Interfaces lógicas (LIFs)

ONTAP 9

NetApp
January 17, 2025

Índice

Interfaces lógicas (LIFs)

Visão geral da LIF

Configure a visão geral dos LIFs

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:

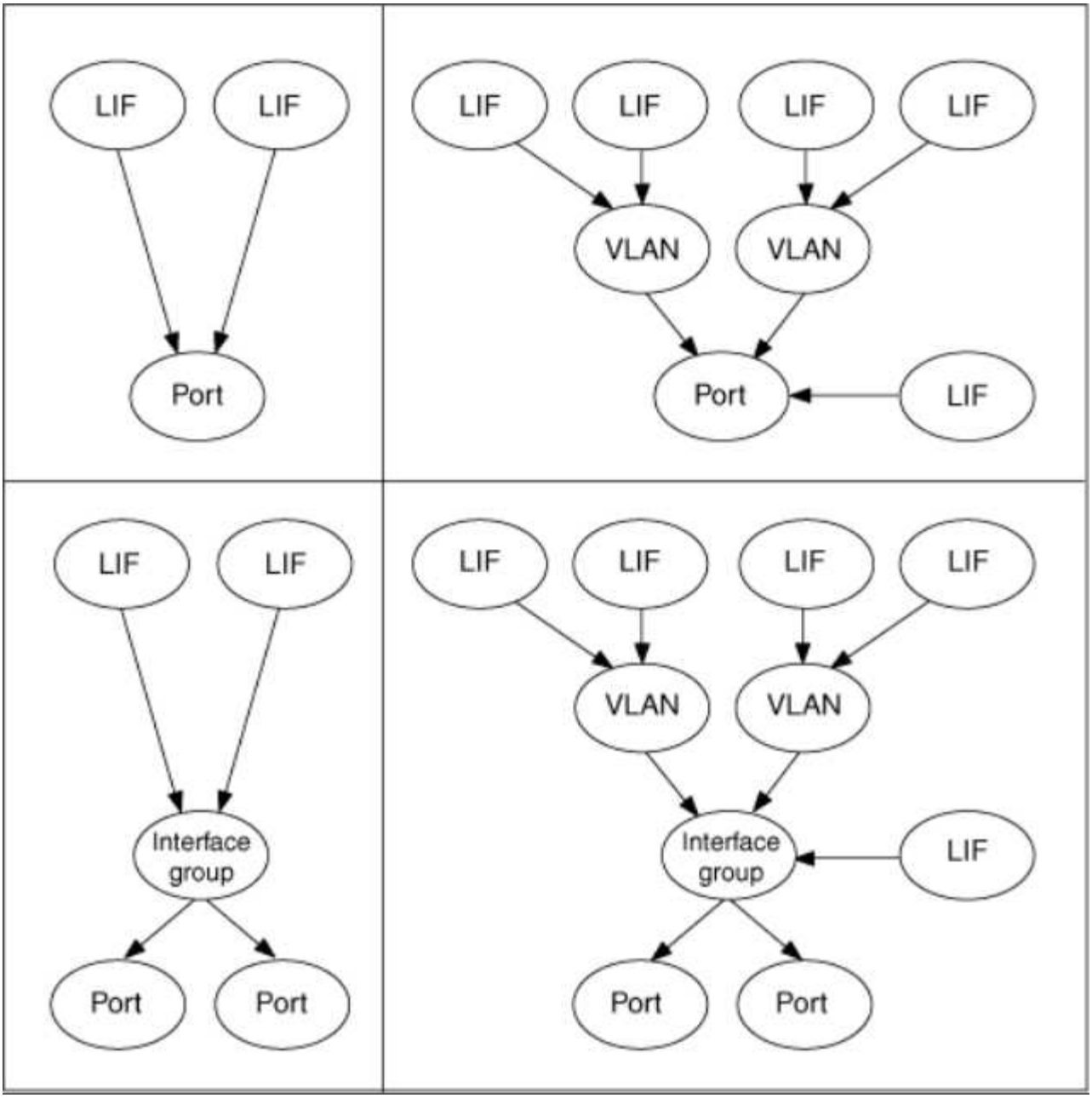
- Portas físicas que não fazem parte dos grupos de interfaces
- Grupos de interfaces
- VLANs
- Portas físicas ou grupos de interface que hospedam VLANs
- Portas IP virtual (VIP)

  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.

Compatibilidade 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 .

Gerencie o tráfego suportado no 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 .

LIFs e políticas de serviço (ONTAP 9.6 e posteriores)

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.

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

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 os 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	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-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 utilizem 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 quaisquer 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.

Funções de LIF (ONTAP 9 .5 e anteriores)

LIFs com papéis diferentes têm caraterísticas diferentes. Uma função LIF determina o tipo de tráfego suportado pela interface, juntamente com as regras de failover aplicáveis, as restrições de firewall que estão em vigor, a segurança, o balanceamento de carga e o comportamento de roteamento para cada LIF. Um LIF pode ter qualquer uma das seguintes funções: Cluster, gerenciamento de cluster, dados, clusters, gerenciamento de nós e undef (undefined). O papel undef é usado para LIFs BGP.

A partir do ONTAP 9.6, as funções de LIF são obsoletas. Você deve especificar políticas de serviço para LIFs em vez de uma função. Não é necessário especificar uma função LIF ao criar um LIF com uma política de serviço.

Segurança LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Requer sub-rede IP privada?	Não	Sim	Não	Não	Não
Requer rede segura?	Não	Sim	Não	Não	Sim
Política de firewall predefinida	Muito restritivo	Completamente aberto	Média	Média	Muito restritivo
O firewall é personalizável?	Sim	Não	Sim	Sim	Sim

Failover de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters

Comportamento padrão	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF e em um nó de parceiro não-SFO	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF	Qualquer porta no mesmo grupo de failover	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF
É personalizável?	Sim	Não	Sim	Sim	Sim

Encaminhamento de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Quando é necessária uma rota predefinida?	Quando os clientes ou o controlador de domínio estão em sub-rede IP diferente	Nunca	Quando qualquer um dos tipos principais de tráfego requer acesso a uma sub-rede IP diferente	Quando o administrador estiver se conetando a partir de outra sub-rede IP	Quando outras LIFs de clusters estão em uma sub-rede IP diferente
Quando é necessária uma rota estática para uma sub-rede IP específica?	Raro	Nunca	Raro	Raro	Quando os nós de outro cluster têm suas LIFs de clusters em sub-redes IP diferentes
Quando é necessária uma rota de host estática para um servidor específico?	Para ter um dos tipos de tráfego listados em LIF de gerenciamento de nós, passe por um LIF de dados em vez de um LIF de gerenciamento de nós. Isso requer uma alteração de firewall correspondente.	Nunca	Raro	Raro	Raro

Rebalanceamento de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
DNS: Usar como servidor DNS?	Sim	Não	Não	Não	Não
DNS: Exportar como zona?	Sim	Não	Não	Não	Não

Tipos de tráfego primário de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Tipos de tráfego principais	Servidor NFS, servidor CIFS, cliente NIS, ative Directory, LDAP, WINS, cliente e servidor DNS, servidor iSCSI e FC	Sem brilho	Servidor SSH, servidor HTTPS, cliente NTP, SNMP, cliente AutoSupport, cliente DNS, carregamento de atualizações de software	Servidor SSH, servidor HTTPS	Replicação entre clusters

Gerenciar LIFs

Configurar políticas de serviço de LIF

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.

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`

Criar um LIF (interface de rede)

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.

- 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).
- 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.
- Somente um LIF NVMe que manipula o tráfego de dados pode ser configurado por SVM.
- 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 Gerenciador de sistemas 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
```

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

   `network subnet show -ipspace` *`ipspace1`*

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.

   - `-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. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
   - `-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 comando Network ndp prefix show para exibir a lista de prefixos RA aprendidos em várias interfaces.

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

   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
```

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 um LIF

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 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
   ```

2. Verifique se os endereços IP estão acessíveis.

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

Migração de um LIF

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
```

Reverter um LIF para sua porta inicial

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`

ONTAP 9.8 e posterior: Recupere de um cluster 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.
```

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 revelam quais portas não têm conetividade entre si.

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
   ```

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
   ```

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.

Eliminar um LIF

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 *`

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.

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
0x7465737420736563726574
```

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.

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 utilizar 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"

Informações sobre direitos autorais

Informações sobre marcas comerciais