Configure LIFs (cluster administrators only)

ONTAP System Manager

NetApp
December 16, 2020

Table of Contents

Configure LIFs (cluster administrators only)

Overview

A LIF represents a network access point to a node in the cluster. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

A cluster administrator can create, view, modify, migrate, or delete LIFs. An SVM administrator can only view the LIFs associated with the SVM.

What LIFs are

A LIF (logical interface) is an IP address or WWPN with associated characteristics, such as a service policy, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

LIFs can be hosted on the following ports:

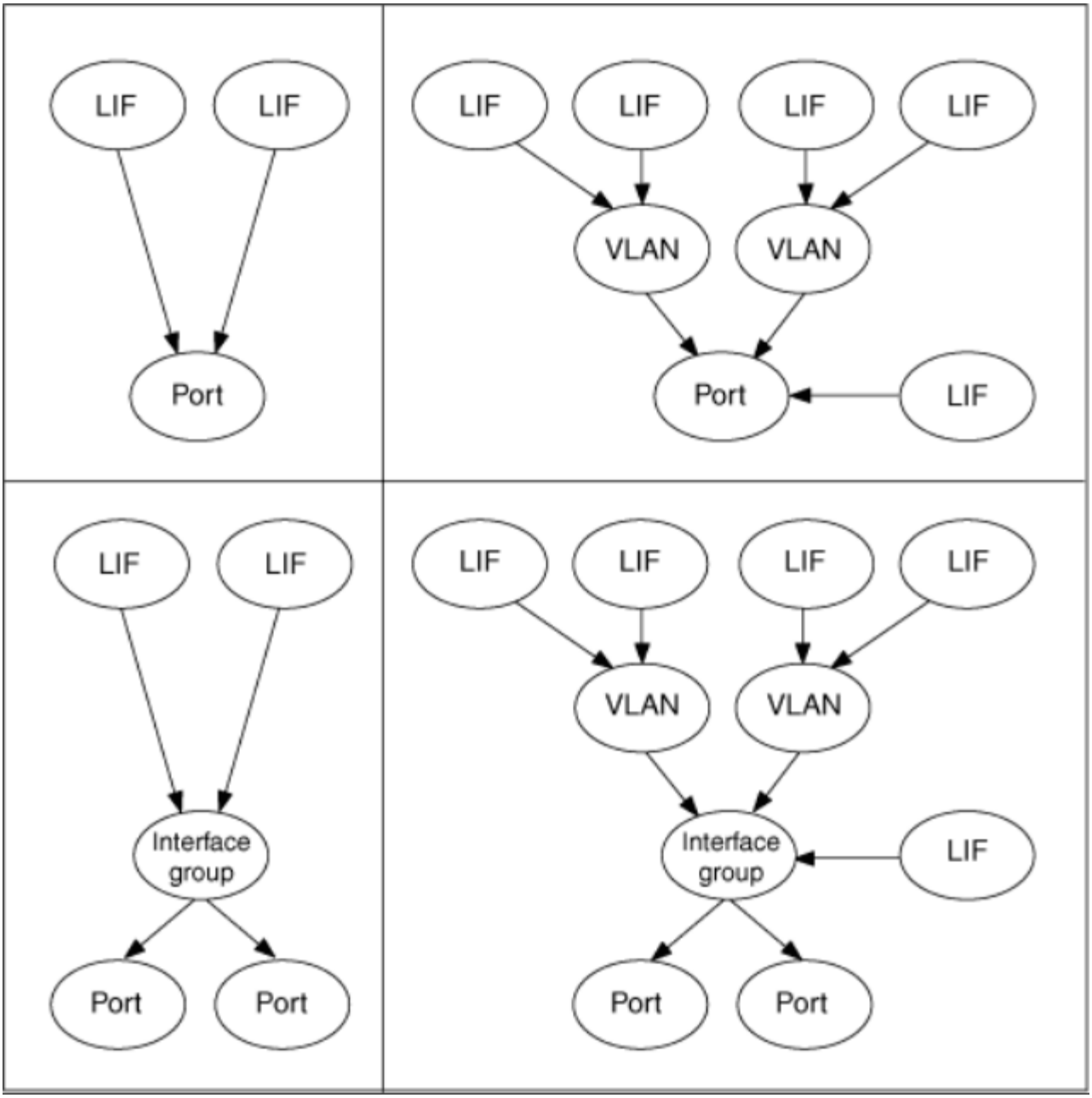
- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs
- Virtual IP (VIP) ports

  VIP LIFs are supported and are hosted on VIP ports.

While configuring SAN protocols such as FC on a LIF, it will be associated with a WWPN.

SAN administration

The following figure illustrates the port hierarchy in an ONTAP system:



LIFs and service policies

You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.

Service policies for system SVMs

The admin SVM and any system SVM contain service policies that can be used for LIFs in that SVM, including management and intercluster LIFs. These policies are automatically created by the system when an IPspace is created. The following table lists the built-in policies for LIFs in system SVMs:

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core	intercluster	Used by LIFs carrying intercluster traffic. Note: Available from ONTAP 9.5 with the name net-intercluster service policy.
default-route-announce	management-bgp	-	Used by LIFs carrying BGP peer connections Note: Available from ONTAP 9.5 with the name net-route-announce service policy.
default-management	management-core, management-ems, management-ssh, management-https, management-autosupport	node-mgmt, or cluster-mgmt	Used by LIFs handling management requests. Management-ems controls which LIFs can publish EMS content.

The following table lists the services that can be used on a system SVM along with any restrictions each service imposes on a LIF's failover policy:

Service	Failover limitations	Description
intercluster-core	home-node-only	Core intercluster services
management-core	-	Core management services
management-ssh	-	Services for SSH management access
management-https	-	Services for HTTPS management access
management-autosupport	-	Services related to posting AutoSupport payloads
management-bgp	home-port-only	Services related to BGP peer interactions

Service policies for data SVMs

All data SVMs contain service policies that can be used by LIFs in that SVM. The following table lists the built-in policies for LIFs in data SVMs:

Policy	Included services	Equivalent data protocol	Description
default-management	management-ssh, management-https	none	Used by LIFs handling management requests

Policy	Included services	Equivalent data protocol	Description
default-data-blocks	data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic
default-data-files	data-nfs, data-cifs, data-flexcache, data-fpolicy-client	nfs, cifs, fcache	Used by LIFs carrying file-oriented NAS data traffic.

The following table lists the services that can be used on a data SVM along with any restrictions each service imposes on a LIF's failover policy:

Policy	Included services	Equivalent data protocol	Description
management-ssh	-	-	Services for SSH management access
management-https	-	-	Services for HTTPS management access
data-core	-	data-only	Core data services (see for more details.
data-nfs	-	data-only	Protocols related to NFS data service
data-cifs	-	data-only	Protocols related to CIFS data service
data-flexcache	-	data-only	Protocols related to FlexCache data service
data-iscsi	home-port-only	data-only	Protocols related to iSCSI data service

You should be aware of how the service policies are assigned to the LIFs in data SVMs:

- If a data SVM is created with a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using the specified services.
- If a data SVM is created without specifying a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using a default list of data services.

  The default data services list includes the iSCSI, NFS, SMB, and FlexCache services.

- When a LIF is created with a list of data protocols, a service policy equivalent to the specified data protocols is assigned to the LIF.

  If an equivalent service policy does not exist, a custom service policy is created.

- When a LIF is created without a service policy or list of data protocols, the default-data-files service policy is assigned to the LIF by default.

Data-core service

The data-core service allows components that previously used LIFs with the data role to work as expected on clusters that have been upgraded to manage LIFs using service policies instead of LIF roles (which are deprecated in ONTAP 9.6).

Specifying data-core as a service does not open any ports in the firewall, but the service should be included in any service policy in a data SVM. For example, the default-data-files service policy contains the following services by default:

- data-core
- data-nfs
- data-cifs
- data-flexcache

The data-core service should be included in the policy to ensure all applications using the LIF work as expected, but the other three services can be removed, if desired.

Configure LIF service policies

You can configure LIF service policies to identify a single service or a list of services that will use a LIF.

Create a service policy for LIFs

You can create a service policy for LIFs. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.

About this task

Built-in services and service policies are available for managing data and management traffic on both data and system SVMs. Most use cases are satisfied using a built-in service policy rather than creating a custom service policy.

You can modify these built-in service policies, if required.

Steps

1. View the services that are available in the cluster:

   ```
   network interface service show
   ```

   Services represent the applications accessed by a LIF as well as the applications served by the cluster. Each service includes zero or more TCP and UDP ports on which the application is listening.

The following additional data and management services are available:

```
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. Create a service policy:

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

   - "service_name" specifies a list of services that should be included in the policy.
   - "IP_address/mask" specifies the list of subnet masks for addresses that are allowed to access the services in the service policy. By default, all specified services are added with a default allowed address list of 0.0.0.0/0, which allows traffic from all subnets. When a non-default allowed address list is provided, LIFs using the policy are configured to block all requests with a source address that does not match any of the specified masks.

     The following example shows how to create a data service policy, svm1_data_policy, for an SVM that includes NFS and SMB services:

     ```
     network interface service-policy create -vserver svm1 -policy svm1_data_policy -
     services data-nfs,data-cifs,data-core -allowed-addresses 10.1.0.0/16
     ```

     The following example shows how to create an intercluster service policy:

     ```
     network interface service-policy create -vserver cluster1 -policy intercluster1 -
     services intercluster-core -allowed-addresses 10.1.0.0/16
     ```

3. Verify that the service policy is created.

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

The following output shows the service policies that are available:

```
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.
```

After you finish

Assign the service policy to a LIF either at the time of creation or by modifying an existing LIF.

Assign a service policy to a LIF

You can assign a service policy to a LIF either at the time of creating the LIF or by modifying the LIF. A

service policy defines the list of services that can be used with the LIF.

About this task

You can assign service policies for LIFs in the admin and data SVMs.

Step

Depending on when you want to assign the service policy to a LIF, perform one of the following actions:

If you are...	Assign the service policy by entering the following command...
Creating a LIF	network interface create -vserver svm_name -lif <lif_name> -home -node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifying a LIF	network interface modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

When you specify a service policy for a LIF, you need not specify the data protocol and role for the LIF. Creating LIFs by specifying the role and data protocols is also supported.

A service policy can only be used by LIFs in the same SVM that you specified when creating the service policy.

Examples

The following example shows how to modify the service policy of a LIF to use the default- management service policy:

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

Commands for managing LIF service policies

Use the "network interface service-policy" commands to manage LIF service policies.

If you want to...	Use this command...
Create a service policy	`network interface service-policy create`
Add an additional service entry to an existing service policy	`network interface service-policy add- service`
Clone an existing service policy	`network interface service-policy clone`
Modify a service entry in an existing service policy	`network interface service-policy modify- service`

If you want to...	Use this command...
Remove a service entry from an existing service policy	`network interface service-policy remove- service`
Rename an existing service policy	`network interface service-policy rename`
Delete an existing service policy	`network interface service-policy delete`
Restore a built-in service-policy to its original state	`network interface service-policy restore-defaults`
Display existing service policies	`network interface service-policy show`

Related information

ONTAP 9 commands

Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- LIFs use service policies to specify the type of traffic it handles.

About this task

- You cannot assign NAS and SAN protocols to the same LIF.

  The supported protocols are SMB, NFS, FlexCache, iSCSI, and FC; iSCSI and FC cannot be combined with other protocols. However, NAS and Ethernet-based SAN protocols can be present on the same physical port.

- You can create both IPv4 and IPv6 LIFs on the same network port.
- All the name mapping and host-name resolution services used by an SVM, such as DNS, NIS, LDAP, and Active Directory, must be reachable from at least one LIF handling data traffic of the SVM.
- A LIF handling intracluster traffic between nodes should not be on the same subnet as a LIF

handling management traffic or a LIF handling data traffic.

- Creating a LIF that does not have a valid failover target results in a warning message.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- If other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

  If you are creating an FC-NVMe LIF you should be aware of the following:

  - The NVMe protocol must be supported by the FC adapter on which the LIF is created.
  - FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM.

Steps

1. Create a LIF:

   ```
   network interface create -vserver vserver_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address IP_address -
   netmask IP_address | -subnet-name subnet_name} -firewall- policy policy -auto-revert
   {true|false}
   ```

   - `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

     You can also specify whether the LIF should automatically revert to the home-node and home-port with the -auto-revert option.

   - `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
   - You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
   - When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` man page contains information about creating a static route within an SVM.
- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `true` depending on network management policies in your environment.
- `-service-policy` allows you to control which network services and data protocols are supported by a LIF. You can select a predefined policy provided by the system or create additional policies with specialized collections of services.
- `-data-protocol` allows you to create a LIF that supports the Fibre Channel Protocol (FCP) or NVMe/FC protocols. This option is not required when creating an IP LIF.

2. **Optional**: If you want to assign an IPv6 address in the -address option:
   a. Use the network ndp prefix show command to view the list of RA prefixes learned on various interfaces.

      The `network ndp prefix show` command is available at the advanced privilege level.

   b. Use the format `prefix::id` to construct the IPv6 address manually.

      `prefix` is the prefix learned on various interfaces.

      For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created successfully by using the `network interface show` command.
4. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	network ping
IPv6 address	network ping6

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
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
```

The following command creates a LIF and assigns IP address and network mask values from the

specified subnet (named 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
```

The following command creates an NVMe/FC LIF and specifies the `nvme-fc` data protocol:

```
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
```

Modify a LIF

You can modify a LIF by changing the attributes, such as home node or current node, administrative status, IP address, netmask, failover policy, firewall policy, and service policy. You can also change the address family of a LIF from IPv4 to IPv6.

About this task

- When modifying a LIF's administrative status to down, any outstanding NFSv4 locks are held until the LIF's administrative status is returned to up.

  To avoid lock conflicts that can occur when other LIFs attempt to access the locked files, you must move the NFSv4 clients to a different LIF before setting the administrative status to down.

- You cannot modify the data protocols used by an FC LIF. However, you can modify the services assigned to a service policy or change the service policy assigned to an IP LIF.

  To modify the data protocols used by a FC LIF, you must delete and re-create the LIF. To make service policy changes to an IP LIF, there is a brief outage while the updates occur.

- You cannot modify either the home node or the current node of a node-scoped management LIF.
- When using a subnet to change the IP address and network mask value for a LIF, an IP address is allocated from the specified subnet; if the LIF's previous IP address is from a different subnet, the IP address is returned to that subnet.
- To modify the address family of a LIF from IPv4 to IPv6, you must use the colon notation for the IPv6 address and add a new value for the `-netmask-length` parameter.
- You cannot modify the auto-configured link-local IPv6 addresses.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

You can create service policies for several data and management services.

Steps

1. Modify a LIF's attributes by using the "network interface modify" command.

   The following example shows how to modify the IP address and network mask of LIF datalif2 using an IP address and the network mask value from subnet client1_sub:

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

   The following example shows how to modify the service policy of a LIF.

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

2. Verify that the IP addresses are reachable.

If you are using...	Then use...
IPv4 addresses	`network ping`
IPv6 addresses	`network ping6`

Migrate a LIF

You might have to migrate a LIF to a different port on the same node or a different node within the cluster, if the port is either faulty or requires maintenance. Migrating a LIF is similar to LIF failover, but LIF migration is a manual operation, while LIF failover is the automatic migration of a LIF in response to a link failure on the LIF's current network port.

Before you begin

- A failover group must have been configured for the LIFs.
- The destination node and ports must be operational and must be able to access the same network as the source port.

About this task

- You must migrate LIFs hosted on the ports belonging to a NIC to other ports in the cluster, before removing the NIC from the node.

- You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.
- A node-scoped LIF, such as a node-scoped management LIF, cluster LIF, intercluster LIF, cannot be migrated to a remote node.
- When an NFSv4 LIF is migrated between nodes, a delay of up to 45 seconds results before the LIF is available on a new port.

  To work around this problem, use NFSv4.1 where no delay is encountered.

- You cannot migrate iSCSI LIFs from one node to another node.

  To work around this restriction, you must create an iSCSI LIF on the destination node. For information about guidelines for creating an iSCSI LIF, see SAN administration.

- VMware VAAI copy offload operations fail when you migrate the source or the destination LIF. For more information about VMware VAAI, see NFS reference or SAN administration.

Step

Depending on whether you want to migrate a specific LIF or all the LIFs, perform the appropriate action:

If you want to migrate...	Enter the following command...
A specific LIF	`network interface migrate`
All the data and cluster- management LIFs on a node	`network interface migrate-all`
All of the LIFs off of a port	`network interface migrate-all -node <node> -port <port>`

The following example shows how to migrate a LIF named datalif1 on the SVM vs0 to the port e0d on node0b:

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

The following example shows how to migrate all the data and cluster-management LIFs from the current (local) node:

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

Revert a LIF to its home port

You can revert a LIF to its home port after it fails over or is migrated to a different

port either manually or automatically. If the home port of a particular LIF is unavailable, the LIF remains at its current port and is not reverted.

About this task

- If you administratively bring the home port of a LIF to the up state before setting the automatic revert option, the LIF is not returned to the home port.
- The node management LIF does not automatically revert unless the value of the "auto-revert" option is set to true.
- You must ensure that the "auto-revert" option is enabled for the cluster LIFs to revert to their home ports.

Step

Revert a LIF to its home port manually or automatically:

If you want to revert a LIF to its home port...	Then enter the following command...
Manually	network interface revert -vserver vserver_name -lif lif_name
Automatically	network interface modify -vserver vserver_name -lif lif_name -auto-revert true

Recover from an incorrectly configured cluster LIF

A cluster cannot be created when the cluster network is cabled to a switch but not all of the ports configured in the Cluster IPspace can reach the other ports configured in the Cluster IPspace.

About this task

In a switched cluster, if a cluster network interface (LIF) is configured on the wrong port, or if a cluster port is wired into the wrong network, the `cluster create` command can fail with the following error:

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

The results of the `network port show` command might show that several ports are added to the Cluster IPspace because they are connected to a port that is configured with a cluster LIF. However, the results of the `network port reachability show -detail` command reveal which ports do not have connectivity to one another.

To recover from a cluster LIF configured on a port that is not reachable to the other ports configured

with cluster LIFs, perform the following steps:

Steps

1. Reset the home port of the cluster LIF to the correct port:

```
net port modify -home-port
```

2. Remove the ports that do not have cluster LIFs configured on them from the cluster broadcast domain:

```
net port broadcast-domain remove-ports
```

3. Create the cluster:

```
cluster create
```

Result

When you complete the cluster creation, the system detects the correct configuration and places the ports into the correct broadcast domains.

Delete a LIF

You can delete a network interface (LIF) that is no longer required.

Before you begin

LIFs to be deleted must not be in use.

Steps

1. Mark the LIFs you want to delete as administratively down using the following command:

```
-status-admin down
```

2. Use the `network interface delete` command to delete one or all LIFs:

If you want to delete...	Enter the command ...
A specific LIF	`network interface delete -lif lif_name`
All LIFs	`network interface delete -lif`

The following command deletes the LIF mgmtlif2:

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

3. Use the `network interface show` command to confirm that the LIF is deleted.

Configure virtual IP (VIP) LIFs

Some next-generation data centers use Network-Layer-3 mechanisms that require LIFs to be failed over across subnets. VIP data LIFs and the associated routing protocol, border gateway protocol (BGP), are supported, which enable ONTAP to participate in these next- generation networks.

About this task

A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a BGP LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces. Because multiple physical adapters carry the data traffic, the entire load is not concentrated on a single adapter and the associated subnet. The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

VIP data LIFs provide the following advantages:

- LIF portability beyond a broadcast domain or subnet: VIP data LIFs can fail over to any subnet in the network by announcing the current location of each VIP data LIF to routers through BGP.
- Aggregate throughput: VIP data LIFs can support aggregate throughput that exceeds the bandwidth of any individual port because the VIP LIFs can send or receive data from multiple subnets or ports simultaneously.

Set up border gateway protocol (BGP)

Before creating VIP LIFs, you must set up BGP, which is the routing protocol used for announcing the existence of a VIP LIF to peer routers.

Before you begin

The peer router must be configured to accept a BGP connection from the BGP LIF for the configured autonomous system number (ASN).

ONTAP does not process any incoming route announcements from the router; therefore, you should configure the peer router for not sending any route updates to the cluster.

About this task

Setting up BGP involves optionally creating a BGP configuration, creating a BGP LIF, and creating a BGP peer group. ONTAP automatically creates a default BGP configuration with default values when the first BGP peer group is created on a given node. A BGP LIF is used to establish BGP TCP sessions with peer routers. For a peer router, a BGP LIF is the next hop to reach a VIP LIF. Failover is disabled for the BGP LIF. A BGP peer group advertises the VIP routes for all the SVMs in the peer group's IPspace.

These fields have been added to the `network bgp peer-group` command.

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

These BGP attributes allows you to configure the AS Path and community attributes for the BGP peer group. For more information, see Network features by release.

Steps

1. Log in to the advanced privilege level:

   `set -privilege advanced`

2. Optional: Create a BGP configuration or modify the default BGP configuration of the cluster by performing one of the following actions:

   a. Create a BGP configuration:

   ```
   network bgp config create -node {node_name | local} -asn asn_integer -holdtime
   hold_time -routerid local_router_IP_address

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

   b. Modify the default BGP configuration:

   ```
   network bgp defaults modify -asn asn_integer -holdtime hold_time
   network bgp defaults modify -asn 65502
   ```

   - `asn_integer` specifies the ASN. ASN for BGP is a non-negative 16-bit integer. The default ASN is 65501.
   - `hold_time` specifies the hold time in seconds. The default value is 180s.

3. Create a BGP LIF for the system SVM:

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

You can use the `net-route-announce` service policy for the BGP LIF.

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

4. Create a BGP peer group that is used to establish BGP sessions with the remote peer routers and configure the VIP route information that is advertised to the peer routers:

```
network bgp peer-group create -peer-group group_name -ipspace ipspace_name -local-lif
bgp_lif -peer-address peer-router_ip_address -peer-asn 65502 -route-preference integer
-asn-prepend-type ASN_prepend_type> -asn-prepend-count integer -community BGP
community list <0-65535>:<0-65535>
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -local-lif bgp1
-peer-address 10.10.10.1 -peer-asn 65502 -route-preference 100 -asn-prepend-type
local-asn -asn-prepend-count 2 -community 9000:900,8000:800
```

Create a virtual IP (VIP) data LIF

You can create a VIP data LIF. The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

Before you begin

- The BGP peer group must be set up and the BGP session for the SVM on which the LIF is to be created must be active.
- A static route to the BGP router or any other router in the BGP LIF's subnet must be created for any outgoing VIP traffic for the SVM.
- You should turn on multipath routing so that the outgoing VIP traffic can utilize all the available routes.

  If multipath routing is not enabled, all the outgoing VIP traffic goes from a single interface.

Steps

1. Create a VIP data LIF:

```
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
```

A VIP port is automatically selected if you do not specify the home port with the `network interface create` command.

By default, the VIP data LIF belongs to the system-created broadcast domain named 'Vip', for each IPspace. You cannot modify the VIP broadcast domain.

A VIP data LIF is reachable simultaneously on all ports hosting a BGP LIF of an IPspace. If there is no active BGP session for the VIP's SVM on the local node, the VIP data LIF fails over to the next VIP port on the node that has a BGP session established for that SVM.

2. Verify that the BGP session is in the up status for the SVM of the VIP data LIF:

```
network bgp vserver-status show

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

If the BGP status is `down` for the SVM on a node, the VIP data LIF fails over to a different node where the BGP status is up for the SVM. If BGP status is `down` on all the nodes, the VIP data LIF cannot be hosted anywhere, and has LIF status as down.

Commands for managing the BGP

You use the `network bgp` commands to manage the BGP sessions in ONTAP.

Manage BGP configuration

If you want to...	Use this command...
Create a BGP configuration	network bgp config create
Modify BGP configuration	network bgp config modify
Delete BGP configuration	network bgp config delete
Display BGP configuration	network bgp config show
Displays the BGP status for the SVM of the VIP LIF	network bgp vserver-status show

Manage BGP default values

If you want to…	Use this command…
Modify BGP default values	network bgp defaults modify
Display BGP default values	network bgp defaults show

Manage BGP peer groups

If you want to…	Use this command…
Create a BGP peer group	network bgp peer-group create
Modify a BGP peer group	network bgp peer-group modify
Delete a BGP peer group	network bgp peer-group delete
Display BGP peer groups information	network bgp peer-group show
Rename a BGP peer group	network bgp peer-group rename

Related information: ONTAP 9 commands