Gerenciamento de rede

ONTAP 9

NetApp
February 12, 2026

Índice

Gerenciamento de rede

Comece agora

Visualize a rede ONTAP usando o Gerenciador do sistema

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para exibir um gráfico que mostra os componentes e a configuração da sua rede, permitindo que você veja os caminhos de conexão de rede entre hosts, portas, SVMs, volumes e muito mais. A partir do ONTAP 9.12,1, você pode visualizar a associação LIF e sub-rede na grade interfaces de rede.

O gráfico é exibido quando você seleciona **rede > Visão geral** ou quando você seleciona → na seção **rede** do painel.

As seguintes categorias de componentes são mostradas no gráfico:

- Hosts
- Portas de storage
- Interfaces de rede
- VMs de storage
- Componentes de acesso a dados

Cada seção mostra detalhes adicionais sobre os quais você pode passar o Mouse ou selecionar para executar tarefas de gerenciamento e configuração de rede.

Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), "Gerir a rede"consulte .

Exemplos

Veja a seguir alguns exemplos das muitas maneiras de interagir com o gráfico para visualizar detalhes sobre cada componente ou iniciar ações para gerenciar sua rede:

- Clique em um host para ver sua configuração: Portas, interfaces de rede, VMs de storage e componentes de acesso a dados associados a ele.
- Passe o Mouse sobre o número de volumes em uma VM de armazenamento para selecionar um volume para exibir seus detalhes.
- Selecione uma interface iSCSI para visualizar o seu desempenho na última semana.
- Clique em ⋮ ao lado de um componente para iniciar ações para modificar esse componente.
- Determine rapidamente onde os problemas podem ocorrer em sua rede, indicado por um "X" ao lado de componentes não saudáveis.

Vídeo de visualização de rede do System Manager

Saiba mais sobre os componentes de rede de um cluster ONTAP

Você deve se familiarizar com os componentes de rede de um cluster antes de configurar o cluster. A configuração dos componentes físicos de rede de um cluster em componentes lógicos fornece a funcionalidade de flexibilidade e alocação a vários clientes no ONTAP.

Os vários componentes de rede em um cluster são os seguintes:

- Portas físicas

  Placas de interface de rede (NICs) e adaptadores de barramento de host (HBAs) fornecem conexões físicas (Ethernet e Fibre Channel) de cada nó para as redes físicas (redes de gerenciamento e dados).

  Para obter informações sobre os requisitos do local, informações sobre o switch, informações sobre o cabeamento da porta integrada da controladora e o cabeamento da porta integrada, consulte o Hardware Universe em "hwu.NetApp.com".

- Portas lógicas

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

- IPspaces

  Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

- Domínios de broadcast

  Um domínio de broadcast reside em um IPspace e contém um grupo de portas de rede, potencialmente de muitos nós no cluster, que pertencem à mesma rede de camada 2. As portas do grupo são usadas em uma SVM para tráfego de dados.

- Sub-redes

  Uma sub-rede é criada dentro de um domínio de broadcast e contém um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Esse conjunto de endereços IP simplifica a alocação de endereços IP durante a criação de LIF.

- Interfaces lógicas

  Uma interface lógica (LIF) é um endereço IP ou um nome de porta mundial (WWPN) associado a uma porta. Ela está associada a atributos como grupos de failover, regras de failover e regras de firewall. Um LIF se comunica através da rede através da porta (física ou lógica) à qual está atualmente vinculado.

  Os diferentes tipos de LIFs em um cluster são LIFs de dados, LIFs de gerenciamento com escopo de cluster, LIFs de gerenciamento com escopo de nó, LIFs entre clusters e LIFs de cluster. A propriedade dos LIFs depende do SVM onde o LIF reside. Os data LIFs são propriedade de Data SVMs, LIFs de gerenciamento com escopo de nó, gerenciamento com escopo de cluster e LIFs entre clusters são de propriedade das SVMs de administrador e os LIFs de cluster são de propriedade do cluster SVM.

- Zonas DNS

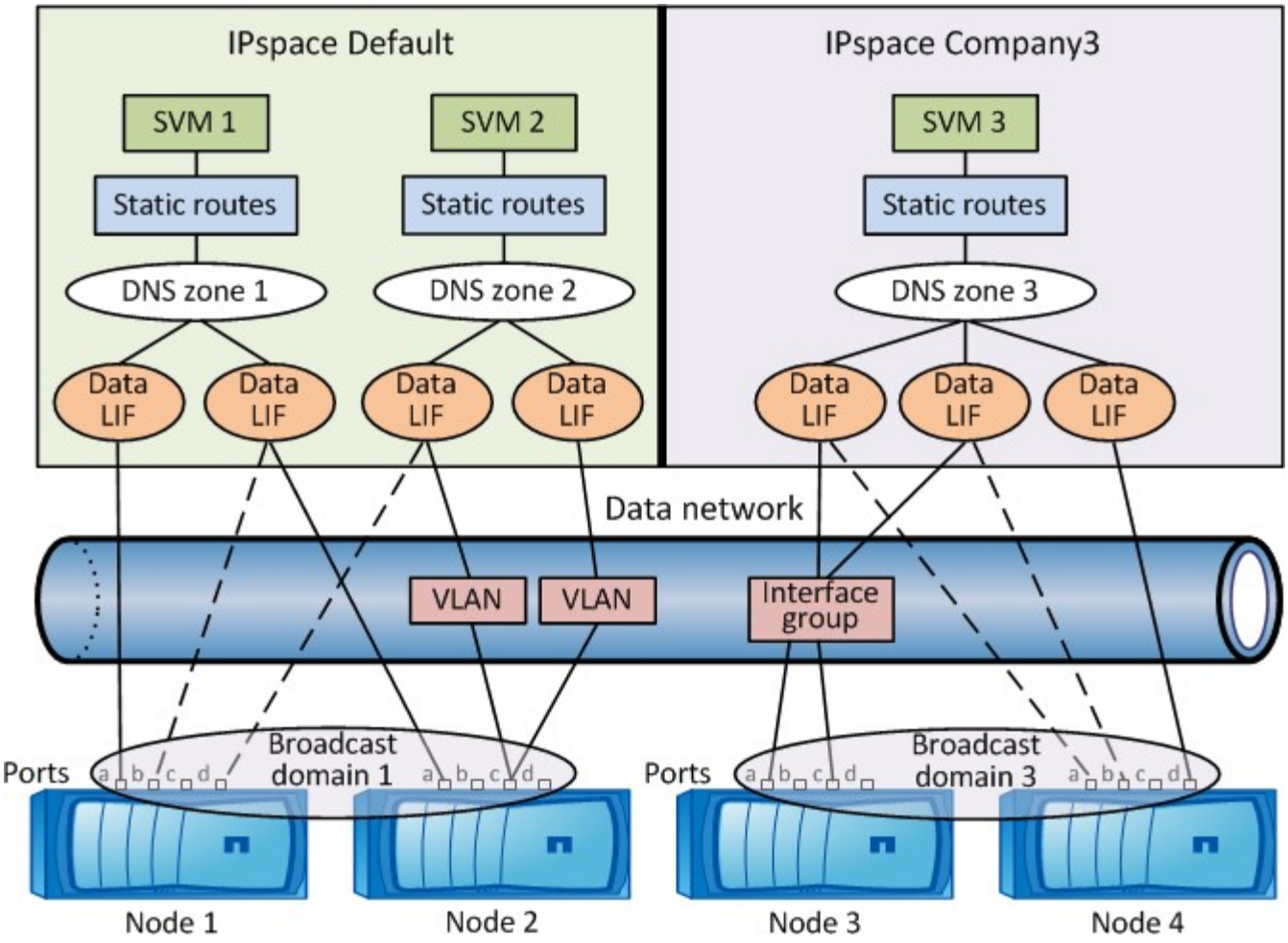
  A zona DNS pode ser especificada durante a criação do LIF, fornecendo um nome para o LIF ser exportado através do servidor DNS do cluster. Vários LIFs podem compartilhar o mesmo nome, permitindo que o recurso de balanceamento de carga DNS distribua endereços IP para o nome de acordo com a carga.

  Os SVMs podem ter várias zonas DNS.

- Roteamento

  Cada SVM é autossuficiente em relação à rede. Um SVM possui LIFs e rotas que podem alcançar cada um dos servidores externos configurados.

  A figura a seguir ilustra como os diferentes componentes de rede estão associados em um cluster de quatro nós:

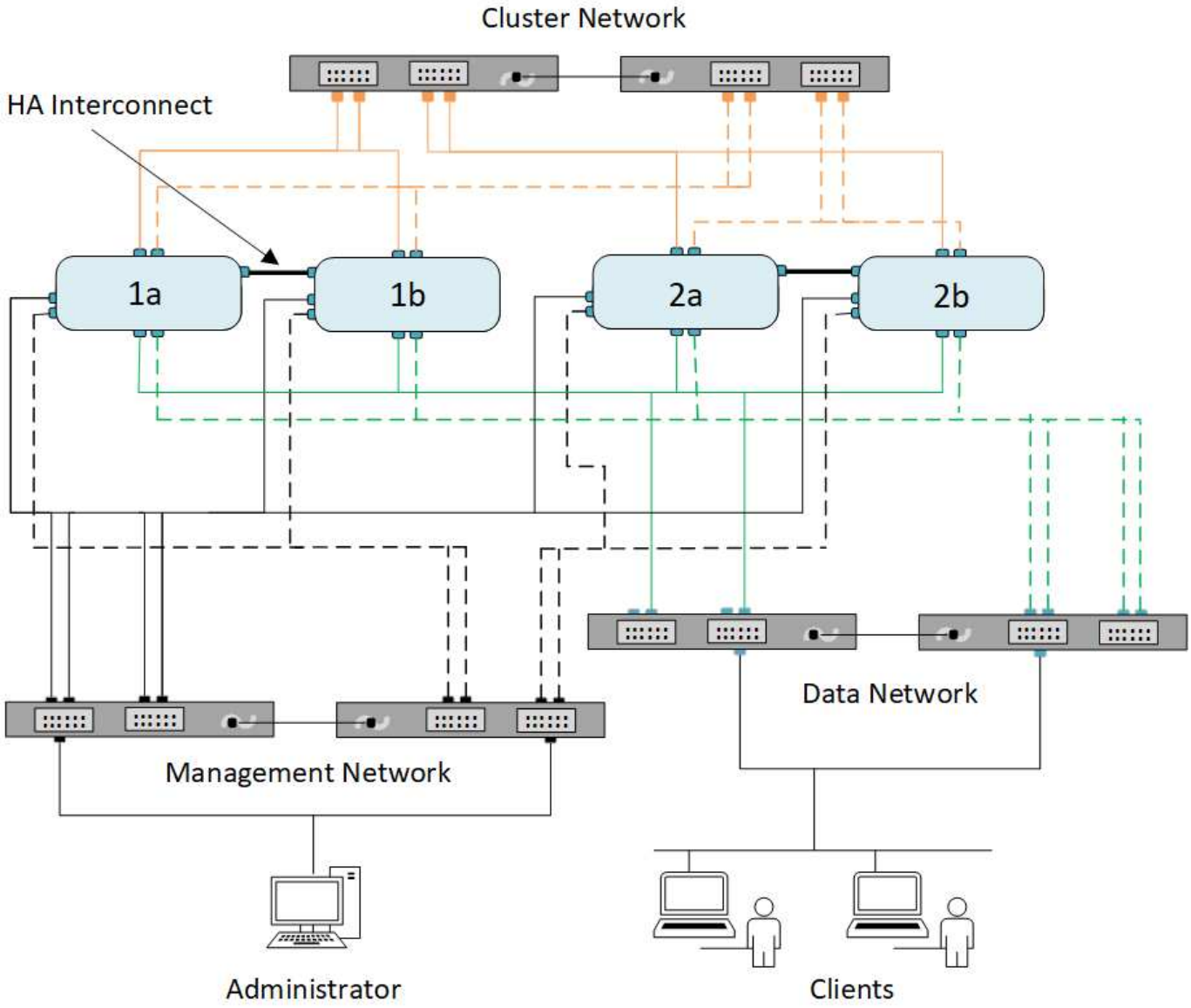


Práticas recomendadas para cabeamento de rede ONTAP

As práticas recomendadas de cabeamento de rede separam o tráfego nas seguintes redes: Cluster, gerenciamento e dados.

Você deve fazer um cabeamento de um cluster para que o tráfego do cluster esteja em uma rede separada de todo o outro tráfego. É uma prática opcional, mas recomendada, separar o tráfego de gerenciamento de rede dos dados e do tráfego entre clusters. Ao manter redes separadas, você pode obter melhor desempenho, facilidade de administração e maior segurança e acesso de gerenciamento aos nós.

O diagrama a seguir ilustra o cabeamento de rede de um cluster HA de quatro nós que inclui três redes separadas:



Você deve seguir certas diretrizes ao fazer cabeamento de conexões de rede:

- Cada nó deve ser conetado a três redes distintas.

  Uma rede é para gerenciamento, outra para acesso aos dados e outra para comunicação entre clusters. A gestão e as redes de dados podem ser logicamente separadas.

- Você pode ter mais de uma conexão de rede de dados para cada nó para melhorar o fluxo de tráfego do cliente (dados).
- Um cluster pode ser criado sem conexões de rede de dados, mas deve incluir uma conexão de interconexão de cluster.
- Sempre deve haver duas ou mais conexões de cluster para cada nó.

Para obter mais informações sobre cabeamento de rede, consulte "Centro de Documentação do sistema AFF e FAS" e "Hardware Universe" .

Determine qual política de failover de LIF deve ser usada em uma rede ONTAP

Domínios de broadcast, grupos de failover e políticas de failover trabalham em conjunto para determinar qual porta assumirá quando o nó ou a porta na qual um LIF é configurado falhar.

Um domínio de broadcast lista todas as portas alcançáveis na mesma rede Ethernet de camada 2. Um pacote de broadcast Ethernet enviado de uma das portas é visto por todas as outras portas no domínio de broadcast. Essa caraterística de acessibilidade comum de um domínio de broadcast é importante para LIFs porque se um LIF falhasse para qualquer outra porta no domínio de broadcast, ele ainda poderia alcançar todos os hosts locais e remotos que estavam acessíveis a partir da porta original.

Os grupos de failover definem as portas dentro de um domínio de broadcast que fornecem cobertura de failover de LIF entre si. Cada domínio de broadcast tem um grupo de failover que inclui todas as suas portas. Esse grupo de failover que contém todas as portas no domínio de broadcast é o grupo de failover padrão e recomendado para o LIF. Você pode criar grupos de failover com subconjuntos menores que você definir, como um grupo de portas de failover que têm a mesma velocidade de link em um domínio de broadcast.

Uma política de failover dita como um LIF usa as portas de um grupo de failover quando um nó ou porta é desativado. Considere a política de failover como um tipo de filtro aplicado a um grupo de failover. Os destinos de failover para um LIF (o conjunto de portas para as quais um LIF pode fazer failover) são determinados aplicando a política de failover de LIF ao grupo de failover de LIF no domínio de broadcast.

Você pode exibir os destinos de failover para um LIF usando o seguinte comando CLI:

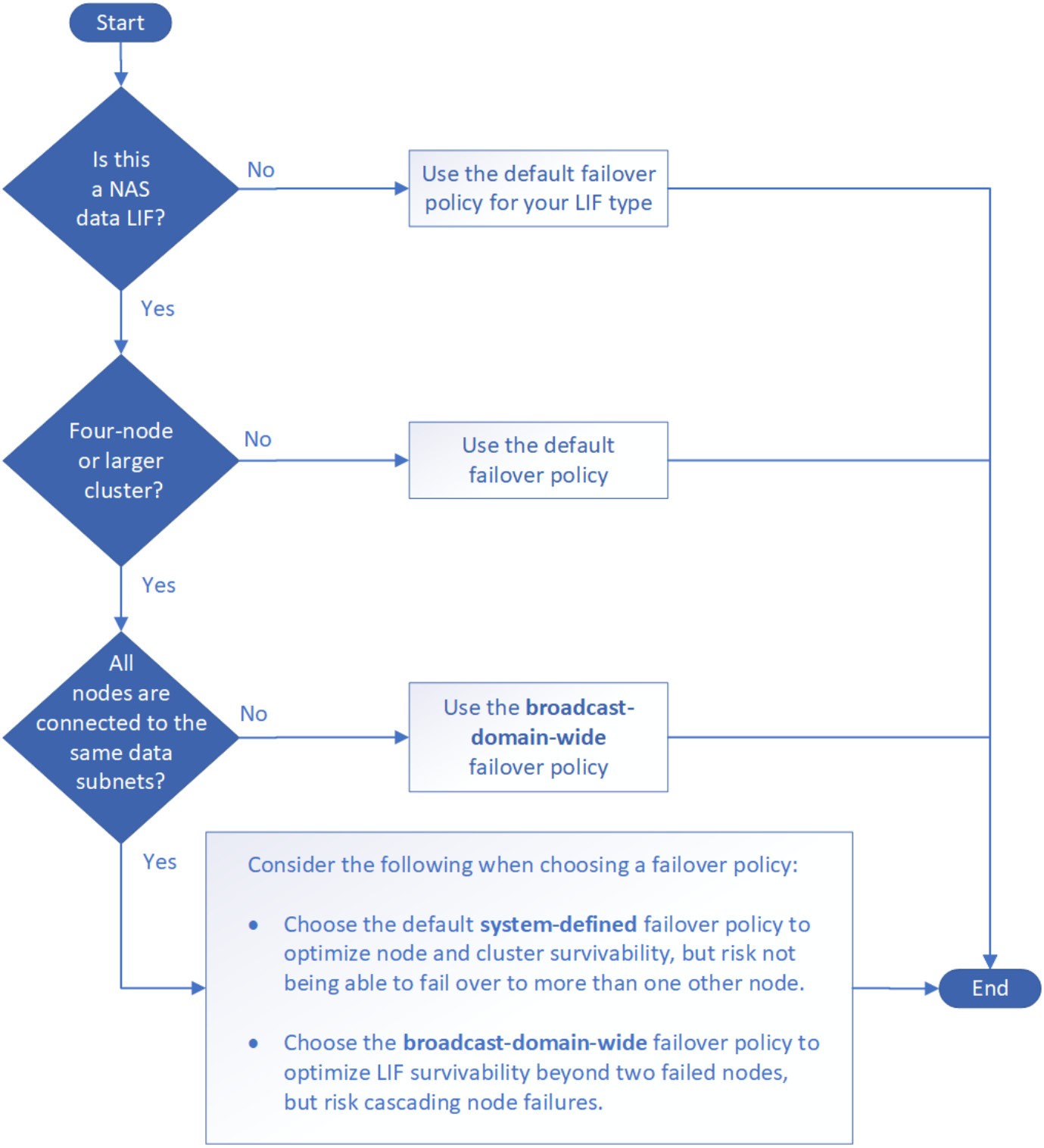
```
network interface show -failover
```

O NetApp recomenda fortemente o uso da política de failover padrão para o seu tipo de LIF.

Decida qual política de failover de LIF usar

Decida se deseja usar a política de failover padrão recomendada ou se deseja alterá-la com base no seu tipo e ambiente de LIF.

Árvore de decisões de política de failover



Políticas de failover padrão por tipo de LIF

Tipo de LIF	Política de failover padrão	Descrição
BGP LIFs	desativado	O LIF não faz failover para outra porta.
LIFs de cluster	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIF de cluster-mgmt	broadcast-domain-wide	O LIF faz failover para portas no mesmo domínio de broadcast, em todos e em todos os nós do cluster.

LIFs entre clusters	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIFs de dados nas	definido pelo sistema	O LIF faz failover para um outro nó que não é o parceiro de HA.
LIFs de gerenciamento de nós	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIFs de dados SAN	desativado	O LIF não faz failover para outra porta.

A política de failover "somente para parceiros sfo" não é padrão, mas pode ser usada quando você deseja que o LIF faça failover para uma porta no nó inicial ou apenas para parceiros SFO.

Informações relacionadas

- "mostra da interface de rede"

Fluxo de trabalho de failover de caminho nas

Configurar failover de caminho nas na rede ONTAP

Se você já estiver familiarizado com os conceitos básicos de rede, poderá economizar tempo configurando sua rede revisando esse fluxo de trabalho "prático" para a configuração de failover de caminho nas.

> O fluxo de trabalho para configurar o failover de caminho nas é diferente no ONTAP 9,7 e versões anteriores. Se você precisar configurar o failover nas em uma rede executando o ONTAP 9,7 e anterior, consulte o fluxo de trabalho "Fluxo de trabalho de failover de caminho nas (ONTAP 9.7 e anterior)".

Um LIF nas migra automaticamente para uma porta de rede sobrevivente após uma falha de link em sua porta atual. Você pode confiar nos padrões do ONTAP para gerenciar o failover de caminho.

> Um SAN LIF não migra (a menos que você o mova manualmente após a falha do link). Em vez disso, a tecnologia multipathing no host desvia o tráfego para um LIF diferente. Para obter mais informações, "Administração da SAN"consulte .

1. **"Complete a Planilha"**

Use a Planilha para Planejar o failover de caminho nas.

2. **"Crie IPspaces"**

Crie um espaço de endereço IP distinto para cada SVM em um cluster.

3. **"Mover domínios de broadcast para IPspaces"**

Mover domínios de broadcast para IPspaces.

4 **"Crie SVMs"**

Crie SVMs para fornecer dados aos clientes.

5 **"Crie LIFs"**

Crie LIFs nas portas que você deseja usar para acessar dados.

6 **"Configurar serviços DNS para o SVM"**

Configure os serviços DNS para o SVM antes de criar um servidor NFS ou SMB.

Planilha para failover de caminho nas na rede ONTAP

Você deve concluir todas as seções da Planilha antes de configurar o failover de caminho nas.

As informações para failover nas na rede ONTAP são diferentes no ONTAP 9,7 e versões anteriores. Se você precisar configurar o failover nas em uma rede executando o ONTAP 9,7 e anterior, "Planilha para a configuração de failover de caminho nas (ONTAP 9.7 e anterior)"consulte .

Configuração IPspace

Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Informações	Obrigatório?	Seus valores
IPspace name o identificador exclusivo do IPspace.	Sim	

Configuração do domínio de difusão

Um domínio de broadcast agrupa portas que pertencem à mesma rede de camada 2 e define a MTU para as portas do domínio de broadcast.

Os domínios de broadcast são atribuídos a um IPspace. Um IPspace pode conter um ou mais domínios de broadcast.

A porta para a qual um LIF falha deve ser membro do grupo de failover para o LIF. Para cada domínio de broadcast criado pelo ONTAP, também é criado um grupo de failover com o mesmo nome que contém todas as portas no domínio de broadcast.

Informações	Obrigatório?	Seus valores

IPspace name o IPspace ao qual o domínio de broadcast é atribuído. Este espaço IPspace tem de existir.	Sim	
Nome de domínio de broadcast o nome do domínio de broadcast. Esse nome deve ser único no IPspace.	Sim	
MTU o valor máximo da unidade de transmissão para o domínio de transmissão, normalmente definido como **1500** ou **9000**. O valor MTU é aplicado a todas as portas no domínio de broadcast e a todas as portas que forem adicionadas posteriormente ao domínio de broadcast. O valor MTU deve corresponder a todos os dispositivos ligados a essa rede. Observe que o gerenciamento de gerenciamento de portas e0M e o tráfego do processador de serviços devem ter o MTU definido para não mais de 1500 bytes.	Sim	
As portas são atribuídas a domínios de broadcast com base na acessibilidade. Depois que a atribuição de porta estiver concluída, verifique a acessibilidade executando o `network port reachability show` comando. Essas portas podem ser portas físicas, VLANs ou grupos de interface. Saiba mais sobre `network port reachability show` o "Referência do comando ONTAP"na .	Sim	

Configuração de sub-rede

Uma sub-rede contém pools de endereços IP e um gateway padrão que pode ser atribuído a LIFs usados por SVMs residentes no IPspace.

- Ao criar um LIF em uma SVM, você pode especificar o nome da sub-rede em vez de fornecer um endereço IP e uma sub-rede.
- Como uma sub-rede pode ser configurada com um gateway padrão, você não precisa criar o gateway padrão em uma etapa separada ao criar um SVM.
- Um domínio de broadcast pode conter uma ou mais sub-redes.

- Você pode configurar LIFs SVM que estão em sub-redes diferentes associando mais de uma sub-rede ao domínio de broadcast do IPspace.
- Cada sub-rede deve conter endereços IP que não se sobreponham aos endereços IP atribuídos a outras sub-redes no mesmo espaço IPspace.
- Você pode atribuir endereços IP específicos a LIFs de dados do SVM e criar um gateway padrão para o SVM em vez de usar uma sub-rede.

Informações	Obrigatório?	Seus valores
IPspace name o IPspace ao qual a sub-rede será atribuída. Este espaço IPspace tem de existir.	Sim	
Nome da sub-rede o nome da sub-rede. Esse nome deve ser único no IPspace.	Sim	
Nome de domínio de broadcast o domínio de broadcast ao qual a sub-rede será atribuída. Esse domínio de broadcast deve residir no espaço IPspace especificado.	Sim	
Nome da sub-rede e mascarar a sub-rede e a máscara em que residem os endereços IP.	Sim	
Gateway você pode especificar um gateway padrão para a sub-rede. Se você não atribuir um gateway ao criar a sub-rede, poderá atribuir um mais tarde.	Não	
Intervalos de endereços IP você pode especificar um intervalo de endereços IP ou endereços IP específicos. Por exemplo, você pode especificar um intervalo como: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` Se você não especificar um intervalo de endereços IP, todo o intervalo de endereços IP na sub-rede especificada estará disponível para atribuir a LIFs.	Não	

Force update of LIF associations especifica se deve forçar a atualização das associações de LIF existentes. Por padrão, a criação de sub-rede falhará se qualquer interface de processador de serviço ou interfaces de rede estiver usando os endereços IP nos intervalos fornecidos. O uso deste parâmetro associa quaisquer interfaces endereçadas manualmente à sub-rede e permite que o comando seja bem-sucedido.	Não	

Configuração SVM

Você usa SVMs para fornecer dados a clientes e hosts.

Os valores que você Registra são para criar um SVM de dados padrão. Se você estiver criando uma SVM de origem MetroCluster, consulte "Guia de instalação e configuração do MetroCluster conectado à malha"ou "Guia de instalação e configuração do Stretch MetroCluster".

Informações	Obrigatório?	Seus valores
SVM nomeie o nome de domínio totalmente qualificado (FQDN) do SVM. Esse nome deve ser único em ligas de cluster.	Sim	
Nome do volume raiz o nome do volume raiz do SVM.	Sim	
Agregar nome o nome do agregado que contém o volume raiz da SVM. Este agregado deve existir.	Sim	
Estilo de segurança o estilo de segurança do volume raiz da SVM. Os valores possíveis são **NTFS**, **unix** e **Mixed**.	Sim	
IPspace nomeie o IPspace ao qual o SVM é atribuído. Este espaço IPspace tem de existir.	Não	
Linguagem SVM que define o idioma padrão a ser usado para o SVM e seus volumes. Se você não especificar um idioma padrão, o idioma SVM padrão será definido como **C.UTF-8**. A configuração de idioma SVM determina o conjunto de carateres usado para exibir nomes e dados de arquivos para todos os volumes nas no SVM. Você pode modificar o idioma após a criação do SVM.	Não	

Configuração LIF

Um SVM fornece dados a clientes e hosts por meio de uma ou mais interfaces lógicas de rede (LIFs).

Informações	Obrigatório?	Seus valores
SVM nomeie o nome do SVM para o LIF.	Sim	
LIF nome o nome do LIF. Você pode atribuir várias LIFs de dados por nó e pode atribuir LIFs a qualquer nó no cluster, desde que o nó tenha portas de dados disponíveis. Para fornecer redundância, você deve criar pelo menos duas LIFs de dados para cada sub-rede de dados e as LIFs atribuídas a uma sub-rede específica devem ser atribuídas portas residenciais em diferentes nós. **Importante:** se você estiver configurando um servidor SMB para hospedar Hyper-V ou SQL Server em SMB para soluções de operação sem interrupções, o SVM deve ter pelo menos um LIF de dados em cada nó no cluster.	Sim	
Política de serviço Política de serviço para o LIF. A política de serviço define quais serviços de rede podem usar o LIF. Serviços incorporados e políticas de serviço estão disponíveis para gerenciar dados e tráfego de gerenciamento em SVMs de dados e do sistema.	Sim	
Os LIFs baseados em IP não exigem protocolos permitidos, use a linha de diretiva de serviço. Especifique protocolos permitidos para SAN LIFs em portas Fibre Channel. Estes são os protocolos que podem usar esse LIF. Os protocolos que usam o LIF não podem ser modificados após a criação do LIF. Você deve especificar todos os protocolos ao configurar o LIF.	Não	
Nó inicial o nó para o qual o LIF retorna quando o LIF é revertido para sua porta inicial. Você deve gravar um nó inicial para cada LIF de dados.	Sim	
A porta inicial ou domínio de broadcast escolheu um dos seguintes: **Port**: Especifique a porta para a qual a interface lógica retorna quando o LIF é revertido para sua porta inicial. Isso só é feito para o primeiro LIF na sub-rede de um espaço IPspace, caso contrário, não é necessário. **Domínio de transmissão**: Especifique o domínio de transmissão e o sistema selecionará a porta apropriada para a qual a interface lógica retorna quando o LIF é revertido para sua porta inicial.	Sim	

Subrede nomeie a sub-rede a ser atribuída ao SVM. Todas as LIFs de dados usadas para criar conexões SMB continuamente disponíveis para servidores de aplicativos devem estar na mesma sub-rede.	Sim (se estiver usando uma sub-rede)	

Configuração DNS

Você deve configurar o DNS na SVM antes de criar um servidor NFS ou SMB.

Informações	Obrigatório?	Seus valores
SVM nomeie o nome do SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Nome de domínio DNS Uma lista de nomes de domínio a anexar a um nome de host ao executar a resolução de nome de host para IP. Liste primeiro o domínio local, seguido pelos nomes de domínio para os quais as consultas DNS são mais frequentemente feitas.	Sim	
Endereços IP dos servidores DNS Lista de endereços IP para os servidores DNS que fornecem resolução de nomes para o servidor NFS ou SMB. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor SMB irá ingressar. O Registro SRV é usado para mapear o nome de um serviço para o nome de computador DNS de um servidor que oferece esse serviço. A criação do servidor SMB falhará se o ONTAP não conseguir obter os Registros de localização do serviço por meio de consultas DNS locais. A maneira mais simples de garantir que o ONTAP possa localizar os Registros SRV do ative Directory é configurar servidores DNS integrados ao ative Directory como servidores DNS SVM. Você pode usar servidores DNS não integrados ao ative Directory desde que o administrador DNS tenha adicionado manualmente os Registros SRV à zona DNS que contém informações sobre os controladores de domínio do ative Directory. Para obter informações sobre os Registros SRV integrados ao ative Directory, consulte o "Como o suporte DNS para ative Directory funciona no Microsoft TechNet"tópico .	Sim	

Configuração de DNS dinâmico

Antes de poder utilizar o DNS dinâmico para adicionar automaticamente entradas de DNS aos servidores DNS integrados do ative Directory, tem de configurar o DNS dinâmico (DDNS) no SVM.

Registros DNS são criados para cada LIF de dados na SVM. Ao criar vários dados LIFS no SVM, você pode equilibrar as conexões de clientes com os endereços IP de dados atribuídos. A carga de DNS equilibra as conexões que são feitas usando o nome do host para os endereços IP atribuídos de forma redonda.

Informações	Obrigatório?	Seus valores
SVM nomeie o SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Se usar o DDNS especifica se deve-se usar o DDNS. Os servidores DNS configurados no SVM devem oferecer suporte a DDNS. Por padrão, o DDNS está desativado.	Sim	
Se usar DDNS seguro o DDNS seguro é suportado apenas com DNS integrado ao ative Directory. Se o DNS integrado ao ative Directory permitir apenas atualizações seguras de DDNS, o valor deste parâmetro deve ser verdadeiro. Por padrão, o DDNS seguro está desativado. O DDNS seguro só pode ser ativado depois de um servidor SMB ou uma conta do ative Directory ter sido criada para o SVM.	Não	
FQDN do domínio DNS o FQDN do domínio DNS. Você deve usar o mesmo nome de domínio configurado para serviços de nome DNS na SVM.	Não	

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

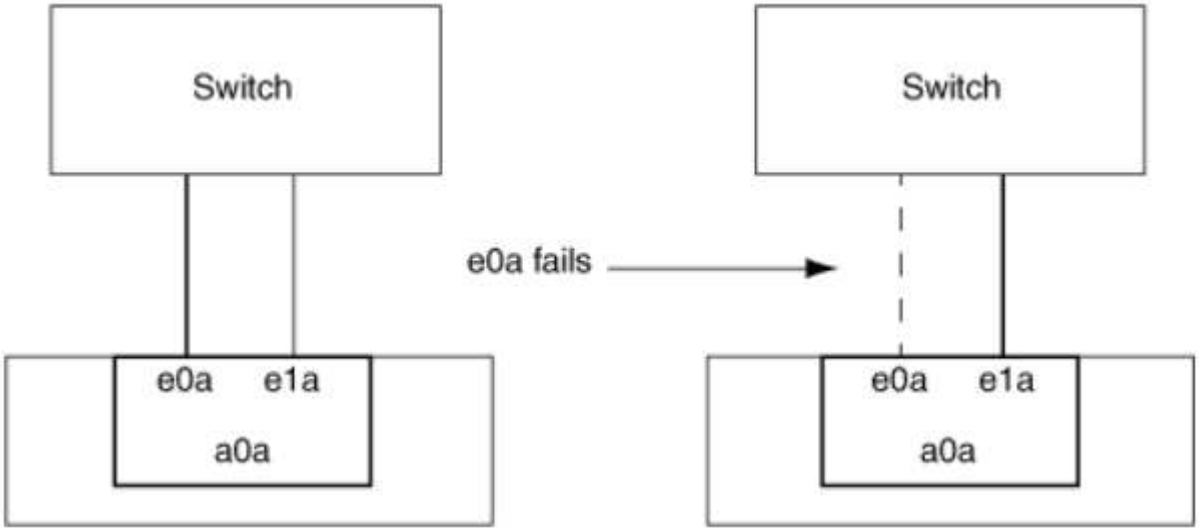
Em um grupo de interface de modo único, apenas uma das interfaces no grupo de interfaces está ativa. As outras interfaces estão em espera, prontas para assumir se a interface ativa falhar.

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.

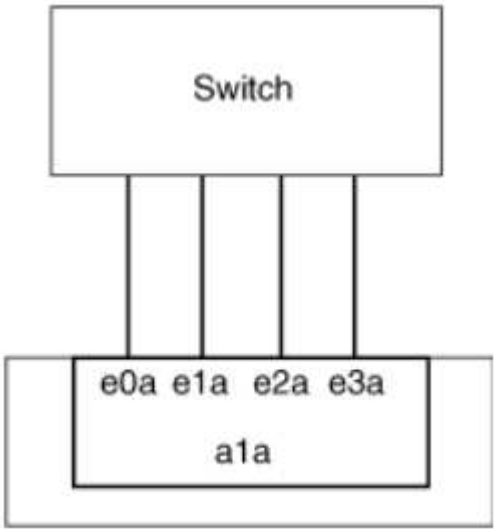
A seguir estão as caraterísticas de um grupo de interfaces multimodo estático:

- 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).

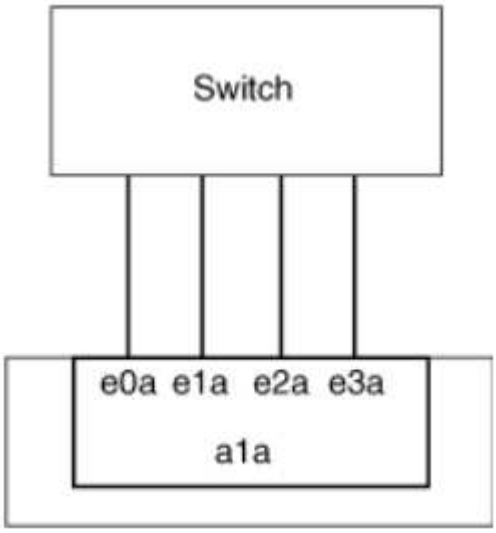
O algoritmo de balanceamento de carga do ONTAP determina a porta membro a ser usada para transmitir tráfego de saída e não controla como os quadros de entrada são recebidos. O switch determina o membro (porta física individual) de seu grupo de canais de portas a ser usado para transmissão, com base no 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.

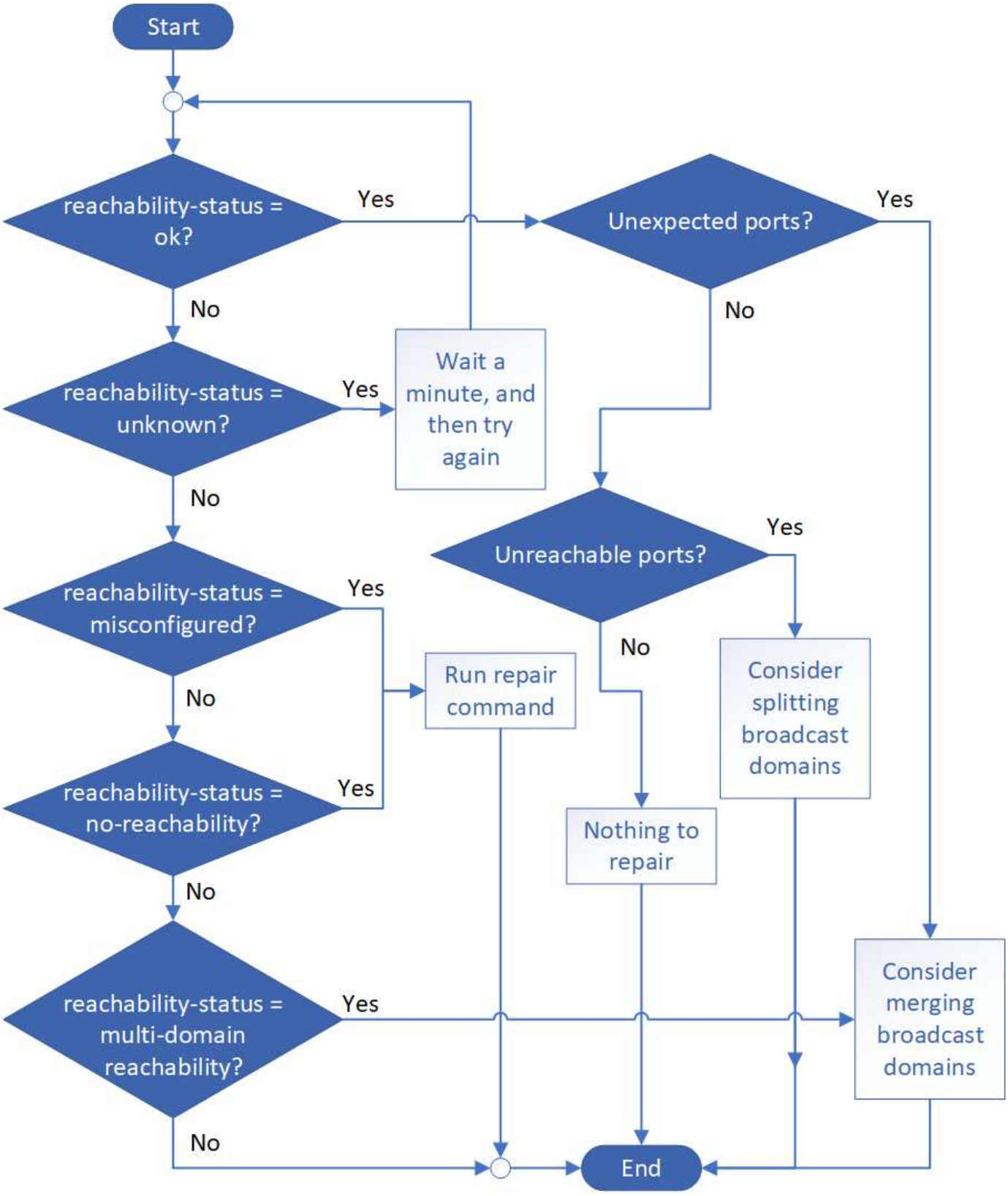
Passo

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

IPspaces

Saiba mais sobre a configuração do ONTAP IPspace

Os IPspaces permitem configurar um único cluster ONTAP para que ele possa ser acessado por clientes de mais de um domínio de rede administrativamente separado, mesmo que esses clientes estejam usando o mesmo intervalo de sub-rede de endereço

IP. Isso permite a separação do tráfego do cliente para privacidade e segurança.

Um espaço IPspace define um espaço de endereço IP distinto no qual as máquinas virtuais de armazenamento (SVMs) residem. As portas e os endereços IP definidos para um espaço IP são aplicáveis apenas nesse espaço IPspace. Uma tabela de roteamento distinta é mantida para cada SVM em um IPspace. Portanto, não ocorre roteamento de tráfego entre SVM ou entre IPspace.

Os IPspaces suportam endereços IPv4 e IPv6 em seus domínios de roteamento.

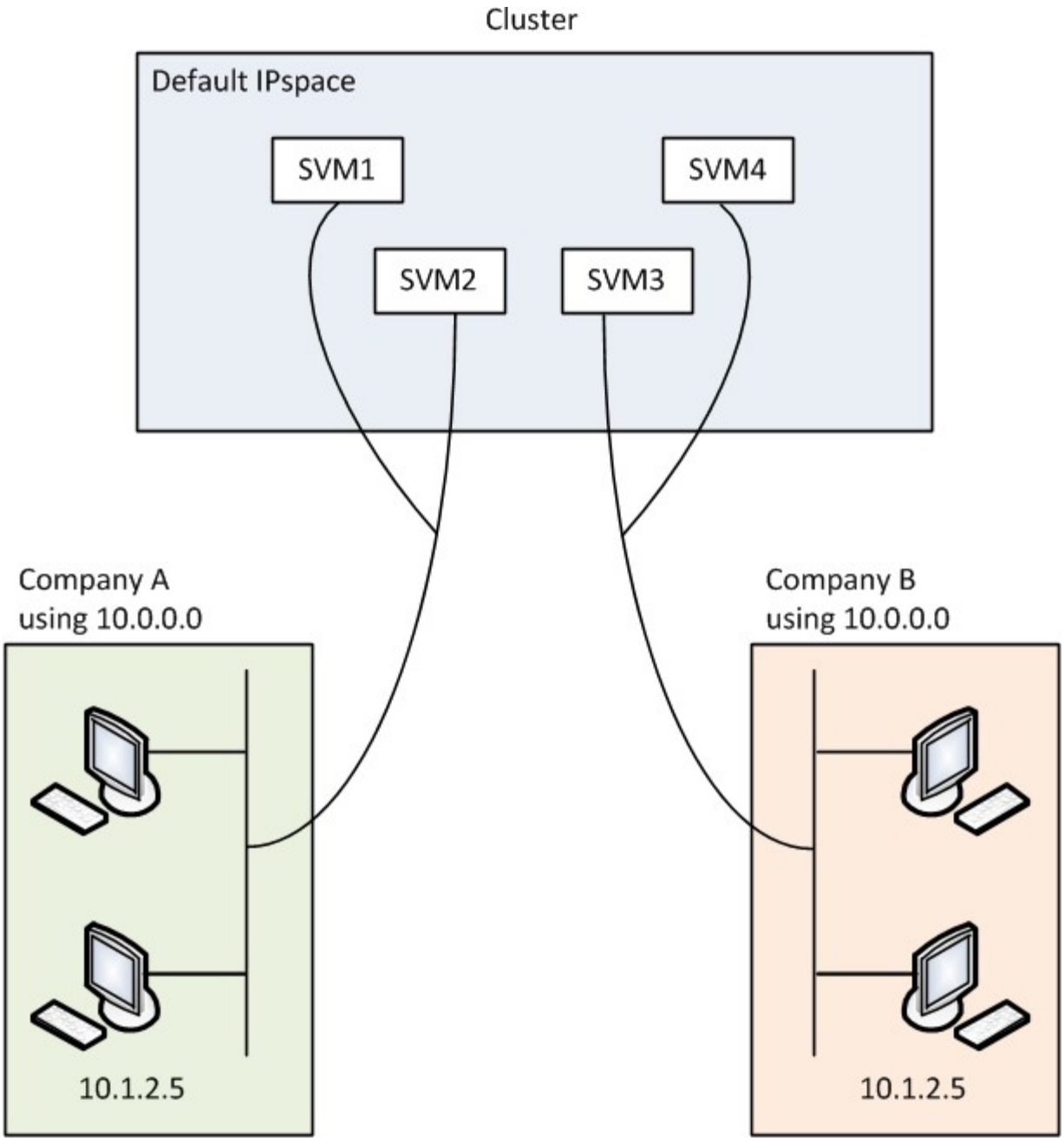
Se você estiver gerenciando o armazenamento para uma única organização, não será necessário configurar os IPspaces. Se você estiver gerenciando o armazenamento para várias empresas em um único cluster do ONTAP e tiver certeza de que nenhum dos seus clientes tem configurações de rede conflitantes, você também não precisa usar espaços IPspaces. Em muitos casos, o uso de máquinas virtuais de armazenamento (SVMs), com suas próprias tabelas de roteamento IP distintas, pode ser usado para segregar configurações de rede exclusivas em vez de usar IPspaces.

Exemplo de uso de IPspaces

Um aplicativo comum para usar espaços IPspaces é quando um provedor de serviços de armazenamento (SSP) precisa conetar clientes das empresas A e B a um cluster ONTAP nas instalações do SSP e ambas as empresas estão usando os mesmos intervalos de endereços IP privados.

O SSP cria SVMs no cluster para cada cliente e fornece um caminho de rede dedicado de dois SVMs para a rede da empresa A e dos outros dois SVMs para a rede da empresa B.

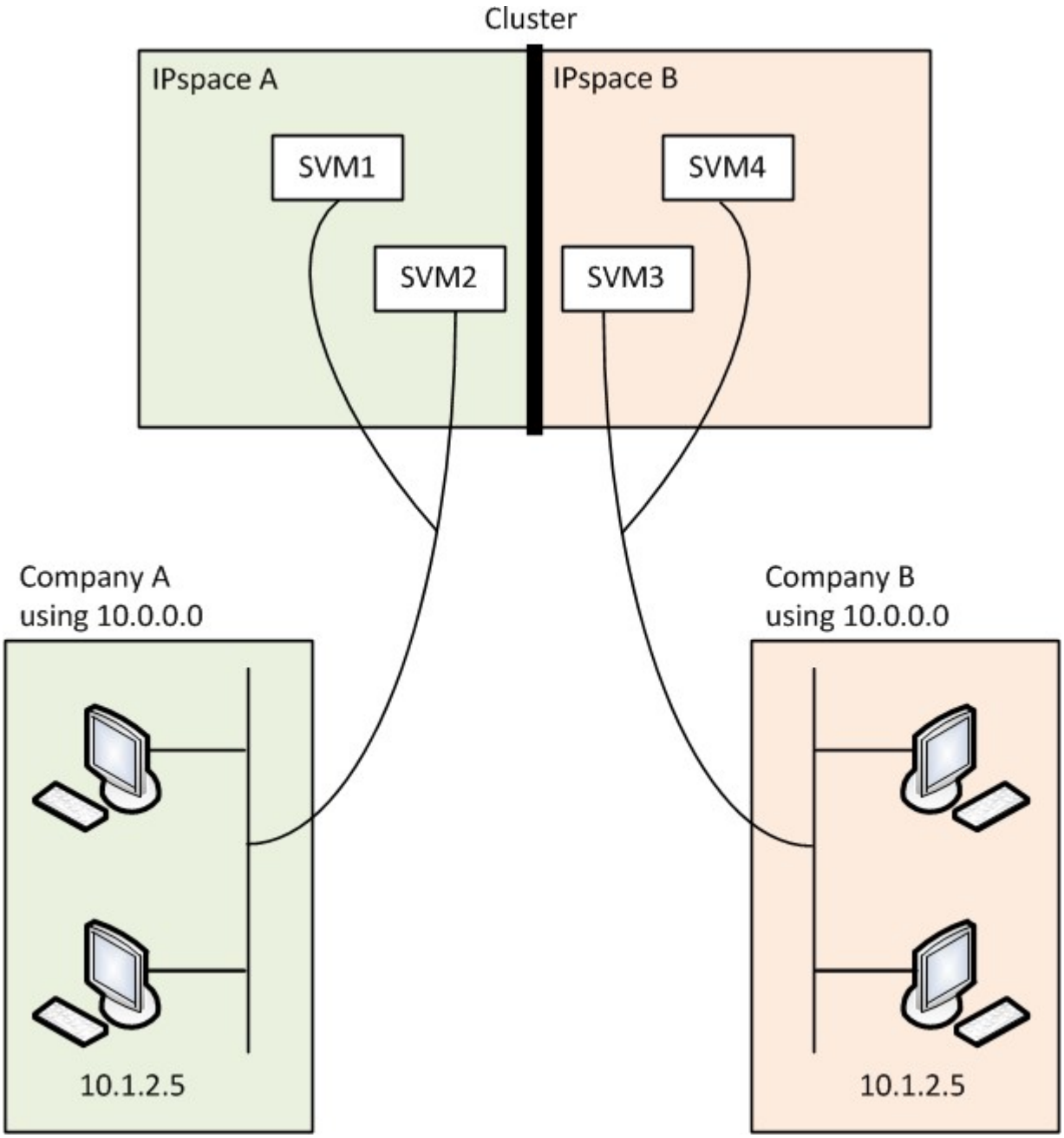
Esse tipo de implantação é mostrado na ilustração a seguir e funciona se ambas as empresas usarem intervalos de endereços IP não privados. No entanto, a ilustração mostra ambas as empresas que usam os mesmos intervalos de endereços IP privados, o que causa problemas.



Ambas as empresas usam a sub-rede de endereço IP privado 10,0.0,0, causando os seguintes problemas:

- Os SVMs no cluster no local SSP têm endereços IP conflitantes se ambas as empresas decidirem usar o mesmo endereço IP para seus respetivos SVMs.
- Mesmo que as duas empresas concordem em usar endereços IP diferentes para seus SVMs, problemas podem surgir.
- Por exemplo, se qualquer cliente na rede De Um tiver o mesmo endereço IP que um cliente na rede B, os pacotes destinados a um cliente no espaço de endereço De Um podem ser roteados para um cliente no espaço de endereço de B e vice-versa.
- Se as duas empresas decidirem usar espaços de endereço mutuamente exclusivos (por exemplo, A usa 10.0.0.0 com uma máscara de rede de 255.128.0.0 e B usa 10.128.0.0 com uma máscara de rede de 255.128.0.0), o SSP precisa configurar rotas estáticas no cluster para rotear o tráfego adequadamente para as redes A e B.

- Essa solução não é escalável (por causa de rotas estáticas) nem segura (o tráfego de broadcast é enviado para todas as interfaces do cluster). Para superar esses problemas, o SSP define dois IPspaces no cluster – um para cada empresa. Como nenhum tráfego cross-IPspace é roteado, os dados de cada empresa são roteados com segurança para sua respetiva rede, mesmo que todos os SVMs estejam configurados no espaço de endereço 10.0.0.0, como mostrado na ilustração a seguir:



Além disso, os endereços IP referidos pelos vários arquivos de configuração, como o `/etc/ hosts` arquivo, o `/etc/hosts.equiv` arquivo e `the /etc/rc` o arquivo, são relativos a esse espaço IPspace. Portanto, os IPspaces permitem que o SSP configure o mesmo endereço IP para os dados de configuração e autenticação para vários SVMs, sem conflito.

Propriedades padrão de IPspaces

IPspaces especiais são criados por padrão quando o cluster é criado pela primeira vez. Além disso, máquinas virtuais de armazenamento especiais (SVMs) são criadas para cada espaço IPspace.

Dois IPspaces são criados automaticamente quando o cluster é inicializado:

- Espaço IPspace "predefinido"

  Esse IPspace é um contêiner para portas, sub-redes e SVMs que atendem dados. Se sua configuração não precisar de IPspaces separados para clientes, todos os SVMs podem ser criados neste IPspace. Este IPspace também contém o gerenciamento de cluster e as portas de gerenciamento de nós.

- Espaço IPspace "cluster"

  Este espaço IPspace contém todas as portas de cluster de todos os nós do cluster. Ele é criado automaticamente quando o cluster é criado. Ele fornece conetividade à rede interna de cluster privado. À medida que nós adicionais se juntam ao cluster, as portas de cluster desses nós são adicionadas ao espaço IPspace "Cluster".

Existe um SVM de "sistema" para cada espaço de IPspace. Quando você cria um IPspace, um SVM do sistema padrão com o mesmo nome é criado:

- O sistema SVM para o IPspace "Cluster" transporta o tráfego de cluster entre nós de um cluster na rede interna de cluster privado.

  Ele é gerenciado pelo administrador do cluster e tem o nome "Cluster".

- O SVM do sistema para o IPspace "padrão" transporta o tráfego de gerenciamento para o cluster e nós, incluindo o tráfego entre clusters.

  Ele é gerenciado pelo administrador do cluster e usa o mesmo nome do cluster.

- O SVM do sistema de um IPspace personalizado que você cria transporta o tráfego de gerenciamento para esse SVM.

  Ele é gerenciado pelo administrador do cluster e usa o mesmo nome que o IPspace.

Um ou mais SVMs para clientes podem existir em um IPspace. Cada SVM de cliente tem seus próprios volumes e configurações de dados, e é administrado independentemente de outras SVMs.

Crie espaços IPspaces para a rede ONTAP

Os IPspaces são espaços de endereço IP distintos nos quais as máquinas virtuais de armazenamento (SVMs) residem. Você pode criar IPspaces quando precisar que seus SVMs tenham seu próprio armazenamento, administração e roteamento seguros. Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Sobre esta tarefa

Há um limite de 512 IPspaces em todo o cluster. O limite de todo o cluster é reduzido para 256 IPspaces para clusters que contêm nós com 6 GB de RAM. Consulte o Hardware Universe para determinar se limites adicionais se aplicam à sua plataforma.

"NetApp Hardware Universe"

Um nome IPspace não pode ser "All" porque "All" é um nome reservado ao sistema.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Criar um espaço IPspace:

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

`ipspace_name` É o nome do IPspace que você deseja criar. O comando a seguir cria o IPspace ipspace1 em um cluster:

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

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

2. Apresentar os IPspaces:

`network ipspace show`

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

O IPspace é criado, juntamente com o sistema SVM para o IPspace. O SVM do sistema transporta tráfego de gerenciamento.

Depois de terminar

Se você criar um espaço de IPspace em um cluster com uma configuração MetroCluster, os objetos de IPspace devem ser replicados manualmente para os clusters de parceiros. Quaisquer SVMs criadas e atribuídas a um IPspace antes da replicação do IPspace não serão replicadas para os clusters de parceiros.

Os domínios de broadcast são criados automaticamente no IPspace "padrão" e podem ser movidos entre IPspaces usando o seguinte comando:

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

Por exemplo, se você quiser mover um domínio de broadcast de "padrão" para "IPS1", usando o seguinte comando:

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

Veja IPspaces na rede ONTAP

Você pode exibir a lista de IPspaces que existem em um cluster e pode exibir as máquinas virtuais de armazenamento (SVMs), domínios de broadcast e portas que são atribuídas a cada IPspace.

Passo

Exibir os IPspaces e SVMs em um cluster:

```
network ipspace show [-ipspace ipspace_name]
```

O comando a seguir exibe todos os domínios IPspaces, SVMs e broadcast no cluster:

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

O comando a seguir exibe os nós e as portas que fazem parte do IPspace ipspace1:

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

Saiba mais sobre `network ipspace show` o "Referência do comando ONTAP"na .

Eliminar espaços IPspaces da rede ONTAP

Se você não precisar mais de um IPspace, você pode excluí-lo.

Antes de começar

Não deve haver domínios de broadcast, interfaces de rede ou SVMs associados ao IPspace que você deseja

excluir.

Os espaços IPspaces "Default" e "Cluster" definidos pelo sistema não podem ser eliminados.

Passo

Eliminar um espaço IPspace:

```
network ipspace delete -ipspace ipspace_name
```

O comando a seguir exclui o IPspace ipspace1 do cluster:

```
network ipspace delete -ipspace ipspace1
```

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

Domínios de broadcast

Saiba mais sobre domínios de broadcast do ONTAP

Os domínios de broadcast destinam-se a agrupar portas de rede que pertencem à mesma rede de camada 2. As portas do grupo podem ser usadas por uma máquina virtual de storage (SVM) para tráfego de dados ou gerenciamento.

> O gerenciamento de domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se você precisar gerenciar domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Visão geral do domínio de broadcast (ONTAP 9 .7 e anteriores)"consulte .

Um domínio de broadcast reside em um IPspace. Durante a inicialização do cluster, o sistema cria dois domínios de broadcast padrão:

- O domínio de broadcast "padrão" contém portas que estão no espaço IPspace "padrão".

  Essas portas são usadas principalmente para fornecer dados. As portas de gerenciamento de clusters e de nós também estão neste domínio de transmissão.

- O domínio de broadcast "Cluster" contém portas que estão no espaço IPspace "Cluster".

  Essas portas são usadas para comunicação de cluster e incluem todas as portas de cluster de todos os nós no cluster.

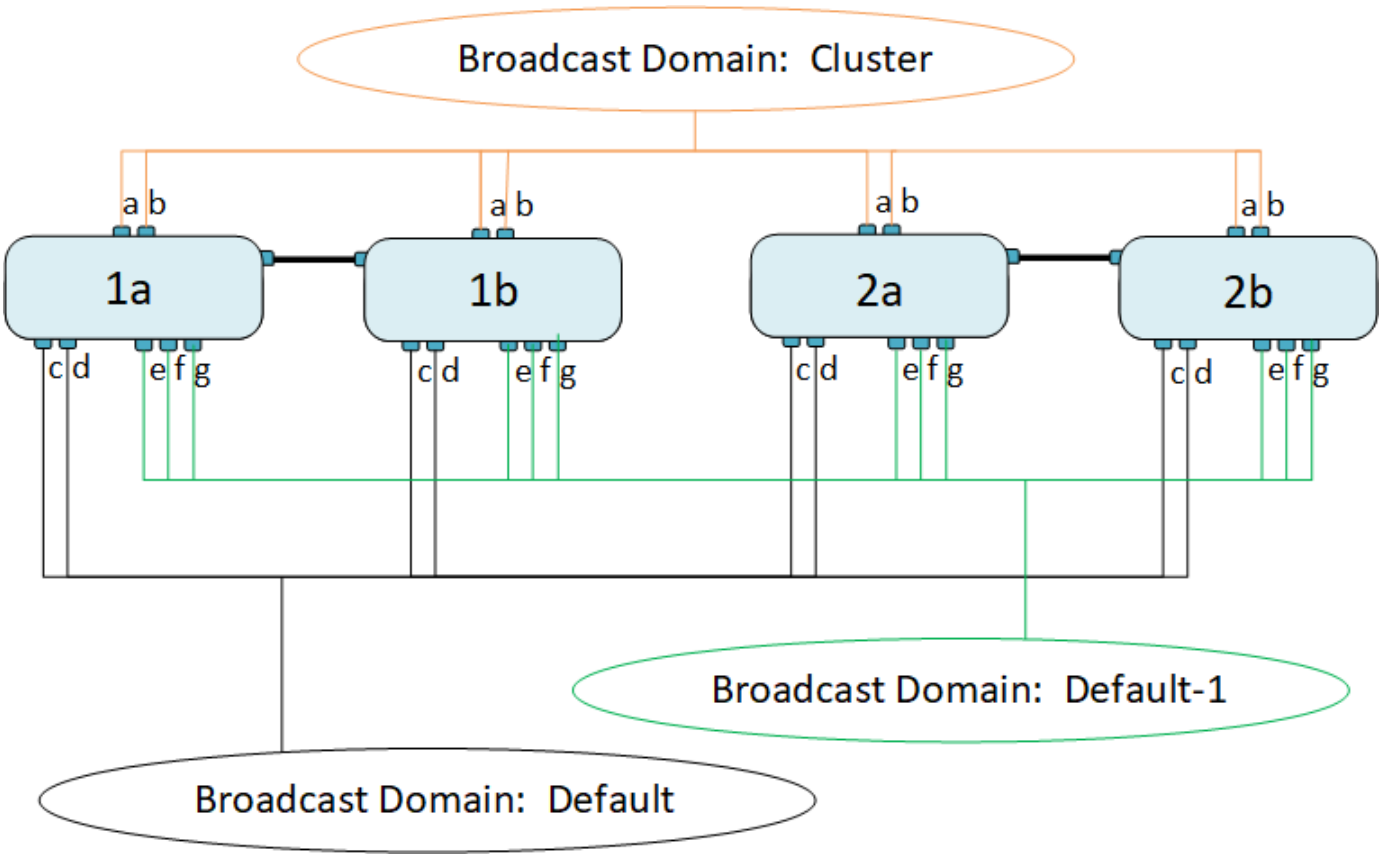
  O sistema cria domínios de broadcast adicionais no IPspace padrão quando necessário. O domínio de broadcast "padrão" contém a porta inicial do LIF de gerenciamento, além de quaisquer outras portas que tenham acessibilidade da camada 2 a essa porta. Domínios de broadcast adicionais são denominados "default-1", "default-2", e assim por diante.

Exemplo de uso de domínios de broadcast

Um domínio de broadcast é um conjunto de portas de rede no mesmo IPspace que também tem acessibilidade da camada 2 umas às outras, normalmente incluindo portas de muitos nós no cluster.

A ilustração mostra as portas atribuídas a três domínios de broadcast em um cluster de quatro nós:

- O domínio de broadcast "Cluster" é criado automaticamente durante a inicialização do cluster e contém as portas a e b de cada nó no cluster.
- O domínio de broadcast "padrão" também é criado automaticamente durante a inicialização do cluster e contém as portas c e d de cada nó no cluster.
- O sistema cria automaticamente quaisquer domínios de broadcast adicionais durante a inicialização do cluster com base na acessibilidade da rede da camada 2. Esses domínios de broadcast adicionais são nomeados default-1, default-2 e assim por diante.



Um grupo de failover com o mesmo nome e com as mesmas portas de rede que cada um dos domínios de broadcast é criado automaticamente. Esse grupo de failover é gerenciado automaticamente pelo sistema, o que significa que, à medida que as portas são adicionadas ou removidas do domínio de broadcast, elas são adicionadas ou removidas automaticamente desse grupo de failover.

Criar domínios de broadcast do ONTAP

Os domínios de broadcast agrupam portas de rede no cluster que pertencem à mesma rede de camada 2. As portas podem então ser usadas por SVMs.

Os domínios de broadcast são criados automaticamente durante a operação de criação ou associação de cluster. A partir do ONTAP 9.12,0, além dos domínios de broadcast criados automaticamente, você pode adicionar manualmente um domínio de broadcast no Gerenciador de sistema.

O procedimento para criar domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se você precisar criar domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Criar um domínio de broadcast (ONTAP 9.7 e anteriores)"consulte .

Antes de começar

As portas que pretende adicionar ao domínio de difusão não devem pertencer a outro domínio de difusão. Se as portas que você deseja usar pertencerem a outro domínio de broadcast, mas não forem utilizadas, remova essas portas do domínio de broadcast original.

Sobre esta tarefa

- Todos os nomes de domínio de broadcast devem ser exclusivos dentro de um espaço IPspace.
- As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de agregação de links/grupos de interface (LAGs/ifgrps).
- Se as portas que você deseja usar pertencerem a outro domínio de broadcast, mas não forem utilizadas, remova-as do domínio de broadcast existente antes de adicioná-las ao novo.
- A unidade máxima de transmissão (MTU) das portas adicionadas a um domínio de broadcast são atualizadas para o valor MTU definido no domínio de broadcast.
- O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.
- Se você não especificar um nome de IPspace, o domínio de broadcast será criado no IPspace "padrão".

Para facilitar a configuração do sistema, um grupo de failover com o mesmo nome é criado automaticamente que contém as mesmas portas.

System Manager

Passos

1. Selecione **rede > Visão geral > domínio Broadcast**.
2. Clique em + Add
3. Nomeie o domínio de broadcast.
4. Defina a MTU.
5. Selecione o espaço IPspace.
6. Salve o domínio de broadcast.

Você pode editar ou excluir um domínio de broadcast depois que ele foi adicionado.

CLI

Se você estiver usando o ONTAP 9.8 e posterior, os domínios de broadcast serão criados automaticamente com base na acessibilidade da camada 2. Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

Você também pode criar manualmente um domínio de broadcast.

Passos

1. Exibir as portas que não estão atualmente atribuídas a um domínio de broadcast:

   `network port show`

   Se a exibição for grande, use o `network port show -broadcast-domain` comando para exibir somente portas não atribuídas.

2. Criar um domínio de broadcast:

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

   a. `broadcast_domain_name` é o nome do domínio de broadcast que você deseja criar.

   b. `mtu_value` É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.

      Esse valor é aplicado a todas as portas que são adicionadas a esse domínio de broadcast.

   c. `ipspace_name` É o nome do IPspace ao qual este domínio de broadcast será adicionado.

      O espaço IPspace "padrão" é usado a menos que você especifique um valor para este parâmetro.

   d. `ports_list` é a lista de portas que serão adicionadas ao domínio de broadcast.

      As portas são adicionadas no formato `node_name:port_number`, por exemplo, `node1:e0c`.

3. Verifique se o domínio de broadcast foi criado conforme desejado:

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

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

Exemplo

O comando a seguir cria o domínio de broadcast bcast1 no IPspace padrão, define o MTU como 1500 e adiciona quatro portas:

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

Saiba mais sobre `network port broadcast-domain create` o "Referência do comando ONTAP"na .

Depois de terminar

Você pode definir o pool de endereços IP que estará disponível no domínio de broadcast criando uma sub-rede ou pode atribuir SVMs e interfaces ao IPspace neste momento. Para obter mais informações, "Peering de cluster e SVM"consulte .

Se você precisar alterar o nome de um domínio de broadcast existente, use o `network port broadcast-domain rename` comando.

Saiba mais sobre `network port broadcast-domain rename` o "Referência do comando ONTAP"na .

Adicione ou remova portas de um domínio de broadcast do ONTAP

Os domínios de broadcast são criados automaticamente durante a operação de criação ou associação de cluster. Não é necessário remover manualmente as portas dos domínios de broadcast.

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e uma porta de rede pertencer a um domínio de broadcast diferente, consulte o seguinte tópico:

"Acessibilidade da porta de reparo"

O procedimento para adicionar ou remover portas para domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se for necessário adicionar ou remover portas de domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Adicionar ou remover portas de um domínio de broadcast (ONTAP 9.7 e anterior)"consulte .

System Manager

A partir do ONTAP 9.14,1, você pode usar o Gerenciador do sistema para reatribuir portas Ethernet em domínios de broadcast. É recomendável atribuir todas as portas Ethernet a um domínio de broadcast. Portanto, se você cancelar a atribuição de uma porta Ethernet de um domínio de broadcast, será necessário reatribuí-la a um domínio de broadcast diferente.

Passos

Para reatribuir portas Ethernet, execute as seguintes etapas:

1. Selecione **rede > Visão geral**.
2. Na seção **Broadcast Domains**, selecione ⋮ ao lado do nome de domínio.
3. No menu suspenso, selecione **Editar**.
4. Na página **Editar domínio de transmissão**, desmarque as portas Ethernet que deseja reatribuir a outro domínio.
5. Para cada porta desmarcada, a janela **Reatribuir porta Ethernet** é exibida. Selecione o domínio de broadcast ao qual deseja reatribuir a porta e selecione **Reatribuir**.
6. Selecione todas as portas que você deseja atribuir ao domínio de broadcast atual e salve as alterações.

CLI

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e uma porta de rede pertencer a um domínio de broadcast diferente, consulte o seguinte tópico:

"Acessibilidade da porta de reparo"

Como alternativa, você pode adicionar ou remover portas manualmente de domínios de broadcast usando o `network port broadcast-domain add-ports` comando ou `network port broadcast-domain remove-ports` .

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- As portas que pretende adicionar a um domínio de difusão não devem pertencer a outro domínio de difusão.
- As portas que já pertencem a um grupo de interfaces não podem ser adicionadas individualmente a um domínio de broadcast.

Sobre esta tarefa

As regras a seguir se aplicam ao adicionar e remover portas de rede:

Ao adicionar portas…	Ao remover portas…
As portas podem ser portas de rede, VLANs ou grupos de interface (ifgrps).	N/A.
As portas são adicionadas ao grupo de failover definido pelo sistema do domínio de broadcast.	As portas são removidas de todos os grupos de failover no domínio de broadcast.
A MTU das portas é atualizada para o valor MTU definido no domínio de broadcast.	A MTU das portas não muda.

O IPspace das portas é atualizado para o valor IPspace do domínio de broadcast.	As portas são movidas para o espaço IPspace 'padrão' sem atributo de domínio de broadcast.

Se você remover a última porta membro de um grupo de interfaces usando o `network port ifgrp remove-port` comando, isso fará com que a porta do grupo de interfaces seja removida do domínio de broadcast porque uma porta de grupo de interfaces vazia não é permitida em um domínio de broadcast. Saiba mais sobre `network port ifgrp remove-port` o "Referência do comando ONTAP"na .

Passos

1. Exiba as portas que estão atualmente atribuídas ou não atribuídas a um domínio de broadcast usando o `network port show` comando.
2. Adicionar ou remover portas de rede do domínio de broadcast:

Se você quiser…	Utilizar…
Adicionar portas a um domínio de broadcast	`network port broadcast-domain add-ports`
Remover portas de um domínio de broadcast	`network port broadcast-domain remove-ports`

3. Verifique se as portas foram adicionadas ou removidas do domínio de broadcast:

   `network port show`

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

Exemplos de adição e remoção de portas

O comando a seguir adiciona a porta e0g no cluster de nó-1-01 e a porta e0g no cluster de nó-1-02 para transmitir o domínio bcast1 no IPspace padrão:

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

O comando a seguir adiciona duas portas de cluster ao cluster de domínio de broadcast no Cluster IPspace:

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

O comando a seguir remove a porta e0e no nó cluster1-01 do domínio de broadcast bcast1 no IPspace padrão:

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

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

Informações relacionadas

- "Referência do comando ONTAP"

Reparar acessibilidade da porta ONTAP

Domínios de broadcast são criados automaticamente. No entanto, se uma porta for recarregada ou a configuração do switch mudar, uma porta pode precisar ser reparada em um domínio de broadcast diferente (novo ou existente).

O ONTAP pode detetar e recomendar automaticamente soluções para problemas de fiação de rede com base na acessibilidade da camada 2 de um componente de domínio de transmissão (portas ethernet).

A fiação incorreta durante pode causar uma atribuição inesperada da porta do domínio de broadcast. A partir do ONTAP 9.10,1, o cluster verifica automaticamente problemas de fiação de rede verificando a acessibilidade da porta após a configuração do cluster ou quando um novo nó se junta a um cluster existente.

System Manager

Se for detetado um problema de acessibilidade da porta, o System Manager recomenda uma operação de reparo para resolver o problema.

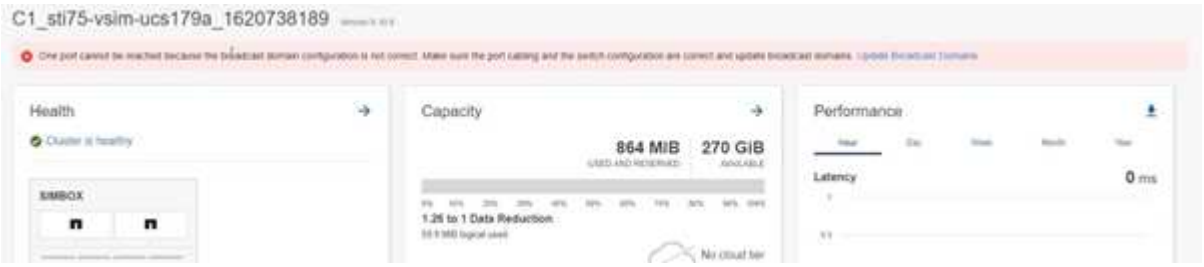
Depois de configurar o cluster, os problemas de fiação de rede são relatados no Dashboard.

Depois de unir um novo nó a um cluster, os problemas de fiação de rede aparecem na página nós.

Também pode ver o estado da cablagem da rede no diagrama da rede. Os problemas de acessibilidade da porta são indicados no diagrama de rede por um ícone de erro vermelho.

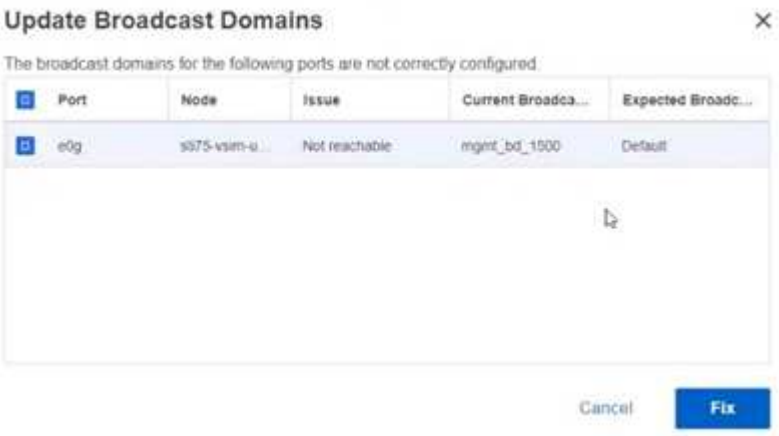
Configuração pós-cluster

Depois de configurar o cluster, se o sistema detetar um problema de fiação de rede, uma mensagem será exibida no Dashboard.



Passos

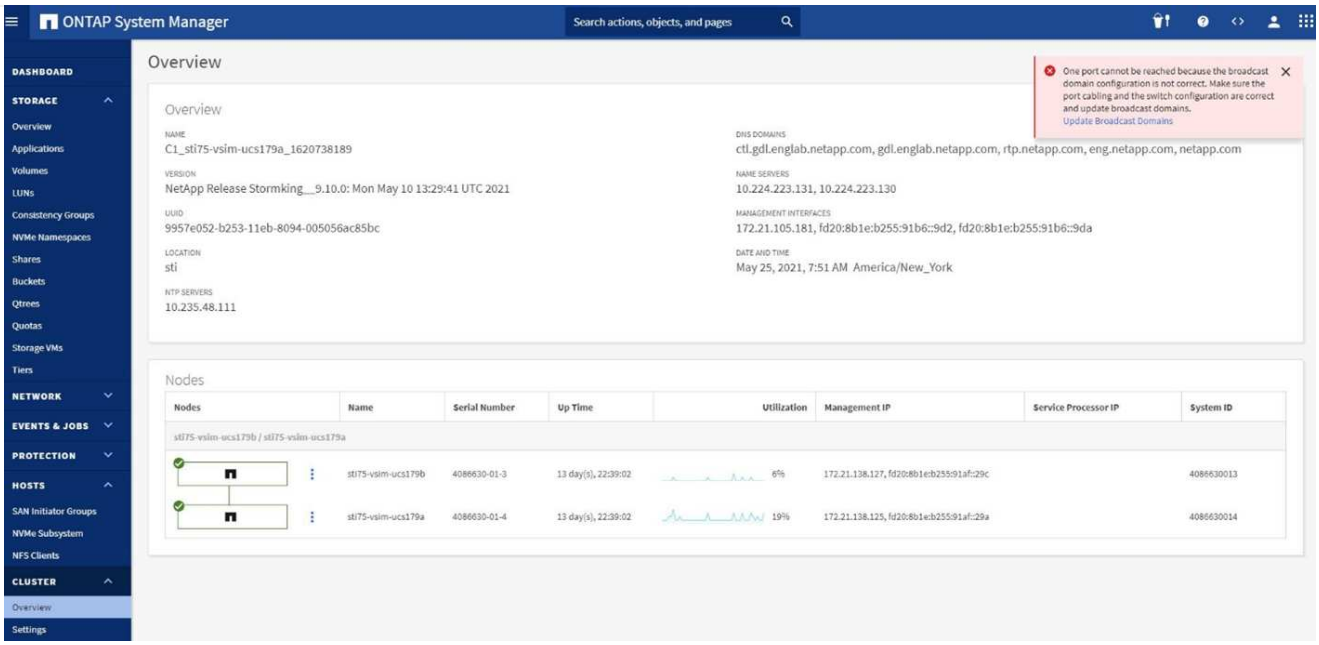
1. Corrija a fiação conforme sugerido na mensagem.
2. Clique no link para iniciar a caixa de diálogo Atualizar domínios de transmissão. A caixa de diálogo Atualizar domínios de transmissão é aberta.



3. Revise as informações sobre a porta, incluindo o nó, os problemas, o domínio de broadcast atual e o domínio de broadcast esperado.
4. Selecione as portas que deseja reparar e clique em **Fix**. O sistema moverá as portas do domínio de broadcast atual para o domínio de broadcast esperado.

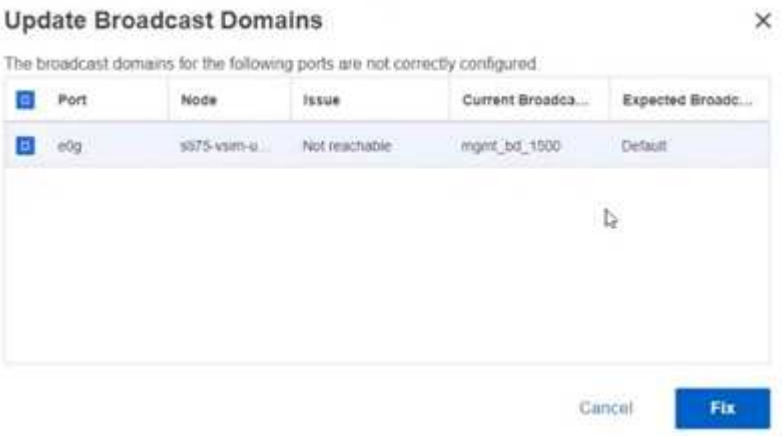
Post node join

Depois de unir um novo nó a um cluster, se o sistema detetar um problema de fiação de rede, uma mensagem será exibida na página nós.



Passos

1. Corrija a fiação conforme sugerido na mensagem.
2. Clique no link para iniciar a caixa de diálogo Atualizar domínios de transmissão. A caixa de diálogo Atualizar domínios de transmissão é aberta.



3. Revise as informações sobre a porta, incluindo o nó, os problemas, o domínio de broadcast atual e o domínio de broadcast esperado.
4. Selecione as portas que deseja reparar e clique em **Fix**. O sistema moverá as portas do domínio de broadcast atual para o domínio de broadcast esperado.

CLI

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Sobre esta tarefa

Um comando está disponível para reparar automaticamente a configuração do domínio de broadcast para uma porta baseada na acessibilidade da camada 2 detetada pelo ONTAP.

Passos

1. Verifique a configuração e o cabeamento do switch.

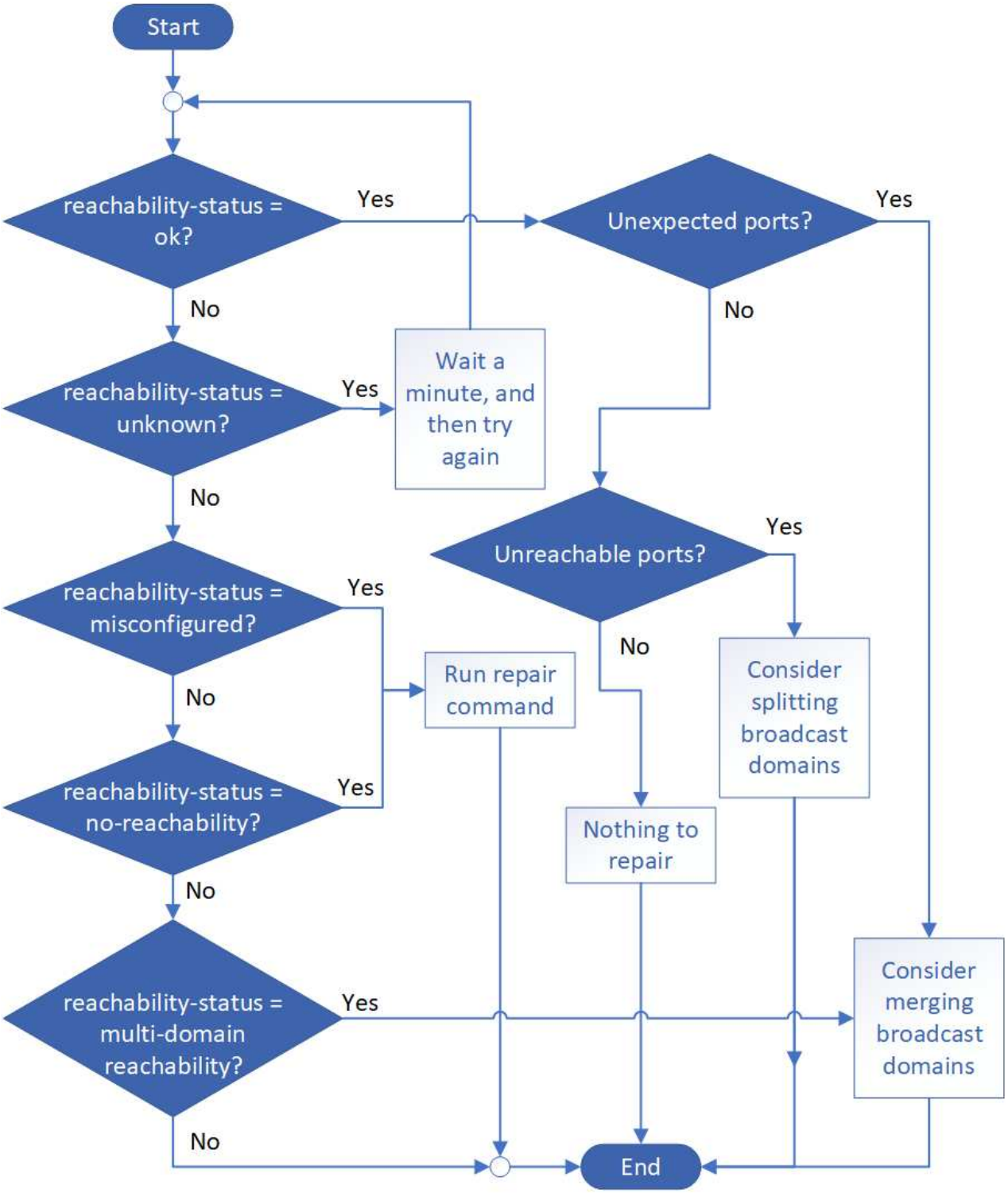
2. Verifique a acessibilidade da porta:

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

   O comando output contém resultados de acessibilidade.

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

3. Use a tabela e a árvore de decisão a seguir para entender os resultados de acessibilidade e determinar o que, se alguma coisa, fazer a seguir.



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`

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` **Nota:** se todas as portas membros do grupo de interfaces (ifgrp) reportarem `no-reachability`, executar o `network port reachability repair` comando em cada porta membro faria com que cada uma fosse removida do ifgrp e colocada em um novo domínio de broadcast, eventualmente fazendo com que o próprio ifgrp fosse removido. Antes de executar o `network port reachability repair` comando, verifique se o domínio de broadcast acessível da porta é o que você espera com base na topologia física da rede. 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, "Mesclar domínios de broadcast"consulte .
desconhecido	Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.

Depois de reparar uma porta, verifique se há 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.

LIFs

Quando uma porta é reparada e movida para um domínio de broadcast diferente, todos os LIFs que foram configurados na porta reparada receberão automaticamente uma nova porta inicial. Essa porta inicial é selecionada a partir do mesmo domínio de broadcast no mesmo nó, se possível. Alternativamente, uma porta inicial de outro nó é selecionada ou, se não existirem portas residenciais adequadas, a porta inicial será limpa.

Se a porta inicial de um LIF for movida para outro nó ou for limpa, então o LIF é considerado como "deslocado". Você pode visualizar esses LIFs deslocados com o seguinte comando:

```
displaced-interface show
```

Se houver LIFs deslocados, você deve:

- Restaure a casa do LIF deslocado:

```
displaced-interface restore
```

- Defina a casa do LIF manualmente:

  ```
  network interface modify -home-port -home-node
  ```

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

- Remova a entrada da tabela "interface deslocada" se estiver satisfeito com a página inicial atualmente configurada do LIF:

  ```
  displaced-interface delete
  ```

VLANs

Se a porta reparada tivesse VLANs, essas VLANs serão excluídas automaticamente, mas também serão registradas como tendo sido "deslocadas". Você pode exibir essas VLANs deslocadas:

```
displaced-vlans show
```

Se houver quaisquer VLANs deslocadas, você deve:

- Restaure as VLANs para outra porta:

  ```
  displaced-vlans restore
  ```

- Remova a entrada da tabela "Displaced-vlans":

  ```
  displaced-vlans delete
  ```

Grupos de interfaces

Se a porta reparada fizer parte de um grupo de interfaces, ela será removida desse grupo de interfaces. Se fosse a única porta membro atribuída ao grupo de interfaces, o próprio grupo de interfaces será removido.

Informações relacionadas

- "Verifique a configuração da rede após a atualização"
- "Monitore a acessibilidade das portas de rede"
- "Referência do comando ONTAP"

Mover domínios de broadcast ONTAP para espaços IPspaces

A partir do ONTAP 9,8, você pode mover os domínios de broadcast que o sistema criou com base na acessibilidade da camada 2 para os IPspaces criados.

Antes de mover o domínio de broadcast, você deve verificar a acessibilidade das portas em seus domínios de broadcast.

A verificação automática das portas pode determinar quais portas podem alcançar umas às outras e colocá-las no mesmo domínio de broadcast, mas essa verificação não consegue determinar o espaço IPspace apropriado. Se o domínio de broadcast pertencer a um espaço IPspace não padrão, você deve movê-lo

manualmente usando as etapas desta seção.

Antes de começar

Os domínios de broadcast são configurados automaticamente como parte das operações de criação e associação de cluster. O ONTAP define o domínio de broadcast "padrão" como o conjunto de portas que têm conetividade de camada 2 à porta inicial da interface de gerenciamento no primeiro nó criado no cluster. Outros domínios de broadcast são criados, se necessário, e são nomeados **default-1**, **default-2**, e assim por diante.

Quando um nó se une a um cluster existente, suas portas de rede se juntam automaticamente aos domínios de broadcast existentes com base em sua acessibilidade da camada 2. Se eles não tiverem acessibilidade a um domínio de broadcast existente, as portas serão colocadas em um ou mais novos domínios de broadcast.

Sobre esta tarefa

- As portas com LIFs de cluster são colocadas automaticamente no espaço IPspace "Cluster".
- As portas com acessibilidade à porta inicial do LIF de gerenciamento de nó são colocadas no domínio de broadcast "padrão".
- Outros domínios de broadcast são criados automaticamente pelo ONTAP como parte da operação de criação ou associação de cluster.
- À medida que você adiciona VLANs e grupos de interface, eles são automaticamente colocados no domínio de broadcast apropriado cerca de um minuto após serem criados.

Passos

1. Verifique a acessibilidade das portas em seus domínios de broadcast. O ONTAP monitora automaticamente a acessibilidade da camada 2. Use o seguinte comando para verificar se cada porta foi adicionada a um domínio de broadcast e tem acessibilidade "ok".

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

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

2. Se necessário, mova domínios de broadcast para outros IPspaces:

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

   Por exemplo, se você quiser mover um domínio de broadcast de "padrão" para "IPS1":

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

Informações relacionadas

- "movimentação de domínio de broadcast da porta de rede"

Dividir domínios de broadcast do ONTAP

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e um grupo de portas de rede previamente configuradas em um único domínio de broadcast tiver sido particionado em dois conjuntos de acessibilidade diferentes, você pode dividir um domínio de broadcast para sincronizar a configuração do ONTAP com a topologia de rede física.

O procedimento para dividir domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se você precisar dividir domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Domínios de broadcast divididos (ONTAP 9,7 ou anterior)"consulte .

Para determinar se um domínio de broadcast de porta de rede está particionado em mais de um conjunto de acessibilidade, use o `network port reachability show -details` comando e preste atenção às portas que não têm conetividade entre si ("portas inacessíveis"). 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. Saiba mais sobre `network port reachability show` o "Referência do comando ONTAP"na .

Passo

Divida um domínio de broadcast em dois domínios de broadcast:

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

- `ipspace_name` é o nome do ipspace onde reside o domínio de broadcast.
- `-broadcast-domain` é o nome do domínio de broadcast que será dividido.
- `-new-broadcast-domain` é o nome do novo domínio de broadcast que será criado.
- `-ports` é o nome e a porta do nó a serem adicionados ao novo domínio de broadcast.

Informações relacionadas

- "divisão de domínio de transmissão da porta de rede"

Mesclar domínios de broadcast ONTAP

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e dois grupos de portas de rede previamente configurados em vários domínios de broadcast agora todos compartilham acessibilidade, a mesclagem de dois domínios de broadcast pode ser usada para sincronizar a configuração do ONTAP com a topologia de rede física.

O procedimento para mesclar domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se você precisar mesclar domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Mesclar domínios de broadcast (ONTAP 9,7 ou anterior)"consulte .

Para determinar se vários domínios de transmissão pertencem a um conjunto de acessibilidade, use o `network port reachability show -details` comando e preste atenção em quais portas configuradas em outro domínio de transmissão realmente têm conectividade entre si ("Portas inesperadas"). Normalmente, a lista de portas inesperadas define o conjunto de portas que devem ser mescladas no domínio de broadcast depois de verificar se a configuração física e do switch é precisa.

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

Passo

Mesclar as portas de um domínio de broadcast em um domínio de broadcast existente:

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

- `ipspace_name` é o nome do ipspace onde os domínios de broadcast residem.
- `-broadcast-domain` é o nome do domínio de broadcast que será mesclado.
- `-into-broadcast-domain` é o nome do domínio de broadcast que receberá portas adicionais.

Informações relacionadas

- "broadcast-domain-merge da porta de rede"

Altere o valor MTU para portas em um domínio de broadcast ONTAP

Você pode modificar o valor MTU de um domínio de broadcast para alterar o valor MTU para todas as portas nesse domínio de broadcast. Isso pode ser feito para suportar alterações de topologia que foram feitas na rede.

O procedimento para alterar o valor MTU para portas de domínio de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se for necessário alterar o valor MTU para portas de domínio de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Alterar o valor MTU para portas em um domínio de broadcast (ONTAP 9.7 e anterior)"consulte .

System Manager

A partir do ONTAP 9.12.1, você pode usar System Manager para modificar o valor de MTU de um domínio de broadcast para alterar o valor de MTU de todas as portas nesse domínio de broadcast.

Passos

1. Selecione **Network > Broadcast Domains**.
2. Na seção **Broadcast Domains**, selecione o nome do broadcast domain para o qual você deseja alterar o valor de MTU.
3. Uma mensagem será exibida confirmando que você deseja alterar o valor de MTU para todas as portas no domínio de broadcast. Clique em **Sim** para prosseguir com a alteração.
4. Modifique o valor de MTU conforme necessário e salve suas alterações.

   O sistema aplica o novo valor de MTU a todas as portas no domínio de broadcast, o que causa uma breve interrupção no tráfego sobre essas portas.

CLI

Antes de começar

O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.

Sobre esta tarefa

Alterar o valor de MTU causa uma breve interrupção no tráfego nas portas afetadas. O sistema exibe uma mensagem que você deve responder com **y** para fazer a alteração de MTU.

Passo

Altere o valor MTU para todas as portas em um domínio de broadcast:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

Onde:

- `broadcast_domain` é o nome do domínio de broadcast.
- `mtu` É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.
- `ipspace` é o nome do IPspace no qual este domínio de broadcast reside. O IPspace "Default" é usado a menos que você especifique um valor para esta opção.

  O seguinte comando altera o MTU para 9000 para todas as portas no domínio de broadcast bcast1:

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

Informações relacionadas

- "modificação do domínio de difusão da porta de rede"

Veja domínios de broadcast do ONTAP

Você pode exibir a lista de domínios de broadcast dentro de cada espaço IPspace em um cluster. A saída também mostra a lista de portas e o valor MTU para cada domínio de broadcast.

O procedimento para exibir domínios de broadcast é diferente no ONTAP 9,7 e versões anteriores. Se for necessário exibir domínios de broadcast em uma rede executando o ONTAP 9,7 e anterior, "Exibir domínios de broadcast (ONTAP 9,7 ou anterior)"consulte .

Passo

Exiba os domínios de broadcast e as portas associadas no cluster:

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

O comando a seguir exibe todos os domínios de broadcast e portas associadas no cluster:

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

O comando a seguir exibe as portas no domínio de broadcast padrão-1 que têm um status de atualização de erro, o que indica que a porta não pôde ser atualizada corretamente:

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

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

Informações relacionadas

- "exibição de domínio de broadcast da porta de rede"

Excluir domínios de broadcast do ONTAP

Se você não precisar mais de um domínio de broadcast, você pode excluí-lo. Isso move as portas associadas a esse domínio de broadcast para o espaço IPspace "padrão".

Antes de começar

Não deve haver sub-redes, interfaces de rede ou SVMs associadas ao domínio de broadcast que você deseja excluir.

Sobre esta tarefa

- O domínio de broadcast "Cluster" criado pelo sistema não pode ser excluído.
- Todos os grupos de failover relacionados ao domínio de broadcast são removidos quando você exclui o domínio de broadcast.

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

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador de sistema para excluir um domínio de broadcast

A opção de exclusão não é exibida quando o domínio de broadcast contém portas ou está associado a uma sub-rede.

Passos

1. Selecione **rede > Visão geral > domínio Broadcast**.
2. Selecione **> Excluir** ao lado do domínio de broadcast que deseja remover.

CLI

Use a CLI para excluir um domínio de broadcast

Passo

Excluir um domínio de broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

O seguinte comando exclui o domínio de broadcast default-1 no IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Informações relacionadas

- "exclusão de domínio de broadcast da porta de rede"

Grupos e políticas de failover

Saiba mais sobre o failover de LIF em redes ONTAP

Failover de LIF refere-se à migração automática de um LIF para uma porta de rede diferente em resposta a uma falha de link na porta atual do LIF. Este é um componente chave para fornecer alta disponibilidade para as conexões com SVMs. A configuração do failover de LIF envolve a criação de um grupo de failover, a modificação do LIF para usar o grupo de failover e a especificação de uma política de failover.

Um grupo de failover contém um conjunto de portas de rede (portas físicas, VLANs e grupos de interfaces) de um ou mais nós em um cluster. As portas de rede que estão presentes no grupo failover definem os destinos de failover disponíveis para o LIF. Um grupo de failover pode ter gerenciamento de clusters, gerenciamento de nós, clusters e LIFs de dados nas atribuídos a ele.

Quando um LIF é configurado sem um destino de failover válido, ocorre uma interrupção quando o LIF tenta fazer failover. Você pode usar o `network interface show -failover` comando para verificar a configuração de failover. Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Quando você cria um domínio de broadcast, um grupo de failover com o mesmo nome é criado automaticamente que contém as mesmas portas de rede. Esse grupo de failover é gerenciado automaticamente pelo sistema, o que significa que, à medida que as portas são adicionadas ou removidas do domínio de broadcast, elas são adicionadas ou removidas automaticamente desse grupo de failover. Isso é fornecido como uma eficiência para administradores que não desejam gerenciar seus próprios grupos de failover.

Criar grupos de failover do ONTAP

Você cria um grupo de failover de portas de rede para que um LIF possa migrar automaticamente para uma porta diferente se ocorrer uma falha de link na porta atual do LIF. Isto permite que o sistema redirecione o tráfego de rede para outras portas disponíveis no cluster.

Sobre esta tarefa

Use o `network interface failover-groups create` comando para criar o grupo e adicionar portas ao grupo.

- As portas adicionadas a um grupo de failover podem ser portas de rede, VLANs ou grupos de interface (ifgrps).
- Todas as portas adicionadas ao grupo failover devem pertencer ao mesmo domínio de broadcast.
- Uma única porta pode residir em vários grupos de failover.
- Se você tiver LIFs em diferentes VLANs ou domínios de broadcast, configure grupos de failover para cada VLAN ou domínio de broadcast.
- Os grupos de failover não se aplicam a ambientes SAN iSCSI ou FC.

Passo

Criar um grupo de failover:

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

- *`vserver_name`* É o nome do SVM que pode usar o grupo failover.
- *`failover_group_name`* é o nome do grupo de failover que você deseja criar.
- *`ports_list`* é a lista de portas que serão adicionadas ao grupo failover. As portas são adicionadas no formato *node_name>:<port_number>*, por exemplo, node1:e0c.

O comando a seguir cria o grupo de failover FG3 para SVM VS3 e adiciona duas portas:

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

Depois de terminar

- Você deve aplicar o grupo failover a um LIF agora que o grupo failover foi criado.
- A aplicação de um grupo de failover que não forneça um destino de failover válido para um LIF resulta em uma mensagem de aviso.

Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

- Saiba mais sobre `network interface failover-groups create` o "Referência do comando ONTAP"na .

Configure as configurações de failover do ONTAP em um LIF

Você pode configurar um LIF para fazer failover para um grupo específico de portas de rede aplicando uma política de failover e um grupo de failover ao LIF. Você também pode desativar um LIF de falhar para outra porta.

Sobre esta tarefa

- Quando um LIF é criado, o failover de LIF é ativado por padrão e a lista de portas de destino disponíveis é determinada pelo grupo de failover padrão e pela política de failover com base no tipo de LIF e na política de serviço.

  A partir de 9,5, você pode especificar uma política de serviço para o LIF que define quais serviços de rede podem usar o LIF. Alguns serviços de rede impõem restrições de failover em um LIF.

  Se a política de serviço de LIF for alterada de uma forma que restrinja ainda mais o failover, a política de failover de LIF é atualizada automaticamente pelo sistema.

- Você pode modificar o comportamento de failover de LIFs especificando valores para os parâmetros -failover-group e -failover-policy no comando Network Interface Modify.
- A modificação de um LIF que faz com que o LIF não tenha um destino de failover válido resulta em uma mensagem de aviso.

  Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

- A partir do ONTAP 9.11,1, em plataformas de array all-flash SAN (ASA), o failover de LIF iSCSI é ativado automaticamente em LIFs iSCSI recém-criadas em VMs de storage recém-criadas.

  Além disso, você pode "Ative manualmente o failover de iSCSI LIF em iSCSI LIFs pré-existentes", significando LIFs que foram criados antes da atualização para o ONTAP 9.11,1 ou posterior.

- A lista a seguir descreve como a configuração de política -failover afeta as portas de destino selecionadas no grupo failover:

  Para failover de LIF iSCSI, apenas as políticas de failover `local-only` , `sfo-partner-only` e `disabled` são suportadas.

  - `broadcast-domain-wide` aplica-se a todas as portas em todos os nós do grupo failover.
  - `system-defined` Aplica-se apenas às portas no nó inicial do LIF e a um outro nó no cluster, normalmente um parceiro não SFO, se existir.
  - `local-only` Aplica-se apenas às portas no nó inicial do LIF.
  - `sfo-partner-only` Aplica-se apenas às portas no nó inicial do LIF e ao seu parceiro SFO.
  - `disabled` Indica que o LIF não está configurado para failover.

Passos

Configurar as configurações de failover para uma interface existente:

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

Exemplos de configuração de configurações de failover e desativação de failover

O comando a seguir define a política de failover para broadcast-domain-wide e usa as portas no grupo de failover FG3 como destinos de failover para LIF data1 na SVM VS3:

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

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

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

O seguinte comando desativa o failover para LIF data1 na SVM VS3:

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

Informações relacionadas

- "interface de rede"

Comandos ONTAP para gerenciar grupos e políticas de failover

Você pode usar os `network interface failover-groups` comandos para gerenciar grupos de failover. Você usa o `network interface modify` comando para gerenciar os grupos de failover e as políticas de failover aplicadas a um LIF.

Se você quiser…	Use este comando…
Adicionar portas de rede a um grupo de failover	`network interface failover-groups add-targets`
Remova as portas de rede de um grupo de failover	`network interface failover-groups remove-targets`
Modifique as portas de rede em um grupo de failover	`network interface failover-groups modify`

Exibir os grupos de failover atuais	`network interface failover-groups show`
Configurar failover em um LIF	`network interface modify -failover -group -failover-policy`
Exibir o grupo de failover e a política de failover que estão sendo usados por cada LIF	`network interface show -fields failover-group, failover-policy`
Renomeie um grupo de failover	`network interface failover-groups rename`
Excluir um grupo de failover	`network interface failover-groups delete`

Modificar um grupo de failover de modo que ele não forneça um destino de failover válido para qualquer LIF no cluster pode resultar em uma interrupção quando um LIF tenta fazer failover.

Informações relacionadas

- "interface de rede"

Sub-redes (somente administradores de cluster)

Saiba mais sobre sub-redes para a rede ONTAP

As sub-redes permitem alocar blocos ou pools específicos de endereços IP para a configuração da rede ONTAP. Isso permite que você crie LIFs mais facilmente especificando um nome de sub-rede em vez de precisar especificar o endereço IP e os valores de máscara de rede.

Uma sub-rede é criada dentro de um domínio de broadcast e contém um conjunto de endereços IP que pertencem à mesma sub-rede de camada 3. Os endereços IP em uma sub-rede são alocados às portas no domínio de broadcast quando os LIFs são criados. Quando os LIFs são removidos, os endereços IP são retornados ao pool de sub-redes e estão disponíveis para LIFs futuros.

É recomendável que você use sub-redes porque elas facilitam muito o gerenciamento de endereços IP e tornam a criação de LIFs um processo mais simples. Além disso, se você especificar um gateway ao definir uma sub-rede, uma rota padrão para esse gateway será adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.

Crie sub-redes para a rede ONTAP

Você pode criar uma sub-rede para alocar blocos específicos de endereços IPv4 ou IPv6 a serem usados posteriormente quando você criar LIFs para o SVM.

Isso permite que você crie LIFs mais facilmente especificando um nome de sub-rede em vez de precisar especificar o endereço IP e os valores de máscara de rede para cada LIF.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

O domínio de broadcast e o IPspace onde você pretende adicionar a sub-rede já devem existir.

Sobre esta tarefa

- Todos os nomes de sub-rede devem ser exclusivos dentro de um espaço IPspace.
- Ao adicionar intervalos de endereços IP a uma sub-rede, você deve garantir que não haja endereços IP sobrepostos na rede para que diferentes sub-redes ou hosts não tentem usar o mesmo endereço IP.
- Se você especificar um gateway ao definir uma sub-rede, uma rota padrão para esse gateway será adicionada automaticamente ao SVM quando um LIF for criado usando essa sub-rede. Se você não usar sub-redes ou se não especificar um gateway ao definir uma sub-rede, precisará usar o `route create` comando para adicionar uma rota ao SVM manualmente.
- O NetApp recomenda a criação de objetos de sub-rede para todas as LIFs em SVMs de dados. Isso é especialmente importante para as configurações do MetroCluster, onde o objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque cada objeto de sub-rede tem um domínio de broadcast associado.

Passos

Você pode criar uma sub-rede com o Gerenciador de sistema do ONTAP ou com a CLI do ONTAP.

System Manager

A partir do ONTAP 9.12,0, você pode usar o Gerenciador do sistema para criar uma sub-rede.

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Clique + Add para criar uma sub-rede.
3. Nomeie a sub-rede.
4. Especifique o endereço IP da sub-rede.
5. Defina a máscara de sub-rede.
6. Defina o intervalo de endereços IP que compõem a sub-rede.
7. Se útil, especifique um gateway.
8. Selecione o domínio de broadcast ao qual a sub-rede pertence.
9. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para criar uma sub-rede.

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

- `subnet_name` é o nome da sub-rede da camada 3 que você deseja criar.

  O nome pode ser uma cadeia de texto como "Mgmt" ou pode ser um valor IP de sub-rede específico como 192,0.2,0/24.

- `broadcast_domain_name` é o nome do domínio de broadcast onde a sub-rede residirá.
- `ipspace_name` É o nome do IPspace do qual o domínio de broadcast faz parte.

  O espaço IPspace "padrão" é usado a menos que você especifique um valor para esta opção.

- `subnet_address` É o endereço IP e a máscara da sub-rede; por exemplo, 192,0.2,0/24.
- `gateway_address` é o gateway para a rota padrão da sub-rede; por exemplo, 192,0.2,1.
- `ip_address_list` É a lista, ou intervalo, de endereços IP que serão alocados à sub-rede.

  Os endereços IP podem ser endereços individuais, um intervalo de endereços IP ou uma combinação em uma lista separada por vírgulas.

- O valor `true` pode ser definido para a `-force-update-lif-associations` opção.

  Este comando falhará se algum processador de serviço ou interfaces de rede estiverem usando os endereços IP no intervalo especificado. Definir este valor como verdadeiro associa quaisquer interfaces endereçadas manualmente à sub-rede atual e permite que o comando seja bem-sucedido.

O comando a seguir cria a sub-rede SUB1 no domínio de broadcast default-1 no espaço IPspace padrão. Ele adiciona um endereço IP de sub-rede IPv4 e uma máscara, o gateway e um intervalo de endereços IP:

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

O comando a seguir cria a sub-rede sub2 no padrão de domínio de broadcast no IPspace "padrão". Ele adiciona um intervalo de endereços IPv6:

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

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

Depois de terminar

Você pode atribuir SVMs e interfaces a um espaço IPspace usando os endereços na sub-rede.

Se você precisar alterar o nome de uma sub-rede existente, use o `network subnet rename` comando.

Saiba mais sobre `network subnet rename` o "Referência do comando ONTAP"na .

Adicione ou remova endereços IP de uma sub-rede para a rede ONTAP

Você pode adicionar endereços IP ao criar inicialmente uma sub-rede ou adicionar endereços IP a uma sub-rede que já existe. Você também pode remover endereços IP de uma sub-rede existente. Isso permite alocar apenas os endereços IP necessários para SVMs.

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

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para adicionar ou remover endereços IP de ou para uma sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Editar** ao lado da sub-rede que deseja alterar.
3. Adicionar ou remover endereços IP.
4. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para adicionar ou remover endereços IP de ou para uma sub-rede

Sobre esta tarefa

Ao adicionar endereços IP, você receberá um erro se qualquer processador de serviço ou interfaces de rede estiver usando os endereços IP no intervalo que está sendo adicionado. Se pretender associar quaisquer interfaces endereçadas manualmente à sub-rede atual, pode definir a `-force-update-lif-associations` opção como `true`.

Ao remover endereços IP, você receberá um erro se qualquer processador de serviço ou interfaces de rede estiver usando os endereços IP sendo removidos. Se pretender que as interfaces continuem a utilizar os endereços IP após serem removidos da sub-rede, pode definir a `-force-update-lif-associations` opção como `true`.

Passo

Adicionar ou remover endereços IP de uma sub-rede:

Se você quiser…	Use este comando…
Adicione endereços IP a uma sub-rede	extensões de sub-rede
Remover endereços IP de uma sub-rede	remover-intervalos de sub-rede

O comando a seguir adiciona endereços IP 192.0.2.82 a 192.0.2.85 à sub-rede SUB1:

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

O seguinte comando remove o endereço IP 198.51.100.9 da sub-rede sub3:

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

Se o intervalo atual inclui 1 a 10 e 20 a 40, e você deseja adicionar 11 a 19 e 41 a 50 (basicamente permitindo 1 a 50), você pode sobrepor o intervalo existente de endereços usando o seguinte comando. Este comando adiciona apenas os novos endereços e não afeta os endereços existentes:

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

Saiba mais sobre `network subnet add-ranges` e `network subnet remove-ranges` no "Referência do comando ONTAP".

Altere as propriedades da sub-rede para a rede ONTAP

Você pode alterar o endereço de sub-rede e o valor da máscara, o endereço de gateway ou o intervalo de endereços IP em uma sub-rede existente.

Sobre esta tarefa

- Ao modificar endereços IP, você deve garantir que não haja endereços IP sobrepostos na rede para que diferentes sub-redes ou hosts não tentem usar o mesmo endereço IP.
- Se você adicionar ou alterar o endereço IP do gateway, o gateway modificado será aplicado a novos SVMs quando um LIF é criado neles usando a sub-rede. Uma rota padrão para o gateway é criada para o SVM se a rota ainda não existir. Talvez seja necessário adicionar manualmente uma nova rota ao SVM ao alterar o endereço IP do gateway.

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

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para alterar as propriedades da sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Editar** ao lado da sub-rede que deseja alterar.
3. Faça alterações.
4. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para alterar as propriedades da sub-rede

Passo

Modificar propriedades de sub-rede:

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

- `subnet_name` é o nome da sub-rede que você deseja modificar.
- `ipspace` É o nome do espaço IPspace onde reside a sub-rede.
- `subnet` é o novo endereço e máscara da sub-rede, se aplicável; por exemplo, 192,0.2,0/24.
- `gateway` é o novo gateway da sub-rede, se aplicável; por exemplo, 192,0.2,1. A introdução de **''** remove a entrada do gateway.
- `ip_ranges` É a nova lista, ou intervalo, de endereços IP que serão alocados à sub-rede, se aplicável. Os endereços IP podem ser endereços individuais, um intervalo ou endereços IP ou uma combinação em uma lista separada por vírgulas. O intervalo especificado aqui substitui os endereços IP existentes.
- `force-update-lif-associations` É necessário quando você altera o intervalo de endereços IP. Você pode definir o valor para **true** para essa opção ao modificar o intervalo de endereços IP. Este comando falhará se algum processador de serviço ou interfaces de rede estiver usando os endereços IP no intervalo especificado. Definir este valor como **True** associa quaisquer interfaces endereçadas manualmente à sub-rede atual e permite que o comando seja bem-sucedido.

O seguinte comando modifica o endereço IP do gateway da sub-rede sub3:

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

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

Exibir sub-redes para a rede ONTAP

Você pode exibir a lista de endereços IP alocados para cada sub-rede dentro de um espaço IPspace. A saída também mostra o número total de endereços IP disponíveis em cada sub-rede e o número de endereços que estão sendo usados atualmente.

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

System Manager

Começando com o ONTAP 9.12,0, você pode usar o Gerenciador do sistema para exibir sub-redes

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Veja a lista de sub-redes.

CLI

Use a CLI para exibir sub-redes

Passo

Exiba a lista de sub-redes e os intervalos de endereços IP associados que são usados nessas sub-redes:

```
network subnet show
```

O comando a seguir exibe as sub-redes e as propriedades da sub-rede:

```
network subnet show

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

Saiba mais sobre `network subnet show` o "Referência do comando ONTAP"na .

Excluir sub-redes da rede ONTAP

Se você não precisar mais de uma sub-rede e quiser desalocar os endereços IP atribuídos à sub-rede, você pode excluí-la.

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

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para excluir uma sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Excluir** ao lado da sub-rede que deseja remover.
3. Salve suas alterações.

CLI

Use a CLI para excluir uma sub-rede

Sobre esta tarefa

Você receberá um erro se algum processador de serviço ou interfaces de rede estiver usando endereços IP nos intervalos especificados. Se você quiser que as interfaces continuem a usar os endereços IP mesmo depois que a sub-rede é excluída, você pode definir a opção -force-update-lif-associations como true para remover a associação da sub-rede com os LIFs.

Passo

Eliminar uma sub-rede:

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

O comando a seguir exclui a sub-rede SUB1 no IPspace ipspace1:

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

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

Crie SVMs para a rede ONTAP

Você precisa criar um SVM para servir dados aos clientes.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve saber qual estilo de segurança o volume raiz da SVM terá.

  Se você pretende implementar uma solução Hyper-V ou SQL Server sobre SMB neste SVM, você deve usar o estilo de segurança NTFS para o volume raiz. Os volumes que contêm ficheiros Hyper-V ou ficheiros de base de dados SQL têm de ser definidos para segurança NTFS no momento em que são criados. Ao definir o estilo de segurança do volume raiz como NTFS, você garante que não crie

inadvertidamente volumes de dados UNIX ou mistos de estilo de segurança.

- A partir do ONTAP 9.13.1, é possível definir uma capacidade máxima para uma VM de storage. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

System Manager

Você pode usar o System Manager para criar uma VM de storage.

Passos

1. Selecione **Storage VMs**.
2. Clique + Add em para criar uma VM de armazenamento.
3. Nomeie a VM de storage.
4. Selecione o protocolo de acesso:
   - SMB/CIFS, NFS
   - ISCSI
   - FC
   - NVMe
     i. Se selecionar **Ativar SMB/CIFS**, conclua a seguinte configuração:

Campo ou caixa de verificação	Descrição
Nome do administrador	Especifique o nome de usuário do administrador para a VM de storage SMB/CIFS.
Palavra-passe	Especifique a senha de administrador para a VM de armazenamento SMB/CIFS.
Nome do servidor	Especifique o nome do servidor para a VM de armazenamento SMB/CIFS.
Domínio do ative Directory	Especifique o domínio do diretório ativo para fornecer autenticação de usuário para a VM de storage SMB/CIFS.
Unidade organizacional	Especifique a unidade organizacional no domínio do ative Directory associado ao servidor SMB/CIFS. "Computadores" é o valor padrão, que pode ser modificado.
Criptografa dados enquanto acessa os compartilhamentos na VM de storage	Marque essa caixa de seleção para criptografar dados usando o SMB 3,0 para impedir o acesso não autorizado a arquivos nos compartilhamentos na VM de armazenamento SMB/CIFS.
Domínios	Adicione, remova ou reordene os domínios listados para a VM de armazenamento SMB/CIFS.
Servidores de nomes	Adicione, remova ou reordene os servidores de nomes para a VM de armazenamento SMB/CIFS.

Idioma padrão	Especifica a configuração padrão de codificação de idioma para a VM de armazenamento e seus volumes. Use a CLI para alterar as configurações de volumes individuais em uma VM de armazenamento.
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NFS**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Caixa de verificação permitir acesso do cliente NFS	Marque essa caixa de seleção quando todos os volumes criados na VM de armazenamento NFS devem usar o caminho do volume raiz "/" para montar e percorrer. Adicione regras à política de exportação "default" para permitir a passagem ininterrupta de montagem.

Regras	Clique + Add para criar regras. • Especificação do cliente: Especifique os nomes de host, endereços IP, grupos de rede ou domínios. • Protocolos de acesso: Selecione uma combinação das seguintes opções: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Detalhes de Acesso: Para cada tipo de usuário, especifique o nível de acesso, somente leitura, leitura/gravador ou superusuário. Os tipos de utilizador incluem: ◦ Tudo ◦ Todos (como utilizador anónimo) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5P ◦ NTLM Salve a regra.
Idioma padrão	Especifica a configuração padrão de codificação de idioma para a VM de armazenamento e seus volumes. Use a CLI para alterar as configurações de volumes individuais em uma VM de armazenamento.
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.

Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se selecionar **Ativar iSCSI**, efetue a seguinte configuração:

Campo ou caixa de verificação	Descrição
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar FC**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Configurar portas FC	Selecione as interfaces de rede nos nós que você deseja incluir na VM de storage. Duas interfaces de rede por nó são recomendadas.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NVMe/FC**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição

Configurar portas FC	Selecione as interfaces de rede nos nós que você deseja incluir na VM de storage. Duas interfaces de rede por nó são recomendadas.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NVMe/TCP**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Salve suas alterações.

CLI

Use a CLI do ONTAP para criar uma sub-rede.

Passos

1. Determine quais agregados são candidatos a conter o volume raiz da SVM.

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

   Você deve escolher um agregado que tenha pelo menos 1 GB de espaço livre para conter o volume raiz. Se você pretende configurar a auditoria nas na SVM, você deve ter um mínimo de 3 GB de espaço livre extra no agregado raiz, com o espaço extra sendo usado para criar o volume de teste de auditoria quando a auditoria estiver ativada.

Se a auditoria nas já estiver habilitada em um SVM existente, o volume de preparo do agregado será criado imediatamente após a criação do agregado ser concluída com sucesso.

2. Registre o nome do agregado no qual você deseja criar o volume raiz do SVM.
3. Se você planeja especificar um idioma ao criar o SVM e não souber o valor a ser usado, identifique e Registre o valor do idioma que deseja especificar:

   ```
   vserver create -language ?
   ```

4. Se você planeja especificar uma política de snapshot ao criar o SVM e não souber o nome da política, liste as políticas disponíveis e identifique e Registre o nome da política de snapshot que deseja usar:

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

5. Se você planeja especificar uma política de cota ao criar o SVM e não souber o nome da política, liste as políticas disponíveis e identifique e Registre o nome da política de cota que deseja usar:

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

6. Criar um SVM:

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

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

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

7. Verifique se a configuração SVM está correta.

   ```
   vserver show -vserver vs1
   ```

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

Neste exemplo, o comando cria o SVM chamado "VS1" no IPspace "ipspace1". O volume raiz é chamado "VS1_root" e é criado em aggr3 com estilo de segurança NTFS.

A partir do ONTAP 9.13.1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e um limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Interfaces lógicas (LIFs)

Visão geral da LIF

Saiba mais sobre a configuração de LIF para um cluster ONTAP

Um LIF (interface lógica) representa um ponto de acesso à rede para um nó no cluster. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede.

Um administrador de cluster pode criar, exibir, modificar, migrar, reverter ou excluir LIFs. O administrador do SVM só pode visualizar os LIFs associados ao SVM.

Um LIF é um endereço IP ou WWPN com caraterísticas associadas, como uma política de serviço, uma porta inicial, um nó inicial, uma lista de portas para as quais fazer failover e uma política de firewall. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede.

> A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

Os LIFs podem ser hospedados nas seguintes portas:

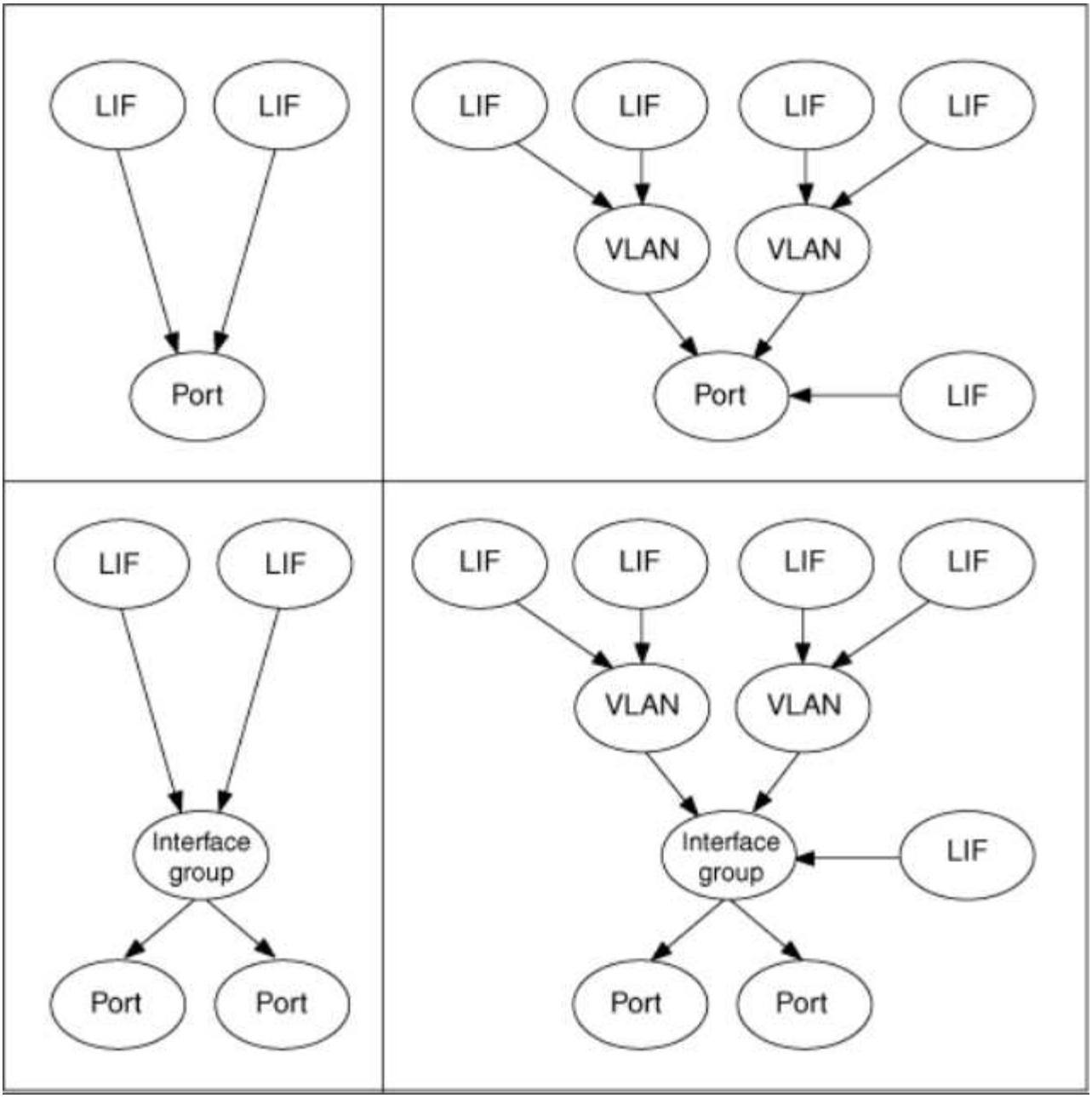
- Portas físicas que não fazem parte dos grupos de interfaces
- Grupos de interfaces
- VLANs
- Portas físicas ou grupos de interface que hospedam VLANs
- Portas IP virtual (VIP)

  A partir do ONTAP 9.5, os LIFs VIP são suportados e são hospedados em portas VIP.

Ao configurar protocolos SAN como FC em um LIF, ele será associado a um WWPN.

"Administração da SAN"

A figura a seguir ilustra a hierarquia de portas em um sistema ONTAP:



Failover de LIF e giveback

Um failover de LIF ocorre quando um LIF passa de seu nó ou porta inicial para o nó ou porta do parceiro de HA. Um failover de LIF pode ser acionado automaticamente pelo ONTAP ou manualmente por um administrador de cluster para certos eventos, como um link físico de Ethernet para baixo ou um nó que sai do quórum de banco de dados replicado (RDB). Quando ocorre um failover de LIF, o ONTAP continua a operação normal no nó do parceiro até que o motivo do failover seja resolvido. Quando o nó inicial ou a porta recupera a integridade, o LIF é revertido do parceiro HA de volta para o nó ou porta inicial. Esta reversão é chamada de giveback.

Para failover de LIF e giveback, as portas de cada nó precisam pertencer ao mesmo domínio de broadcast. Para verificar se as portas relevantes em cada nó pertencem ao mesmo domínio de broadcast, consulte o seguinte:

- ONTAP 9.8 e posterior: "Acessibilidade da porta de reparo"
- ONTAP 9.7 e anteriores: "Adicionar ou remover portas de um domínio de broadcast"

Para LIFs com failover de LIF ativado (automático ou manualmente), o seguinte se aplica:

- Para LIFs usando uma política de serviço de dados, você pode verificar restrições de política de failover:
  - ONTAP 9.6 e posterior: "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"
  - ONTAP 9.5 e anteriores: "Funções de LIF no ONTAP 9.5 e anteriores"
- A reversão automática de LIFs ocorre quando a reversão automática é definida como `true` e quando a porta inicial do LIF está saudável e capaz de hospedar o LIF.
- Em um takeover de nós planejado ou não planejado, o LIF no nó assumido faz failover para o parceiro de HA. A porta em que o LIF falha é determinada pelo Gerenciador de VIF.
- Após a conclusão do failover, o LIF opera normalmente.
- Quando um giveback é iniciado, o LIF volta para seu nó e porta inicial, se a reversão automática estiver definida como `true`.
- Quando um link ethernet é desativado em uma porta que hospeda um ou mais LIFs, o Gerenciador de VIF migra os LIFs da porta para uma porta diferente no mesmo domínio de broadcast. A nova porta pode estar no mesmo nó ou em seu parceiro de HA. Depois que o link for restaurado e se a reversão automática estiver definida como `true`, o Gerenciador de VIF reverte os LIFs de volta ao nó inicial e à porta inicial.
- Quando um nó sai do quórum de banco de dados replicado (RDB), o VIF Manager migra os LIFs do nó de ausência de quorum para seu parceiro de HA. Depois que o nó voltar ao quórum e se a reversão automática estiver definida como `true`, o Gerenciador de VIF reverte os LIFs de volta ao nó inicial e à porta inicial.

Saiba mais sobre a compatibilidade ONTAP LIF com tipos de portas

LIFs podem ter caraterísticas diferentes para suportar diferentes tipos de portas.

Quando os LIFs de gerenciamento e clusters são configurados na mesma sub-rede, o tráfego de gerenciamento pode ser bloqueado por um firewall externo e as conexões AutoSupport e NTP podem falhar. Você pode recuperar o sistema executando o `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` comando para alternar o LIF entre clusters. No entanto, você deve definir o LIF e o LIF de gerenciamento em diferentes sub-redes para evitar esse problema.

LIF	Descrição
LIF de dados	Um LIF associado a uma máquina virtual de storage (SVM) e usado para comunicação com clientes. Você pode ter vários LIFs de dados em uma porta. Essas interfaces podem migrar ou fazer failover em todo o cluster. É possível modificar um LIF de dados para servir como um LIF de gerenciamento de SVM modificando sua política de firewall para mgmt. As sessões estabelecidas nos servidores NIS, LDAP, ative Directory, WINS e DNS usam LIFs de dados.

LIF de cluster	LIF usado para transportar tráfego entre clusters entre nós em um cluster. As LIFs de cluster sempre devem ser criadas nas portas do cluster. As LIFs de cluster podem fazer failover entre as portas de cluster no mesmo nó, mas não podem ser migradas ou falhadas para um nó remoto. Quando um novo nó se junta a um cluster, os endereços IP são gerados automaticamente. No entanto, se você quiser atribuir endereços IP manualmente aos LIFs de cluster, certifique-se de que os novos endereços IP estejam no mesmo intervalo de sub-rede que os LIFs de cluster existentes.
LIF de gerenciamento de clusters	LIF que fornece uma única interface de gerenciamento para todo o cluster. Um LIF de gerenciamento de cluster pode fazer failover para qualquer nó no cluster. Não pode fazer failover para portas de cluster ou clusters
LIF entre clusters	Um LIF usado para comunicação, backup e replicação entre clusters. É necessário criar um LIF entre clusters em cada nó do cluster antes que uma relação de peering de cluster possa ser estabelecida. Essas LIFs só podem fazer failover para portas no mesmo nó. Eles não podem ser migrados ou falhados para outro nó no cluster.
LIF de gerenciamento de nós	Um LIF que fornece um endereço IP dedicado para gerenciar um nó específico em um cluster. As LIFs de gerenciamento de nós são criadas no momento da criação ou junção do cluster. Esses LIFs são usados para manutenção do sistema, por exemplo, quando um nó fica inacessível do cluster.
LIF VIP	Um LIF VIP é qualquer LIF de dados criado em uma porta VIP. Para saber mais, "Configurar LIFs de IP virtual (VIP)"consulte .

Informações relacionadas

- "modificação da interface de rede"

Políticas e funções de serviço de LIF suportadas para a sua versão do ONTAP

Ao longo do tempo, a forma como o ONTAP gerencia o tipo de tráfego suportado nos LIFs mudou.

- O ONTAP 9.5 e versões anteriores usam funções de LIF e serviços de firewall.
- ONTAP 9.6 e versões posteriores usam políticas de serviço LIF:
  - A versão ONTAP 9.5 introduziu políticas de serviço de LIF.
  - O ONTAP 9.6 substituiu as funções de LIF por políticas de serviço de LIF.
  - O ONTAP 9.10,1 substituiu os serviços de firewall por políticas de serviço LIF.

O método que você configura depende da versão do ONTAP que você está usando.

Para saber mais sobre:

- Políticas de firewall, "Comando: Firewall-policy-show"consulte .
- Funções de LIF, "Funções de LIF (ONTAP 9 .5 e anteriores)"consulte a .
- Políticas de serviço de LIF, "LIFs e políticas de serviço (ONTAP 9.6 e posteriores)"consulte .

Saiba mais sobre LIFs e políticas de serviço do ONTAP

Você pode atribuir políticas de serviço (em vez de funções de LIF ou políticas de firewall) a LIFs que determinam o tipo de tráfego suportado para os LIFs. As políticas de serviço definem uma coleção de serviços de rede suportados por um LIF. O ONTAP fornece um conjunto de políticas de serviço integradas que podem ser associadas a um LIF.

O método de gerenciamento de tráfego de rede é diferente no ONTAP 9,7 e versões anteriores. Se precisar gerenciar o tráfego em uma rede executando o ONTAP 9,7 e anterior, "Funções de LIF (ONTAP 9 .5 e anteriores)"consulte .

Os protocolos FCP e NVMe/FCP atualmente não exigem uma service-policy.

Você pode exibir as políticas de serviço e seus detalhes usando o seguinte comando:
`network interface service-policy show`

Saiba mais sobre `network interface service-policy show` o "Referência do comando ONTAP"na .

Os recursos que não estão vinculados a um serviço específico usarão um comportamento definido pelo sistema para selecionar LIFs para conexões de saída.

Os aplicativos em um LIF com uma política de serviço vazia podem se comportar inesperadamente.

Políticas de serviço para SVMs do sistema

O SVM admin e qualquer SVM do sistema contêm políticas de serviço que podem ser usadas para LIFs nesse SVM, incluindo gerenciamento e LIFs entre clusters. Essas políticas são criadas automaticamente pelo sistema quando um IPspace é criado.

A tabela a seguir lista as políticas internas para LIFs em SVMs do sistema a partir do ONTAP 9.12.1. Para outras versões, exiba as políticas de serviço e seus detalhes usando o seguinte comando:

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

Política	Serviços incluídos	Função equivalente	Descrição
padrão-clusters	núcleo entre clusters, gerenciamento-https	entre clusters	Usado por LIFs que transportam tráfego entre clusters. Observação: O Service entre clusters-core está disponível no ONTAP 9.5 com o nome da política de serviços de rede.
default-route-announce	gestão-bgp	-	Usado por LIFs que transportam conexões de pares BGP Nota: Disponível a partir do ONTAP 9.5 com o nome net-route-announce Service policy.

gerenciamento padrão	management-core, management-https, management-http, management-ssh, management-AutoSupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt ou cluster-mgmt	Use essa política de gerenciamento de escopo do sistema para criar LIFs de gerenciamento com escopo de nó e cluster pertencentes a um SVM do sistema. Esses LIFs podem ser usados para conexões de saída para servidores DNS, AD, LDAP ou NIS, bem como algumas conexões adicionais para suportar aplicativos executados em nome de todo o sistema. A partir do ONTAP 9.12.1, você pode usar o `management-log-forwarding` serviço para controlar quais LIFs são usados para encaminhar logs de auditoria para um servidor syslog remoto.

A tabela a seguir lista os serviços que LIFs podem usar em um SVM do sistema a partir do ONTAP 9.11.1:

Serviço	Limitações de failover	Descrição
núcleo entre clusters	somente nó inicial	Serviços básicos entre clusters
núcleo de gerenciamento	-	Serviços de gerenciamento central
gestão-ssh	-	Serviços para acesso de gerenciamento SSH
http de gerenciamento	-	Serviços para acesso de gerenciamento HTTP
gerenciamento-https	-	Serviços para acesso de gerenciamento HTTPS
management-AutoSupport	-	Serviços relacionados com a publicação de cargas úteis AutoSupport
gestão-bgp	apenas porta inicial	Serviços relacionados com interações entre pares BGP
backup-controle ndmp	-	Serviços para controles de backup NDMP
gestão-ems	-	Serviços para acesso de mensagens de gerenciamento
gerenciamento-ntp-cliente	-	Introduzido no ONTAP 9.10,1. Serviços para acesso de cliente NTP.
servidor de gerenciamento ntp	-	Introduzido no ONTAP 9.10,1. Serviços para acesso de gerenciamento de servidor NTP

gerenciamento-portmap	-	Serviços para gerenciamento de portmap
management-rsh-server	-	Serviços para gerenciamento de servidores rsh
management-snmp-server	-	Serviços para gerenciamento de servidores SNMP
management-tetelnet-server	-	Serviços para gerenciamento de servidores telnet
encaminhamento de logs de gerenciamento	-	Introduzido no ONTAP 9.12,1. Serviços para encaminhamento de logs de auditoria

Políticas de serviço para SVMs de dados

Todas as SVMs de dados contêm políticas de serviço que podem ser usadas por LIFs nesse SVM.

A tabela a seguir lista as políticas internas para LIFs em SVMs de dados a partir do ONTAP 9.11.1. Para outras versões, exiba as políticas de serviço e seus detalhes usando o seguinte comando:

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

Política	Serviços incluídos	Protocolo de dados equivalente	Descrição
gerenciamento padrão	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nenhum	Use essa política de gerenciamento com escopo da SVM para criar LIFs de gerenciamento de SVM de propriedade de um data SVM. Esses LIFs podem ser usados para fornecer acesso SSH ou HTTPS aos administradores do SVM. Quando necessário, esses LIFs podem ser usados para conexões de saída para servidores DNS, AD, LDAP ou NIS externos.
blocos de dados padrão	data-core, data-iscsi	iscsi	Usado por LIFs que transportam tráfego de dados SAN orientado a blocos. A partir do ONTAP 9.10.1, a política "default-data-blocks" está obsoleta. Em vez disso, utilize a política de serviço "Default-data-iscsi".

arquivos-dados-padrão	data-core, data-fpolicy-client, data-dns-server, data-FlexCache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Use a política arquivos de dados padrão para criar LIFs nas que suportam protocolos de dados baseados em arquivos. Às vezes, há apenas um LIF presente no SVM, portanto, essa política permite que o LIF seja usado para conexões de saída a um servidor DNS, AD, LDAP ou NIS externo. Você pode remover esses serviços dessa política se preferir que essas conexões usem apenas LIFs de gerenciamento.
padrão-data-iscsi	data-core, data-iscsi	iscsi	Usado por LIFs que transportam tráfego de dados iSCSI.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Usado por LIFs que transportam tráfego de dados NVMe/TCP.

A tabela a seguir lista os serviços que podem ser usados em um SVM de dados, juntamente com todas as restrições que cada serviço impõe à política de failover de LIF a partir do ONTAP 9.11.1:

Serviço	Restrições de failover	Descrição
gestão-ssh	-	Serviços para acesso de gerenciamento SSH
http de gerenciamento	-	Introduzido nos Serviços ONTAP 9.10,1 para acesso de gerenciamento HTTP
gerenciamento-https	-	Serviços para acesso de gerenciamento HTTPS
gerenciamento-portmap	-	Serviços para acesso ao gerenciamento de portmap
management-snmp-server	-	Introduzido nos Serviços ONTAP 9.10,1 para acesso de gestão de servidores SNMP
núcleo de dados	-	Serviços de dados básicos
data-nfs	-	Serviço de dados NFS
data-cifs	-	Serviço de dados CIFS
data-FlexCache	-	Serviço de dados FlexCache
dados-iscsi	Apenas porta inicial para AFF/FAS; apenas parceiro sfo para ASA	Serviço de dados iSCSI

backup-controle ndmp	-	Introduzido no ONTAP 9.10,1 Backup NDMP controla o serviço de dados
servidor-dns de dados	-	Introduzido no serviço de dados do servidor DNS ONTAP 9.10,1
data-fpolicy-client	-	Serviço de dados de política de triagem de arquivos
data-nvme-tcp	apenas porta inicial	Introduzido no serviço de dados TCP NVMe ONTAP 9.10,1
data-s3-server	-	Serviço de dados de servidor Simple Storage Service (S3)

Você deve estar ciente de como as políticas de serviço são atribuídas aos LIFs em SVMs de dados:

- Se um SVM de dados for criado com uma lista de serviços de dados, as políticas de serviço incorporadas "arquivos de dados padrão" e "blocos de dados padrão" nesse SVM serão criadas usando os serviços especificados.
- Se um SVM de dados for criado sem especificar uma lista de serviços de dados, as políticas de serviço incorporadas "default-data-files" e "default-data-blocks" nesse SVM serão criadas usando uma lista padrão de serviços de dados.

  A lista de serviços de dados padrão inclui os serviços iSCSI, NFS, NVMe, SMB e FlexCache.

- Quando um LIF é criado com uma lista de protocolos de dados, uma política de serviço equivalente aos protocolos de dados especificados é atribuída ao LIF.
- Se não existir uma política de serviço equivalente, é criada uma política de serviço personalizada.
- Quando um LIF é criado sem uma política de serviço ou lista de protocolos de dados, a política de serviço de arquivos de dados padrão é atribuída ao LIF por padrão.

Serviço de data center

O serviço data-core permite que componentes que usaram LIFs anteriormente com a função de dados funcionem como esperado em clusters que foram atualizados para gerenciar LIFs usando políticas de serviço em vez de funções LIF (que são depreciadas no ONTAP 9.6).

Especificar o data-core como um serviço não abre portas no firewall, mas o serviço deve ser incluído em qualquer política de serviço em um data SVM. Por exemplo, a política de serviço default-data-files contém os seguintes serviços por padrão:

- núcleo de dados
- data-nfs
- data-cifs
- data-FlexCache

O serviço de núcleo de dados deve ser incluído na política para garantir que todos os aplicativos que usam o LIF funcionem conforme esperado, mas os outros três serviços podem ser removidos, se desejado.

Serviço de LIF do lado do cliente

A partir do ONTAP 9.10,1, o ONTAP fornece serviços de LIF do lado do cliente para várias aplicações. Esses serviços fornecem controle sobre quais LIFs são usados para conexões de saída em nome de cada aplicativo.

Os novos serviços a seguir fornecem aos administradores controle sobre quais LIFs são usados como endereços de origem para determinados aplicativos.

Serviço	Restrições da SVM	Descrição
gestão-ad-cliente	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente do ative Directory para conexões de saída a um servidor AD externo.
management-dns-client	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente DNS para conexões de saída a um servidor DNS externo.
gerenciamento-ldap-cliente	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente LDAP para conexões de saída a um servidor LDAP externo.
management-nis-client	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente NIS para conexões de saída a um servidor NIS externo.
gerenciamento-ntp-cliente	apenas sistema	A partir do ONTAP 9.10,1, o ONTAP fornece serviço de cliente NTP para conexões de saída a um servidor NTP externo.
data-fpolicy-client	somente dados	A partir do ONTAP 9.8, o ONTAP fornece serviço de cliente para conexões FPolicy de saída.

Cada um dos novos serviços é incluído automaticamente em algumas das políticas de serviço incorporadas, mas os administradores podem removê-los das políticas incorporadas ou adicioná-los a políticas personalizadas para controlar quais LIFs são usados para conexões de saída em nome de cada aplicativo.

Informações relacionadas

- "show de política de serviço de interface de rede"

Gerenciar LIFs

Configurar políticas de serviço LIF para um cluster ONTAP

Você pode configurar políticas de serviço de LIF para identificar um único serviço ou uma lista de serviços que usarão um LIF.

Crie uma política de serviço para LIFs

Você pode criar uma política de serviço para LIFs. Você pode atribuir uma política de serviço a um ou mais LIFs, permitindo assim que o LIF transporte tráfego para um único serviço ou uma lista de serviços.

Você precisa de Privileges avançado para executar o `network interface service-policy create` comando.

Sobre esta tarefa

Serviços incorporados e políticas de serviço estão disponíveis para gerenciar dados e tráfego de gerenciamento em SVMs de dados e do sistema. A maioria dos casos de uso é satisfeita usando uma política de serviço integrada em vez de criar uma política de serviço personalizada.

Você pode modificar essas políticas de serviço integradas, se necessário.

Passos

1. Veja os serviços disponíveis no cluster:

   ```
   network interface service show
   ```

   Os serviços representam os aplicativos acessados por um LIF, bem como os aplicativos servidos pelo cluster. Cada serviço inclui zero ou mais portas TCP e UDP nas quais o aplicativo está escutando.

   Estão disponíveis os seguintes serviços de gerenciamento e dados adicionais:

   ```
   cluster1::> network interface service show

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

2. Veja as políticas de serviço que existem no cluster:

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

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Criar uma política de serviço:

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

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

- "service_name" especifica uma lista de serviços que devem ser incluídos na política.
- "IP_address/mask" especifica a lista de máscaras de sub-rede para endereços que têm permissão para acessar os serviços na política de serviço. Por padrão, todos os serviços especificados são adicionados com uma lista de endereços padrão permitidos de 0,0.0,0/0, que permite o tráfego de todas as sub-redes. Quando uma lista de endereços permitidos não padrão é fornecida, LIFs usando a diretiva são configurados para bloquear todas as solicitações com um endereço de origem que não corresponde a nenhuma das máscaras especificadas.

  O exemplo a seguir mostra como criar uma política de serviço de dados, *svm1_data_policy*, para um SVM que inclui serviços *NFS* e *SMB*:

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

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

  O exemplo a seguir mostra como criar uma política de serviços entre clusters:

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

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

4. Verifique se a política de serviço foi criada.

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

A saída a seguir mostra as políticas de serviço que estão disponíveis:

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

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
--------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Depois de terminar

Atribua a política de serviço a um LIF no momento da criação ou modificando um LIF existente.

Atribua uma política de serviço a um LIF

Você pode atribuir uma política de serviço a um LIF no momento da criação do LIF ou modificando o LIF. Uma política de serviço define a lista de serviços que podem ser usados com o LIF.

Sobre esta tarefa

Você pode atribuir políticas de serviço para LIFs nos SVMs de administração e de dados.

Passo

Dependendo de quando você deseja atribuir a política de serviço a um LIF, execute uma das seguintes ações:

Se você é…	Atribuir a política de serviço…
Criando um LIF	Crie -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> ((-address <IP_address> -netmask <IP_address>) -sub-rede-name <subnet_name>) -Service-policy <service_policy_name>
Modificação de um LIF	interface de rede modificar -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

Ao especificar uma política de serviço para um LIF, não é necessário especificar o protocolo de dados e a função para o LIF. A criação de LIFs especificando a função e os protocolos de dados também é suportada.

Uma política de serviço só pode ser usada por LIFs no mesmo SVM que você especificou ao criar a política de serviço.

Exemplos

O exemplo a seguir mostra como modificar a política de serviço de um LIF para usar a política de serviço de gerenciamento padrão:

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

Comandos para gerenciar políticas de serviço LIF

Use os `network interface service-policy` comandos para gerenciar políticas de serviço LIF.

Saiba mais sobre `network interface service-policy` o "Referência do comando ONTAP"na .

Antes de começar

Modificar a política de serviço de um LIF em uma relação do SnapMirror ativa interrompe a programação de replicação. Se você converter um LIF entre clusters (ou vice-versa), essas alterações não serão replicadas para o cluster com peering. Para atualizar o cluster de pares depois de modificar a política de serviço LIF, execute primeiro a `snapmirror abort` operação e ressincronize a relação de replicaçãodepois .

Se você quiser…	Use este comando…
Criar uma política de serviço (Privileges avançado necessário)	`network interface service-policy create`

Se você quiser…	Use este comando…
Adicionar uma entrada de serviço adicional a uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy add-service`
Clonar uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy clone`
Modificar uma entrada de serviço em uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy modify-service`
Remover uma entrada de serviço de uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy remove-service`
Renomear uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy rename`
Excluir uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy delete`
Restaurar uma política de serviço incorporada ao seu estado original (Privileges avançado necessário)	`network interface service-policy restore-defaults`
Exibir políticas de serviço existentes	`network interface service-policy show`

Informações relacionadas

- "show de serviço de interface de rede"
- "política de serviço de interface de rede"
- "aborto do snapmirror"

Crie LIFs ONTAP

Um SVM fornece dados a clientes por meio de uma ou mais interfaces lógicas de rede (LIFs). Você deve criar LIFs nas portas que deseja usar para acessar dados. Um LIF (interface de rede) é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

Prática recomendada

As portas de switch conetadas ao ONTAP devem ser configuradas como portas de borda de spanning-tree para reduzir atrasos durante a migração de LIF.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- A porta de rede física ou lógica subjacente deve ter sido configurada para o estado de funcionamento administrativo.

- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o System Manager ou o `network subnet create` comando.

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

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Não é possível atribuir protocolos nas e SAN ao mesmo LIF.

  Os protocolos compatíveis são SMB, NFS, FlexCache, iSCSI e FC; iSCSI e FC não podem ser combinados com outros protocolos. No entanto, os protocolos SAN baseados em nas e Ethernet podem estar presentes na mesma porta física.

  - Você não deve configurar LIFs que transportam tráfego SMB para reverter automaticamente para seus nós domésticos. Esta recomendação é obrigatória se o servidor SMB for hospedar uma solução para operações ininterruptas com Hyper-V ou SQL Server sobre SMB.
- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Todos os serviços de mapeamento de nomes e resolução de nomes de host usados por um SVM, como DNS, NIS, LDAP e ative Directory, devem ser acessíveis a partir de pelo menos um LIF que manipula o tráfego de dados do SVM.
- Um tráfego entre nós que lida com LIF não deve estar na mesma sub-rede que um tráfego de gerenciamento de manipulação de LIF ou um tráfego de dados de manipulação de LIF.
- Criar um LIF que não tenha um destino de failover válido resulta em uma mensagem de aviso.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster:
  - Gerenciador do sistema: Começando com ONTAP 9.12,0, visualize o throughput na grade de interface de rede.
  - CLI: Use o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível avançado de privilégio).

    Saiba mais sobre `network interface capacity show` e `network interface capacity details show` no "Referência do comando ONTAP".

- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

  A partir do ONTAP 9.4, o FC-NVMe é compatível. Se você estiver criando um LIF FC-NVMe, deve estar ciente do seguinte:

  - O protocolo NVMe precisa ser compatível com o adaptador FC no qual o LIF é criado.
  - O FC-NVMe pode ser o único protocolo de dados em LIFs de dados.
- Um tráfego de gerenciamento de manipulação de LIF deve ser configurado para cada máquina virtual de

storage (SVM) que suporte SAN.

- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- É possível configurar, no máximo, duas LIFs NVMe que manipulam o tráfego de dados por SVM, por nó.
- Quando você cria uma interface de rede com uma sub-rede, o ONTAP seleciona automaticamente um endereço IP disponível na sub-rede selecionada e o atribui à interface de rede. Você pode alterar a sub-rede se houver mais de uma sub-rede, mas não pode alterar o endereço IP.
- Ao criar (adicionar) um SVM, para uma interface de rede, não é possível especificar um endereço IP que esteja no intervalo de uma sub-rede existente. Você receberá um erro de conflito de sub-rede. Esse problema ocorre em outros fluxos de trabalho para uma interface de rede, como criar ou modificar interfaces de rede entre clusters nas configurações de SVM ou configurações de cluster.
- A partir do ONTAP 9.10,1, os `network interface` comandos CLI incluem um `-rdma-protocols` parâmetro para NFS sobre configurações RDMA. A criação de interfaces de rede para NFS em configurações RDMA é suportada no System Manager a partir do ONTAP 9.12.1. Para obter mais informações, Configure o LIFS para NFS através do RDMAconsulte .
- A partir do ONTAP 9.11,1, o failover automático de LIF iSCSI está disponível em plataformas de array all-flash SAN (ASA).

  O failover de LIF iSCSI é ativado automaticamente (a política de failover é definida como `sfo-partner-only` e o valor de reversão automática é definido como `true`) em iSCSI LIFs recém-criados se não existirem LIFs iSCSI na SVM especificada ou se todas as LIFs iSCSI existentes na SVM especificada já estiverem habilitadas com failover de LIF iSCSI.

  Se após a atualização para o ONTAP 9.11,1 ou posterior, você tiver LIFs iSCSI existentes em uma SVM que não tenha sido habilitada com o recurso de failover de LIF iSCSI e criar novas LIFs iSCSI na mesma SVM, os novos LIFs iSCSI assumirão a mesma política de failover (`disabled`) das LIFs iSCSI existentes na SVM.

  "Failover de LIF iSCSI para plataformas ASA"

A partir do ONTAP 9.7, o ONTAP escolhe automaticamente a porta inicial de um LIF, desde que pelo menos um LIF já exista na mesma sub-rede nesse espaço. O ONTAP escolhe uma porta inicial no mesmo domínio de broadcast que outros LIFs nessa sub-rede. Você ainda pode especificar uma porta inicial, mas ela não é mais necessária (a menos que ainda não existam LIFs nessa sub-rede no espaço IPspace especificado).

A partir do ONTAP 9.12,0, o procedimento a seguir depende da interface que você usa — Gerenciador de sistema ou CLI:

System Manager

Use o System Manager para adicionar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. + Add Selecione .
3. Selecione uma das seguintes funções de interface:
   a. Dados
   b. Entre clusters
   c. Gerenciamento de SVM
4. Selecione o protocolo:
   a. SMB/CIFS E NFS
   b. ISCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Nomeie o LIF ou aceite o nome gerado a partir de suas seleções anteriores.
6. Aceite o nó inicial ou utilize a lista pendente para selecionar um.
7. Se pelo menos uma sub-rede estiver configurada no espaço IPspace do SVM selecionado, a lista suspensa de sub-rede será exibida.
   a. Se você selecionar uma sub-rede, escolha-a na lista suspensa.
   b. Se você continuar sem uma sub-rede, o menu suspenso domínio de broadcast será exibido:
      i. Especifique o endereço IP. Se o endereço IP estiver a ser utilizado, é apresentada uma mensagem de aviso.
      ii. Especifique uma máscara de sub-rede.
8. Selecione a porta inicial no domínio de transmissão, automaticamente (recomendado) ou selecionando uma no menu suspenso. O controle de porta inicial é exibido com base no domínio de broadcast ou na seleção de sub-rede.
9. Salve a interface de rede.

CLI

Use a CLI para criar um LIF

Passos

1. Determine quais portas de domínio de broadcast você deseja usar para o LIF.

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

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

Saiba mais sobre `network port broadcast-domain show` o "Referência do comando ONTAP"na .

2. Verifique se a sub-rede que você deseja usar para os LIFs contém endereços IP não utilizados suficientes.

   `network subnet show -ipspace ipspace1`

   Saiba mais sobre `network subnet show` o "Referência do comando ONTAP"na .

3. Crie um ou mais LIFs nas portas que você deseja usar para acessar dados.

   > O NetApp recomenda a criação de objetos de sub-rede para todas as LIFs em SVMs de dados. Isso é especialmente importante para as configurações do MetroCluster, onde o objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque cada objeto de sub-rede tem um domínio de broadcast associado. Para obter instruções, "Crie uma sub-rede"consulte .

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

   - `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a opção -auto-revert.

   Saiba mais sobre `network interface revert` o "Referência do comando ONTAP"na .

   - `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
   - Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
   - Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao

SVM quando um LIF é criado usando essa sub-rede.

- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. Saiba mais sobre `network route create` o "Referência do comando ONTAP"na .
- `-auto-revert` Permite que você especifique se um LIF de dados é automaticamente revertido para seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `true` dependendo das políticas de gerenciamento de rede em seu ambiente.
- `-service-policy` A partir do ONTAP 9.5, você pode atribuir uma política de serviço para o LIF com a `-service-policy` opção. Quando uma política de serviço é especificada para um LIF, a política é usada para criar uma função padrão, política de failover e lista de protocolos de dados para o LIF. No ONTAP 9.5, as políticas de serviço são suportadas apenas para serviços de pares entre clusters e BGP. No ONTAP 9.6, você pode criar políticas de serviço para vários serviços de dados e gerenciamento.
- `-data-protocol` Permite criar um LIF compatível com os protocolos FCP ou NVMe/FC. Esta opção não é necessária ao criar um IP LIF.

4. **Opcional**: Atribua um endereço IPv6 na opção -address:

   a. Use o `network ndp prefix show` comando para visualizar a lista de prefixos RA aprendidos em várias interfaces.

      O `network ndp prefix show` comando está disponível no nível de privilégio avançado.

      Saiba mais sobre `network ndp prefix show` o "Referência do comando ONTAP"na .

   b. Use o formato `prefix::id` para construir o endereço IPv6 manualmente.

      `prefix` é o prefixo aprendido em várias interfaces.

   Para derivar o `id`, escolha um número hexadecimal aleatório de 64 bits.

5. Verifique se a configuração da interface LIF está correta.

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

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

   Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

6. Verifique se a configuração do grupo de failover é a desejada.

   `network interface show -failover -vserver vs1`

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

7. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	ping de rede
Endereço IPv6	rede ping6

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

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

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

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

O comando a seguir cria um LIF NVMe/FC e especifica o `nvme-fc` protocolo de dados:

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

Modificar LIFs ONTAP

Você pode modificar um LIF alterando os atributos, como nó inicial ou nó atual, status administrativo, endereço IP, máscara de rede, política de failover, política de firewall e

política de serviço. Você também pode alterar a família de endereços de um LIF de IPv4 para IPv6.

Sobre esta tarefa

- Ao modificar o status administrativo de um LIF para baixo, todos os bloqueios NFSv4 pendentes são mantidos até que o status administrativo do LIF seja retornado para cima.

  Para evitar conflitos de bloqueio que podem ocorrer quando outros LIFs tentam acessar os arquivos bloqueados, você deve mover os clientes NFSv4 para um LIF diferente antes de definir o status administrativo para baixo.

- Não é possível modificar os protocolos de dados usados por um LIF FC. No entanto, você pode modificar os serviços atribuídos a uma política de serviço ou alterar a política de serviço atribuída a um IP LIF.

  Para modificar os protocolos de dados usados por um LIF FC, você deve excluir e recriar o LIF. Para fazer alterações de política de serviço em um IP LIF, há uma breve interrupção enquanto as atualizações ocorrem.

- Não é possível modificar o nó inicial ou o nó atual de um LIF de gerenciamento com escopo de nó.
- Ao usar uma sub-rede para alterar o endereço IP e o valor da máscara de rede para um LIF, um endereço IP é alocado da sub-rede especificada; se o endereço IP anterior do LIF for de uma sub-rede diferente, o endereço IP será retornado a essa sub-rede.
- Para modificar a família de endereços de um LIF de IPv4 a IPv6, você deve usar a notação de dois pontos para o endereço IPv6 e adicionar um novo valor para o `-netmask-length` parâmetro.
- Não é possível modificar os endereços IPv6 locais de link auto-configurados.
- A modificação de um LIF que faz com que o LIF não tenha um destino de failover válido resulta em uma mensagem de aviso.

  Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

- A partir do ONTAP 9.5, você pode modificar a política de serviço associada a um LIF.

  No ONTAP 9.5, as políticas de serviço são suportadas apenas para serviços de pares entre clusters e BGP. No ONTAP 9.6, você pode criar políticas de serviço para vários serviços de dados e gerenciamento.

- A partir do ONTAP 9.11,1, o failover automático de LIF iSCSI está disponível em plataformas de array all-flash SAN (ASA).

  Para LIFs iSCSI pré-existentes, ou seja, LIFs criadas antes da atualização para o 9.11.1 ou posterior, você pode modificar a política de failover para "Ativar failover automático de LIF iSCSI"o .

- O ONTAP utiliza o Network Time Protocol (NTP) para sincronizar o tempo no cluster. Após alterar os endereços IP do LIF, talvez seja necessário atualizar a configuração do NTP para evitar falhas de sincronização. Para mais informações, consulte o"Base de conhecimento da NetApp : falha na sincronização do NTP após alteração do IP do LIF" .

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

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador de sistema para editar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione **> Editar** ao lado da interface de rede que deseja alterar.
3. Altere uma ou mais definições da interface de rede. Para obter detalhes, "Crie um LIF"consulte .
4. Salve suas alterações.

CLI

Use a CLI para modificar um LIF

Passos

1. Modifique os atributos de um LIF usando o `network interface modify` comando.

   O exemplo a seguir mostra como modificar o endereço IP e a máscara de rede do LIF datalif2 usando um endereço IP e o valor da máscara de rede da sub-rede client1_sub:

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

   O exemplo a seguir mostra como modificar a política de serviço de um LIF.

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

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

2. Verifique se os endereços IP estão acessíveis.

Se você estiver usando…	Então use…
Endereços IPv4	`network ping`
Endereços IPv6	`network ping6`

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

Migrar LIFs ONTAP

Você pode ter que migrar um LIF para uma porta diferente no mesmo nó ou em um nó diferente dentro do cluster, se a porta estiver com defeito ou precisar de manutenção. A

migração de um LIF é semelhante ao failover de LIF, mas a migração de LIF é uma operação manual, enquanto o failover de LIF é a migração automática de um LIF em resposta a uma falha de link na porta de rede atual do LIF.

Antes de começar

- Um grupo de failover deve ter sido configurado para os LIFs.
- O nó de destino e as portas devem estar operacionais e ter acesso à mesma rede que a porta de origem.

Sobre esta tarefa

- Os LIFs BGP residem na porta inicial e não podem ser migrados para nenhum outro nó ou porta.
- Você deve migrar LIFs hospedadas nas portas pertencentes a uma NIC para outras portas no cluster, antes de remover a NIC do nó.
- Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.
- Um LIF com escopo de nó, como um LIF de gerenciamento com escopo de nó, LIF de cluster e LIF entre clusters, não pode ser migrado para um nó remoto.
- Quando um NFSv4 LIF é migrado entre nós, um atraso de até 45 segundos resulta antes que o LIF esteja disponível em uma nova porta.

  Para contornar esse problema, use NFSv4,1 onde nenhum atraso é encontrado.

- É possível migrar iSCSI LIFs em plataformas de array SAN all-flash (ASA) executando o ONTAP 9.11,1 ou posterior.

  A migração de iSCSI LIFs está limitada a portas no nó inicial ou no parceiro de HA.

- Se a sua plataforma não for uma plataforma ASA (All-Flash SAN Array) executando o ONTAP versão 9.11.1 ou posterior, não será possível migrar LIFs iSCSI de um nó para outro.

  Para contornar essa restrição, você deve criar um iSCSI LIF no nó de destino. Saiba mais "A criar iSCSI LIFs"sobre .

- Se você quiser migrar um LIF (interface de rede) para NFS por RDMA, você deve garantir que a porta de destino seja compatível com RoCE. Você deve estar executando o ONTAP 9.10,1 ou posterior para migrar um LIF com a CLI ou o ONTAP 9.12,1 para migrar usando o Gerenciador de sistema. No System Manager, depois de selecionar sua porta de destino compatível com RoCE, marque a caixa ao lado de **usar portas RoCE** para concluir a migração com êxito. Saiba mais "Configurando LIFs para NFS em RDMA"sobre o .
- As operações de descarga de cópia do VMware VAAI falham ao migrar a LIF de origem ou de destino. Saiba mais sobre a cópia off-load:
  - "Ambientes NFS"
  - "AMBIENTES SAN"

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

System Manager

Use o System Manager para migrar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione ⋮ **> migrar** ao lado da interface de rede que deseja alterar.

   Para um iSCSI LIF, na caixa de diálogo **Migrate Interface**, selecione o nó de destino e a porta do parceiro de HA.

   Se pretender migrar o iSCSI LIF permanentemente, selecione a caixa de verificação. O iSCSI LIF deve estar offline antes de ser migrado permanentemente. Além disso, uma vez que um iSCSI LIF é migrado permanentemente, ele não pode ser desfeito. Não há opção de reversão.

3. Clique em **Migrate**.
4. Salve suas alterações.

CLI

Use a CLI para migrar um LIF

Passo

Dependendo se você deseja migrar um LIF específico ou todos os LIFs, execute a ação apropriada:

Se você quiser migrar…	Digite o seguinte comando…
Um LIF específico	`network interface migrate`
Todas as LIFs de gerenciamento de cluster e dados em um nó	`network interface migrate-all`
Todos os LIFs fora de um porto	`network interface migrate-all -node <node> -port <port>`

O exemplo a seguir mostra como migrar um LIF `datalif1` nomeado no SVM `vs0` para a porta `e0d` no `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

O exemplo a seguir mostra como migrar todos os LIFs de gerenciamento de cluster e dados do nó atual (local):

```
network interface migrate-all -node local
```

Informações relacionadas

- "migração da interface de rede"

Reverter um LIF para sua porta inicial após um failover de nó ONTAP ou migração de porta

Você pode reverter um LIF para sua porta inicial depois que ele falha ou é migrado para uma porta diferente manualmente ou automaticamente. Se a porta inicial de um determinado LIF não estiver disponível, o LIF permanece em sua porta atual e não é revertido.

Sobre esta tarefa

- Se você administrativamente levar a porta inicial de um LIF para o estado up antes de definir a opção de reversão automática, o LIF não será retornado à porta inicial.
- O LIF não reverte automaticamente a menos que o valor da opção "auto-revert" esteja definido como verdadeiro.
- Você deve garantir que a opção "reversão automática" esteja ativada para que os LIFs revertam para suas portas residenciais.

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

System Manager

Use o System Manager para reverter uma interface de rede para sua porta inicial

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione ⋮ **> Reverter** ao lado da interface de rede que deseja alterar.
3. Selecione **Revert** para reverter uma interface de rede para sua porta inicial.

CLI

Use a CLI para reverter um LIF para sua porta inicial

Passo

Reverter um LIF para sua porta inicial manualmente ou automaticamente:

Se você quiser reverter um LIF para sua porta inicial…	Em seguida, digite o seguinte comando…
Manualmente	`network interface revert -vserver vserver_name -lif lif_name`
Automaticamente	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

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

Recupere um ONTAP LIF configurado incorretamente

Um cluster não pode ser criado quando a rede do cluster é cabeada para um switch, mas

nem todas as portas configuradas no Cluster IPspace podem alcançar as outras portas configuradas no Cluster IPspace.

Sobre esta tarefa

Em um cluster comutado, se uma interface de rede de cluster (LIF) estiver configurada na porta errada ou se uma porta de cluster estiver conetada à rede errada, o `cluster create` comando poderá falhar com o seguinte erro:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Saiba mais sobre `cluster create` o "Referência do comando ONTAP"na .

Os resultados do `network port show` comando podem mostrar que várias portas são adicionadas ao Cluster IPspace porque estão conetadas a uma porta configurada com um cluster LIF. No entanto, os resultados do `network port reachability show -detail` comando revela quais portas não têm conectividade entre si.

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

Para recuperar de um cluster LIF configurado em uma porta que não é acessível às outras portas configuradas com cluster LIFs, execute as seguintes etapas:

Passos

1. Redefina a porta inicial do LIF do cluster para a porta correta:

   ```
   network port modify -home-port
   ```

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

2. Remova as portas que não têm LIFs de cluster configuradas a partir do domínio de broadcast do cluster:

   ```
   network port broadcast-domain remove-ports
   ```

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

3. Crie o cluster:

   ```
   cluster create
   ```

Resultado

Ao concluir a criação do cluster, o sistema deteta a configuração correta e coloca as portas nos domínios de broadcast corretos.

Informações relacionadas

- "mostra a acessibilidade da porta de rede"

Eliminar ONTAP LIFs

Você pode excluir uma interface de rede (LIF) que não seja mais necessária.

Antes de começar

Os LIFs a serem excluídos não devem estar em uso.

Passos

1. Marque os LIFs que você deseja excluir como administrativamente para baixo usando o seguinte comando:

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. Use o `network interface delete` comando para excluir um ou todos os LIFs:

Se você quiser excluir…	Introduza o comando …
Um LIF específico	`network interface delete -vserver vserver_name -lif lif_name`
Todos os LIFs	`network interface delete -vserver vserver_name -lif *`

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

   O comando a seguir exclui o LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Use o `network interface show` comando para confirmar que o LIF é excluído.

   Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Configurar LIFs ONTAP virtual IP (VIP)

Alguns data centers de última geração usam mecanismos de rede de camada 3 (IP) que exigem falha de LIFs nas sub-redes. O ONTAP suporta LIFs de dados de IP virtual (VIP) e o protocolo de roteamento associado, protocolo de gateway de borda (BGP), para atender aos requisitos de failover dessas redes de próxima geração.

Sobre esta tarefa

Um LIF de dados VIP é um LIF que não faz parte de qualquer sub-rede e é acessível a partir de todas as portas que hospedam um LIF BGP no mesmo espaço IPspace. Um LIF de dados VIP elimina a dependência de um host em interfaces de rede individuais. Como vários adaptadores físicos transportam o tráfego de

dados, toda a carga não se concentra em um único adaptador e na sub-rede associada. A existência de um LIF de dados VIP é anunciada para roteadores peer através do protocolo de roteamento, Border Gateway Protocol (BGP).

Os LIFs de dados VIP oferecem as seguintes vantagens:

- Portabilidade de LIF além de um domínio de broadcast ou sub-rede: LIFs de dados VIP podem falhar em qualquer sub-rede na rede, anunciando a localização atual de cada LIF de dados VIP para roteadores através do BGP.
- Taxa de transferência agregada: Os LIFs de dados VIP podem oferecer suporte a taxa de transferência agregada que excede a largura de banda de qualquer porta individual porque os LIFs VIP podem enviar ou receber dados de várias sub-redes ou portas simultaneamente.

Configurar o protocolo de gateway de borda (BGP)

Antes de criar LIFs VIP, você deve configurar o BGP, que é o protocolo de roteamento usado para anunciar a existência de um LIF VIP para roteadores peer.

A partir do ONTAP 9.9,1, o VIP fornece automação de rota padrão opcional usando grupos de pares BGP para simplificar a configuração.

O ONTAP tem uma maneira simples de aprender rotas padrão usando os pares BGP como roteadores de próximo salto quando o par BGP está na mesma sub-rede. Para usar o recurso, defina o `-use-peer-as-next-hop` atributo como `true`. Por padrão, esse atributo é `false`.

Se você tiver rotas estáticas configuradas, elas ainda serão preferidas sobre essas rotas padrão automatizadas.

Antes de começar

O roteador peer deve ser configurado para aceitar uma conexão BGP do BGP LIF para o ASN (número de sistema autônomo) configurado.

> O ONTAP não processa quaisquer anúncios de rota de entrada a partir do router; por conseguinte, deve configurar o router ponto-a-ponto para não enviar quaisquer atualizações de rota para o cluster. Isso reduz o tempo necessário para que a comunicação com o peer se torne totalmente funcional e reduz o uso de memória interna no ONTAP.

Sobre esta tarefa

Configurar o BGP envolve, opcionalmente, criar uma configuração BGP, criar um BGP LIF e criar um grupo de pares BGP. O ONTAP cria automaticamente uma configuração BGP padrão com valores padrão quando o primeiro grupo de pares BGP é criado em um determinado nó.

Um BGP LIF é usado para estabelecer sessões BGP TCP com roteadores peer. Para um roteador peer, um BGP LIF é o próximo salto para alcançar um VIP LIF. O failover está desativado para o BGP LIF. Um grupo de pares BGP anuncia as rotas VIP para todos os SVMs no IPspace usado pelo grupo de pares. O IPspace usado pelo grupo de pares é herdado do BGP LIF.

A partir do ONTAP 9.16,1, a autenticação MD5 é suportada em grupos de pares BGP para proteger sessões BGP. Quando o MD5 está ativado, as sessões de BGP só podem ser estabelecidas e processadas entre pares autorizados, evitando possíveis interrupções da sessão por um ator não autorizado.

Os seguintes campos foram adicionados `network bgp peer-group create` aos comandos e `network bgp peer-group modify`:

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Esses parâmetros permitem configurar um grupo de pares BGP com uma assinatura MD5 para maior segurança. Os seguintes requisitos aplicam-se ao uso da autenticação MD5.1X:

- Só é possível especificar o `-md5-secret` parâmetro quando o `-md5-enabled` parâmetro estiver definido como `true`.
- O IPsec deve estar ativado globalmente antes de poder ativar a autenticação BGP MD5. O BGP LIF não é necessário para ter uma configuração IPsec ativa. "Configurar a segurança IP (IPsec) através da criptografia por fio"Consulte a .
- A NetApp recomenda que você configure o MD5 no roteador antes de configurá-lo no controlador ONTAP.

A partir de ONTAP 9.9,1, estes campos foram adicionados:

- `-asn` Ou `-peer-asn` (valor de 4 bytes) o atributo em si não é novo, mas agora usa um inteiro de 4 bytes.
- `-med`
- `-use-peer-as-next-hop`

Pode fazer seleções de rota avançadas com suporte Multi-Exit discriminator (MED) para a priorização de caminho. MED é um atributo opcional na mensagem de atualização do BGP que informa aos roteadores para selecionar a melhor rota para o tráfego. O MED é um número inteiro de 32 bits não assinado (0 - 4294967295); valores mais baixos são preferidos.

A partir de ONTAP 9.8, esses campos foram adicionados ao `network bgp peer-group` comando:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Esses atributos BGP permitem que você configure os atributos caminho COMO e comunidade para o grupo de pares BGP.

> Embora o ONTAP ofereça suporte aos atributos BGP acima, os roteadores não precisam honrá-los. A NetApp recomenda fortemente que você confirme quais atributos são suportados pelo seu roteador e configure os grupos de pares BGP de acordo. Para obter detalhes, consulte a documentação BGP fornecida pelo seu roteador.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Opcional: Crie uma configuração BGP ou modifique a configuração BGP padrão do cluster executando uma das seguintes ações:

   a. Criar uma configuração BGP:

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- O `-routerid` parâmetro aceita um valor de 32 bits decimal pontilhado que só precisa ser exclusivo dentro de um DOMÍNIO AS. A NetApp recomenda que você use o endereço IP de gerenciamento de nós (v4) para `<router_id>` o qual garanta a exclusividade.
- Embora o ONTAP BGP suporte números ASN de 32 bits, apenas a notação decimal padrão é suportada. Notação ASN pontilhada, como 65000,1 em vez de 4259840001 para um ASN privado, não é suportada.

Amostra com um ASN de 2 bytes:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Amostra com um ASN de 4 bytes:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. Modifique a configuração padrão do BGP:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` Especifica o número ASN. Começando com ONTAP 9.8, o ASN para BGP suporta um inteiro não negativo de 2 bytes. Este é um número de 16 bits (1 a 65534 valores disponíveis). Começando com ONTAP 9.9,1, o ASN para BGP suporta um inteiro não negativo de 4 bytes (1 a 4294967295). O ASN padrão é 65501. O ASN 23456 é reservado para estabelecimento de sessão ONTAP com pares que não anunciam capacidade ASN de 4 bytes.
- `<hold_time>` especifica o tempo de espera em segundos. O valor padrão é 180s.

O ONTAP suporta apenas um global `<asn_number>`, , `<hold_time>` e `<router_id>`, mesmo que você configure o BGP para vários IPspaces. O BGP e todas as informações de roteamento IP são completamente isolados dentro de um espaço IPspace. Um espaço IPspace é equivalente a uma instância de roteamento e encaminhamento virtual (VRF).

3. Crie um BGP LIF para o SVM do sistema:

Para o IPspace padrão, o nome do SVM é o nome do cluster. Para IPspaces adicionais, o nome SVM é idêntico ao nome IPspace.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

Você pode usar a `default-route-announce` política de serviço para o BGP LIF ou qualquer política de serviço personalizado que contenha o serviço "Management-bgp".

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Crie um grupo de pares BGP que seja usado para estabelecer sessões BGP com os roteadores peer remotos e configurar as informações de rota VIP que são anunciadas aos roteadores peer:

   Exemplo 1: Crie um grupo de pares sem uma rota padrão automática

   Neste caso, o administrador precisa criar uma rota estática para o peer BGP.

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
   type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
   {-community BGP community list <0-65535>:<0-65535>}
   ```

   ```
   network bgp peer-group create -peer-group group1 -ipspace Default -bgp
   -lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
   -asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
   9000:900,8000:800
   ```

   Exemplo 2: Crie um grupo de pares com uma rota padrão automática

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
   preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
   prepend-count <integer>} {-med <integer>} {-community BGP community list
   <0-65535>:<0-65535>}
   ```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Exemplo 3: Crie um grupo de pares com o MD5 ativado

a. Ativar IPsec:

```
security ipsec config modify -is-enabled true
```

b. Crie o grupo de pares BGP com o MD5 ativado:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Exemplo usando uma chave sextavada:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657400
```

Exemplo usando uma cadeia de carateres:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Depois de criar o grupo de pares BGP, uma porta ethernet virtual (começando com v0a..v0z,v1a…) é listada quando você executa o `network port show` comando. A MTU desta interface é sempre relatada em 1500. A MTU real usada para tráfego é derivada da porta física (BGP LIF), que é determinada quando o tráfego é enviado. Saiba mais sobre `network port show` o "Referência do comando ONTAP"na .

Crie um IP virtual (VIP) data LIF

A existência de um LIF de dados VIP é anunciada para roteadores peer através do protocolo de roteamento, Border Gateway Protocol (BGP).

Antes de começar

- O grupo de pares BGP deve ser configurado e a sessão BGP para o SVM no qual o LIF deve ser criado deve estar ativa.
- Uma rota estática para o roteador BGP ou qualquer outro roteador na sub-rede BGP LIF deve ser criada

para qualquer tráfego VIP de saída para o SVM.

- Você deve ativar o roteamento multipath para que o tráfego VIP de saída possa usar todas as rotas disponíveis.

  Se o roteamento multipath não estiver habilitado, todo o tráfego VIP de saída será de uma única interface.

Passos

1. Crie um LIF de dados VIP:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   Uma porta VIP será selecionada automaticamente se você não especificar a porta inicial com o `network interface create` comando.

   Por padrão, o LIF de dados VIP pertence ao domínio de broadcast criado pelo sistema chamado 'VIP', para cada espaço IPspace. Não é possível modificar o domínio de transmissão VIP.

   Um LIF de dados VIP é acessível simultaneamente em todas as portas que hospedam um LIF BGP de um IPspace. Se não houver uma sessão de BGP ativa para o SVM do VIP no nó local, o LIF de dados VIP fará failover para a próxima porta VIP no nó que tiver uma sessão de BGP estabelecida para esse SVM.

2. Verifique se a sessão BGP está no status up para o SVM do LIF de dados VIP:

```
network bgp vserver-status show

Node        Vserver  bgp status
        ----------  -------- ---------
        node1       vs1      up
```

   Se o status do BGP for `down` para o SVM em um nó, o LIF de dados VIP fará o failover para um nó diferente no qual o status do BGP está ativo para o SVM. Se o status do BGP estiver `down` em todos os nós, o LIF de dados VIP não pode ser hospedado em qualquer lugar e tem status de LIF como inativo.

Comandos para gerenciar o BGP

A partir do ONTAP 9.5, você usa os `network bgp` comandos para gerenciar as sessões BGP no ONTAP.

Gerenciar a configuração do BGP

Se você quiser…	Use este comando…
Crie uma configuração BGP	`network bgp config create`
Modificar a configuração do BGP	`network bgp config modify`
Eliminar configuração BGP	`network bgp config delete`

Apresentar a configuração BGP	`network bgp config show`
Exibe o status do BGP para o SVM do VIP LIF	`network bgp vserver-status show`

Gerenciar valores padrão BGP

Se você quiser…	Use este comando…
Modificar valores padrão BGP	`network bgp defaults modify`
Exibir valores padrão BGP	`network bgp defaults show`

Gerenciar grupos de pares BGP

Se você quiser…	Use este comando…
Crie um grupo de pares BGP	`network bgp peer-group create`
Modificar um grupo de pares BGP	`network bgp peer-group modify`
Excluir um grupo de pares BGP	`network bgp peer-group delete`
Exibir informações de grupos de pares BGP	`network bgp peer-group show`
Renomeie um grupo de pares BGP	`network bgp peer-group rename`

Gerencie grupos de pares BGP com MD5

A partir do ONTAP 9.16,1, você pode ativar ou desativar a autenticação MD5 em um grupo de pares BGP existente.

> Se você ativar ou desativar o MD5 em um grupo de pares BGP existente, a conexão BGP será encerrada e recriada para aplicar as alterações de configuração do MD5.

Se você quiser…	Use este comando…
Ative MD5 em um grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Desative o MD5 em um grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Informações relacionadas

- "Referência do comando ONTAP"
- "rede bgp"
- "interface de rede"
- "modificação de configuração de segurança ipsec"

Equilibre as cargas da rede

Otimize o tráfego de rede ONTAP usando o balanceamento de carga DNS

Você pode configurar seu cluster para atender solicitações de clientes a partir de LIFs adequadamente carregados. Isso resulta em uma utilização mais equilibrada de LIFs e portas, o que, por sua vez, permite um melhor desempenho do cluster.

O balanceamento de carga DNS ajuda a selecionar um LIF de dados carregado adequadamente e equilibrar o tráfego de rede do usuário em todas as portas disponíveis (físicas, grupos de interfaces e VLANs).

Com o balanceamento de carga DNS, LIFs são associados à zona de balanceamento de carga de um SVM. Um servidor DNS em todo o site é configurado para encaminhar todas as solicitações DNS e retornar o LIF menos carregado com base no tráfego de rede e na disponibilidade dos recursos da porta (uso da CPU, taxa de transferência, conexões abertas, etc.). O balanceamento de carga DNS oferece os seguintes benefícios:

- Novas conexões de clientes equilibradas entre os recursos disponíveis.
- Nenhuma intervenção manual é necessária para decidir quais LIFs usar ao montar um SVM específico.
- O balanceamento de carga DNS suporta NFSv3, NFSv4, NFSv4,1, SMB 2,0, SMB 2,1, SMB 3,0 e S3.

Saiba mais sobre o balanceamento de carga DNS para a rede ONTAP

Os clientes montam um SVM especificando um endereço IP (associado a um LIF) ou um nome de host (associado a vários endereços IP). Por padrão, os LIFs são selecionados pelo servidor DNS em todo o site de forma round-robin, que equilibra a carga de trabalho em todos os LIFs.

O balanceamento de carga round-robin pode resultar em sobrecarga de alguns LIFs, então você tem a opção de usar uma zona de balanceamento de carga DNS que lida com a resolução de nome de host em um SVM. Usando uma zona de balanceamento de carga DNS, garante um melhor equilíbrio das novas conexões de clientes entre os recursos disponíveis, levando a um melhor desempenho do cluster.

Uma zona de balanceamento de carga DNS é um servidor DNS dentro do cluster que avalia dinamicamente a carga em todos os LIFs e retorna um LIF carregado adequadamente. Em uma zona de balanceamento de carga, o DNS atribui um peso (métrica), com base na carga, a cada LIF.

Cada LIF é atribuído um peso com base na carga da porta e na utilização da CPU do seu nó inicial. LIFs que estão em portas menos carregadas têm uma maior probabilidade de serem retornadas em uma consulta DNS. Os pesos também podem ser atribuídos manualmente.

Crie zonas de balanceamento de carga DNS para a rede ONTAP

Você pode criar uma zona de balanceamento de carga DNS para facilitar a seleção dinâmica de um LIF com base na carga, ou seja, o número de clientes montados em um LIF. Você pode criar uma zona de balanceamento de carga ao criar um LIF de dados.

Antes de começar

O encaminhador DNS no servidor DNS de todo o site deve ser configurado para encaminhar todas as solicitações para a zona de balanceamento de carga para os LIFs configurados.

O"Base de conhecimento da NetApp : como configurar o balanceamento de carga de DNS no modo de cluster" contém mais informações sobre como configurar o balanceamento de carga de DNS usando encaminhamento condicional.

Sobre esta tarefa

- Qualquer LIF de dados pode responder a consultas DNS para um nome de zona de balanceamento de carga DNS.
- Uma zona de balanceamento de carga DNS deve ter um nome exclusivo no cluster e o nome da zona deve atender aos seguintes requisitos:
  - Não deve exceder 256 carateres.
  - Deve incluir pelo menos um período.
  - O primeiro e o último caráter não devem ser um período ou qualquer outro caráter especial.
  - Não pode incluir espaços entre carateres.
  - Cada rótulo no nome DNS não deve exceder 63 carateres.

    Um rótulo é o texto que aparece antes ou depois do período. Por exemplo, a zona DNS chamada storage.company.com tem três rótulos.

Passo

Use o `network interface create` comando com a `dns-zone` opção para criar uma zona de balanceamento de carga DNS. Saiba mais sobre `network interface create` o "Referência do comando ONTAP"na .

Se a zona de balanceamento de carga já existir, o LIF é adicionado a ela.

O exemplo a seguir demonstra como criar uma zona de balanceamento de carga DNS chamada storage.company.com ao criar o LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Adicione ou remova um ONTAP LIF de uma zona de balanceamento de carga

Você pode adicionar ou remover um LIF da zona de balanceamento de carga DNS de uma máquina virtual (SVM). Você também pode remover todos os LIFs simultaneamente de uma zona de balanceamento de carga.

Antes de começar

- Todas as LIFs em uma zona de balanceamento de carga devem pertencer ao mesmo SVM.
- Um LIF pode fazer parte de apenas uma zona de balanceamento de carga DNS.
- Os grupos de failover para cada sub-rede devem ter sido configurados, se os LIFs pertencerem a diferentes sub-redes.

Sobre esta tarefa

Um LIF que está no status administrativo inativo é temporariamente removido da zona de balanceamento de

carga DNS. Quando o LIF retorna ao status administrativo up, o LIF é adicionado automaticamente à zona de balanceamento de carga DNS.

Passo

Adicione um LIF ou remova um LIF de uma zona de balanceamento de carga:

Se você quiser…	Digite…
Adicione um LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Exemplo: `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`
Remova um único LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none` Exemplo: `network interface modify -vserver vs1 -lif data1 -dns-zone none`
Remova todas as LIFs	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none` Exemplo: `network interface modify -vserver vs0 -lif * -dns-zone none` Você pode remover um SVM de uma zona de balanceamento de carga removendo todas as LIFs na SVM dessa zona.

Informações relacionadas

- "modificação da interface de rede"

Configurar serviços DNS para a rede ONTAP

Você deve configurar serviços DNS para o SVM antes de criar um servidor NFS ou SMB. Geralmente, os servidores de nomes DNS são os servidores DNS integrados ao ative Directory para o domínio em que o servidor NFS ou SMB se juntará.

Sobre esta tarefa

Os servidores DNS integrados ao ative Directory contêm os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio. Se o SVM não conseguir localizar os servidores LDAP e os controladores de domínio do ative Directory, a configuração do servidor NFS ou SMB falhará.

Os SVMs usam o banco de dados ns-switch de serviços de nome de hosts para determinar quais serviços de nome usar e em qual ordem ao procurar informações sobre hosts. Os dois serviços de nomes suportados para o banco de dados hosts são arquivos e dns.

Você deve garantir que o dns seja uma das fontes antes de criar o servidor SMB.

Para exibir as estatísticas dos serviços de nome DNS para o processo mgwd e o processo SecD, use a IU Estatística.

Passos

1. Determine qual é a configuração atual para o banco de dados de serviços de nome do host. Neste exemplo, o banco de dados do serviço de nomes de hosts usa as configurações padrão.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Execute as seguintes ações, se necessário.

   a. Adicione o serviço de nomes DNS ao banco de dados do serviço de nomes hosts na ordem desejada ou reordene as fontes.

      Neste exemplo, o banco de dados hosts é configurado para usar arquivos DNS e locais nessa ordem.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database hosts
      -sources dns,files
      ```

   b. Verifique se a configuração dos serviços de nome está correta.

      ```
      vserver services name-service ns-switch show -vserver vs1 -database hosts
      ```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configurar serviços DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```

> O comando vserver services name-service dns create executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

4. Verifique se a configuração DNS está correta e se o serviço está ativado.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Valide o status dos servidores de nomes.

```
vserver services name-service dns check -vserver vs1
```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configurar DNS dinâmico na SVM

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS de um servidor NFS ou SMB no DNS, você deverá configurar o DNS dinâmico (DDNS) no SVM.

Antes de começar

Os serviços de nomes DNS devem ser configurados no SVM. Se você estiver usando o DDNS seguro, use servidores de nomes DNS integrados ao ative Directory e crie um servidor NFS ou SMB ou uma conta do ative Directory para o SVM.

Sobre esta tarefa

O nome de domínio totalmente qualificado (FQDN) especificado deve ser exclusivo:

O nome de domínio totalmente qualificado (FQDN) especificado deve ser exclusivo:

- Para NFS, o valor especificado em `-vserver-fqdn` como parte `vserver services name-service dns dynamic-update` do comando torna-se o FQDN registrado para os LIFs.
- Para SMB, os valores especificados como o nome NetBIOS do servidor CIFS e o nome de domínio totalmente qualificado do servidor CIFS tornam-se o FQDN registrado para os LIFs. Isso não é configurável no ONTAP. No cenário a seguir, o FQDN de LIF é "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Para evitar uma falha de configuração de um FQDN SVM que não esteja em conformidade com as regras RFC para atualizações DDNS, use um nome FQDN compatível com RFC. Para obter mais informações, "RFC 1123"consulte .

Passos

1. Configurar o DDNS na SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asteriscos não podem ser usados como parte do FQDN personalizado. Por exemplo, `*.netapp.com` não é válido.

2. Verifique se a configuração DDNS está correta:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Configurar serviços DNS dinâmicos para a rede ONTAP

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS de um servidor NFS ou SMB no DNS, você deverá configurar o DNS dinâmico (DDNS) no SVM.

Antes de começar

Os serviços de nomes DNS devem ser configurados no SVM. Se você estiver usando o DDNS seguro, use servidores de nomes DNS integrados ao ative Directory e crie um servidor NFS ou SMB ou uma conta do ative Directory para o SVM.

Sobre esta tarefa

O FQDN especificado deve ser exclusivo.

> Para evitar uma falha de configuração de um FQDN SVM que não esteja em conformidade com as regras RFC para atualizações DDNS, use um nome FQDN compatível com RFC.

Passos

1. Configurar o DDNS na SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asteriscos não podem ser usados como parte do FQDN personalizado. Por exemplo, `*.netapp.com` não é válido.

2. Verifique se a configuração DDNS está correta:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Resolução do nome do host

Saiba mais sobre a resolução do nome do host para a rede ONTAP

O ONTAP deve ser capaz de traduzir nomes de host para endereços IP numéricos, a fim de fornecer acesso aos clientes e aos serviços de acesso. Você deve configurar máquinas virtuais de armazenamento (SVMs) para usar serviços de nome locais ou externos para resolver informações de host. O ONTAP suporta a configuração de um servidor DNS externo ou a configuração do arquivo hosts local para resolução de nome de host.

Ao usar um servidor DNS externo, você pode configurar o DNS dinâmico (DDNS), que envia automaticamente informações DNS novas ou alteradas do seu sistema de armazenamento para o servidor DNS. Sem atualizações de DNS dinâmicas, você deve adicionar manualmente informações de DNS (nome de DNS e endereço IP) aos servidores DNS identificados quando um novo sistema é colocado on-line ou quando as informações de DNS existentes forem alteradas. Este processo é lento e propenso a erros. Durante a recuperação de desastres, a configuração manual pode resultar em um longo tempo de inatividade.

Configurar DNS para resolução de nome de host para a rede ONTAP

Você usa o DNS para acessar fontes locais ou remotas para obter informações sobre o host. Você deve configurar o DNS para acessar uma ou ambas as fontes.

O ONTAP deve ser capaz de procurar informações de host para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços DNS locais ou externos para obter as informações do host.

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX.

Configurar uma SVM e LIFs de dados para resolução de nome de host usando um servidor DNS externo

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os nomes de host são resolvidos usando servidores DNS externos.

Antes de começar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

Consulte Configurar serviços DNS dinâmicos para obter mais informações sobre como configurar o DNS dinâmico no SVM.

Passos

1. Habilite o DNS na SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> O `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
-------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

Para obter informações sobre políticas de serviço relacionadas ao DNS, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

Configure a Tabela de interrutores do serviço de nomes para resolução de nome de host

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte o serviço de nomes local ou externo para recuperar informações do host.

Antes de começar

Você deve ter decidido qual serviço de nomes usar para mapeamento de host em seu ambiente.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Exemplo

O exemplo a seguir modifica uma entrada na tabela de switch de serviço de nomes para SVM VS1 para primeiro usar o arquivo hosts locais e, em seguida, um servidor DNS externo para resolver nomes de host:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

Comandos ONTAP para gerenciar a tabela hosts do ONTAP

Um administrador de cluster pode adicionar, modificar, excluir e exibir as entradas de nome de host na tabela hosts da máquina virtual de armazenamento de administrador (SVM). Um administrador do SVM pode configurar as entradas de nome de host somente para o SVM atribuído.

Comandos para gerenciar entradas locais de nome de host

Você pode usar o `vserver services name-service dns hosts` comando para criar, modificar ou excluir entradas de tabela de host DNS.

Ao criar ou modificar as entradas de nome de host DNS, você pode especificar vários endereços de alias separados por vírgulas.

Se você quiser…	Use este comando…
Crie uma entrada de nome de host DNS	`vserver services name-service dns hosts create`
Modificar uma entrada de nome de host DNS	`vserver services name-service dns hosts modify`
Excluir uma entrada de nome de host DNS	`vserver services name-service dns hosts delete`

Para obter mais informações sobre os `vserver services name-service dns hosts` comandos, consulte "Referência do comando ONTAP" .

Proteja a sua rede

Configurar a segurança de rede ONTAP usando FIPS para todas as conexões SSL

O ONTAP está em conformidade com o padrão FIPS 140-2 (Federal Information Processing Standards) para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas dentro do ONTAP.

Por padrão, o SSL no ONTAP é definido com a conformidade FIPS desativada e com os seguintes protocolos TLS ativados:

- TLSv1,3 (começando com ONTAP 9.11.1)
- TLSv1.2

As versões anteriores do ONTAP tinham os seguintes protocolos TLS ativados por padrão:

- TLSv1,1 (desativado por padrão a partir do ONTAP 9.12.1)
- TLSv1 (desativado por padrão a partir do ONTAP 9,8)

Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

Se você quiser que as contas de administrador acessem SVMs com uma chave pública SSH, certifique-se de que o algoritmo da chave do host seja suportado antes de ativar o modo SSL FIPS.

Nota: o suporte ao algoritmo da chave do host foi alterado no ONTAP 9.11,1 e versões posteriores.

Lançamento do ONTAP	Tipos de chave suportados	Tipos de chave não suportados
9.11.1 e mais tarde	ecdsa-sha2-nistp256	rsa-sha2-512 mais rsa-sha2-256 mais ssh-ed25519 mais ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ssh-dss e ssh-rsa

Contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado antes de ativar o FIPS, ou a autenticação do administrador falhará.

Para obter mais informações, "Ativar contas de chave pública SSH"consulte .

O ONTAP 9.18.1 introduz suporte para os algoritmos criptográficos pós-computação quântica ML-KEM, ML-DSA e SLH-DSA para SSL, fornecendo uma camada adicional de segurança contra possíveis futuros ataques de computadores quânticos. Esses algoritmos só estão disponíveis quandoO FIPS está desativado. . Os algoritmos criptográficos pós-quânticos são negociados quando o FIPS está desativado e o par os suporta.

Ativar FIPS

É recomendável que todos os usuários seguros ajustem sua configuração de segurança imediatamente após a instalação ou atualização do sistema. Quando o modo SSL FIPS está ativado, a comunicação SSL do

ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

> Quando o FIPS está ativado, não é possível instalar ou criar um certificado com um comprimento de chave RSA de 4096.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ativar FIPS:

   ```
   security config modify * -is-fips-enabled true
   ```

3. Quando solicitado a continuar, digite `y`
4. A partir do ONTAP 9.9.1, não é necessário reinicializar. Se você estiver executando o ONTAP 9.8 ou anterior, reinicie manualmente cada nó no cluster, um por um.

Exemplo

Se estiver a executar o ONTAP 9.9,1 ou posterior, não verá a mensagem de aviso.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Saiba mais sobre `security config modify` a configuração do modo SSL FIPS no "Referência do comando ONTAP".

Desativar FIPS

A partir da versão 9.18.1 do ONTAP , o SSL no ONTAP oferece suporte aos algoritmos criptográficos pós-computação quântica ML-KEM, ML-DSA e SLH-DSA. Esses algoritmos só estão disponíveis quando o FIPS está desativado e o servidor par os suporta.

Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Desative o FIPS digitando:

```
security config modify -is-fips-enabled false
```

3. Quando solicitado a continuar, digite `y`.
4. A partir do ONTAP 9.9.1, não é necessário reinicializar. Se você estiver executando o ONTAP 9.8 ou anterior, reinicie manualmente cada nó no cluster.

Se precisar usar o protocolo SSLv3, você deve desativar o FIPS seguindo o procedimento acima. O SSLv3 só pode ser ativado quando o FIPS estiver desativado.

Você pode habilitar o SSLv3 com o seguinte comando. Se você estiver executando o ONTAP 9.9.1 ou posterior, não verá a mensagem de aviso.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Visualizar o status de conformidade FIPS

Você pode ver se todo o cluster está executando as configurações de segurança atuais.

Passos

1. Se você estiver executando o ONTAP 9.8 ou anterior, reinicie manualmente cada nó no cluster, um por um.
2. Exibir o status de conformidade atual:

```
security config show
```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

Saiba mais sobre `security config show` o "Referência do comando ONTAP"na .

Informações relacionadas

- "FIPS 203: Padrão de Mecanismo de Encapsulamento de Chaves Baseado em Reticulado de Módulos (ML-KEM)"
- "FIPS 204: Padrão de Assinatura Digital Baseado em Módulo-Reticulado (ML-DSA)"
- "FIPS 205: Padrão de Assinatura Digital Baseada em Hash Sem Estado (SLH-DSA)"

Configurar a criptografia IPsec em trânsito

Prepare-se para usar a segurança IP na rede ONTAP

A partir do ONTAP 9.8, você tem a opção de usar a segurança IP (IPsec) para proteger o tráfego de rede. IPsec é uma das várias opções de criptografia de dados em movimento ou em trânsito disponíveis com o ONTAP. Você deve se preparar para configurar o IPsec antes de usá-lo em um ambiente de produção.

Implementação de segurança IP no ONTAP

IPsec é um padrão de Internet mantido pelo IETF. Ele fornece criptografia e integridade de dados, bem como autenticação para o tráfego que flui entre os endpoints da rede em um nível IP.

Com o ONTAP, o IPsec protege todo o tráfego IP entre o ONTAP e os vários clientes, incluindo os protocolos NFS, SMB e iSCSI. Além da privacidade e integridade dos dados, o tráfego de rede é protegido contra vários ataques, como repetição e ataques man-in-the-middle. O ONTAP usa a implementação do modo de transporte IPsec. Ele aproveita o protocolo IKE (Internet Key Exchange) versão 2 para negociar o material chave entre o ONTAP e os clientes usando IPv4 ou IPv6.

Quando o recurso IPsec está ativado em um cluster, a rede requer uma ou mais entradas no banco de dados de diretiva de segurança (SPD) do ONTAP que correspondam às várias caraterísticas de tráfego. Essas entradas mapeiam para os detalhes de proteção específicos necessários para processar e enviar os dados (como, por exemplo, conjunto de codificações e método de autenticação). Uma entrada SPD correspondente também é necessária em cada cliente.

Para certos tipos de tráfego, outra opção de criptografia de dados em movimento pode ser preferível. Por exemplo, para a criptografia do tráfego de peering de cluster e NetApp SnapMirror, o protocolo TLS (Transport Layer Security) geralmente é recomendado em vez de IPsec. Isso ocorre porque o TLS oferece melhor desempenho na maioria das situações.

Informações relacionadas

- "Internet Engineering Task Force"
- "RFC 4301: Arquitetura de segurança para o Protocolo de Internet"

Evolução da implementação IPsec do ONTAP

O IPsec foi introduzido pela primeira vez com o ONTAP 9.8. A implementação continuou a evoluir nas versões subsequentes do ONTAP , conforme descrito abaixo.

ONTAP 9.18.1

O suporte para descarregamento de hardware IPsec foi estendido ao tráfego IPv6.

ONTAP 9.17.1

O suporte para descarregamento de hardware IPsec é estendido para "grupos de agregação de links" . "Chaves pré-compartilhadas pós-quânticas (PPKs)" são suportados para autenticação de chaves pré-compartilhadas (PSK) IPsec.

ONTAP 9.16,1

Várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa NIC suportada. Consulte Recurso de descarga de hardware IPsec para obter mais informações.

ONTAP 9.12,1

O suporte ao protocolo de host front-end IPsec está disponível nas configurações de conexão de malha MetroCluster IP e MetroCluster. O suporte IPsec fornecido com clusters MetroCluster é limitado ao tráfego de host front-end e não é compatível com LIFs MetroCluster entre clusters.

ONTAP 9.10,1

Além dos PSKs, certificados podem ser usados para autenticação IPsec. Antes do ONTAP 9.10.1, apenas PSKs eram suportados para autenticação.

ONTAP 9.9,1

Os algoritmos de criptografia usados pelo IPsec são validados pelo FIPS 140-2. Esses algoritmos são processados pelo módulo criptográfico NetApp no ONTAP, que carrega a validação FIPS 140-2.

ONTAP 9,8

O suporte para IPsec torna-se inicialmente disponível com base na implementação do modo de transporte.

Recurso de descarga de hardware IPsec

Se você estiver usando o ONTAP 9.16,1 ou posterior, terá a opção de descarregar determinadas operações computacionalmente intensivas, como verificações de criptografia e integridade, para uma placa de controlador de interface de rede (NIC) instalada no nó de armazenamento. A taxa de transferência para operações descarregadas para a placa NIC é de aproximadamente 5% ou menos. Isso pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido pelo IPsec.

Requisitos e recomendações

Há vários requisitos que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

Placas Ethernet suportadas

Você precisa instalar e usar apenas placas Ethernet compatíveis. As seguintes placas Ethernet são compatíveis a partir do ONTAP 9.16.1:

- X50131A (controlador Ethernet 2P, 40G/100g/200g/400G)
- X60132A (controlador Ethernet 4P, 10G/25G)

O ONTAP 9.17.1 adiciona suporte para as seguintes placas Ethernet:

- X50135A (Controlador Ethernet 2p, 40G/100G)
- X60135A (Controlador Ethernet 2p, 40G/100G)

As placas X50131A e X50135A são suportadas nas seguintes plataformas:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

As placas X60132A e X60135A são suportadas nas seguintes plataformas:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Veja o "NetApp Hardware Universe" para mais informações sobre as plataformas e placas suportadas.

Escopo do cluster

O recurso de descarga de hardware IPsec é configurado globalmente para o cluster. E assim, por exemplo, o comando `security ipsec config` se aplica a todos os nós no cluster.

Configuração consistente

As placas NIC suportadas devem ser instaladas em todos os nós do cluster. Se uma placa NIC suportada estiver disponível apenas em alguns dos nós, você poderá ver uma degradação significativa do desempenho após um failover se algumas LIFs não estiverem hospedadas em uma NIC compatível com descarga.

Desativar a anti-repetição

Você deve desativar a proteção anti-replay IPsec no ONTAP (configuração padrão) e nos clientes IPsec. Se não estiver desativado, a fragmentação e o multi-path (rota redundante) não serão suportados.

Se a configuração IPsec do ONTAP tiver sido alterada do padrão para ativar a proteção anti-replay, use este comando para desativá-la:

```
security ipsec config modify -replay-window 0
```

Você deve garantir que a proteção anti-replay IPsec esteja desativada no cliente. Consulte a documentação IPsec do cliente para desativar a proteção anti-replay.

Limitações

Há várias limitações que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

IPv6

A partir da versão 9.18.1 do ONTAP , o IPv6 é suportado para o recurso de descarregamento de hardware IPsec. Antes da versão 9.18.1 do ONTAP , o descarregamento de hardware IPsec não suportava IPv6.

Números de sequência alargados

Os números de sequência estendida IPsec não são suportados com o recurso de descarga de hardware. Apenas são utilizados os números normais de sequência de 32 bits.

Agregação de links

A partir do ONTAP 9.17.1, você pode usar o recurso de descarregamento de hardware IPsec com um "grupo de agregação de links" .

Antes da versão 9.17.1, o recurso de descarregamento de hardware IPsec não suportava agregação de links. Ele não pode ser usado com uma interface ou grupo de agregação de links administrados pelo `network port ifgrp` comandos no ONTAP CLI.

Suporte à configuração na CLI do ONTAP

Três comandos CLI existentes são atualizados no ONTAP 9.16,1 para suportar o recurso de descarga de hardware IPsec, conforme descrito abaixo. Consulte também "Configure a segurança IP no ONTAP"para obter mais informações.

Comando ONTAP	Atualização
`security ipsec config show`	O parâmetro booleano `Offload Enabled` mostra o status atual de descarga da NIC.
`security ipsec config modify`	O parâmetro `is-offload-enabled` pode ser usado para ativar ou desativar o recurso de descarga de NIC.
`security ipsec config show-ipsecsa`	Quatro novos contadores foram adicionados para exibir o tráfego de entrada, bem como de saída em bytes e pacotes.

Suporte à configuração na API REST do ONTAP

Dois endpoints de API REST existentes são atualizados no ONTAP 9.16,1 para oferecer suporte ao recurso de descarga de hardware IPsec, conforme descrito abaixo.

Endpoint da REST	Atualização
`/api/security/ipsec`	O parâmetro `offload_enabled` foi adicionado e está disponível com o método DE PATCH.
`/api/security/ipsec/security_association`	Dois novos valores de contador foram adicionados para rastrear o total de bytes e pacotes processados pelo recurso de descarga.

Saiba mais sobre a API REST do ONTAP, incluindo "Novidades com a API REST do ONTAP", na documentação de automação do ONTAP. Você também deve consultar a documentação de automação do ONTAP para obter detalhes sobre "Pontos de extremidade IPsec"o .

Informações relacionadas

- "segurança ipsec"

Configure a segurança IP para a rede ONTAP

Há várias tarefas que você precisa executar para configurar e ativar a criptografia IPsec em trânsito no cluster do ONTAP.

> Certifique-se de revisar "Prepare-se para usar a segurança IP" antes de configurar o IPsec. Por exemplo, talvez seja necessário decidir se deve usar o recurso de descarga de hardware IPsec disponível a partir do ONTAP 9.16,1.

Ative o IPsec no cluster

Você pode habilitar o IPsec no cluster para garantir que os dados estejam criptografados continuamente e seguros enquanto estiverem em trânsito.

Passos

1. Descubra se o IPsec já está habilitado:

   ```
   security ipsec config show
   ```

   Se o resultado incluir `IPsec Enabled: false`, avance para o passo seguinte.

2. Ativar IPsec:

   ```
   security ipsec config modify -is-enabled true
   ```

   Você pode ativar o recurso de descarga de hardware IPsec usando o parâmetro booleano `is-offload-enabled` .

3. Execute o comando Discovery novamente:

   ```
   security ipsec config show
   ```

   O resultado agora `IPsec Enabled: true`inclui .

Prepare-se para a criação de diretiva IPsec com autenticação de certificado

Você pode ignorar esta etapa se estiver usando apenas chaves pré-compartilhadas (PSKs) para autenticação e não usar autenticação de certificado.

Antes de criar uma diretiva IPsec que usa certificados para autenticação, você deve verificar se os seguintes pré-requisitos são atendidos:

- Tanto o ONTAP quanto o cliente devem ter o certificado CA da outra parte instalado para que os certificados da entidade final (ONTAP ou cliente) sejam verificáveis por ambos os lados
- Um certificado é instalado para o ONTAP LIF que participa da política

ONTAP LIFs podem compartilhar certificados. Não é necessário um mapeamento individual entre certificados e LIFs.

Passos

1. Instale todos os certificados de CA usados durante a autenticação mútua, incluindo CAs do lado do ONTAP e do lado do cliente, no gerenciamento de certificados do ONTAP, a menos que ele já esteja instalado (como é o caso de uma CA raiz autoassinada do ONTAP).
   - Exemplo de comando*
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. Para garantir que a CA instalada esteja dentro do caminho de pesquisa da CA IPsec durante a autenticação, adicione as CAs de gerenciamento de certificados ONTAP ao módulo IPsec usando o `security ipsec ca-certificate add` comando.
   - Exemplo de comando*
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. Crie e instale um certificado para uso pelo ONTAP LIF. A CA do emissor deste certificado já deve ser instalada no ONTAP e adicionada ao IPsec.
   - Exemplo de comando*
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

Para obter mais informações sobre certificados no ONTAP, consulte os comandos do certificado de segurança na documentação do ONTAP 9.

Definir o banco de dados de políticas de segurança (SPD)

O IPsec requer uma entrada SPD antes de permitir que o tráfego flua na rede. Isso é verdade se você estiver usando um PSK ou um certificado para autenticação.

Passos

1. Use o `security ipsec policy create` comando para:
   a. Selecione o endereço IP do ONTAP ou a sub-rede de endereços IP para participar do transporte IPsec.
   b. Selecione os endereços IP do cliente que se conetarão aos endereços IP do ONTAP.

O cliente deve suportar o Internet Key Exchange versão 2 (IKEv2) com uma chave pré-compartilhada (PSK).

c. Opcionalmente, selecione os parâmetros de tráfego mais detalhados, como os protocolos da camada superior (UDP, TCP, ICMP, etc.), os números das portas locais e remotas para proteger o tráfego. Os parâmetros correspondentes são `protocols` , `local-ports` e `remote-ports` respectivamente.

   Ignore esta etapa para proteger todo o tráfego entre o endereço IP do ONTAP e o endereço IP do cliente. Proteger todo o tráfego é o padrão.

d. Insira PSK ou infra-estrutura de chave pública (PKI) para `auth-method` o parâmetro para o método de autenticação desejado.

   i. Se você inserir um PSK, inclua os parâmetros e pressione <enter> para que o prompt digite e verifique a chave pré-compartilhada.

      Os `local-identity` parâmetros e `remote-identity` são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

   ii. Se introduzir uma PKI, terá de introduzir também os `cert-name` `local-identity` parâmetros , . `remote-identity` Se a identidade do certificado do lado remoto for desconhecida ou se forem esperadas várias identidades de cliente, insira a identidade `ANYTHING`especial .

e. A partir do ONTAP 9.17.1, opcionalmente insira uma identidade de chave pré-compartilhada pós-quântica (PPK) com o `ppk-identity` parâmetro. PPKs oferecem uma camada adicional de segurança contra potenciais ataques futuros a computadores quânticos. Ao inserir uma identidade PPK, você será solicitado a inserir o segredo PPK. PPKs são compatíveis apenas com autenticação PSK.

Saiba mais sobre `security ipsec policy create` no "Referência do comando ONTAP" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

O tráfego IP não pode fluir entre o cliente e o servidor até que o ONTAP e o cliente tenham configurado as diretivas IPsec correspondentes e as credenciais de autenticação (PSK ou certificado) estejam no lugar em ambos os lados.

Use identidades IPsec

Para o método de autenticação de chave pré-compartilhada, identidades locais e remotas são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

Para o método de autenticação PKI/certificado, as identidades locais e remotas são obrigatórias. As identidades especificam qual identidade é certificada no certificado de cada lado e são usadas no processo de verificação. Se a identidade remota for desconhecida ou se puder ser muitas identidades diferentes, use a identidade `ANYTHING`especial .

Sobre esta tarefa

Dentro do ONTAP, as identidades são especificadas modificando a entrada SPD ou durante a criação da política SPD. O SPD pode ser um endereço IP ou um nome de identidade de formato de cadeia de carateres.

Passos

1. Use o seguinte comando para modificar uma configuração de identidade SPD existente:

```
security ipsec policy modify
```

Exemplo de comando

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configuração de vários clientes IPsec

Quando um pequeno número de clientes precisa aproveitar o IPsec, usar uma única entrada SPD para cada cliente é suficiente. No entanto, quando centenas ou mesmo milhares de clientes precisam utilizar o IPsec, o NetApp recomenda o uso de uma configuração de vários clientes IPsec.

Sobre esta tarefa

O ONTAP é compatível com a conexão de vários clientes em várias redes a um único endereço IP SVM com IPsec ativado. Você pode fazer isso usando um dos seguintes métodos:

- **Configuração de sub-rede**

  Para permitir que todos os clientes em uma sub-rede específica (por exemplo, 192.168.134.0/24) se conetem a um único endereço IP SVM usando uma única entrada de política SPD, você deve especificar o `remote-ip-subnets` formulário de sub-rede in. Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta.

  > Ao usar uma única entrada de diretiva em uma configuração de sub-rede, os clientes IPsec nessa sub-rede compartilham a identidade IPsec e a chave pré-compartilhada (PSK). No entanto, isso não é verdade com a autenticação de certificado. Ao usar certificados, cada cliente pode usar seu próprio certificado exclusivo ou um certificado compartilhado para autenticar. O IPsec do ONTAP verifica a validade do certificado com base nas CAs instaladas em seu armazenamento de confiança local. O ONTAP também suporta verificação de lista de revogação de certificados (CRL).

- **Permitir a configuração de todos os clientes**

  Para permitir que qualquer cliente, independentemente do endereço IP de origem, se conete ao endereço IP habilitado para IPsec SVM, use o `0.0.0.0/0` caractere curinga ao especificar o `remote-ip-subnets` campo.

  Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta. Para autenticação de certificado, pode introduzir `ANYTHING`.

Além disso, quando o `0.0.0.0/0` caractere curinga é usado, você deve configurar um número de porta local ou remota específico para usar. Por exemplo, `NFS port 2049`.

Passos

a. Use um dos comandos a seguir para configurar o IPsec para vários clientes.

   i. Se você estiver usando **configuração de sub-rede** para oferecer suporte a vários clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
   IP_address/subnet -local-identity local_id -remote-identity remote_id
   ```

Exemplo de comando

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

   i. Se você estiver usando **permitir que a configuração de todos os clientes** ofereça suporte a vários clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
   -ports port_number -local-identity local_id -remote-identity remote_id
   ```

Exemplo de comando

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Exibir estatísticas IPsec

Por meio da negociação, um canal de segurança chamado Associação de Segurança IKE (SA) pode ser estabelecido entre o endereço IP do ONTAP SVM e o endereço IP do cliente. As SAS IPsec são instaladas em ambos os endpoints para fazer o trabalho real de criptografia e descriptografia de dados. Você pode usar comandos de estatísticas para verificar o status de SAS IPsec e SAS IKE.

> Se você estiver usando o recurso de descarga de hardware IPsec, vários novos contadores serão exibidos com o comando `security ipsec config show-ipsecsa`.

Comandos de exemplo

Comando de exemplo IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Comando e saída de amostra IPsec SA:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Comando e saída de amostra IPsec SA:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Informações relacionadas

- "instalação do certificado de segurança"
- "segurança ipsec"

Configure a criptografia de rede do cluster de back-end ONTAP.

A partir do ONTAP 9.18.1, é possível configurar a criptografia Transport Layer Security (TLS) para dados em trânsito na rede do cluster de back-end. Essa criptografia protege os dados do cliente armazenados no ONTAP quando são transmitidos entre os nós do ONTAP na rede do cluster de back-end.

Sobre esta tarefa

- A criptografia de rede do cluster de backend está desativada por padrão.
- Quando a criptografia de rede do cluster de backend está habilitada, todos os dados do cliente armazenados no ONTAP são criptografados durante a transmissão entre os nós do ONTAP na rede do cluster de backend. Alguns tráfegos de rede do cluster, como dados do caminho de controle, não são criptografados.
- Por padrão, a criptografia de rede do cluster de backend usará certificados gerados automaticamente para cada nó do cluster. Você podeGerenciar certificados de criptografia de rede de cluster Em cada nó, será utilizado um certificado personalizado instalado.

Antes de começar

- Você precisa ser um administrador do ONTAP no `admin` Nível de privilégio necessário para executar as seguintes tarefas.
- Todos os nós do cluster devem estar executando o ONTAP 9.18.1 ou posterior para habilitar a criptografia de rede do cluster no backend.

Ativar ou desativar a criptografia para comunicação em rede de cluster

Passos

1. Veja o status atual da criptografia da rede do cluster:

   ```
   security cluster-network show
   ```

   Este comando mostra o estado atual da criptografia da rede do cluster:

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Ativar ou desativar a criptografia de rede TLS no cluster de backend:

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Este comando habilita ou desabilita a comunicação criptografada para dados do cliente em trânsito na rede do cluster de back-end.

Gerenciar certificados de criptografia de rede de cluster

1. Veja as informações atuais do certificado de criptografia da rede do cluster:

   ```
   security cluster-network certificate show
   ```

   Este comando exibe as informações atuais do certificado de criptografia de rede do cluster:

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

O certificado e o nome da autoridade certificadora (CA) são exibidos para cada nó do cluster.

2. Modifique o certificado de criptografia de rede do cluster para um nó:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Este comando modifica o certificado de criptografia da rede do cluster para um nó específico. O certificado deve ser instalado e assinado por uma Autoridade Certificadora (CA) instalada antes da execução deste comando. Para obter mais informações sobre gerenciamento de certificados, consulte"Gerencie certificados ONTAP com o Gerenciador de sistemas" . Se `-name` Caso não seja especificado, será utilizado o certificado padrão gerado automaticamente.

Configurar políticas de firewall para LIFs na rede ONTAP

A configuração de um firewall aumenta a segurança do cluster e ajuda a impedir o acesso não autorizado ao sistema de armazenamento. Por padrão, o firewall integrado é configurado para permitir acesso remoto a um conjunto específico de serviços IP para dados, gerenciamento e LIFs entre clusters.

Começando com ONTAP 9.10,1:

- As políticas de firewall são obsoletas e são substituídas por políticas de serviço LIF. Anteriormente, o firewall integrado era gerenciado usando políticas de firewall. Essa funcionalidade agora é realizada usando uma política de serviço LIF.
- Todas as políticas de firewall estão vazias e não abrem nenhuma porta no firewall subjacente. Em vez disso, todas as portas devem ser abertas usando uma política de serviço LIF.
- Nenhuma ação é necessária após uma atualização para 9.10.1 ou posterior para a transição de políticas de firewall para políticas de serviço LIF. O sistema constrói automaticamente políticas de serviço LIF consistentes com as políticas de firewall em uso na versão anterior do ONTAP. Se você usar scripts ou outras ferramentas que criam e gerenciam políticas de firewall personalizadas, talvez seja necessário atualizar esses scripts para criar políticas de serviço personalizadas.

Para saber mais, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

As políticas de firewall podem ser usadas para controlar o acesso a protocolos de serviço de gerenciamento,

como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS ou SNMP. Não é possível definir políticas de firewall para protocolos de dados como NFS ou SMB.

Você pode gerenciar o serviço de firewall e as políticas das seguintes maneiras:

- Ativar ou desativar o serviço de firewall
- Exibindo a configuração atual do serviço de firewall
- Criar uma nova política de firewall com o nome da política e os serviços de rede especificados
- Aplicar uma política de firewall a uma interface lógica
- Criar uma nova política de firewall que seja uma cópia exata de uma política existente

  Use isso para criar uma política com características semelhantes no mesmo SVM ou para copiar a política para um SVM diferente.

- Exibindo informações sobre políticas de firewall
- Modificar os endereços IP e as máscaras de rede que são usadas por uma política de firewall
- Eliminar uma política de firewall que não está a ser utilizada por um LIF

Políticas de firewall e LIFs

As políticas de firewall LIF são usadas para restringir o acesso ao cluster em cada LIF. Você precisa entender como a política de firewall padrão afeta o acesso do sistema sobre cada tipo de LIF e como você pode personalizar uma política de firewall para aumentar ou diminuir a segurança sobre um LIF.

Ao configurar um LIF usando o `network interface create` comando ou `network interface modify`, o valor especificado para o `-firewall-policy` parâmetro determina os protocolos de serviço e os endereços IP que têm acesso permitido ao LIF. Saiba mais sobre `network interface` o "Referência do comando ONTAP"na .

Em muitos casos, você pode aceitar o valor padrão da política de firewall. Em outros casos, talvez seja necessário restringir o acesso a determinados endereços IP e a determinados protocolos de serviço de gerenciamento. Os protocolos de serviço de gerenciamento disponíveis incluem SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS e SNMP.

A política de firewall para todas as LIFs de cluster é padrão `""` e não pode ser modificada.

A tabela a seguir descreve as políticas de firewall padrão que são atribuídas a cada LIF, dependendo de sua função (ONTAP 9.5 e anterior) ou diretiva de serviço (ONTAP 9.6 e posterior), quando você cria o LIF:

Política de firewall	Protocolos de serviço padrão	Acesso predefinido	LIFs aplicadas a
gestão	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualquer endereço (0,0.0,0/0)	Gerenciamento de clusters, gerenciamento de SVM e LIFs de gerenciamento de nós
gerenciamento nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualquer endereço (0,0.0,0/0)	LIFs de dados que também são compatíveis com o acesso de gerenciamento da SVM

entre clusters	https, ndmp, ndmps	Qualquer endereço (0,0.0,0/0)	Todos os LIFs entre clusters
dados	dns, ndmp, ndmps, portmap	Qualquer endereço (0,0.0,0/0)	Todos os dados LIFs

Configuração do serviço portmap

O serviço portmap mapeia os serviços RPC para as portas nas quais eles escutam.

O serviço portmap estava sempre acessível no ONTAP 9.3 e anterior, tornou-se configurável no ONTAP 9.4 através do ONTAP 9.6 e é gerenciado automaticamente a partir do ONTAP 9.7.

- No ONTAP 9.3 e anteriores, o serviço portmap (rpcbind) estava sempre acessível na porta 111 em configurações de rede que dependiam do firewall ONTAP integrado em vez de um firewall de terceiros.
- Do ONTAP 9.4 ao ONTAP 9.6, você pode modificar políticas de firewall para controlar se o serviço portmap está acessível em LIFs específicos.
- A partir do ONTAP 9.7, o serviço de firewall portmap é eliminado. Em vez disso, a porta portmap é aberta automaticamente para todos os LIFs que suportam o serviço NFS.

O serviço portmap é configurável no firewall no ONTAP 9.4 através do ONTAP 9.6.

O restante deste tópico discute como configurar o serviço de firewall do portmap para as versões do ONTAP 9.4 através do ONTAP 9.6.

Dependendo da sua configuração, você poderá desativar o acesso ao serviço em tipos específicos de LIFs, geralmente de gerenciamento e LIFs entre clusters. Em algumas circunstâncias, você pode até mesmo ser capaz de proibir o acesso em LIFs de dados.

Que comportamento você pode esperar

O comportamento do ONTAP 9.4 até o ONTAP 9.6 foi projetado para fornecer uma transição perfeita na atualização. Se o serviço portmap já estiver sendo acessado sobre tipos específicos de LIFs, ele continuará acessível sobre esses tipos de LIFs. Como no ONTAP 9.3 e anteriores, você pode especificar os serviços acessíveis no firewall na política de firewall para o tipo LIF.

Todos os nós no cluster devem estar executando o ONTAP 9.4 a ONTAP 9.6 para que o comportamento entre em vigor. Apenas o tráfego de entrada é afetado.

As novas regras são as seguintes:

- Ao atualizar para a versão 9,4 até 9,6, o ONTAP adiciona o serviço portmap a todas as políticas de firewall existentes, padrão ou personalizado.
- Quando você cria um novo cluster ou um novo espaço de IPspace, o ONTAP adiciona o serviço de portmap apenas à política de dados padrão, não ao gerenciamento padrão ou às políticas entre clusters.
- Você pode adicionar o serviço portmap a políticas padrão ou personalizadas conforme necessário e remover o serviço conforme necessário.

Como adicionar ou remover o serviço portmap

Para adicionar o serviço portmap a uma diretiva de firewall de cluster ou SVM (torná-lo acessível dentro do firewall), digite:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Para remover o serviço portmap de uma diretiva de firewall de cluster ou SVM (torná-lo inacessível no firewall), digite:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Você pode usar o comando Network Interface Modify para aplicar a política de firewall a um LIF existente. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Crie uma política de firewall e atribua-a a um LIF

As políticas de firewall padrão são atribuídas a cada LIF quando você cria o LIF. Em muitos casos, as configurações padrão do firewall funcionam bem e você não precisa alterá-las. Se você quiser alterar os serviços de rede ou endereços IP que podem acessar um LIF, você pode criar uma política de firewall personalizada e atribuí-la ao LIF.

Sobre esta tarefa

- Não é possível criar uma política de firewall com o `policy` nome `data`, `intercluster`, `cluster`, ou `mgmt`.

  Esses valores são reservados para as políticas de firewall definidas pelo sistema.

- Não é possível definir ou modificar uma política de firewall para LIFs de cluster.

  A política de firewall para LIFs de cluster está definida como 0,0.0.0/0 para todos os tipos de serviços.

- Se você precisar remover um serviço de uma política, exclua a política de firewall existente e crie uma nova política.
- Se o IPv6 estiver ativado no cluster, você poderá criar políticas de firewall com endereços IPv6.

  Depois que o IPv6 estiver ativado, `data` `intercluster`, e `mgmt` as políticas de firewall incluem ::/0, o curinga IPv6, em sua lista de endereços aceitos.

- Ao usar o System Manager para configurar a funcionalidade de proteção de dados entre clusters, você deve garantir que os endereços IP LIF sejam incluídos na lista permitida e que o serviço HTTPS seja permitido tanto nas LIFs entre clusters quanto nas firewalls de propriedade da empresa.

  Por padrão, a `intercluster` política de firewall permite o acesso de todos os endereços IP (0,0.0,0/0, ou ::/0 para IPv6) e habilita os serviços HTTPS, NDMP e NDMPS. Se você modificar essa política padrão ou criar sua própria política de firewall para LIFs entre clusters, adicione cada endereço IP LIF entre clusters à lista permitida e ative o serviço HTTPS.

- A partir do ONTAP 9.6, os serviços de firewall HTTPS e SSH não são suportados.

  No ONTAP 9.6, os `management-https` serviços e `management-ssh` LIF estão disponíveis para acesso de gerenciamento HTTPS e SSH.

Passos

1. Crie uma política de firewall que estará disponível para os LIFs em um SVM específico:

`system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

Você pode usar este comando várias vezes para adicionar mais de um serviço de rede e lista de endereços IP permitidos para cada serviço na política de firewall.

2. Verifique se a política foi adicionada corretamente usando o `system services firewall policy show` comando.
3. Aplique a política de firewall a um LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Verifique se a política foi adicionada corretamente ao LIF usando o `network interface show -fields firewall-policy` comando.

   Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Exemplo de criar uma política de firewall e atribuí-la a um LIF

O comando a seguir cria uma política de firewall chamada data_http que habilita o acesso de protocolos HTTP e HTTPS a partir de endereços IP na sub-rede 10,10, aplica essa política ao LIF chamado data1 na SVM VS1 e, em seguida, mostra todas as políticas de firewall no cluster:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Comandos ONTAP para gerenciar o serviço e as políticas de firewall

Você pode usar os `system services firewall` comandos para gerenciar o serviço de firewall, os `system services firewall policy` comandos para gerenciar políticas de firewall e o `network interface modify` comando para gerenciar configurações de firewall para LIFs.

Começando com ONTAP 9.10,1:

- As políticas de firewall são obsoletas e são substituídas por políticas de serviço LIF. Anteriormente, o firewall integrado era gerenciado usando políticas de firewall. Essa funcionalidade agora é realizada usando uma política de serviço LIF.
- Todas as políticas de firewall estão vazias e não abrem nenhuma porta no firewall subjacente. Em vez disso, todas as portas devem ser abertas usando uma política de serviço LIF.
- Nenhuma ação é necessária após uma atualização para 9.10.1 ou posterior para a transição de políticas de firewall para políticas de serviço LIF. O sistema constrói automaticamente políticas de serviço LIF consistentes com as políticas de firewall em uso na versão anterior do ONTAP. Se você usar scripts ou outras ferramentas que criam e gerenciam políticas de firewall personalizadas, talvez seja necessário atualizar esses scripts para criar políticas de serviço personalizadas.

Para saber mais, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

Se você quiser…	Use este comando…
Ativar ou desativar o serviço de firewall	`system services firewall modify`
Exibir a configuração atual do serviço de firewall	`system services firewall show`
Crie uma política de firewall ou adicione um serviço a uma política de firewall existente	`system services firewall policy create`
Aplique uma política de firewall a um LIF	`network interface modify -lif lifname -firewall-policy`
Modifique os endereços IP e as máscaras de rede associadas a uma política de firewall	`system services firewall policy modify`
Exibir informações sobre políticas de firewall	`system services firewall policy show`
Crie uma nova política de firewall que seja uma cópia exata de uma política existente	`system services firewall policy clone`
Exclua uma política de firewall que não seja usada por um LIF	`system services firewall policy delete`

Informações relacionadas

- "firewall dos serviços do sistema"

- "modificação da interface de rede"

Marcação de QoS (apenas administradores de cluster)

Saiba mais sobre a qualidade do serviço (QoS) da rede ONTAP

A marcação de qualidade de serviço (QoS) da rede ajuda a priorizar diferentes tipos de tráfego com base nas condições da rede para usar efetivamente os recursos da rede. Você pode definir o valor de ponto de código de serviços diferenciados (DSCP) dos pacotes IP de saída para os tipos de tráfego suportados por espaço de IPspace.

Marcação DSCP para conformidade com UC

Você pode ativar a marcação DSCP (Differentiated Services Code Point) no tráfego de pacotes IP de saída (saída) para um determinado protocolo com um código DSCP padrão ou fornecido pelo usuário. A marcação DSCP é um mecanismo para classificar e gerenciar o tráfego de rede e é um componente da conformidade com a capacidade Unificada (UC).

A marcação DSCP (também conhecida como *marcação QoS* ou *marcação de qualidade de serviço*) é ativada fornecendo um valor IPspace, protocolo e DSCP. Os protocolos nos quais a marcação DSCP pode ser aplicada são NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet e SNMP.

Se você não fornecer um valor DSCP ao ativar a marcação DSCP para um determinado protocolo, um padrão será usado:

- O valor predefinido para protocolos/tráfego de dados é 0x0A (10).
- O valor predefinido para protocolos de controlo/tráfego é 0x30 (48).

Modificar valores de marcação de QoS de rede ONTAP

Você pode modificar os valores de marcação de qualidade do serviço (QoS) para diferentes protocolos, para cada IPspace.

Antes de começar

Todos os nós no cluster devem estar executando a mesma versão do ONTAP.

Passo

Modifique os valores de marcação de QoS usando o `network qos-marking modify` comando.

- O `-ipspace` parâmetro especifica o espaço IPspace para o qual a entrada de marcação QoS deve ser modificada.
- O `-protocol` parâmetro especifica o protocolo para o qual a entrada de marcação QoS deve ser modificada.
- O `-dscp` parâmetro especifica o valor DSCP (Differentiated Services Code Point). Os valores possíveis variam de 0 a 63.
- O `-is-enabled` parâmetro é utilizado para ativar ou desativar a marcação QoS para o protocolo especificado no espaço IPspace fornecido pelo `-ipspace` parâmetro.

O comando a seguir habilita a marcação QoS para o protocolo NFS no IPspace padrão:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

O comando a seguir define o valor DSCP como 20 para o protocolo NFS no IPspace padrão:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Saiba mais sobre `network qos-marking modify` os possíveis valores do protocolo no "Referência do comando ONTAP".

Exibir valores de marcação de QoS de rede ONTAP

Você pode exibir os valores de marcação de QoS para diferentes protocolos, para cada espaço IPspace.

Passo

Exiba valores de marcação de QoS usando o `network qos-marking show` comando.

O comando a seguir exibe a marcação QoS para todos os protocolos no espaço IPspace padrão:

```
network qos-marking show -ipspace Default
IPspace              Protocol           DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                 10  false
                     FTP                  48  false
                     HTTP-admin           48  false
                     HTTP-filesrv         10  false
                     NDMP                 10  false
                     NFS                  10  true
                     SNMP                 48  false
                     SSH                  48  false
                     SnapMirror           10  false
                     Telnet               48  false
                     iSCSI                10  false
11 entries were displayed.
```

Saiba mais sobre `network qos-marking show` o "Referência do comando ONTAP"na .

Gerenciar SNMP (somente administradores de cluster)

Saiba mais sobre o SNMP na rede ONTAP

Você pode configurar o SNMP para monitorar SVMs em seu cluster para evitar problemas antes que eles ocorram e responder a problemas se eles ocorrerem. O

gerenciamento do SNMP envolve a configuração de usuários SNMP e a configuração de destinos de host SNMP (estações de trabalho de gerenciamento) para todos os eventos SNMP. O SNMP está desativado por padrão em LIFs de dados.

Você pode criar e gerenciar usuários SNMP somente leitura no data SVM. As LIFs de dados devem ser configuradas para receber solicitações SNMP no SVM.

As estações de trabalho de gerenciamento de rede SNMP, ou gerentes, podem consultar o agente SNMP SVM para obter informações. O agente SNMP reúne informações e as encaminha para os gerentes SNMP. O agente SNMP também gera notificações de intercetação sempre que ocorrem eventos específicos. O agente SNMP no SVM tem Privileges somente leitura; ele não pode ser usado para nenhuma operação definida ou para tomar uma ação corretiva em resposta a uma armadilha. O ONTAP fornece um agente SNMP compatível com as versões v1, v2c e v3 do SNMP. O SNMPv3 oferece segurança avançada usando senhas e criptografia.

Para obter mais informações sobre o suporte SNMP em sistemas ONTAP, "TR-4220: Suporte SNMP no Data ONTAP" consulte .

Visão geral da MIB

Um MIB (Management Information base) é um arquivo de texto que descreve objetos e traps SNMP.

As MIBs descrevem a estrutura dos dados de gerenciamento do sistema de armazenamento e usam um namespace hierárquico contendo identificadores de objeto (OIDs). Cada OID identifica uma variável que pode ser lida usando SNMP.

Como MIBs não são arquivos de configuração e o ONTAP não lê esses arquivos, a funcionalidade SNMP não é afetada por MIBs. O ONTAP fornece o seguinte arquivo MIB:

- Um MIB personalizado NetApp (`netapp.mib`)

O ONTAP suporta MIBs IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), que mostram dados IPv4 e IPv6, são suportados.

O ONTAP também fornece uma breve referência cruzada entre identificadores de objeto (OIDs) e nomes curtos de objetos no `traps.dat` arquivo.

> As versões mais recentes dos arquivos MIBs ONTAP e 'traps.dat' estão disponíveis no site de suporte da NetApp. No entanto, as versões desses arquivos no site de suporte não correspondem necessariamente aos recursos SNMP de sua versão do ONTAP. Esses arquivos são fornecidos para ajudá-lo a avaliar os recursos SNMP na versão mais recente do ONTAP.

Traps SNMP

Os traps SNMP capturam informações de monitoramento do sistema que são enviadas como uma notificação assíncrona do agente SNMP para o gerenciador SNMP.

Existem três tipos de traps SNMP: Padrão, embutido e definido pelo usuário. Os traps definidos pelo usuário não são suportados no ONTAP.

Uma armadilha pode ser usada para verificar periodicamente se há limites operacionais ou falhas que são definidos na MIB. Se um limite for atingido ou uma falha for detetada, o agente SNMP enviará uma mensagem (trap) aos hosts que os alertam sobre o evento.

ONTAP suporta armadilhas SNMPv1 e SNMPv3. ONTAP não suporta SNMPv2c armadilhas e informa.

Traps SNMP padrão

Esses traps são definidos no RFC 1215. Existem cinco traps SNMP padrão que são suportados pelo ONTAP: Coldstart, warmStart, linkDown, linkup e autenticationFailure.

A armadilha autenticationFailure é desativada por padrão. Você deve usar o `system snmp authtrap` comando para ativar a armadilha. Saiba mais sobre `system snmp authtrap` o "Referência do comando ONTAP"na .

Traps SNMP incorporados

Os traps incorporados são predefinidos no ONTAP e são enviados automaticamente para as estações de gerenciamento de rede na lista de traphost se ocorrer um evento. Essas armadilhas, como diskFailedShutdown, cpuTooBusy e volumeNearlyFull, são definidas no MIB personalizado.

Cada armadilha incorporada é identificada por um código de armadilha exclusivo.

Crie comunidades SNMP para a rede ONTAP

Você pode criar uma comunidade SNMP que atua como um mecanismo de autenticação entre a estação de gerenciamento e a máquina virtual de armazenamento (SVM) ao usar SNMPv1 e SNMPv2c.

Ao criar comunidades SNMP em um SVM de dados, você pode executar comandos como `snmpwalk` e `snmpget` nas LIFs de dados.

Sobre esta tarefa

- Em novas instalações do ONTAP, o SNMPv1 e o SNMPv2c são desativados por padrão.

  SNMPv1 e SNMPv2c são ativados depois de criar uma comunidade SNMP.

- O ONTAP suporta comunidades somente leitura.
- Por padrão, a política de firewall de "dados" atribuída a LIFs de dados tem serviço SNMP definido como `deny`.

  Você deve criar uma nova política de firewall com serviço SNMP definido como `allow` ao criar um usuário SNMP para um SVM de dados.

  A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- Você pode criar comunidades SNMP para usuários SNMPv1 e SNMPv2c para o SVM admin e o SVM de dados.
- Como um SVM não faz parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Passos

1. Crie uma comunidade SNMP usando o `system snmp community add` comando. O comando a seguir mostra como criar uma comunidade SNMP no cluster SVM admin-1:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

   O comando a seguir mostra como criar uma comunidade SNMP nos dados SVM VS1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verifique se as comunidades foram criadas usando o comando system snmp Community show.

   O comando a seguir mostra as duas comunidades criadas para SNMPv1 e SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Verifique se o SNMP é permitido como um serviço na política de firewall de "dados" usando o `system services firewall policy show` comando.

   O comando a seguir mostra que o serviço snmp não é permitido na política de firewall "dados" padrão (o serviço snmp é permitido somente na política de firewall "mgmt"):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Crie uma nova política de firewall que permita o acesso usando `snmp` o serviço usando o `system services firewall policy create` comando.

   Os comandos a seguir criam uma nova política de firewall de dados chamada "data1" que permite o. `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Aplique a política de firewall a um LIF de dados usando o `network interface modify` comando com o parâmetro -firewall-policy.

O comando a seguir atribui a nova política de firewall "data1" ao LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

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

Configure SNMPv3 usuários em um cluster do ONTAP

O SNMPv3 é um protocolo seguro quando comparado ao SNMPv1 e ao SNMPv2c. Para utilizar o SNMPv3, tem de configurar um utilizador SNMPv3 para executar os utilitários SNMP a partir do gestor SNMP.

Passo

Use o `security login create` comando para criar um usuário SNMPv3.

Você é solicitado a fornecer as seguintes informações:

- ID do motor: O valor predefinido e recomendado é ID do motor local
- Protocolo de autenticação
- Palavra-passe de autenticação
- Protocolo de privacidade
- Senha do protocolo de privacidade

Resultado

O utilizador SNMPv3 pode iniciar sessão a partir do gestor SNMP utilizando o nome de utilizador e a palavra-passe e executar os comandos do utilitário SNMP.

SNMPv3 parâmetros de segurança

O SNMPv3 inclui um recurso de autenticação que, quando selecionado, exige que os usuários digitem seus nomes, um protocolo de autenticação, uma chave de autenticação e seu nível de segurança desejado ao invocar um comando.

A tabela a seguir lista os parâmetros de segurança SNMPv3 :

Parâmetro	Opção de linha de comando	Descrição
EngineID	-E EngineID	ID do motor do agente SNMP. O valor padrão é local EngineID (recomendado).
SecurityName	-U Nome	O nome de utilizador não deve exceder 32 carateres.
AuthProtocol	-A [none	MD5

SHA	SHA-256]	O tipo de autenticação pode ser None, MD5, SHA ou SHA-256.
Authkey	-UMA FRASE-PASSE	Frase-passe com um mínimo de oito carateres.
Segurançanível	-L [authNoPriv	authPriv
noAuthNoPriv]	O nível de segurança pode ser Autenticação, sem Privacidade; Autenticação, Privacidade; ou sem Autenticação, sem Privacidade.	PrivProtocol
aes128	O protocolo de privacidade pode ser nenhum, des ou AES128	PrivPassword

Exemplos para diferentes níveis de segurança

Este exemplo mostra como um usuário SNMPv3 criado com diferentes níveis de segurança pode usar os comandos do lado do cliente SNMP, como `snmpwalk`, para consultar os objetos do cluster.

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

Você deve usar `snmpwalk` 5.3.1 ou posterior quando o protocolo de autenticação for SHA.

Nível de segurança: AuthPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Modo FIPS

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: AuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade. Como resultado, não é possível configurar um usuário authNoPriv SNMPv3 no modo FIPS.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: NoAuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança noAuthNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Saiba mais sobre `security login create` o "Referência do comando ONTAP"na .

Configure os hosts traphosts para SNMP na rede ONTAP

Você pode configurar o traphost (gerenciador SNMP) para receber notificações (PDUs de intercetação SNMP) quando os traps SNMP são gerados no cluster. Você pode especificar o nome do host ou o endereço IP (IPv4 ou IPv6) do traphost SNMP.

Antes de começar

- Os traps SNMP e SNMP devem estar ativados no cluster.

> As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do traphost.
- O IPv6 deve estar ativado no cluster para configurar os traphosts SNMP usando endereços IPv6.
- Você deve ter especificado a autenticação de um modelo de segurança predefinido baseado no usuário (USM) e credenciais de privacidade ao criar hosts tradicionais.

Passo

Adicionar um traphost SNMP:

```
system snmp traphost add
```

> Os traps só podem ser enviados quando pelo menos uma estação de gerenciamento SNMP é especificada como um traphost.

O comando a seguir adiciona um novo host SNMPv3 chamado yyy.example.com com um usuário USM conhecido:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

O comando a seguir adiciona um traphost usando o endereço IPv6 do host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Verifique a polling SNMP em um cluster ONTAP

Depois de configurar o SNMP, você deve verificar se você pode poll o cluster.

Sobre esta tarefa

Para fazer polling de um cluster, você precisa usar um comando de terceiros, `snmpwalk` como o .

Passos

1. Envie um comando SNMP para poll o cluster a partir de um cluster diferente.

   Para sistemas que executam o SNMPv1, use o comando CLI `snmpwalk -v version -c`

`community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Para sistemas que executam o SNMPv2c, use o comando CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Para sistemas que executam o SNMPv3, use o comando CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Comandos ONTAP para gerenciar SNMP, traps e traphosts

Você pode usar os `system snmp` comandos para gerenciar SNMP, traps e traphosts. Você pode usar os `security` comandos para gerenciar usuários SNMP por SVM. Você pode usar os `event` comandos para gerenciar eventos relacionados a traps SNMP.

Comandos para configurar o SNMP

Se você quiser…	Use este comando…
Ative o SNMP no cluster	`options -option-name snmp.enable -option-value on` O serviço SNMP tem de ser permitido na política de firewall de gestão (mgmt). Você pode verificar se o SNMP é permitido usando o comando show de política de firewall de serviços do sistema.
Desative o SNMP no cluster	`options -option-name snmp.enable -option-value off`

Comandos para gerenciar usuários SNMP v1, v2c e v3

Se você quiser…	Use este comando…
Configurar utilizadores SNMP	`security login create`
Exibir usuários SNMP	`security snmpusers`e `security login show -application snmp`
Eliminar utilizadores SNMP	`security login delete`

Modifique o nome da função de controle de acesso de um método de login para usuários SNMP	`security login modify`

Comandos para fornecer informações de Contato e localização

Se você quiser…	Use este comando…
Apresentar ou modificar os detalhes de contacto do cluster	`system snmp contact`
Exiba ou modifique os detalhes de localização do cluster	`system snmp location`

Comandos para gerenciar comunidades SNMP

Se você quiser…	Use este comando…
Adicione uma comunidade somente leitura (ro) para um SVM ou para todos os SVMs no cluster	`system snmp community add`
Exclua uma comunidade ou todas as comunidades	`system snmp community delete`
Exiba a lista de todas as comunidades	`system snmp community show`

Como os SVMs não fazem parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando para exibir valores de opção SNMP

Se você quiser…	Use este comando…
Exiba os valores atuais de todas as opções SNMP, incluindo Contato de cluster, localização de Contato, se o cluster está configurado para enviar traps, a lista de traphosts e lista de comunidades e tipo de controle de acesso	`system snmp show`

Comandos para gerenciar traps e traphosts SNMP

Se você quiser…	Use este comando…
Ativar traps SNMP enviados a partir do cluster	`system snmp init -init 1`
Desative traps SNMP enviados a partir do cluster	`system snmp init -init 0`

Adicione um traphost que receba notificações SNMP para eventos específicos no cluster	`system snmp traphost add`
Excluir um traphost	`system snmp traphost delete`
Exibir a lista de hosts	`system snmp traphost show`

Comandos para gerenciar eventos relacionados a traps SNMP

Se você quiser…	Use este comando…
Exibir os eventos para os quais são gerados traps SNMP (internos)	`event route show` Utilize o `-snmp-support true` parâmetro para visualizar apenas eventos relacionados com SNMP. Use o `instance -messagename <message>` parâmetro para exibir uma descrição detalhada do motivo pelo qual um evento pode ter ocorrido e qualquer ação corretiva. O roteamento de eventos individuais de intercetação SNMP para destinos específicos de traphost não é suportado. Todos os eventos de intercetação SNMP são enviados para todos os destinos de traphost.
Exibir uma lista de Registros de histórico de trap SNMP, que são notificações de eventos que foram enviadas para traps SNMP	`event snmphistory show`
Eliminar um registo de histórico de trap SNMP	`event snmphistory delete`

Informações relacionadas

- "snmp do sistema"
- "usuários de segurança"
- "segurança"
- "evento"
- "login de segurança"

Gerenciar o roteamento em uma SVM

Saiba mais sobre o roteamento SVM na rede ONTAP

A tabela de roteamento de um SVM determina o caminho de rede que o SVM usa para se comunicar com um destino. É importante entender como as tabelas de roteamento funcionam para que você possa evitar problemas de rede antes que eles ocorram.

As regras de roteamento são as seguintes:

- A ONTAP encaminha o tráfego para a rota mais específica disponível.
- O ONTAP roteia o tráfego por uma rota de gateway padrão (com 0 bits de máscara de rede) como último recurso, quando rotas mais específicas não estão disponíveis.

No caso de rotas com o mesmo destino, máscara de rede e métrica, não há garantia de que o sistema usará a mesma rota após uma reinicialização ou após uma atualização. Isso é especialmente um problema se você tiver configurado várias rotas padrão.

É uma prática recomendada configurar apenas uma rota padrão para uma SVM. Para evitar interrupções, você deve garantir que a rota padrão seja capaz de alcançar qualquer endereço de rede que não possa ser alcançado por uma rota mais específica. Para mais informações, consulte"Base de conhecimento da NetApp : SU134 - O acesso à rede pode ser interrompido por configuração de roteamento incorreta no ONTAP em cluster"

Crie rotas estáticas para a rede ONTAP

Você pode criar rotas estáticas em uma máquina virtual de armazenamento (SVM) para controlar como os LIFs usam a rede para tráfego de saída.

Quando você cria uma entrada de rota associada a um SVM, a rota será usada por todos os LIFs que são de propriedade do SVM especificado e que estão na mesma sub-rede que o gateway.

Passo

Use o `network route create` comando para criar uma rota.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

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

Ative o roteamento multipath para a rede ONTAP

Se várias rotas tiverem a mesma métrica para um destino, apenas uma das rotas será selecionada para o tráfego de saída. Isso leva a que outras rotas não sejam utilizadas para enviar tráfego de saída. Você pode habilitar o roteamento multipath para o balanceamento de carga em todas as rotas disponíveis proporcionalmente às suas métricas, em vez do roteamento ECMP, que equilibra a carga entre as rotas disponíveis da mesma métrica.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ativar o roteamento multipath:

   ```
   network options multipath-routing modify -is-enabled true
   ```

O roteamento multipath está habilitado para todos os nós no cluster.

```
network options multipath-routing modify -is-enabled true
```

Saiba mais sobre `network options multipath-routing modify` o "Referência do comando ONTAP"na .

Eliminar rotas estáticas da rede ONTAP

Você pode excluir uma rota estática desnecessária de uma máquina virtual de armazenamento (SVM).

Passo

Use o `network route delete` comando para excluir uma rota estática.

O exemplo a seguir exclui uma rota estática associada ao SVM vs0 com um gateway de 10.63.0.1 e um endereço IP de destino de 0,0.0,0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

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

Exibir informações de roteamento do ONTAP

Você pode exibir informações sobre a configuração de roteamento para cada SVM no cluster. Isso pode ajudá-lo a diagnosticar problemas de roteamento envolvendo problemas de conetividade entre aplicativos ou serviços cliente e um LIF em um nó no cluster.

Passos

1. Use o `network route show` comando para exibir rotas dentro de um ou mais SVMs. O exemplo a seguir mostra uma rota configurada no vs0 SVM:

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Use o `network route show-lifs` comando para exibir a associação de rotas e LIFs em um ou mais SVMs.

   O exemplo a seguir mostra LIFs com rotas pertencentes ao SVM vs0:

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

Saiba mais sobre `network route show` e `network route show-lifs` no "Referência do comando ONTAP".

3. Use o `network route active-entry show` comando para exibir rotas instaladas em um ou mais nós, SVMs, sub-redes ou rotas com destinos especificados.

   O exemplo a seguir mostra todas as rotas instaladas em um SVM específico:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
```

```
Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway               Interface   Metric  Flags
----------------------  --------------------  ---------   ------  -----
127.0.10.1              127.0.20.1            losk            10  UHS
127.0.20.1              127.0.20.1            losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway               Interface   Metric  Flags
----------------------  --------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                              e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4                e0d              0  UC
fd20:8b1e:b255:814e::1  link#4                e0d              0  UHL
11 entries were displayed.
```

Saiba mais sobre `network route active-entry show` o "Referência do comando ONTAP"na .

Remova rotas dinâmicas de tabelas de roteamento para a rede ONTAP

Quando os redirecionamentos ICMP são recebidos para IPv4 e IPv6, as rotas dinâmicas são adicionadas à tabela de roteamento. Por padrão, as rotas dinâmicas são removidas após 300 segundos. Se você quiser manter rotas dinâmicas por um período de tempo diferente, você pode alterar o valor do tempo limite.

Sobre esta tarefa

Você pode definir o valor de tempo limite de 0 a 65.535 segundos. Se você definir o valor como 0, as rotas nunca expiram. A remoção de rotas dinâmicas impede a perda de conetividade causada pela persistência de rotas inválidas.

Passos

1. Apresentar o valor atual do tempo limite.
   - Para IPv4:

     ```
     network tuning icmp show
     ```

   - Para IPv6:

     ```
     network tuning icmp6 show
     ```

2. Modifique o valor de tempo limite.
   - Para IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

   - Para IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. Verifique se o valor de tempo limite foi modificado corretamente.
   - Para IPv4:

```
network tuning icmp show
```

   - Para IPv6:

```
network tuning icmp6 show
```

Saiba mais sobre `network tuning icmp` o "Referência do comando ONTAP"na .

Informações de rede ONTAP

Exibir informações de rede do ONTAP

Usando a CLI, você pode exibir informações relacionadas a portas, LIFs, rotas, regras de failover, grupos de failover, regras de firewall, DNS, NIS e conexões. A partir do ONTAP 9.8, você também pode baixar os dados exibidos no Gerenciador de sistema sobre sua rede.

Essas informações podem ser úteis em situações como a reconfiguração das configurações de rede ou na solução de problemas do cluster.

Se você for um administrador de cluster, poderá exibir todas as informações de rede disponíveis. Se você for um administrador de SVM, poderá exibir apenas as informações relacionadas aos SVMs atribuídos.

No System Manager, quando você exibe informações em uma *List View*, você pode clicar em **Download** e a lista de objetos exibidos é baixada.

- A lista é baixada no formato CSV (valores separados por vírgula).
- Apenas os dados nas colunas visíveis são transferidos.
- O nome do arquivo CSV é formatado com o nome do objeto e um carimbo de hora.

Exibir informações da porta de rede ONTAP

Você pode exibir informações sobre uma porta específica ou sobre todas as portas em todos os nós do cluster.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Nome do nó
- Nome da porta
- Nome do IPspace
- Nome de domínio de broadcast
- Estado da ligação (para cima ou para baixo)
- Definição MTU
- Configuração da velocidade da porta e status operacional (1 Gigabit ou 10 gigabits por segundo)
- Configuração de negociação automática (verdadeiro ou falso)
- Modo duplex e estado operacional (meio ou cheio)
- O grupo de interfaces da porta, se aplicável
- As informações da etiqueta VLAN da porta, se aplicável
- Estado de integridade da porta (estado ou degradado)
- Razões para uma porta ser marcada como degradada

Se os dados de um campo não estiverem disponíveis (por exemplo, o duplex operacional e a velocidade de uma porta inativa não estarão disponíveis), o valor do campo será listado como `-`.

Passo

Exiba as informações da porta de rede usando o `network port show` comando.

Você pode exibir informações detalhadas para cada porta especificando o `-instance` parâmetro ou obter informações específicas especificando nomes de campos usando o `-fields` parâmetro.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

Exibir informações de VLAN do ONTAP

Você pode exibir informações sobre uma VLAN específica ou sobre todas as VLANs no cluster.

Sobre esta tarefa

Você pode exibir informações detalhadas para cada VLAN especificando o `-instance` parâmetro. Você pode exibir informações específicas especificando nomes de campos usando o `-fields` parâmetro.

Passo

Exiba informações sobre VLANs usando o `network port vlan show` comando. O comando a seguir exibe informações sobre todas as VLANs no cluster:

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

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

Exibir informações do grupo de interfaces do ONTAP

Você pode exibir informações sobre um grupo de interfaces para determinar sua configuração.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Nó no qual o grupo de interfaces está localizado
- Lista de portas de rede incluídas no grupo de interfaces
- Nome do grupo de interfaces
- Função de distribuição (MAC, IP, porta ou sequencial)
- Endereço MAC (Media Access Control) do grupo de interfaces
- Status da atividade da porta; ou seja, se todas as portas agregadas estão ativas (participação total), se algumas estão ativas (participação parcial) ou se nenhuma está ativa

Passo

Exiba informações sobre grupos de interface usando o `network port ifgrp show` comando.

Você pode exibir informações detalhadas para cada nó especificando o `-instance` parâmetro. Você pode

exibir informações específicas especificando nomes de campos usando o `-fields` parâmetro.

O comando a seguir exibe informações sobre todos os grupos de interface no cluster:

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

O comando a seguir exibe informações detalhadas do grupo de interfaces para um único nó:

```
network port ifgrp show -instance -node cluster-1-01

                Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

Veja as informações de LIF do ONTAP

Você pode visualizar informações detalhadas sobre um LIF para determinar sua configuração.

Você também pode querer exibir essas informações para diagnosticar problemas básicos de LIF, como verificar endereços IP duplicados ou verificar se a porta de rede pertence à sub-rede correta. Os administradores de máquina virtual de armazenamento (SVM) podem exibir apenas as informações sobre os LIFs associados ao SVM.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Endereço IP associado ao LIF
- Estado administrativo do LIF
- Status operacional do LIF

  O status operacional das LIFs de dados é determinado pelo status do SVM com o qual as LIFs de dados estão associadas. Quando o SVM é interrompido, o status operacional do LIF muda para baixo. Quando o SVM é iniciado novamente, o status operacional muda para up

- Nó e a porta na qual reside o LIF

Se os dados de um campo não estiverem disponíveis (por exemplo, se não houver informações de status estendidas), o valor do campo será listado como `-`.

Passo

Exiba informações de LIF usando o `network interface show` comando.

Você pode visualizar informações detalhadas para cada LIF especificando o parâmetro -instância ou obter informações específicas especificando nomes de campos usando o parâmetro -fields.

O comando a seguir exibe informações gerais sobre todos os LIFs em um cluster:

```
network interface show
            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
example
            lif1         up/up    192.0.2.129/22   node-01
                                                                e0d
false
node
            cluster_mgmt up/up    192.0.2.3/20     node-02
                                                                e0c
false
node-01
            clus1        up/up    192.0.2.65/18    node-01
                                                                e0a
true
            clus2        up/up    192.0.2.66/18    node-01
                                                                e0b
true
            mgmt1        up/up    192.0.2.1/20     node-01
                                                                e0c
true
node-02
            clus1        up/up    192.0.2.67/18    node-02
                                                                e0a
true
            clus2        up/up    192.0.2.68/18    node-02
                                                                e0b
true
            mgmt2        up/up    192.0.2.2/20     node-02
                                                                e0d
true
vs1
            d1           up/up    192.0.2.130/21   node-01
                                                                e0d
false
            d2           up/up    192.0.2.131/21   node-01
                                                                e0d
true
            data3        up/up    192.0.2.132/20   node-02
                                                                e0c
true
```

O comando a seguir mostra informações detalhadas sobre um único LIF:

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
              Operational Status: up
                 Extended Status: -
                         Is Home: false
                 Network Address: 192.0.2.128
                         Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                   Failover Policy: local-only
                   Firewall Policy: data
                       Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Exibir informações de roteamento para a rede ONTAP

É possível exibir informações sobre rotas em um SVM.

Passo

Dependendo do tipo de informações de roteamento que você deseja exibir, digite o comando aplicável:

Para ver informações sobre…	Digite…
Rotas estáticas, por SVM	`network route show`

LIFs em cada rota, por SVM	`network route show-lifs`

Você pode exibir informações detalhadas para cada rota especificando o `-instance` parâmetro. O comando a seguir exibe as rotas estáticas dentro dos SVMs no cluster- 1:

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

O comando a seguir exibe a associação de rotas estáticas e interfaces lógicas (LIFs) em todos os SVMs no cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Saiba mais sobre `network route show` e `network route show-lifs` no "Referência do comando ONTAP".

Exibir entradas da tabela de hosts DNS do ONTAP

As entradas da tabela de hosts DNS mapeiam nomes de host para endereços IP. É possível exibir os nomes de host e os nomes de alias e o endereço IP para o qual eles mapeiam para todos os SVMs em um cluster.

Passo

Exiba as entradas de nome de host para todos os SVMs usando o comando show de hosts dns de serviços vserver.

O exemplo a seguir exibe as entradas da tabela do host:

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os nomes de host são resolvidos usando servidores DNS externos.

Exibir informações de configuração do domínio DNS do ONTAP

Você pode exibir a configuração do domínio DNS de uma ou mais máquinas virtuais de armazenamento (SVMs) no cluster para verificar se ela está configurada corretamente.

Passo

Exibindo as configurações do domínio DNS usando o `vserver services name-service dns show` comando.

O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

```
vserver services name-service dns show
                                                        Name
Vserver         State     Domains                       Servers
--------------- --------- ----------------------------- -------------
cluster-1        enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs1             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs2             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
vs3             enabled   xyz.company.com               192.56.0.129,
                                                        192.56.0.130
```

O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

Exibir informações do grupo de failover do ONTAP

Você pode exibir informações sobre grupos de failover, incluindo a lista de nós e portas em cada grupo de failover, se o failover está ativado ou desativado e o tipo de política de failover que está sendo aplicada a cada LIF.

Passos

1. Exiba as portas de destino para cada grupo de failover usando o `network interface failover-groups show` comando.

   O comando a seguir exibe informações sobre todos os grupos de failover em um cluster de dois nós:

```
network interface failover-groups show
                              Failover
Vserver         Group         Targets
--------------- ------------- --------------------------------
Cluster
                Cluster
                              cluster1-01:e0a, cluster1-01:e0b,
                              cluster1-02:e0a, cluster1-02:e0b
vs1
                Default
                              cluster1-01:e0c, cluster1-01:e0d,
                              cluster1-01:e0e, cluster1-02:e0c,
                              cluster1-02:e0d, cluster1-02:e0e
```

Saiba mais sobre `network interface failover-groups show` o "Referência do comando ONTAP"na .

2. Exiba as portas de destino e o domínio de broadcast para um grupo de failover específico usando o `network interface failover-groups show` comando.

   O comando a seguir exibe informações detalhadas sobre o grupo de failover data12 para SVM VS4:

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Exiba as configurações de failover usadas por todos os LIFs usando o `network interface show` comando.

   O comando a seguir exibe a política de failover e o grupo de failover que está sendo usado por cada LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -----------------  ---------------------  -------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Visualizar destinos de failover de LIF do ONTAP

Talvez seja necessário verificar se as políticas de failover e os grupos de failover de um LIF estão configurados corretamente. Para evitar a configuração incorreta das regras de failover, você pode exibir os destinos de failover para um único LIF ou para todos os LIFs.

Sobre esta tarefa

A exibição de destinos de failover de LIF permite verificar o seguinte:

- Se os LIFs são configurados com o grupo de failover correto e a política de failover
- Se a lista resultante de portas de destino de failover é apropriada para cada LIF
- Se o destino de failover de um LIF de dados não é uma porta de gerenciamento (e0M)

Passo

Exiba os destinos de failover de um LIF usando a `failover` opção `network interface show` do comando.

O comando a seguir exibe informações sobre os destinos de failover para todos os LIFs em um cluster de dois nós. A `Failover Targets` linha mostra a lista (priorizada) de combinações de nó-porta para um determinado LIF.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Veja LIFs do ONTAP em uma zona de balanceamento de carga

Você pode verificar se uma zona de balanceamento de carga está configurada corretamente exibindo todas as LIFs que pertencem a ela. Você também pode visualizar a zona de balanceamento de carga de um LIF específico ou as zonas de balanceamento de carga de todos os LIFs.

Passo

Exiba os LIFs e os detalhes de balanceamento de carga desejados usando um dos seguintes comandos

Para exibir…	Digite…
LIFs em uma determinada zona de balanceamento de carga	`network interface show -dns-zone zone_name` `zone_name` especifica o nome da zona de balanceamento de carga.
A zona de balanceamento de carga de um LIF específico	`network interface show -lif lif_name -fields dns-zone`
As zonas de balanceamento de carga de todos os LIFs	`network interface show -fields dns-zone`

Exemplos de exibição de zonas de balanceamento de carga para LIFs

O comando a seguir exibe os detalhes de todos os LIFs na zona de balanceamento de carga storage.company.com para SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network           Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask      Node      Port    Home
--------- ---------- ---------- ----------------- --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

O comando a seguir exibe os detalhes da zona DNS do LIF data3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

O comando a seguir exibe a lista de todos os LIFs no cluster e suas zonas DNS correspondentes:

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

Veja as conexões do cluster do ONTAP

Você pode exibir todas as conexões ativas no cluster ou uma contagem de conexões ativas no nó por cliente, interface lógica, protocolo ou serviço. Também pode apresentar todas as ligações de audição no cluster.

Exibir conexões ativas pelo cliente (somente administradores de cluster)

Você pode exibir as conexões ativas por cliente para verificar o nó que um cliente específico está usando e para exibir possíveis desequilíbrios entre contagens de clientes por nó.

Sobre esta tarefa

A contagem de conexões ativas por cliente é útil nos seguintes cenários:

- Encontrando um nó ocupado ou sobrecarregado.
- Determinar por que o acesso de um cliente específico a um volume é lento.

  Você pode ver detalhes sobre o nó que o cliente está acessando e compará-lo com o nó no qual o volume reside. Se o acesso ao volume exigir a travessia da rede do cluster, os clientes podem ter um desempenho reduzido devido ao acesso remoto ao volume em um nó remoto substituído.

- Verificar se todos os nós estão sendo usados igualmente para acesso aos dados.
- Encontrando clientes que têm um número inesperadamente alto de conexões.
- Verificando se certos clientes têm conexões com um nó.

Passo

Exibir uma contagem das conexões ativas por cliente em um nó usando o `network connections active show-clients` comando.

Saiba mais sobre `network connections active show-clients` o "Referência do comando ONTAP"na .

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

Exibir conexões ativas por protocolo (somente administradores de cluster)

É possível exibir uma contagem das conexões ativas por protocolo (TCP ou UDP) em um nó para comparar o uso de protocolos dentro do cluster.

Sobre esta tarefa

A contagem de conexões ativas por protocolo é útil nos seguintes cenários:

- Encontrando os clientes UDP que estão perdendo sua conexão.

  Se um nó estiver próximo ao limite de conexão, os clientes UDP serão os primeiros a serem descartados.

- Verificar se não estão a ser utilizados outros protocolos.

Passo

Exibir uma contagem das conexões ativas por protocolo em um nó usando o `network connections active show-protocols` comando.

Saiba mais sobre `network connections active show-protocols` o "Referência do comando ONTAP"na .

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

Exibir conexões ativas por serviço (somente administradores de cluster)

É possível exibir uma contagem das conexões ativas por tipo de serviço (por exemplo, por NFS, SMB, montagem etc.) para cada nó em um cluster. Isso é útil para comparar o uso de serviços no cluster, o que ajuda a determinar a carga de trabalho principal de um nó.

Sobre esta tarefa

A contagem de conexões ativas por serviço é útil nos seguintes cenários:

- Verificar se todos os nós estão sendo usados para os serviços apropriados e se o balanceamento de carga para esse serviço está funcionando.
- Verificar se não estão a ser utilizados outros serviços. Exibir uma contagem das conexões ativas por serviço em um nó usando o `network connections active show-services` comando.

Saiba mais sobre `network connections active show-services` o "Referência do comando ONTAP"na .

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

Exibir conexões ativas por LIF em um nó e SVM

É possível exibir uma contagem de conexões ativas para cada LIF, por nó e máquina virtual de armazenamento (SVM), para visualizar desequilíbrios de conexão entre LIFs no cluster.

Sobre esta tarefa

A contagem de conexões ativas por LIF é útil nos seguintes cenários:

- Encontrando um LIF sobrecarregado comparando o número de conexões em cada LIF.
- Verificando se o balanceamento de carga DNS está funcionando para todas as LIFs de dados.
- Comparando o número de conexões com os vários SVMs para encontrar os SVMs que são mais usados.

Passo

Exiba uma contagem de conexões ativas para cada LIF por SVM e nó usando o `network connections active show-lifs` comando.

Saiba mais sobre `network connections active show-lifs` o "Referência do comando ONTAP"na .

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Exibir conexões ativas em um cluster

Você pode exibir informações sobre as conexões ativas em um cluster para exibir o LIF, a porta, o host remoto, o serviço, as máquinas virtuais de armazenamento (SVMs) e o protocolo usado por conexões individuais.

Sobre esta tarefa

Visualizar as conexões ativas em um cluster é útil nos seguintes cenários:

- Verificar se clientes individuais estão usando o protocolo e o serviço corretos no nó correto.
- Se um cliente estiver tendo problemas para acessar dados usando uma certa combinação de nó, protocolo e serviço, você pode usar este comando para encontrar um cliente semelhante para comparação de configuração ou rastreamento de pacotes.

Passo

Exiba as conexões ativas em um cluster usando o `network connections active show` comando.

Saiba mais sobre `network connections active show` o "Referência do comando ONTAP"na .

O comando a seguir mostra as conexões ativas no nó node1:

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

O comando a seguir mostra as conexões ativas no SVM VS1:

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Exibir conexões de escuta em um cluster

Você pode exibir informações sobre as conexões de escuta em um cluster para exibir os LIFs e as portas que estão aceitando conexões para um determinado protocolo e serviço.

Sobre esta tarefa

Visualizar as conexões de escuta em um cluster é útil nos seguintes cenários:

- Verificar se o protocolo ou serviço desejado está escutando em um LIF se as conexões do cliente a esse LIF falharem consistentemente.
- Verificar se um ouvinte UDP/rclopcp é aberto em cada LIF de cluster se o acesso remoto de dados a um volume em um nó por meio de um LIF em outro nó falhar.
- Verificar se um ouvinte UDP/rclopcp é aberto em cada LIF de cluster se as transferências SnapMirror entre dois nós no mesmo cluster falharem.
- Verificando se um ouvinte TCP/ctlopcp é aberto em cada LIF entre clusters se as transferências SnapMirror entre dois nós em clusters diferentes falharem.

Passo

Exiba as conexões de escuta por nó usando o `network connections listening show` comando.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

Saiba mais sobre `network connections listening show` o "Referência do comando ONTAP"na .

Comandos ONTAP para diagnosticar problemas de rede

Pode diagnosticar problemas na rede utilizando comandos como `ping`, `traceroute`, `ndp`, e `tcpdump`. Você também pode usar comandos como `ping6` e `traceroute6` para diagnosticar problemas do IPv6.

Se você quiser…	Digite este comando…
Teste se o nó pode alcançar outros hosts em sua rede	`network ping`
Teste se o nó pode alcançar outros hosts em sua rede IPv6	`network ping6`
Trace a rota que os pacotes IPv4 levam para um nó de rede	`network traceroute`
Trace a rota que os pacotes IPv6 levam para um nó de rede	`network traceroute6`
Gerenciar o Neighbor Discovery Protocol (NDP)	`network ndp`
Exibir estatísticas sobre pacotes recebidos e enviados em uma interface de rede especificada ou em todas as interfaces de rede	`run -node` *`node_name`* `ifstat` **Nota**: Este comando está disponível no nodeshell.
Exiba informações sobre dispositivos vizinhos que são descobertos de cada nó e porta no cluster, incluindo o tipo de dispositivo remoto e a plataforma do dispositivo	`network device-discovery show`

Visualizar os vizinhos CDP do nó (o ONTAP suporta apenas CDPv1 anúncios)	`run -node node_name cdpd show-neighbors` **Nota**: Este comando está disponível no nodeshell.
Rastreie os pacotes que são enviados e recebidos na rede	`network tcpdump start -node node-name -port port_name` **Nota**: Este comando está disponível no nodeshell.
Meça a latência e a taxa de transferência entre clusters ou nós entre clusters	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` Para obter mais informações, consulte "Gerenciamento de desempenho".

Informações relacionadas

- "Referência do comando ONTAP"
- "ping de rede"
- "traceroute de rede"
- "mostra de deteção de dispositivo de rede"
- "rede ndp"

Veja a conetividade de rede com os protocolos de descoberta de vizinhos

Veja a conetividade de rede ONTAP com os protocolos de descoberta de vizinhos

Em um data center, você pode usar protocolos de descoberta de vizinhos para visualizar a conetividade de rede entre um par de sistemas físicos ou virtuais e suas interfaces de rede. O ONTAP oferece suporte a dois protocolos de descoberta de vizinhos: O Protocolo de descoberta de Cisco (CDP) e o Protocolo de descoberta de camada de enlace (LLDP).

Os protocolos de descoberta de vizinhos permitem que você descubra e visualize automaticamente informações sobre dispositivos habilitados para protocolo diretamente conetados em uma rede. Cada dispositivo anuncia informações de identificação, recursos e conetividade. Essas informações são transmitidas em quadros Ethernet para um endereço MAC multicast e são recebidas por todos os dispositivos habilitados para protocolo vizinhos.

Para que dois dispositivos se tornem vizinhos, cada um deve ter um protocolo ativado e configurado corretamente. A funcionalidade do protocolo Discovery está limitada a redes diretamente ligadas. Os vizinhos podem incluir dispositivos habilitados para protocolo, como switches, roteadores, bridges e assim por diante. O ONTAP suporta dois protocolos de descoberta de vizinhos, que podem ser usados individualmente ou em conjunto.

Protocolo de descoberta de Cisco (CDP)

O CDP é um protocolo de camada de link proprietário desenvolvido pela Cisco Systems. Ele é habilitado por padrão no ONTAP para portas de cluster, mas deve ser habilitado explicitamente para portas de dados.

Protocolo de descoberta de camada de link (LLDP)

LLDP é um protocolo neutro para fornecedores especificado no documento padrões IEEE 802,1AB.3. Ele deve ser habilitado explicitamente para todas as portas.

Use o CDP para detetar a conetividade de rede ONTAP

O uso do CDP para detetar a conetividade de rede consiste em revisar considerações de implantação, habilitá-lo em portas de dados, visualizar dispositivos vizinhos e ajustar os valores de configuração do CDP conforme necessário. O CDP é ativado por padrão nas portas do cluster.

O CDP também deve ser ativado em todos os switches e roteadores antes que as informações sobre dispositivos vizinhos possam ser exibidas.

Lançamento do ONTAP	Descrição
9.10.1 e anteriores	O CDP também é usado pelo monitor de integridade do switch de cluster para descobrir automaticamente seus switches de rede de gerenciamento e cluster.
9.11.1 e mais tarde	O CDP também é usado pelo monitor de integridade do switch de cluster para descobrir automaticamente o cluster, o armazenamento e os switches de rede de gerenciamento.

Informações relacionadas

"Administração do sistema"

Considerações para usar CDP

Por padrão, os dispositivos compatíveis com CDP enviam CDPv2 anúncios. Os dispositivos compatíveis com CDP enviam CDPv1 anúncios apenas quando recebem CDPv1 anúncios. O ONTAP suporta apenas CDPv1. Portanto, quando um nó ONTAP envia anúncios CDPv1, os dispositivos vizinhos compatíveis com CDP enviam CDPv1 anúncios.

Você deve considerar as seguintes informações antes de ativar o CDP em um nó:

- O CDP é suportado para todas as portas.
- Os anúncios CDP são enviados e recebidos por portas que estão no estado up.
- O CDP deve estar ativado nos dispositivos de transmissão e receção para enviar e receber anúncios CDP.
- Os anúncios CDP são enviados em intervalos regulares e você pode configurar o intervalo de tempo.
- Quando os endereços IP são alterados para um LIF, o nó envia as informações atualizadas no próximo anúncio do CDP.
- ONTAP 9.10,1 e anteriores:
  - O CDP está sempre ativado nas portas do cluster.
  - O CDP está desativado, por padrão, em todas as portas que não sejam de cluster.
- ONTAP 9.11,1 e posterior:
  - O CDP está sempre ativado em portas de cluster e armazenamento.

◦ O CDP está desativado, por padrão, em todas as portas que não sejam de cluster e não de armazenamento.

> Às vezes, quando os LIFs são alterados no nó, as informações do CDP não são atualizadas no lado do dispositivo recetor (por exemplo, um switch). Se você encontrar esse problema, você deve configurar a interface de rede do nó para o status de baixo e, em seguida, para o status de cima.

- Apenas endereços IPv4 são anunciados em anúncios CDP.
- Para portas de rede físicas com VLANs, todas as LIFs configuradas nas VLANs nessa porta são anunciadas.
- Para portas físicas que fazem parte de um grupo de interfaces, todos os endereços IP configurados nesse grupo de interfaces são anunciados em cada porta física.
- Para um grupo de interfaces que hospeda VLANs, todas as LIFs configuradas no grupo de interfaces e as VLANs são anunciadas em cada uma das portas de rede.
- Devido aos pacotes CDP serem restritos a não mais de 1500 bytes, em portas configuradas com um grande número de LIFs, apenas um subconjunto desses endereços IP pode ser relatado no switch adjacente.

Ativar ou desativar o CDP

Para descobrir e enviar anúncios para dispositivos vizinhos compatíveis com CDP, o CDP deve estar ativado em cada nó do cluster.

Por padrão no ONTAP 9.10,1 e versões anteriores, o CDP é ativado em todas as portas de cluster de um nó e desativado em todas as portas que não sejam de cluster de um nó.

Por padrão no ONTAP 9.11,1 e posterior, o CDP é ativado em todos os clusters e portas de armazenamento de um nó e desativado em todas as portas que não sejam de cluster e não de armazenamento de um nó.

Sobre esta tarefa

A `cdpd.enable` opção controla se o CDP está ativado ou desativado nas portas de um nó:

- Para o ONTAP 9.10,1 e anterior, o ON ativa o CDP em portas que não sejam de cluster.
- Para o ONTAP 9.11,1 e posterior, o ON ativa o CDP em portas que não sejam de cluster e que não sejam de armazenamento.
- Para ONTAP 9.10,1 e anteriores, Desativar desativa o CDP em portas que não sejam de cluster; não é possível desativar o CDP em portas de cluster.
- Para o ONTAP 9.11,1 e posterior, Desativar desativa o CDP em portas que não sejam de cluster e que não sejam de armazenamento; não é possível desativar o CDP em portas de cluster.

Quando o CDP está desativado em uma porta que está conetada a um dispositivo compatível com CDP, o tráfego de rede pode não ser otimizado.

Passos

1. Exibir a configuração atual de CDP para um nó ou para todos os nós em um cluster:

Para ver a definição CDP de…	Digite…

Um nó	`run - node <node_name> options cdpd.enable`
Todos os nós em um cluster	`options cdpd.enable`

2. Ative ou desative o CDP em todas as portas de um nó ou em todas as portas de todos os nós de um cluster:

Para ativar ou desativar o CDP em…	Digite…
Um nó	`run -node node_name options cdpd.enable {on or off}`
Todos os nós em um cluster	`options cdpd.enable {on or off}`

Exibir informações sobre o vizinho CDP

Você pode exibir informações sobre os dispositivos vizinhos que estão conetados a cada porta dos nós do cluster, desde que a porta esteja conetada a um dispositivo compatível com CDP. Você pode usar o `network device-discovery show -protocol cdp` comando para exibir informações de vizinhos. Saiba mais sobre `network device-discovery show` o "Referência do comando ONTAP"na .

Sobre esta tarefa

No ONTAP 9.10,1 e anterior, como o CDP está sempre ativado para portas de cluster, as informações de vizinhos do CDP são sempre exibidas para essas portas. O CDP deve estar habilitado em portas que não sejam de cluster para que as informações de vizinhos apareçam para essas portas.

No ONTAP 9.11,1 e posterior, uma vez que o CDP está sempre ativado para portas de cluster e armazenamento, as informações do vizinho CDP são sempre exibidas para essas portas. O CDP deve estar habilitado em portas que não sejam de cluster e não de armazenamento para que as informações de vizinhos apareçam para essas portas.

Passo

Exiba informações sobre todos os dispositivos compatíveis com CDP conetados às portas em um nó no cluster:

```
network device-discovery show -node node -protocol cdp
```

O comando a seguir mostra os vizinhos que estão conetados às portas no nó sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

A saída lista os dispositivos Cisco que estão conetados a cada porta do nó especificado.

Configure o tempo de espera para mensagens CDP

Tempo de espera é o período de tempo durante o qual os anúncios CDP são armazenados em cache em dispositivos compatíveis com CDP vizinhos. O tempo de espera é anunciado em cada pacote CDPv1 e é atualizado sempre que um pacote CDPv1 é recebido por um nó.

- O valor `cdpd.holdtime` da opção deve ser definido com o mesmo valor em ambos os nós de um par de HA.
- O valor de tempo de retenção padrão é de 180 segundos, mas você pode inserir valores que variam de 10 segundos a 255 segundos.
- Se um endereço IP for removido antes que o tempo de espera expire, as informações do CDP serão armazenadas em cache até que o tempo de espera expire.

Passos

1. Exibir o tempo atual de retenção do CDP para um nó ou para todos os nós em um cluster:

Para ver o tempo de espera de…	Digite…
Um nó	`run -node node_name options cdpd.holdtime`

Todos os nós em um cluster	`options cdpd.holdtime`

2. Configure o tempo de retenção do CDP em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:

Para definir o tempo de espera em…	Digite…
Um nó	`run -node node_name options cdpd.holdtime holdtime`
Todos os nós em um cluster	`options cdpd.holdtime holdtime`

Defina o intervalo para enviar anúncios CDP

Os anúncios do CDP são enviados para vizinhos do CDP em intervalos periódicos. Você pode aumentar ou diminuir o intervalo para enviar anúncios CDP dependendo do tráfego de rede e alterações na topologia da rede.

- O valor `cdpd.interval` da opção deve ser definido com o mesmo valor em ambos os nós de um par de HA.
- O intervalo padrão é de 60 segundos, mas você pode inserir um valor de 5 segundos a 900 segundos.

Passos

1. Exibir o intervalo de tempo atual do anúncio do CDP para um nó ou para todos os nós em um cluster:

Para ver o intervalo para…	Digite…
Um nó	`run -node node_name options cdpd.interval`
Todos os nós em um cluster	`options cdpd.interval`

2. Configure o intervalo para enviar anúncios CDP para todas as portas de um nó ou para todas as portas de todos os nós em um cluster:

Para definir o intervalo para…	Digite…
Um nó	`run -node node_name options cdpd.interval interval`
Todos os nós em um cluster	`options cdpd.interval interval`

Exibir ou limpar estatísticas CDP

Você pode exibir as estatísticas do CDP para as portas de cluster e não cluster em cada nó para detetar possíveis problemas de conetividade de rede. As estatísticas de CDP são cumulativas a partir do momento em que foram eliminadas pela última vez.

Sobre esta tarefa

No ONTAP 9.10,1 e anterior, como o CDP está sempre ativado para portas, as estatísticas CDP são sempre exibidas para o tráfego nessas portas. O CDP deve estar ativado nas portas para que as estatísticas apareçam para essas portas.

No ONTAP 9.11,1 e posterior, como o CDP está sempre ativado para portas de cluster e armazenamento, as estatísticas CDP são sempre exibidas para o tráfego nessas portas. O CDP deve estar habilitado em portas que não sejam de cluster ou não de armazenamento para que as estatísticas apareçam para essas portas.

Passo

Exibir ou limpar as estatísticas CDP atuais para todas as portas em um nó:

Se você quiser…	Digite…
Veja as estatísticas do CDP	`run -node node_name cdpd show-stats`
Limpe as estatísticas do CDP	`run -node node_name cdpd zero-stats`

Exemplo de estatísticas de exibição e limpeza

O comando a seguir mostra as estatísticas do CDP antes de serem apagadas. A saída exibe o número total de pacotes que foram enviados e recebidos desde a última vez que as estatísticas foram apagadas.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

O seguinte comando limpa as estatísticas CDP:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

Depois que as estatísticas são apagadas, elas começam a se acumular após o próximo anúncio do CDP ser enviado ou recebido.

Conexão a switches Ethernet que não suportam CDP

Vários switches de fornecedores não oferecem suporte ao CDP. Veja o"Base de conhecimento da NetApp : a descoberta de dispositivos ONTAP mostra nós em vez do switch" para mais detalhes.

Existem duas opções para resolver este problema:

- Desative o CDP e ative o LLDP, se suportado. "Use o LLDP para detetar conetividade de rede"Consulte para obter mais detalhes.
- Configure um filtro de pacote de endereços MAC nos switches para soltar anúncios CDP.

Use o LLDP para detetar a conetividade de rede ONTAP

O uso do LLDP para detetar a conetividade de rede consiste em revisar considerações de implantação, habilitá-lo em todas as portas, visualizar dispositivos vizinhos e ajustar os valores de configuração do LLDP conforme necessário.

O LLDP também deve ser ativado em qualquer switch e roteador antes que as informações sobre dispositivos vizinhos possam ser exibidas.

O ONTAP relata atualmente as seguintes estruturas de tipo-comprimento-valor (TLVs):

- ID do chassis
- ID da porta
- Tempo para viver (TTL)
- Nome do sistema

  O nome do sistema TLV não é enviado em dispositivos CNA.

Certos adaptadores de rede convergidos (CNAs), como o adaptador X1143 e as portas integradas UTA2, contêm suporte de descarga para LLDP:

- A descarga LLDP é usada para Data Center Bridging (DCB).
- As informações exibidas podem diferir entre o cluster e o switch.

  Os dados de ID do chassi e ID da porta exibidos pelo switch podem ser diferentes para portas CNA e não CNA.

Por exemplo:

- Para portas não CNA:
  - O ID do chassis é um endereço MAC fixo de uma das portas no nó
  - ID da porta é o nome da porta correspondente no nó
- Para portas CNA:
  - ID do chassis e ID da porta são os endereços MAC das respetivas portas no nó.

No entanto, os dados exibidos pelo cluster são consistentes para esses tipos de portas.

A especificação LLDP define o acesso às informações coletadas por meio de um MIB SNMP. No entanto, o ONTAP não suporta atualmente o MIB LLDP.

Ativar ou desativar o LLDP

Para descobrir e enviar anúncios para dispositivos vizinhos compatíveis com LLDP, o LLDP deve estar habilitado em cada nó do cluster. A partir do ONTAP 9.7, o LLDP é ativado em todas as portas de um nó por padrão.

Sobre esta tarefa

Para o ONTAP 9.10,1 e anterior, a `lldp.enable` opção controla se o LLDP está ativado ou desativado nas portas de um nó:

- `on` Ativa o LLDP em todas as portas.
- `off` Desativa o LLDP em todas as portas.

Para o ONTAP 9.11,1 e posterior, a `lldp.enable` opção controla se o LLDP está ativado ou desativado nas portas que não são de cluster e não são de storage de um nó:

- `on` Habilita o LLDP em todas as portas que não são de cluster e não são de storage.
- `off` Desativa o LLDP em todas as portas que não sejam de cluster e não de armazenamento.

Passos

1. Exibir a configuração atual de LLDP para um nó ou para todos os nós em um cluster:
   - Nó único: `run -node node_name options lldp.enable`
   - Todos os nós: Opções `lldp.enable`
2. Ative ou desative o LLDP em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:

Para ativar ou desativar o LLDP em…	Digite…

Um nó	`run -node node_name options lldp.enable {on
off}`	Todos os nós em um cluster
`options lldp.enable {on	off}`

- Nó único:

```
run -node node_name options lldp.enable {on|off}
```

- Todos os nós:

```
options lldp.enable {on|off}
```

Ver informações do vizinho LLDP

Você pode exibir informações sobre os dispositivos vizinhos que estão conetados a cada porta dos nós do cluster, desde que a porta esteja conetada a um dispositivo compatível com LLDP. Você usa o comando network device-Discovery show para exibir informações de vizinhos.

Passo

1. Exiba informações sobre todos os dispositivos compatíveis com LLDP conetados às portas em um nó no cluster:

```
network device-discovery show -node node -protocol lldp
```

O comando a seguir mostra os vizinhos que estão conetados às portas no cluster de nó-1_01. A saída lista os dispositivos habilitados para LLDP que estão conetados a cada porta do nó especificado. Se a `-protocol` opção for omitida, a saída também lista dispositivos habilitados para CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Ajuste o intervalo para transmitir anúncios LLDP

Anúncios LLDP são enviados para vizinhos LLDP em intervalos periódicos. Você pode aumentar ou diminuir o intervalo para enviar anúncios LLDP dependendo do tráfego de rede e alterações na topologia da rede.

Sobre esta tarefa

O intervalo padrão recomendado pelo IEEE é de 30 segundos, mas você pode inserir um valor de 5 segundos a 300 segundos.

Passos

1. Exibir o intervalo de tempo de anúncio LLDP atual para um nó ou para todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - Todos os nós:

     ```
     options lldp.xmit.interval
     ```

2. Ajuste o intervalo para o envio de anúncios LLDP para todas as portas de um nó ou para todas as portas de todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - Todos os nós:

     ```
     options lldp.xmit.interval <interval>
     ```

Ajuste o valor time-to-live para anúncios LLDP

Time-to-Live (TTL) é o período de tempo para o qual os anúncios LLDP são armazenados em cache em dispositivos compatíveis com LLDP vizinhos. TTL é anunciado em cada pacote LLDP e é atualizado sempre que um pacote LLDP é recebido por um nó. TTL pode ser modificado em quadros LLDP de saída.

Sobre esta tarefa

- TTL é um valor calculado, o produto do intervalo de transmissão (`lldp.xmit.interval`) e o multiplicador de retenção (`lldp.xmit.hold`) mais um.
- O valor multiplicador de retenção padrão é 4, mas você pode inserir valores que variam de 1 a 100.
- O TTL padrão é, portanto, 121 segundos, como recomendado pelo IEEE, mas ajustando os valores do multiplicador de intervalo de transmissão e retenção, você pode especificar um valor para quadros de saída de 6 segundos a 30001 segundos.
- Se um endereço IP for removido antes do TTL expirar, as informações do LLDP serão armazenadas em cache até que o TTL expire.

Passos

1. Exibir o valor multiplicador de retenção atual para um nó ou para todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - Todos os nós:

     ```
     options lldp.xmit.hold
     ```

2. Ajuste o valor multiplicador de retenção em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - Todos os nós:

     ```
     options lldp.xmit.hold <hold_value>
     ```

Exibir ou limpar estatísticas LLDP

Você pode exibir as estatísticas do LLDP para as portas de cluster e não cluster em cada nó para detetar possíveis problemas de conetividade de rede. As estatísticas LLDP são cumulativas a partir do momento em que foram eliminadas pela última vez.

Sobre esta tarefa

Para o ONTAP 9.10,1 e versões anteriores, como o LLDP está sempre ativado para portas de cluster, as estatísticas do LLDP são sempre exibidas para o tráfego nessas portas. O LLDP deve estar habilitado em portas que não sejam de cluster para que as estatísticas apareçam para essas portas.

Para o ONTAP 9.11,1 e posterior, como o LLDP está sempre ativado para portas de cluster e armazenamento, as estatísticas do LLDP são sempre exibidas para o tráfego nessas portas. O LLDP deve estar habilitado em portas que não sejam de cluster e não de storage para que as estatísticas apareçam para essas portas.

Passo

Exibir ou limpar as estatísticas LLDP atuais para todas as portas em um nó:

Se você quiser…	Digite…
Veja as estatísticas do LLDP	`run -node node_name lldp stats`
Limpe as estatísticas do LLDP	`run -node node_name lldp stats -z`

Mostrar e limpar o exemplo de estatísticas

O comando a seguir mostra as estatísticas LLDP antes de serem limpas. A saída exibe o número total de pacotes que foram enviados e recebidos desde a última vez que as estatísticas foram apagadas.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

O comando a seguir limpa as estatísticas LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

Depois que as estatísticas são apagadas, elas começam a se acumular após o próximo anúncio LLDP ser enviado ou recebido.

Informações sobre direitos autorais

Informações sobre marcas comerciais