Logical interfaces (LIFs)

ONTAP 9

NetApp
February 06, 2026

Table of Contents

Logical interfaces (LIFs)

LIF overview

Learn about LIF configuration for an ONTAP cluster

A LIF (logical interface) 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, revert, or delete LIFs. An SVM administrator can only view the LIFs associated with the SVM.

A LIF 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.

Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

LIFs can be hosted on the following ports:

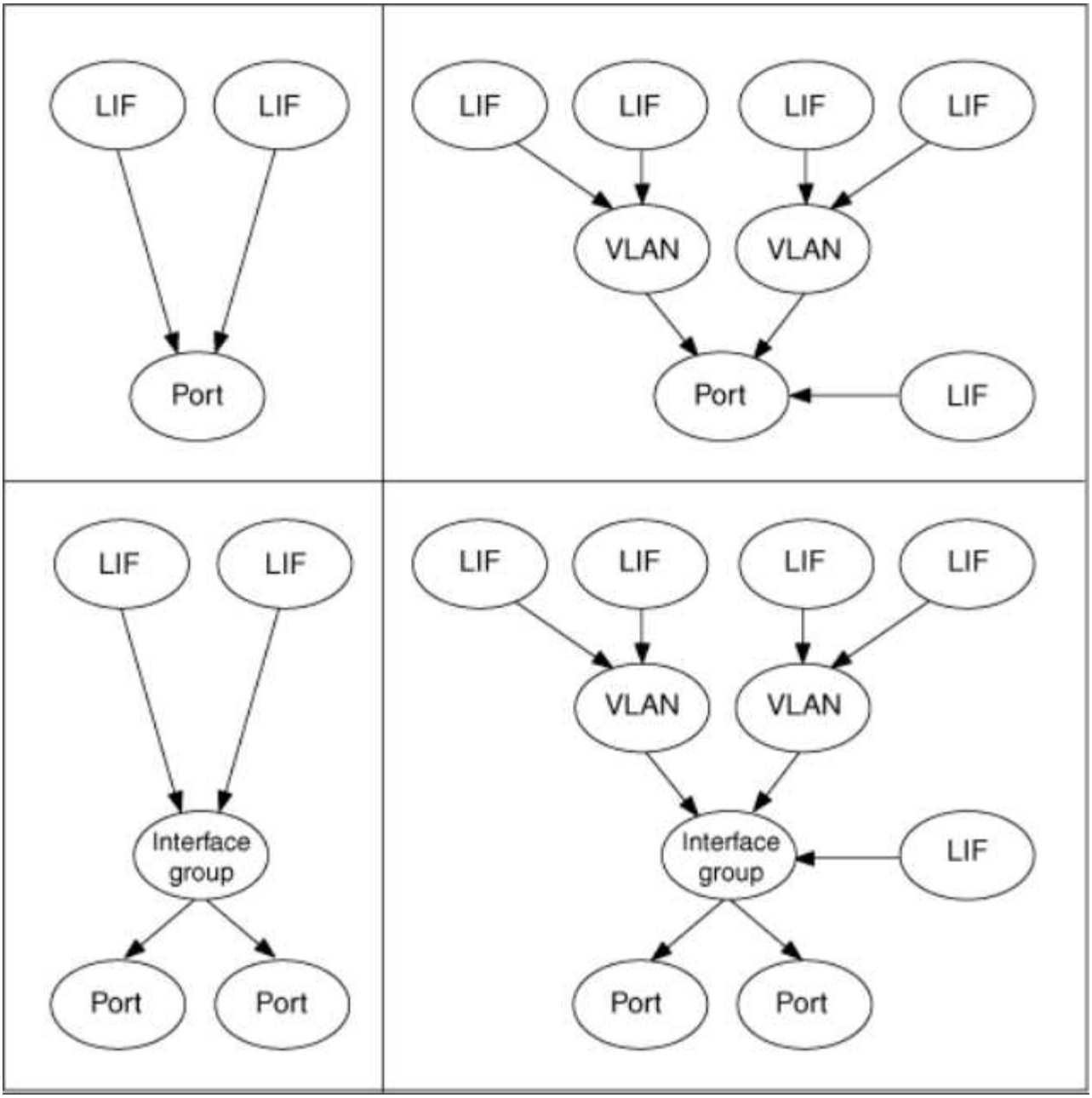
- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs
- Virtual IP (VIP) ports

  Beginning with ONTAP 9.5, 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:



LIF failover and giveback

A LIF failover occurs when a LIF moves from its home node or port to its HA partner node or port. A LIF failover can be triggered automatically by ONTAP or manually by a cluster administrator for certain events such as a down physical Ethernet link or a node dropping out of replicated database (RDB) quorum. When a LIF failover occurs, ONTAP continues normal operation on the partner node until the reason for the failover is resolved. When the home node or port regains health, the LIF is reverted from the HA partner back to its home node or port. This reversion is called a giveback.

For LIF failover and giveback, ports from each node need to belong to the same broadcast domain. To check that the relevant ports on each node belong to the same broadcast domain, see the following:

- ONTAP 9.8 and later: Repair port reachability
- ONTAP 9.7 and earlier: Add or remove ports from a broadcast domain

For LIFs with LIF failover enabled (either automatically or manually), the following applies:

- For LIFs using a data service policy, you can check failover-policy restrictions:
  - ONTAP 9.6 and later: LIFs and service policies in ONTAP 9.6 and later
  - ONTAP 9.5 and earlier: LIF roles in ONTAP 9.5 and earlier
- Auto-revert of LIFs happens when the auto-revert is set to `true` and when the LIF's home port is healthy and able to host the LIF.
- On a planned or unplanned node takeover, the LIF on the node that is taken over, fails over to the HA partner. The port on which the LIF fails over is determined by VIF Manager.
- After the failover is complete, the LIF operates normally.
- When a giveback is initiated, the LIF reverts back to its home node and port, if auto-revert is set to `true`.
- When an ethernet link goes down on a port hosting one or more LIFs, the VIF Manager migrates the LIFs from the down port to a different port in the same broadcast domain. The new port could be in the same node or its HA partner. After the link is restored and if auto-revert is set to `true`, the VIF Manager reverts the LIFs back to their home node and home port.
- When a node drops out of replicated database (RDB) quorum, the VIF Manager migrates the LIFs from the out of quorum node to its HA partner. After the node comes back into quorum and if auto-revert is set to `true`, the VIF Manager reverts the LIFs back to their home node and home port.

Learn about ONTAP LIF compatibility with port types

LIFs can have different characteristics to support different port types.

When intercluster and management LIFs are configured in the same subnet, the management traffic might be blocked by an external firewall and the AutoSupport and NTP connections might fail. You can recover the system by running the `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` command to toggle the intercluster LIF. However, you should set the intercluster LIF and management LIF in different subnets to avoid this issue.

LIF	Description
Data LIF	A LIF that is associated with a storage virtual machine (SVM) and is used for communicating with clients. You can have multiple data LIFs on a port. These interfaces can migrate or fail over throughout the cluster. You can modify a data LIF to serve as an SVM management LIF by modifying its firewall policy to mgmt. Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.
Cluster LIF	A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on cluster ports. Cluster LIFs can fail over between cluster ports on the same node, but they cannot be migrated or failed over to a remote node. When a new node joins a cluster, IP addresses are generated automatically. However, if you want to assign IP addresses manually to the cluster LIFs, you must ensure that the new IP addresses are in the same subnet range as the existing cluster LIFs.

Cluster management LIF	LIF that provides a single management interface for the entire cluster. A cluster management LIF can fail over to any node in the cluster. It cannot fail over to cluster or intercluster ports
Intercluster LIF	A LIF that is used for cross-cluster communication, backup, and replication. You must create an intercluster LIF on each node in the cluster before a cluster peering relationship can be established. These LIFs can only fail over to ports in the same node. They cannot be migrated or failed over to another node in the cluster.
Node management LIF	A LIF that provides a dedicated IP address for managing a particular node in a cluster. Node management LIFs are created at the time of creating or joining the cluster. These LIFs are used for system maintenance, for example, when a node becomes inaccessible from the cluster.
VIP LIF	A VIP LIF is any data LIF created on a VIP port. To learn more, see Configure virtual IP (VIP) LIFs.

Related information

- network interface modify

Supported LIF service policies and roles for your ONTAP version

Over time, the way in which ONTAP manages the type of traffic supported on LIFs has changed.

- ONTAP 9.5 and earlier releases use LIF roles and firewall services.
- ONTAP 9.6 and later releases use LIF service policies:
  - ONTAP 9.5 release introduced LIF service policies.
  - ONTAP 9.6 replaced LIF roles with LIF service policies.
  - ONTAP 9.10.1 replaced firewall services with LIF service policies.

The method you configure depends on the release of ONTAP you are using.

To learn more about:

- Firewall policies, refer to Command: firewall-policy-show.
- LIF roles, refer to LIF roles (ONTAP 9.5 and earlier).
- LIF service policies, refer to LIFs and service policies (ONTAP 9.6 and later).

Learn about ONTAP LIFs and service policies

You can assign service policies (instead of LIF roles or firewall policies) 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.

The method of managing network traffic is different in ONTAP 9.7 and earlier versions. If you need to manage traffic on a network running ONTAP 9.7 and earlier, refer to LIF roles (ONTAP 9.5 and earlier).

FCP and NVMe/FCP protocols do not currently require a service-policy.

You can display service policies and their details using the following command:
`network interface service-policy show`

Learn more about `network interface service-policy show` in the ONTAP command reference.

Features that are not bound to a specific service will use a system-defined behavior to select LIFs for outbound connections.

Applications on a LIF with an empty service policy might behave unexpectedly.

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 beginning with ONTAP 9.12.1. For other releases, display the service policies and their details using the following command:

`network interface service-policy show`

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core, management-https	intercluster	Used by LIFs carrying intercluster traffic. Note: Service intercluster-core is 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-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, or cluster-mgmt	Use this system scoped management policy to create node- and cluster-scoped management LIFs owned by a system SVM. These LIFs can be used for outbound connections to DNS, AD, LDAP, or NIS servers as well as some additional connections to support applications that run on behalf of the entire system. Beginning with ONTAP 9.12.1, you can use the `management-log-forwarding` service to control which LIFs are used to forward audit logs to a remote syslog server.

The following table lists the services that LIFs can use on a system SVM beginning with ONTAP 9.11.1:

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-http	-	Services for HTTP 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
backup-ndmp-control	-	Services for NDMP backup controls
management-ems	-	Services for management messaging access
management-ntp-client	-	Introduced in ONTAP 9.10.1. Services for NTP client access.
management-ntp-server	-	Introduced in ONTAP 9.10.1. Services for NTP server management access
management-portmap	-	Services for portmap management

management-rsh-server	-	Services for rsh server management
management-snmp-server	-	Services for SNMP server management
management-telnet-server	-	Services for telnet server management
management-log-forwarding	-	Introduced in ONTAP 9.12.1. Services for audit log forwarding

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 beginning with ONTAP 9.11.1. For other releases, display the service policies and their details using the following command:

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

Policy	Included services	Equivalent data protocol	Description
default-management	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	none	Use this SVM-scoped management policy to create SVM management LIFs owned by a data SVM. These LIFs can be used to provide SSH or HTTPS access to SVM administrators. When necessary, these LIFs can be used for outbound connections to an external DNS, AD, LDAP, or NIS servers.
default-data-blocks	data-core, data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic. Beginning with ONTAP 9.10.1, the "default-data-blocks" policy is deprecated. Use the "default-data-iscsi" service policy instead.

default-data-files	data-core, data-fpolicy-client, data-dns-server, data-flexcache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Use the default-data-files policy to create NAS LIFs supporting file-based data protocols. Sometimes there is only one LIF present in the SVM, therefore this policy allows the LIF to be used for outbound connections to an external DNS, AD, LDAP, or NIS server. You can remove these services to from this policy if you prefer these connections use only management LIFs.
default-data-iscsi	data-core, data-iscsi	iscsi	Used by LIFs carrying iSCSI data traffic.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Used by LIFs carrying NVMe/TCP 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 beginning with ONTAP 9.11.1:

Service	Failover restrictions	Description
management-ssh	-	Services for SSH management access
management-http	-	Introduced in ONTAP 9.10.1 Services for HTTP management access
management-https	-	Services for HTTPS management access
management-portmap	-	Services for portmap management access
management-snmp-server	-	Introduced in ONTAP 9.10.1 Services for SNMP server management access
data-core	-	Core data services
data-nfs	-	NFS data service
data-cifs	-	CIFS data service
data-flexcache	-	FlexCache data service
data-iscsi	home-port-only for AFF/FAS; sfo-partner-only for ASA	iSCSI data service

backup-ndmp-control	-	Introduced in ONTAP 9.10.1 Backup NDMP controls data service
data-dns-server	-	Introduced in ONTAP 9.10.1 DNS server data service
data-fpolicy-client	-	File-screening policy data service
data-nvme-tcp	home-port-only	Introduced in ONTAP 9.10.1 NVMe TCP data service
data-s3-server	-	Simple Storage Service (S3) server 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, NVMe, 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.

Client-side LIF service

Beginning with ONTAP 9.10.1, ONTAP provides client-side LIF services for multiple applications. These services provide control over which LIFs are used for outbound connections on behalf of each application.

The following new services give administrators control over which LIFs are used as source addresses for certain applications.

Service	SVM restrictions	Description
management-ad-client	-	Beginning with ONTAP 9.11.1, ONTAP provides Active Directory client service for outbound connections to an external AD server.
management-dns-client	-	Beginning with ONTAP 9.11.1, ONTAP provides DNS client service for outbound connections to an external DNS server.
management-ldap-client	-	Beginning with ONTAP 9.11.1, ONTAP provides LDAP client service for outbound connections to an external LDAP server.
management-nis-client	-	Beginning with ONTAP 9.11.1, ONTAP provides NIS client service for outbound connections to an external NIS server.
management-ntp-client	system-only	Beginning with ONTAP 9.10.1, ONTAP provides NTP client service for outbound connections to an external NTP server.
data-fpolicy-client	data-only	Beginning with ONTAP 9.8, ONTAP provides client service for outbound FPolicy connections.

Each of the new services are automatically included in some of the built-in service policies, but administrators can remove them from the built-in policies or add them to custom policies to control which LIFs are used for outbound connections on behalf of each application.

Related information

- network interface service-policy show

Manage LIFs

Configure LIF service policies for an ONTAP cluster

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.

You need advanced privileges to run the `network interface service-policy create` command.

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:

   ```
   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. View the service policies that exist in the 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. Create a service policy:

```
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" 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:

```
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
```

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

```
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. Verify that the service policy is created.

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

   The following output shows the service policies that are available:

```
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.
```

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…
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:

```
cluster1::> 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.

Learn more about `network interface service-policy` in the ONTAP command reference.

Before you begin

Modifying the service policy of a LIF in an active SnapMirror relationship disrupts the replication schedule. If you convert a LIF from intercluster to non-intercluster (or vice versa), those changes are not replicated to the peered cluster. To update the peer cluster after modifying the LIF service policy, first perform the `snapmirror abort` operation then resynchronize the replication relationship.

If you want to…	Use this command…
Create a service policy (advanced privileges required)	`network interface service-policy create`

If you want to…	Use this command…
Add an additional service entry to an existing service policy (advanced privileges required)	`network interface service-policy add-service`
Clone an existing service policy (advanced privileges required)	`network interface service-policy clone`
Modify a service entry in an existing service policy (advanced privileges required)	`network interface service-policy modify-service`
Remove a service entry from an existing service policy (advanced privileges required)	`network interface service-policy remove-service`
Rename an existing service policy (advanced privileges required)	`network interface service-policy rename`
Delete an existing service policy (advanced privileges required)	`network interface service-policy delete`
Restore a built-in service-policy to its original state (advanced privileges required)	`network interface service-policy restore-defaults`
Display existing service policies	`network interface service-policy show`

Related information

- network interface service show
- network interface service-policy
- snapmirror abort

Create ONTAP LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data. A LIF (network interface) 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.

Best practice

Switch ports connected to ONTAP should be configured as spanning-tree edge ports to reduce delays during LIF migration.

Before you begin

- You must be a cluster administrator to perform this task.
- 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 System Manager or the `network subnet create` command.

Learn more about `network subnet create` in the ONTAP command reference.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

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 should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.
- 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:
  - System Manager: Beginning with ONTAP 9.12.0, view the throughput on the Network Interface grid.
  - CLI: Use 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).

    Learn more about `network interface capacity show` and `network interface capacity details show` in the ONTAP command reference.
- Beginning with ONTAP 9.7, 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.

  Beginning with ONTAP 9.4, FC-NVMe is supported. 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.
- A maximum of two NVMe LIFs handling data traffic can be configured per SVM, per node.

- When you create a network interface with a subnet, ONTAP automatically selects an available IP address from the selected subnet and assigns it to the network interface. You can change the subnet if there is more than one subnet, but you cannot change the IP address.
- When you create (add) an SVM, for a network interface, you cannot specify an IP address that is in the range of an existing subnet. You will receive a subnet conflict error. This issue occurs in other workflows for a network interface, such as creating or modifying inter-cluster network interfaces in SVM settings or cluster settings.
- Beginning with ONTAP 9.10.1, the `network interface` CLI commands include an `-rdma-protocols` parameter for NFS over RDMA configurations. Creating network interfaces for NFS over RDMA configurations is supported in System Manager beginning with ONTAP 9.12.1. For more information, see Configure LIFS for NFS over RDMA.
- Beginning with ONTAP 9.11.1, automatic iSCSI LIF failover is available on All-Flash SAN Array (ASA) platforms.

  iSCSI LIF failover is automatically enabled (the failover policy is set to `sfo-partner-only` and the auto-revert value is set to `true`) on newly created iSCSI LIFs if no iSCSI LIFs exist in the specified SVM or if all existing iSCSI LIFs in the specified SVM are already enabled with iSCSI LIF failover.

  If after you upgrade to ONTAP 9.11.1 or later, you have existing iSCSI LIFs in an SVM that have not been enabled with the iSCSI LIF failover feature and you create new iSCSI LIFs in the same SVM, the new iSCSI LIFs assume the same failover policy (`disabled`) of the existing iSCSI LIFs in the SVM.

  iSCSI LIF failover for ASA platforms

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

Beginning with ONTAP 9.12.0, the procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to add a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select + Add .
3. Select one of the following interface roles:
   a. Data
   b. Intercluster
   c. SVM Management
4. Select the protocol:
   a. SMB/CIFS and NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Name the LIF or accept the name generated from your previous selections.
6. Accept the home node or use the drop-down to select one.
7. If at least one subnet is configured in the IPspace of the selected SVM, the subnet drop-down is displayed.
   a. If you select a subnet, choose it from the drop-down.
   b. If you proceed without a subnet, the broadcast domain drop-down is displayed:
      i. Specify the IP address. If the IP address is in use, a warning message will display.
      ii. Specify a subnet mask.
8. Select the home port from the broadcast domain, either automatically (recommended) or by selecting one from the drop-down menu. The Home port control is displayed based on the broadcast domain or subnet selection.
9. Save the network interface.

CLI

Use the CLI to create a LIF

Steps

1. Determine which broadcast domain ports you want to use for the 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
```

Learn more about `network port broadcast-domain show` in the ONTAP command reference.

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

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

   Learn more about `network subnet show` in the ONTAP command reference.

3. Create one or more LIFs on the ports you want to use to access data.

   NetApp recommends creating subnet objects for all LIFs on data SVMs. This is especially important for MetroCluster configurations, where the subnet object enables ONTAP to determine failover targets on the destination cluster because each subnet object has an associated broadcast domain. For instructions, refer to Create a subnet.

```
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` 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.

     Learn more about `network interface revert` in the ONTAP command reference.

   - `-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. Learn more about `network route create` in the ONTAP command reference.

- `-auto-revert` enables 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` Beginning with ONTAP 9.5, you can assign a service policy for the LIF with the `-service-policy` option.
  When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF. In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.
- `-data-protocol` enables you to create a LIF that supports the FCP or NVMe/FC protocols. This option is not required when creating an IP LIF.

4. **Optional**: 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.

      Learn more about `network ndp prefix show` in the ONTAP command reference.

   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.

5. Verify that the LIF interface configuration is correct.

   `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
```

   Learn more about `network interface show` in the ONTAP command reference.

6. Verify that the failover group configuration is as desired.

   `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. 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 ONTAP LIFs

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.

- Beginning with ONTAP 9.5, you can modify the service policy associated with a LIF.

  In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.

- Beginning with ONTAP 9.11.1, the automatic iSCSI LIF failover is available on All-Flash SAN Array (ASA) platforms.

  For pre-existing iSCSI LIFs, meaning LIFs created prior to upgrading to 9.11.1 or later, you can modify the failover policy to enable automatic iSCSI LIF failover.

- ONTAP utilizes Network Time Protocol (NTP) to synchronize time across the cluster. After changing LIF IP addresses, you may need to update the NTP configuration to prevent synchronization failures. For more information, refer to the NetApp Knowledge Base: NTP synchronization fails after LIF IP change.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to edit a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Edit** beside the network interface you want to change.
3. Change one or more of the network interface settings. For details, see Create a LIF.
4. Save your changes.

CLI

Use the CLI to modify a LIF

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
   ```

   Learn more about `network interface modify` in the ONTAP command reference.

2. Verify that the IP addresses are reachable.

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

   Learn more about `network ping` in the ONTAP command reference.

Migrate ONTAP LIFs

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

- BGP LIFs reside on the home-port and cannot be migrated to any other node or port.
- 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 can migrate iSCSI LIFs on All-Flash SAN Array (ASA) platforms running ONTAP 9.11.1 or later.

  Migrating iSCSI LIFs is limited to ports on the home-node or the HA partner.

- If your platform is not an All-Flash SAN Array (ASA) platform running ONTAP version 9.11.1 or later, 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. Learn about creating iSCSI LIFs.

- If you want to migrate a LIF (network interface) for NFS over RDMA, you must ensure the destination port is RoCE capable. You must be running ONTAP 9.10.1 or later to migrate a LIF with the CLI, or ONTAP 9.12.1 to migrate using System Manager. In System Manager, once you have selected your RoCE capable destination-port, you must check the box next to **Use RoCE ports** to complete the migration successfully. Learn more about configuring LIFs for NFS over RDMA.
- VMware VAAI copy offload operations fail when you migrate the source or the destination LIF. Learn about copy off-load:
  - NFS environments
  - SAN environments

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to migrate a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Migrate** beside the network interface you want to change.

   For an iSCSI LIF, in the **Migrate Interface** dialog box, select the destination node and port of the HA partner.

   If you want to migrate the iSCSI LIF permanently, select the checkbox. The iSCSI LIF must be offline before it is permanently migrated. Additionally, once an iSCSI LIF is permanently migrated, it cannot be undone. There is no revert option.

3. Click **Migrate**.
4. Save your changes.

CLI

Use the CLI to migrate a LIF

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
```

Related information

- network interface migrate

Revert a LIF to its home port after an ONTAP node failover or port migration

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 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 LIFs to revert to their home ports.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to revert a network interface to its home port

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **> Revert** beside the network interface you want to change.
3. Select **Revert** to revert a network interface to its home port.

CLI

Use the CLI to revert a LIF to its home port

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`

Learn more about `network interface` in the ONTAP command reference.

Recover an incorrectly configured ONTAP 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.
```

Learn more about `cluster create` in the ONTAP command reference.

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.

Learn more about `network port show` in the ONTAP command reference.

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:

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

   Learn more about `network port modify` in the ONTAP command reference.

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

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

   Learn more about `network port broadcast-domain remove-ports` in the ONTAP command reference.

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.

Related information

- network port reachability show

Delete ONTAP LIFs

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:

```
network interface modify -vserver vserver_name -lif lif_name -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 -vserver vserver_name -lif lif_name`
All LIFs	`network interface delete -vserver vserver_name -lif *`

   Learn more about `network interface delete` in the ONTAP command reference.

   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.

   Learn more about `network interface show` in the ONTAP command reference.

Configure ONTAP virtual IP (VIP) LIFs

Some next-generation data centers use layer-3 (IP) network mechanisms that require LIFs to be failed over across subnets. ONTAP supports virtual IP (VIP) data LIFs and the associated routing protocol, border gateway protocol (BGP), to meet the failover requirements of 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.

Beginning with ONTAP 9.9.1, VIP provides optional default route automation using BGP peer groups to simplify configuration.

ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the `-use-peer-as-next-hop` attribute to `true`. By default, this attribute is `false`.

If you have static routes configured, those are still preferred over these automated default routes.

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 to not send any route updates to the cluster. This reduces the time it takes for communication with the peer to become fully functional and reduces internal memory usage within ONTAP.

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 SVMs in the IPspace used by the peer group. The IPspace used by the peer group is inherited from the BGP LIF.

Beginning with ONTAP 9.16.1, MD5 authentication is supported on BGP peer groups to protect BGP sessions. When MD5 is enabled, BGP sessions can only be established and processed among authorized peers, preventing potential disruptions of the session by an unauthorized actor.

The following fields have been added to the `network bgp peer-group create` and `network bgp peer-group modify` commands:

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

These parameters enable you to configure a BGP peer group with an MD5 signature for enhanced security.

The following requirements apply to using MD5 authentication:

- You can only specify the `-md5-secret` parameter when the `-md5-enabled` parameter is set to `true`.
- IPsec must be enabled globally before you can enable MD5 BGP authentication. The BGP LIF is not required to have an active IPsec configuration. Refer to Configure IP security (IPsec) over wire encryption.
- NetApp recommends that you configure MD5 on the router before configuring it on the ONTAP controller.

Beginning with ONTAP 9.9.1, these fields have been added:

- `-asn` or `-peer-asn` (4-byte value)
  The attribute itself is not new, but it now uses a 4-byte integer.
- `-med`
- `-use-peer-as-next-hop`

You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.

Beginning with ONTAP 9.8, 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.

> While ONTAP supports the above BGP attributes, routers do not need to honor them. NetApp strongly recommends you confirm which attributes are supported by your router and configure BGP peer groups accordingly. For details, refer to the BGP documentation provided by your router.

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_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

- The `-routerid` parameter accepts a dotted-decimal 32-bit value that only needs to be unique within an AS domain. NetApp recommends that you use the node management IP (v4) address for `<router_id>` which guarantees uniqueness.
- Although ONTAP BGP supports 32-bit ASN numbers, only standard decimal notation is supported. Dotted ASN notation, such as 65000.1 instead of 4259840001 for a private ASN, is not supported.

Sample with a 2-byte ASN:

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

Sample with a 4-byte ASN:

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

b. Modify the default BGP configuration:

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

- `<asn_number>` specifies the ASN number. Beginning with ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (1 to 65534 available values). Beginning with ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (1 to 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability.
- `<hold_time>` specifies the hold time in seconds. The default value is 180s.

ONTAP only supports one global `<asn_number>`, `<hold_time>`, and `<router_id>`, even if you configure BGP for multiple IPspaces. The BGP and all IP routing information is completely isolated within one IPspace. An IPspace is equivalent to a virtual routing and forwarding (VRF) instance.

3. Create a BGP LIF for the system SVM:

For the default IPspace, the SVM name is the cluster name. For additional IPspaces, the SVM name is identical to the IPspace name.

```
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>
```

You can use the `default-route-announce` service policy for the BGP LIF or any custom service policy

which contains the "management-bgp" service.

```
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. 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:

   Sample 1: Create a peer group without an auto default route

   In this case, the admin needs to create a static route to the BGP peer.

   ```
   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
   ```

   Sample 2: Create a peer group with an auto default route

   ```
   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
   ```

   Sample 3: Create a peer group with MD5 enabled

   a. Enable IPsec:

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

b. Create the BGP peer group with MD5 enabled:

```
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>}
```

Example using a hex key:

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

Example using a string:

```
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"
```

After you create the BGP peer group, a virtual ethernet port (starting with v0a..v0z,v1a…) is listed when you run the `network port show` command. The MTU of this interface is always reported at 1500. The actual MTU used for traffic is derived from the physical port (BGP LIF), which is determined when traffic is sent. Learn more about `network port show` in the ONTAP command reference.

Create a virtual IP (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 use 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 -failover-policy broadcast-domain-wide
```

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

Beginning with ONTAP 9.5, 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`

Manage BGP peer groups with MD5

Beginning with ONTAP 9.16.1, you can enable or disable MD5 authentication on an existing BGP peer group.

If you enable or disable MD5 on an existing BGP peer group, the BGP connection is terminated and re-created to apply the MD5 configuration changes.

If you want to…	Use this command…
Enable MD5 on an existing BGP peer group	`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>`
Disable MD5 on an existing BGP peer group	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Related information

- ONTAP command reference
- network bgp
- network interface
- security ipsec config modify

Copyright information

Trademark information