do grupo de interfaces. Quando você usa o esquema de balanceamento de carga sequencial, todas as sessões são distribuídas por links disponíveis em uma base pacote a pacote e não são vinculadas a uma interface específica do grupo de interfaces.
- Grupos de interface multimodo estático podem se recuperar de uma falha de até interfaces "n-1", onde n é o número total de interfaces que formam o grupo de interfaces.
- Se uma porta falhar ou for desconetada, o tráfego que estava atravessando o link com falha será automaticamente redistribuído para uma das interfaces restantes.
- Os grupos de interface multimodo estático podem detetar uma perda de link, mas não conseguem detetar uma perda de conetividade com o cliente ou configurações incorretas de switch que possam afetar a conetividade e o desempenho.
- Um grupo de interface multimodo estático requer um switch que suporte a agregação de links em várias portas de switch. O switch é configurado de modo que todas as portas às quais os links de um grupo de interfaces estão conetados façam parte de uma única porta lógica. Alguns switches podem não suportar agregação de links de portas configuradas para quadros jumbo. Para obter mais informações, consulte a documentação do fornecedor do switch.
- Várias opções de balanceamento de carga estão disponíveis para distribuir o tráfego entre as interfaces de um grupo de interfaces multimodo estático.

A figura a seguir é um exemplo de um grupo de interfaces multimodo estático. As interfaces e0a, e1a, E2A e E3A fazem parte do grupo de interfaces multimodo A1A. Todas as quatro interfaces no grupo de interfaces multimodo A1A estão ativas.



Existem várias tecnologias que permitem que o tráfego em um único link agregado seja distribuído entre vários switches físicos. As tecnologias usadas para habilitar essa capacidade variam entre os produtos de

rede. Os grupos de interface multimodo estático no ONTAP estão em conformidade com os padrões IEEE 802,3.3af. Se uma determinada tecnologia de agregação de links de múltiplos switches for considerada interoperacional ou conforme aos padrões IEEE 802,3.1X, ela deverá operar com o ONTAP.

O padrão IEEE 802,3 afirma que o dispositivo transmissor em um link agregado determina a interface física para transmissão. Portanto, o ONTAP é apenas responsável por distribuir tráfego de saída e não pode controlar como os quadros de entrada chegam. Se você quiser gerenciar ou controlar a transmissão de tráfego de entrada em um link agregado, essa transmissão deve ser modificada no dispositivo de rede conetado diretamente.

Grupo de interfaces multimodo dinâmico

Os grupos de interface multimodo dinâmico implementam o Link Aggregation Control Protocol (LACP) para comunicar a associação do grupo ao switch diretamente conetado. O LACP permite detetar a perda do status do link e a incapacidade do nó de se comunicar com a porta do switch de conexão direta.

A implementação dinâmica do grupo de interface multimodo no ONTAP está em conformidade com IEEE 802,3 AD (802,1 AX). O ONTAP não oferece suporte ao Protocolo de agregação de portas (PAgP), que é um protocolo de agregação de links proprietário da Cisco.

Um grupo de interface multimodo dinâmico requer um switch que suporte LACP.

O ONTAP implementa o LACP no modo ativo não configurável que funciona bem com switches configurados no modo ativo ou passivo. O ONTAP implementa os temporizadores LACP longos e curtos (para uso com valores não configuráveis de 3 segundos e 90 segundos), conforme especificado no IEEE 802,3 AD (802,1AX).

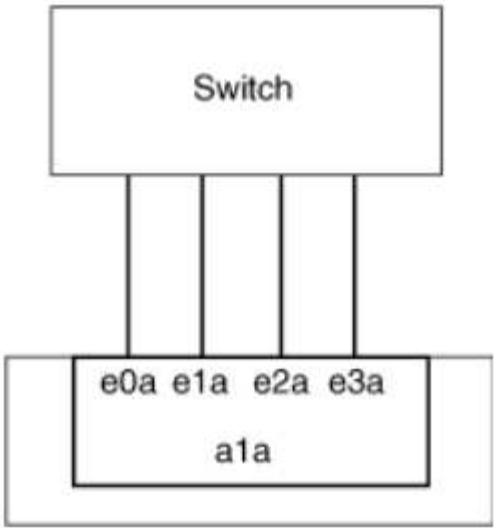
O algoritmo de balanceamento de carga do ONTAP determina a porta membro a ser usada para transmitir tráfego de saída e não controla como os quadros de entrada são recebidos. O switch determina o membro (porta física individual) de seu grupo de canais de portas a ser usado para transmissão, com base no algoritmo de balanceamento de carga configurado no grupo de canais de portas do switch. Portanto, a configuração do switch determina a porta membro (porta física individual) do sistema de armazenamento para receber tráfego. Para obter mais informações sobre como configurar o switch, consulte a documentação do fornecedor do switch.

Se uma interface individual não receber pacotes de protocolo LACP sucessivos, essa interface individual é marcada como "lag_inactive" na saída do comando "ifgrp status". O tráfego existente é automaticamente reencaminhado para quaisquer interfaces ativas restantes.

As regras a seguir se aplicam ao usar grupos de interface multimodo dinâmico:

- Os grupos de interface multimodo dinâmico devem ser configurados para usar os métodos de balanceamento de carga baseados em porta, baseados em IP, baseados em MAC ou round robin.
- Em um grupo de interface multimodo dinâmico, todas as interfaces devem estar ativas e compartilhar um único endereço MAC.

A figura a seguir é um exemplo de um grupo de interface multimodo dinâmico. As interfaces e0a, e1a, E2A e E3A fazem parte do grupo de interfaces multimodo A1A. Todas as quatro interfaces no grupo de interfaces multimodo dinâmico A1A estão ativas.



Balanceamento de carga em grupos de interface multimodo

Você pode garantir que todas as interfaces de um grupo de interfaces multimodo sejam usadas igualmente para o tráfego de saída usando o endereço IP, endereço MAC, métodos de balanceamento de carga sequenciais ou baseados em porta para distribuir o tráfego de rede igualmente pelas portas de rede de um grupo de interfaces multimodo.

O método de balanceamento de carga para um grupo de interfaces multimodo só pode ser especificado quando o grupo de interfaces é criado.

Prática recomendada: O balanceamento de carga baseado em porta é recomendado sempre que possível. Use balanceamento de carga baseado em porta, a menos que haja um motivo específico ou limitação na rede que o impeça.

Balanceamento de carga baseado em porta

O balanceamento de carga baseado em porta é o método recomendado.

Você pode equalizar o tráfego em um grupo de interfaces multimodo com base nas portas da camada de transporte (TCP/UDP) usando o método de balanceamento de carga baseado em porta.

O método de balanceamento de carga baseado em porta usa um algoritmo de hash rápido nos endereços IP de origem e destino, juntamente com o número da porta da camada de transporte.

Balanceamento de carga de endereço IP e endereço MAC

O balanceamento de carga de endereço IP e endereço MAC são os métodos para equalizar o tráfego em grupos de interface multimodo.

Esses métodos de balanceamento de carga usam um algoritmo de hash rápido nos endereços de origem e destino (endereço IP e endereço MAC). Se o resultado do algoritmo de hash mapear para uma interface que não está no estado de link UP, a próxima interface ativa será usada.

Não selecione o método de balanceamento de carga de endereço MAC ao criar grupos de interface em um sistema que se conete diretamente a um roteador. Em tal configuração, para cada quadro IP de saída, o endereço MAC de destino é o endereço MAC do roteador. Como resultado, apenas uma interface do grupo de interfaces é usada.

O balanceamento de carga de endereço IP funciona da mesma forma para endereços IPv4 e IPv6.

Balanceamento de carga sequencial

Você pode usar balanceamento de carga sequencial para distribuir pacotes de forma igual entre vários links usando um algoritmo round robin. Você pode usar a opção sequencial para balanceamento de carga do tráfego de uma única conexão em vários links para aumentar a taxa de transferência de conexão única.

No entanto, como o balanceamento de carga sequencial pode causar a entrega de pacotes fora do pedido, um desempenho extremamente ruim pode resultar. Portanto, o balanceamento de carga sequencial geralmente não é recomendado.

Crie um grupo de interfaces ou LAG

É possível criar um grupo de interfaces ou LAG (modo único, multimodo estático ou multimodo dinâmico (LACP) para apresentar uma única interface aos clientes combinando os recursos das portas de rede agregadas.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar um LAG

Passos

1. Selecione **rede > porta Ethernet > Grupo de agregação de link** para criar um LAG.
2. Selecione o nó na lista suspensa.
3. Escolha uma das seguintes opções:
   a. ONTAP para **selecionar automaticamente o domínio de transmissão (recomendado)**.
   b. Para selecionar manualmente um domínio de broadcast.
4. Selecione as portas para formar o LAG.
5. Selecione o modo:
   a. Único: Apenas uma porta é usada de cada vez.
   b. Múltiplas: Todas as portas podem ser usadas simultaneamente.
   c. LACP: O protocolo LACP determina as portas que podem ser usadas.
6. Selecione o balanceamento de carga:
   a. Baseado em IP
   b. Baseado em Mac
   c. Porta
   d. Sequencial
7. Salve suas alterações.

CLI

Use a CLI para criar um grupo de interfaces

Ao criar um grupo de interfaces multimodo, você pode especificar qualquer um dos seguintes métodos de balanceamento de carga:

- `port`: O tráfego de rede é distribuído com base nas portas da camada de transporte (TCP/UDP). Este é o método de balanceamento de carga recomendado.
- `mac`: O tráfego de rede é distribuído com base em endereços MAC.
- `ip`: O tráfego de rede é distribuído com base em endereços IP.
- `sequential`: O tráfego de rede é distribuído à medida que é recebido.

O endereço MAC de um grupo de interfaces é determinado pela ordem das portas subjacentes e como essas portas são inicializadas durante a inicialização. Portanto, você não deve assumir que o endereço MAC do ifgrp é persistente em reinicializações ou atualizações do ONTAP.

Passo

Use o `network port ifgrp create` comando para criar um grupo de interfaces.

Os grupos de interface devem ser nomeados usando a `a<number><letter>` sintaxe . Por exemplo, a0a, a0b, A1c e A2A são nomes de grupos de interface válidos.

Saiba mais sobre `network port ifgrp create` o "Referência do comando ONTAP"na .

O exemplo a seguir mostra como criar um grupo de interfaces chamado a0a com uma função de distribuição de porta e um modo de multimodo:

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

Adicione uma porta a um grupo de interfaces ou LAG

Você pode adicionar até 16 portas físicas a um grupo de interfaces ou LAG para todas as velocidades de portas.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para adicionar uma porta a um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para editar um LAG.
2. Selecione portas adicionais no mesmo nó para adicionar ao LAG.
3. Salve suas alterações.

CLI

Use a CLI para adicionar portas a um grupo de interfaces

Passo

Adicionar portas de rede ao grupo de interfaces:

```
network port ifgrp add-port
```

O exemplo a seguir mostra como adicionar a porta e0c a um grupo de interfaces chamado a0a:

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

A partir do ONTAP 9.8, os grupos de interface são automaticamente colocados em um domínio de broadcast apropriado cerca de um minuto após a primeira porta física ser adicionada ao grupo de interfaces. Se você não quiser que o ONTAP faça isso e preferir colocar manualmente o ifgrp em um domínio de broadcast, especifique o `-skip-broadcast-domain-placement` parâmetro como parte do `ifgrp add-port` comando.

Saiba mais sobre `network port ifgrp add-port` as restrições de configuração aplicáveis aos grupos de interface de portas no "Referência do comando ONTAP".

Remova uma porta de um grupo de interfaces ou LAG

Você pode remover uma porta de um grupo de interfaces que hospeda LIFs, desde que não seja a última porta no grupo de interfaces. Não há nenhum requisito de que o grupo de interfaces não deve hospedar LIFs ou que o grupo de interfaces não deve ser a porta inicial de um LIF, considerando que você não está removendo a última porta do grupo de interfaces. No entanto, se você estiver removendo a última porta, então

você deve migrar ou mover os LIFs do grupo de interfaces primeiro.

Sobre esta tarefa

Você pode remover até 16 portas (interfaces físicas) de um grupo de interfaces ou LAG.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para remover uma porta de um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para editar um LAG.
2. Selecione as portas a serem removidas do LAG.
3. Salve suas alterações.

CLI

Use a CLI para remover portas de um grupo de interfaces

Passo

Remover portas de rede de um grupo de interfaces:

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

Saiba mais sobre `network port ifgrp remove-port` o "Referência do comando ONTAP"na .

O exemplo a seguir mostra como remover a porta e0c de um grupo de interfaces chamado a0a:

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

Exclua um grupo de interfaces ou LAG

Você pode excluir grupos de interface ou LAGs se quiser configurar LIFs diretamente nas portas físicas subjacentes ou decidir alterar o grupo de interfaces ou o modo LAG ou a função de distribuição.

Antes de começar

- O grupo de interfaces ou LAG não deve estar hospedando um LIF.
- O grupo de interfaces ou LAG não deve ser nem a porta inicial nem o destino de failover de um LIF.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para excluir um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para excluir um LAG.
2. Selecione o LAG que deseja remover.
3. Eliminar o LAG.

CLI

Use a CLI para excluir um grupo de interfaces

Passo

Use o `network port ifgrp delete` comando para excluir um grupo de interfaces.

Saiba mais sobre `network port ifgrp delete` o "Referência do comando ONTAP"na .

O exemplo a seguir mostra como excluir um grupo de interfaces chamado a0b:

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

Configurar VLANS ONTAP em portas físicas

Você pode usar VLANs no ONTAP para fornecer segmentação lógica de redes, criando domínios de broadcast separados que são definidos em uma base de porta de switch, em vez dos domínios de broadcast tradicionais, definidos em limites físicos.

Uma VLAN pode abranger vários segmentos físicos de rede. As estações finais pertencentes a uma VLAN estão relacionadas por função ou aplicação.

Por exemplo, as estações finais em uma VLAN podem ser agrupadas por departamentos, como engenharia e contabilidade, ou por projetos, como release1 e release2. Como a proximidade física das estações finais não é essencial em uma VLAN, você pode dispersar as estações finais geograficamente e ainda conter o domínio de broadcast em uma rede comutada.

No ONTAP 9.14.1 e 9.13.1, portas não marcadas que não são utilizadas por nenhuma interface lógica (LIF) e não têm conectividade VLAN nativa no switch conectado são marcadas como degradadas. Isso ajuda a identificar portas não utilizadas e não indica uma interrupção. VLANs nativas permitem tráfego não marcado na porta base ifgrp, como transmissões ONTAP CFM. Configure VLANs nativas no switch para evitar o bloqueio de tráfego não marcado.

Você pode gerenciar VLANs criando, excluindo ou exibindo informações sobre elas.

> Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

Crie uma VLAN

Você pode criar uma VLAN para manter domínios de broadcast separados dentro do mesmo domínio de rede

usando o System Manager ou o `network port vlan create` comando.

Antes de começar

Confirme se os seguintes requisitos foram cumpridos:

- Os switches implantados na rede devem estar em conformidade com os padrões IEEE 802,1Q.1X ou ter uma implementação de VLANs específica do fornecedor.
- Para suportar várias VLANs, uma estação final deve ser estaticamente configurada para pertencer a uma ou mais VLANs.
- A VLAN não está conetada a uma porta que hospeda um LIF de cluster.
- A VLAN não está conetada às portas atribuídas ao IPspace do cluster.
- A VLAN não é criada em uma porta de grupo de interfaces que não contém portas membro.

Sobre esta tarefa

A criação de uma VLAN coneta a VLAN à porta de rede em um nó especificado em um cluster.

Quando você configura uma VLAN por uma porta pela primeira vez, a porta pode cair, resultando em uma desconexão temporária da rede. As adições subsequentes de VLAN à mesma porta não afetam o estado da porta.

> Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar uma VLAN

A partir do ONTAP 9.12,0, pode selecionar automaticamente o domínio de difusão ou selecionar manualmente ligado na lista. Anteriormente, os domínios de broadcast eram sempre selecionados automaticamente com base na conetividade da camada 2. Se você selecionar manualmente um domínio de broadcast, um aviso será exibido indicando que selecionar manualmente um domínio de broadcast pode resultar em perda de conetividade.

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione o nó na lista suspensa.
3. Escolha uma das seguintes opções:
   a. ONTAP para **selecionar automaticamente o domínio de transmissão (recomendado)**.
   b. Para selecionar manualmente um domínio de broadcast na lista.
4. Selecione as portas para formar a VLAN.
5. Especifique o ID da VLAN.
6. Salve suas alterações.

CLI

Use a CLI para criar uma VLAN

Em certas circunstâncias, se você quiser criar a porta VLAN em uma porta degradada sem corrigir o problema de hardware ou qualquer configuração incorreta de software, então você pode definir o `-ignore-health-status` parâmetro `network port modify` do comando como `true`.

Saiba mais sobre `network port modify` o "Referência do comando ONTAP"na .

Passos

1. Use o `network port vlan create` comando para criar uma VLAN.
2. Você deve especificar `vlan-name` as opções ou `port` e `vlan-id` ao criar uma VLAN. O nome da VLAN é uma combinação do nome da porta (ou grupo de interfaces) e do identificador VLAN do switch de rede, com um hífen entre. Por exemplo, `e0c-24` e `e1c-80` são nomes de VLAN válidos.

O exemplo a seguir mostra como criar uma VLAN `e1c-80` conetada à porta de rede `e1c` no nó `cluster-1-01`:

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

A partir do ONTAP 9.8, as VLANs são automaticamente colocadas em domínios de broadcast apropriados cerca de um minuto após sua criação. Se você não quiser que o ONTAP faça isso e preferir colocar manualmente a VLAN em um domínio de broadcast, especifique o `-skip-broadcast-domain-placement` parâmetro como parte do `vlan create` comando.

Saiba mais sobre `network port vlan create` o "Referência do comando ONTAP"na .

Editar uma VLAN

Você pode alterar o domínio de broadcast ou desativar uma VLAN.

Use o System Manager para editar uma VLAN

A partir do ONTAP 9.12,0, pode selecionar automaticamente o domínio de difusão ou selecionar manualmente ligado na lista. Os domínios de broadcast anteriormente eram sempre selecionados automaticamente com base na conetividade da camada 2. Se você selecionar manualmente um domínio de broadcast, um aviso será exibido indicando que selecionar manualmente um domínio de broadcast pode resultar em perda de conetividade.

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione o ícone de edição.
3. Execute um dos seguintes procedimentos:
   - Altere o domínio de broadcast selecionando um outro da lista.
   - Desmarque a caixa de seleção **Enabled** (habilitado).
4. Salve suas alterações.

Eliminar um VLAN

Talvez seja necessário excluir uma VLAN antes de remover uma NIC do slot. Quando você exclui uma VLAN, ela é automaticamente removida de todas as regras de failover e grupos que a usam.

Antes de começar

Certifique-se de que não existem LIFs associados à VLAN.

Sobre esta tarefa

A exclusão da última VLAN de uma porta pode causar uma desconexão temporária da rede da porta.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para excluir uma VLAN

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione a VLAN que deseja remover.
3. Clique em **Excluir**.

CLI

Use a CLI para excluir uma VLAN

Passo

Use o `network port vlan delete` comando para excluir uma VLAN.

O exemplo a seguir mostra como excluir VLAN `e1c-80` da porta de rede `e1c` no nó `cluster-1-01`:

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

Saiba mais sobre `network port vlan delete` o "Referência do comando ONTAP"na .

Modifique os atributos da porta de rede ONTAP

Você pode modificar as configurações de negociação automática, duplex, controle de fluxo, velocidade e integridade de uma porta de rede física.

Antes de começar

A porta que você deseja modificar não deve estar hospedando nenhum LIFs.

Sobre esta tarefa

- Não é recomendável modificar as configurações administrativas das interfaces de rede de 100 GbE, 40 GbE, 10 GbE ou 1 GbE.

  Os valores definidos para o modo duplex e a velocidade da porta são referidos como definições administrativas. Dependendo das limitações da rede, as configurações administrativas podem diferir das configurações operacionais (ou seja, o modo duplex e a velocidade que a porta realmente usa).

- Não é recomendável modificar as configurações administrativas das portas físicas subjacentes em um grupo de interfaces.

  O `-up-admin` parâmetro (disponível no nível de privilégio avançado) modifica as definições administrativas da porta.

- Não é recomendável definir a `-up-admin` configuração administrativa como falsa para todas as portas em um nó ou para a porta que hospeda o último LIF de cluster operacional em um nó.
- Não é recomendável modificar o tamanho da MTU da porta de gerenciamento, `e0M`.
- O tamanho da MTU de uma porta em um domínio de broadcast não pode ser alterado do valor MTU definido para o domínio de broadcast.

- O tamanho da MTU de uma VLAN não pode exceder o valor do tamanho da MTU de sua porta base.

Passos

1. Modifique os atributos de uma porta de rede:

   `network port modify`

2. Você pode definir o `-ignore-health-status` campo como verdadeiro para especificar que o sistema pode ignorar o status de integridade da porta de rede de uma porta especificada.

   O status de integridade da porta de rede é alterado automaticamente de degradada para saudável, e essa porta agora pode ser usada para hospedar LIFs. Você deve definir o controle de fluxo das portas do cluster como `none`. Por padrão, o controle de fluxo é definido como `full`.

O comando a seguir desativa o controle de fluxo na porta e0b definindo o controle de fluxo como nenhum:

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

Saiba mais sobre `network port modify` o "Referência do comando ONTAP"na .

Crie 10GbE portas para redes ONTAP convertendo 40GbE portas NIC

Pode converter as placas de interface de rede (NICs) X1144A-R6 e X91440A-R6 40GbE para suportar quatro portas 10GbE.

Se você estiver conetando uma plataforma de hardware que suporte uma dessas NICs a um cluster que suporte a interconexão de cluster 10GbE e conexões de dados do cliente, a NIC deve ser convertida para fornecer as conexões 10GbE necessárias.

Antes de começar

Você deve estar usando um cabo multicondutor suportado.

Sobre esta tarefa

Para obter uma lista completa de plataformas que suportam NICs, consulte "Hardware Universe" .

> Na NIC X1144A-R6, somente a porta A pode ser convertida para suportar as quatro conexões 10GbE. Uma vez que a porta A é convertida, a porta e não está disponível para uso.

Passos

1. Entre no modo de manutenção.
2. Converta a NIC do suporte 40GbE para o suporte 10GbE.

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

3. Depois de usar o comando Convert, interrompa o nó.
4. Instale ou substitua o cabo.
5. Dependendo do modelo de hardware, use o SP (processador de serviço) ou o BMC (controlador de

gerenciamento de placa base) para ligar o nó para que a conversão entre em vigor.

Configurar portas UTA X1143A-R6 para a rede ONTAP

Por padrão, o adaptador de destino unificado X1143A-R6 é configurado no modo de destino FC, mas você pode configurar suas portas como portas Ethernet de 10 GB e FCoE (CNA) ou como portas de iniciador FC de 16 GB ou de destino. Isso requer adaptadores SFP diferentes.

Quando configurados para Ethernet e FCoE, os adaptadores X1143A-R6 suportam NIC concorrente e tráfego de destino FCoE na mesma porta de 10 GBE. Quando configurado para FC, cada par de duas portas que compartilha o mesmo ASIC pode ser configurado individualmente para o modo de iniciador FC ou destino. Isso significa que um único adaptador X1143A-R6 pode oferecer suporte ao modo de destino FC em um par de duas portas e no modo iniciador FC em outro par de duas portas. Os pares de portas ligados ao mesmo ASIC têm de ser configurados no mesmo modo.

No modo FC, o adaptador X1143A-R6 se comporta como qualquer dispositivo FC existente com velocidades de até 16 Gbps. No modo CNA, você pode usar o adaptador X1143A-R6 para NIC concorrente e compartilhamento de tráfego FCoE na mesma porta de 10 GbE. O modo CNA só suporta o modo de destino FC para a função FCoE.

Para configurar o adaptador de destino unificado (X1143A-R6), você deve configurar as duas portas adjacentes no mesmo chip no mesmo modo de personalidade.

Passos

1. Veja a configuração da porta:

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

2. Configure as portas conforme necessário para Fibre Channel (FC) ou adaptador de rede convergente (CNA):

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

3. Conete os cabos apropriados para FC ou Ethernet de 10 GB.
4. Verifique se você tem o SFP correto instalado:

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

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB, com base na malha FC conetada.

Converta a porta UTA2 para uso na rede ONTAP

Pode converter a porta UTA2 do modo de adaptador de rede convergente (CNA) para o

modo Fibre Channel (FC) ou vice-versa.

Você deve alterar a personalidade UTA2 do modo CNA para o modo FC quando precisar alterar o meio físico que coneta a porta à sua rede ou para suportar os iniciadores e o destino FC.

Do modo CNA para o modo FC

Passos

1. Coloque o adaptador offline:

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

2. Alterar o modo de porta:

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

3. Reinicie o nó e, em seguida, coloque o adaptador online:

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

4. Notifique seu administrador ou gerenciador de VIF para excluir ou remover a porta, conforme aplicável:
   - Se a porta for usada como uma porta inicial de um LIF, for um membro de um grupo de interfaces (ifgrp) ou hosts VLANs, então um administrador deve fazer o seguinte:
     - Mova os LIFs, remova a porta do ifgrp ou exclua as VLANs, respetivamente.
     - Exclua manualmente a porta executando o `network port delete` comando. Se o `network port delete` comando falhar, o administrador deve resolver os erros e, em seguida, executar o comando novamente.
   - Se a porta não for usada como porta inicial de um LIF, não for membro de um ifgrp e não hospedar VLANs, o gerenciador de VIF deve remover a porta de seus Registros no momento da reinicialização. Se o gerenciador de VIF não remover a porta, o administrador deve removê-la manualmente após a reinicialização usando o `network port delete` comando.

     Saiba mais sobre `network port delete` o "Referência do comando ONTAP"na .

5. Verifique se você tem o SFP correto instalado:

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

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB antes de alterar a configuração no nó.

Do modo FC para o modo CNA

Passos

1. Coloque o adaptador offline:

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

2. Alterar o modo de porta:

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

3. Reinicie o nó
4. Verifique se você tem o SFP correto instalado.

   Para CNA, você deve usar um SFP Ethernet 10Gb.

Converta os módulos óticos CNA/UTA2 para a rede ONTAP

Você deve alterar os módulos óticos no adaptador de destino unificado (CNA/UTA2) para suportar o modo de personalidade que você selecionou para o adaptador.

Passos

1. Verifique o SFP atual usado na placa. Em seguida, substitua o SFP atual pelo SFP apropriado para a personalidade preferida (FC ou CNA).
2. Remova os módulos óticos atuais do adaptador X1143A-R6.
3. Insira os módulos corretos para a ótica do seu modo de personalidade (FC ou CNA) preferido.
4. Verifique se você tem o SFP correto instalado:

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

   Os módulos SFP mais suportados e os cabos de cobre (Twinax) da marca Cisco estão listados na "NetApp Hardware Universe".

Remover NICs dos nós de cluster do ONTAP

Você pode ter que remover uma NIC defeituosa de seu slot ou mover a NIC para outro slot para fins de manutenção.

> O procedimento para remover uma NIC é diferente no ONTAP 9,7 e versões anteriores. Se for necessário remover uma NIC de um nó de cluster do ONTAP executando o ONTAP 9,7 e anterior, consulte o procedimento "Removendo uma NIC do nó (ONTAP 9.7 ou anterior)".

Passos

1. Desligue o nó.
2. Remova fisicamente a NIC do respetivo slot.
3. Ligue o nó.

4. Verifique se a porta foi excluída:

```
network port show
```

> O ONTAP remove automaticamente a porta de qualquer grupo de interface. Se a porta fosse o único membro de um grupo de interfaces, o grupo de interfaces será excluído. Saiba mais sobre `network port show` o "Referência do comando ONTAP"na .

5. Se a porta tiver quaisquer VLANs configuradas, elas serão deslocadas. Você pode exibir VLANs deslocadas usando o seguinte comando:

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

> Os `displaced-interface show` comandos , `displaced-vlans show`, e `displaced-vlans restore` são únicos e não requerem o nome do comando totalmente qualificado, que começa com `cluster controller-replacement network`.

6. Essas VLANs são excluídas, mas podem ser restauradas usando o seguinte comando:

```
displaced-vlans restore
```

7. Se a porta tivesse quaisquer LIFs configuradas nela, o ONTAP escolherá automaticamente novas portas residenciais para esses LIFs em outra porta no mesmo domínio de broadcast. Se nenhuma porta inicial adequada for encontrada no mesmo arquivador, esses LIFs são considerados deslocados. Você pode visualizar LIFs deslocados usando o seguinte comando:

   `displaced-interface show`

8. Quando uma nova porta é adicionada ao domínio de broadcast no mesmo nó, as portas iniciais para os LIFs são restauradas automaticamente. Alternativamente, você pode definir a porta inicial usando `network interface modify -home-port -home-node or use the displaced- interface restore` o comando.

Informações relacionadas

- "rede de substituição do controlador do cluster, eliminação da interface deslocada"
- "modificação da interface de rede"

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` 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.

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.

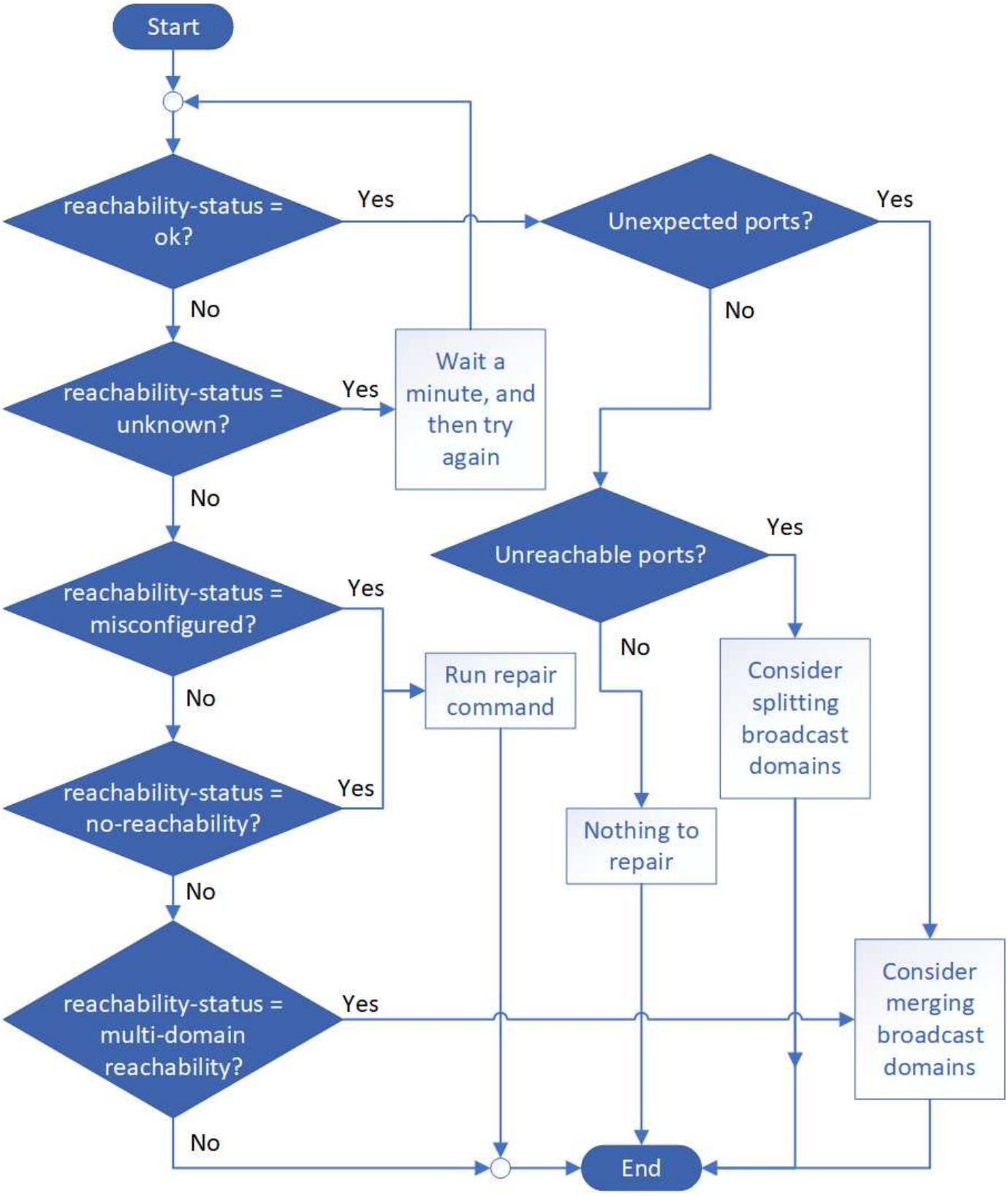
Passo

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	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 . Saiba mais sobre `network port reachability repair` o "Referência do comando ONTAP"na .

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 .

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 ative 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

Informações sobre marcas comerciais