Networking components of a cluster

ONTAP 9

NetApp
November 28, 2022
# Table of Contents

Networking components of a cluster .................................................. 1  
Overview .............................................................................................. 1  
Network cabling guidelines ................................................................. 2  
Relationship between broadcast domains, failover groups, and failover policies ................................. 4
Networking components of a cluster

Overview

You should familiarize yourself with the networking components of a cluster before setting up the cluster. Configuring the physical networking components of a cluster into logical components provides the flexibility and multi-tenancy functionality in ONTAP.

The various networking components in a cluster are as follows:

• Physical ports

  Network interface cards (NICs) and host bus adapters (HBAs) provide physical (Ethernet and Fibre Channel) connections from each node to the physical networks (management and data networks).

  For site requirements, switch information, port cabling information, and controller onboard port cabling, see the Hardware Universe at hwu.netapp.com.

• Logical ports

  Virtual local area networks (VLANs) and interface groups constitute the logical ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate ports.

• IPspaces

  You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

• Broadcast domains

  A broadcast domain resides in an IPspace and contains a group of network ports, potentially from many nodes in the cluster, that belong to the same layer 2 network. The ports in the group are used in an SVM for data traffic.

• Subnets

  A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same layer 3 subnet. This pool of IP addresses simplifies IP address allocation during LIF creation.

• Logical interfaces

  A logical interface (LIF) is an IP address or a worldwide port name (WWPN) that is associated with a port. It is associated with attributes such as failover groups, failover rules, and firewall rules. A LIF communicates over the network through the port (physical or logical) to which it is currently bound.

  The different types of LIFs in a cluster are data LIFs, cluster-scoped management LIFs, node-scoped management LIFs, intercluster LIFs, and cluster LIFs. The ownership of the LIFs depends on the SVM where the LIF resides. Data LIFs are owned by data SVMs, node-scoped management LIFs, cluster-scoped management, and intercluster LIFs are owned by the admin SVMs, and cluster LIFs are owned by the cluster SVM.

• DNS zones
DNS zone can be specified during the LIF creation, providing a name for the LIF to be exported through the cluster’s DNS server. Multiple LIFs can share the same name, allowing the DNS load balancing feature to distribute IP addresses for the name according to load.

SVMs can have multiple DNS zones.

- Routing

Each SVM is self-sufficient with respect to networking. An SVM owns LIFs and routes that can reach each of the configured external servers.

The following figure illustrates how the different networking components are associated in a four-node cluster:

---

**Network cabling guidelines**

Network cabling best practices separate traffic into the following networks: cluster, management, and data.

You should cable a cluster so that the cluster traffic is on a separate network from all other traffic. It is an optional, but recommended practice to have network management traffic separated from data and intracluster traffic. By maintaining separate networks, you can achieve better performance, ease of administration, and improved security and management access to the nodes.
The following diagram illustrates the network cabling of a four-node HA cluster that includes three separate networks:

You should follow certain guidelines when cabling network connections:

- Each node should be connected to three distinct networks.

  One network is for management, one is for data access, and one is for intracluster communication. The management and data networks can be logically separated.

- You can have more than one data network connection to each node for improving the client (data) traffic flow.

- A cluster can be created without data network connections, but it must include a cluster interconnect connection.

- There should always be two or more cluster connections to each node, but nodes on FAS22xx systems can be configured with a single 10-GbE cluster port.

For more information on network cabling, see the AFF and FAS System Documentation Center and the
Relationship between broadcast domains, failover groups, and failover policies

Broadcast domains, failover groups, and failover policies work together to determine which port will take over when the node or port on which a LIF is configured fails.

A broadcast domain lists all the ports reachable in the same layer 2 Ethernet network. An Ethernet broadcast packet sent from one of the ports is seen by all other ports in the broadcast domain. This common-reachability characteristic of a broadcast domain is important to LIFs because if a LIF were to fail over to any other port in the broadcast domain, it could still reach every local and remote host that was reachable from the original port.

Failover groups define the ports within a broadcast domain that provide LIF failover coverage for each other. Each broadcast domain has one failover group that includes all its ports. This failover group containing all ports in the broadcast domain is the default and recommended failover group for the LIF. You can create failover groups with smaller subsets that you define, such as a failover group of ports that have the same link speed within a broadcast domain.

A failover policy dictates how a LIF uses the ports of a failover group when a node or port goes down. Consider the failover policy as a type of filter that is applied to a failover group. The failover targets for a LIF (the set of ports to which a LIF can failover) is determined by applying the LIF’s failover policy to the LIF’s failover group in the broadcast domain.

You can view the failover targets for a LIF using the following CLI command:

```
network interface show -failover
```

NetApp strongly recommends using the default failover policy for your LIF type.

Decide which LIF failover policy to use

Decide whether to use the recommended, default failover policy or whether to change it based on your LIF type and environment.

Failover policy decision tree
Consider the following when choosing a failover policy:

- Choose the default **system-defined** failover policy to optimize node and cluster survivability, but risk not being able to fail over to more than one other node.

- Choose the **broadcast-domain-wide** failover policy to optimize LIF survivability beyond two failed nodes, but risk cascading node failures.

**Default failover policies by LIF type**

<table>
<thead>
<tr>
<th>LIF type</th>
<th>Default failover policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP LIFs</td>
<td>disabled</td>
<td>LIF does not fail over to another port.</td>
</tr>
<tr>
<td>Cluster LIFs</td>
<td>local-only</td>
<td>LIF fails over to ports on the same node only.</td>
</tr>
<tr>
<td>Cluster-mgmt LIF</td>
<td>broadcast-domain-wide</td>
<td>LIF fails over to ports in the same broadcast domain, on any and every node in the cluster.</td>
</tr>
<tr>
<td>Type</td>
<td>Mode</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Intercluster LIFs</td>
<td>local-only</td>
<td>LIF fails over to ports on the same node only.</td>
</tr>
<tr>
<td>NAS data LIFs</td>
<td>system-defined</td>
<td>LIF fails over to one other node that is not the HA partner.</td>
</tr>
<tr>
<td>Node management LIFs</td>
<td>local-only</td>
<td>LIF fails over to ports on the same node only.</td>
</tr>
<tr>
<td>SAN data LIFs</td>
<td>disabled</td>
<td>LIF does not fail over to another port.</td>
</tr>
</tbody>
</table>

The `sfo-partner-only` failover policy is not a default, but can be used when you want the LIF to fail over to a port on the home node or SFO partner only.