



General networking topics (ONTAP 9.7 and earlier)

System Manager Classic

NetApp

September 05, 2025

Table of Contents

General networking topics (ONTAP 9.7 and earlier)	1
Removing a NIC from the node (ONTAP 9.7 or earlier)	1
LIF roles (ONTAP 9.5 and earlier)	1
LIF security	1
LIF failover	2
LIF routing	2
LIF rebalancing	3
LIF primary traffic types	3
Configure DNS services (ONTAP 9.7 and earlier)	3
Configure dynamic DNS on the SVM	5

General networking topics (ONTAP 9.7 and earlier)

Removing a NIC from the node (ONTAP 9.7 or earlier)

This topic applies to ONTAP 9.7 or earlier. You might have to remove a faulty NIC from its slot or move the NIC to another slot for maintenance purposes.

Before you begin

- All LIFs hosted on the NIC ports must have been migrated or deleted.
- None of the NIC ports can be the home ports of any LIFs.
- You must have advanced privileges to delete the ports from a NIC.

Steps

1. Delete the ports from the NIC:

```
network port delete
```

2. Verify that the ports have been deleted:

```
network port show
```

3. Repeat step 1, if the output of the network port show command still shows the deleted port.

LIF roles (ONTAP 9.5 and earlier)

LIFs with different roles have different characteristics. A LIF role determines the kind of traffic that is supported over the interface, along with the failover rules that apply, the firewall restrictions that are in place, the security, the load balancing, and the routing behavior for each LIF. A LIF can have any one of the following roles: cluster, cluster management, data, intercluster, node management, and undef (undefined). The undef role is used for BGP LIFs.

Beginning with ONTAP 9.6, LIF roles are deprecated. You should specify service policies for LIFs instead of a role. It is not necessary to specify a LIF role when creating a LIF with a service policy.

LIF security

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Require private IP subnet?	No	Yes	No	No	No
Require secure network?	No	Yes	No	No	Yes

Default firewall policy	Very restrictive	Completely open	Medium	Medium	Very restrictive
Is firewall customizable?	Yes	No	Yes	Yes	Yes

LIF failover

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Default behavior	Only those ports in the same failover group that are on the LIF's home node and on a non-SFO partner node	Only those ports in the same failover group that are on the LIF's home node	Only those ports in the same failover group that are on the LIF's home node	Any port in the same failover group	Only those ports in the same failover group that are on the LIF's home node
Is customizable?	Yes	No	Yes	Yes	Yes

LIF routing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
When is a default route needed?	When clients or domain controller are on different IP subnet	Never	When any of the primary traffic types require access to a different IP subnet	When administrator is connecting from another IP subnet	When other intercluster LIFs are on a different IP subnet
When is a static route to a specific IP subnet needed?	Rare	Never	Rare	Rare	When nodes of another cluster have their intercluster LIFs in different IP subnets
When is a static host route to a specific server needed?	To have one of the traffic types listed under node management LIF, go through a data LIF rather than a node management LIF. This requires a corresponding firewall change.	Never	Rare	Rare	Rare

LIF rebalancing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
DNS: use as DNS server?	Yes	No	No	No	No
DNS: export as zone?	Yes	No	No	No	No

LIF primary traffic types

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Primary traffic types	NFS server, CIFS server, NIS client, Active Directory, LDAP, WINS, DNS client and server, iSCSI and FC server	Intracluster	SSH server, HTTPS server, NTP client, SNMP, AutoSupport client, DNS client, loading software updates	SSH server, HTTPS server	Cross-cluster replication

Configure DNS services (ONTAP 9.7 and earlier)

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database.

In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.

- Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



The vserver services name-service dns create command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name	Server	Status	Status Details
vs1		10.0.0.50	up	Response time (msec): 2
vs1		10.0.0.51	up	Response time (msec): 2

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

          Vserver: vs1
          CIFS Server NetBIOS Name: CIFS_VS1
          NetBIOS Domain/Workgroup Name: EXAMPLE
          Fully Qualified Domain Name: EXAMPLE.COM
          Organizational Unit: CN=Computers
          Default Site Used by LIFs Without Site Membership:
          Workgroup Name: -
          Kerberos Realm: -
          Authentication Style: domain
          CIFS Server Administrative Status: up
          CIFS Server Description:
          List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver	FQDN	TTL
vs1	true	true		vs1.example.com	24h

Copyright information

Copyright © 2025 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—without 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.