



LIF overview

ONTAP 9

NetApp
February 06, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking/configure_lifs_cluster_administrators_only_overview.html on February 06, 2026. Always check docs.netapp.com for the latest.

Table of Contents

LIF overview	1
Learn about LIF configuration for an ONTAP cluster	1
LIF failover and giveback	2
Learn about ONTAP LIF compatibility with port types	3
Supported LIF service policies and roles for your ONTAP version	4
Learn about ONTAP LIFs and service policies	4
Service policies for system SVMs	5
Service policies for data SVMs	7
Data-core service	9
Client-side LIF service	10

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:

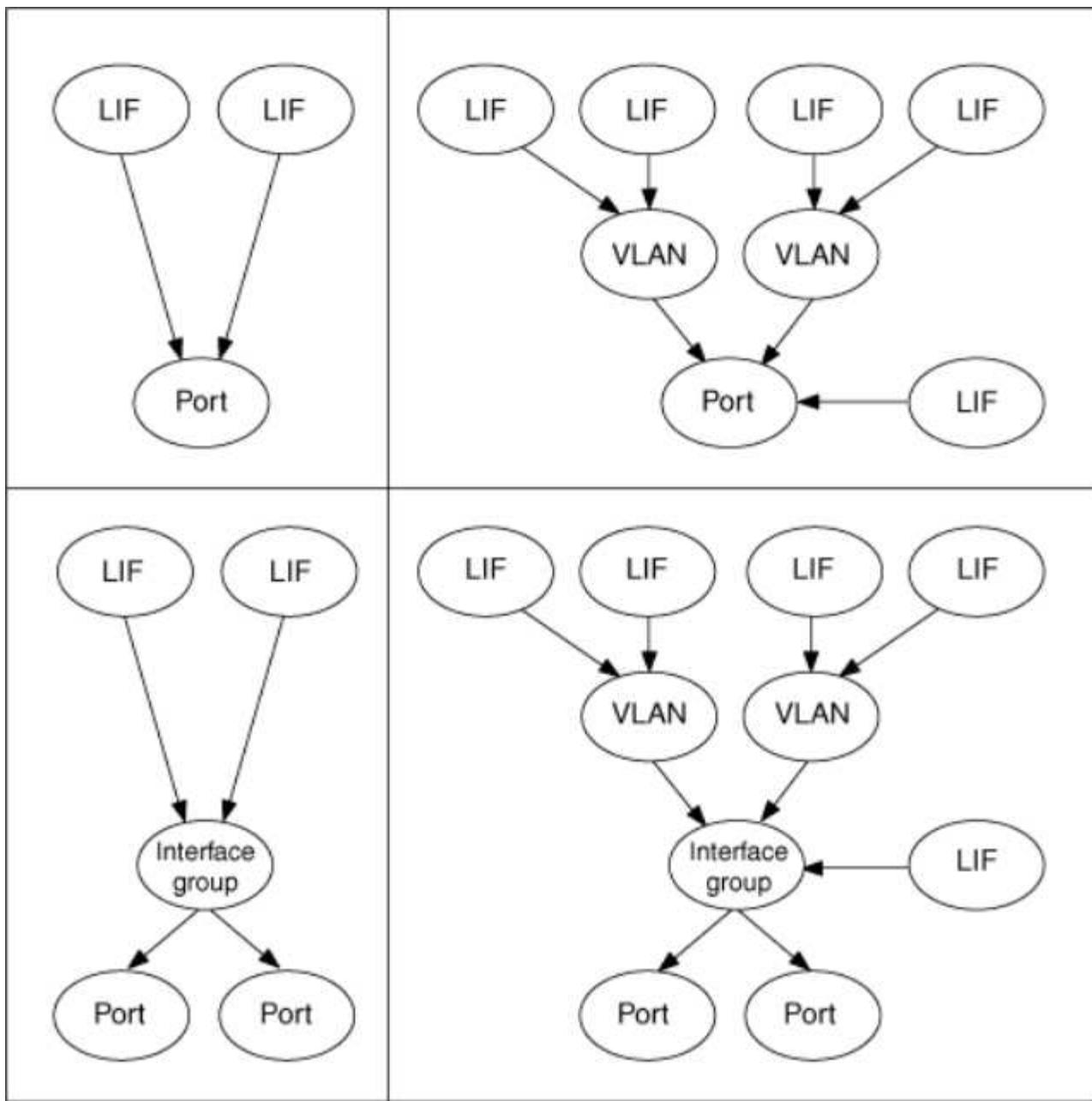
- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs
- Virtual IP (VIP) ports

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 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	<p>A LIF that is associated with a storage virtual machine (SVM) and is used for communicating with clients.</p> <p>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 <code>mgmt</code>.</p> <p>Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.</p>
Cluster LIF	<p>A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on cluster ports.</p> <p>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.</p>

Cluster management LIF	<p>LIF that provides a single management interface for the entire cluster.</p> <p>A cluster management LIF can fail over to any node in the cluster. It cannot fail over to cluster or intercluster ports</p>
Intercluster LIF	<p>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.</p> <p>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.</p>
Node management LIF	<p>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.</p>
VIP LIF	<p>A VIP LIF is any data LIF created on a VIP port. To learn more, see Configure virtual IP (VIP) LIFs.</p>

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 <code>management-log-forwarding</code> 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](#)

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.