



Get started

ONTAP 9

NetApp
February 02, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking/networking_reference.html on February 02, 2026. Always check docs.netapp.com for the latest.


Table of Contents

- Get started 1
 - Visualize the ONTAP network using System Manager 1
 - Examples 1
 - System Manager Network Visualization video 1
 - Learn about the networking components of an ONTAP cluster 2
 - Best practices for ONTAP network cabling 4
 - Determine which LIF failover policy to use in an ONTAP network 6
 - Decide which LIF failover policy to use 6

Get started

Visualize the ONTAP network using System Manager

Beginning with ONTAP 9.8, you can use System Manager to display a graphic that shows the components and configuration of your network, allowing you to see the network connection paths across hosts, ports, SVMs, volumes, and more. Beginning with ONTAP 9.12.1, you can view the LIF and subnet association on the Network Interfaces grid.

The graphic displays when you select **Network > Overview** or when you select  from the **Network** section of the Dashboard.

The following categories of components are shown in the graphic:


- Hosts
- Storage ports
- Network interfaces
- Storage VMs
- Data access components

Each section shows additional details that you can hover your mouse over or select to perform network management and configuration tasks.

If you are using classic System Manager (available only in ONTAP 9.7 and earlier), see [Managing the network](#).

Examples

The following are some examples of the many ways you can interact with the graphic to view details about each component or initiate actions to manage your network:

- Click on a host to see its configuration: the ports, network interfaces, storage VMs, and data access components associated with it.
- Hover the mouse over the number of volumes in a storage VM to select a volume to view its details.
- Select an iSCSI interface to view its performance over the last week.
- Click on  next to a component to initiate actions to modify that component.
- Quickly determine where problems might occur in your network, indicated by an "X" next to unhealthy components.

System Manager Network Visualization video

ONTAP System Manager 9.8

Network Visualization



Tech Clip



Learn about the networking components of an ONTAP cluster

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

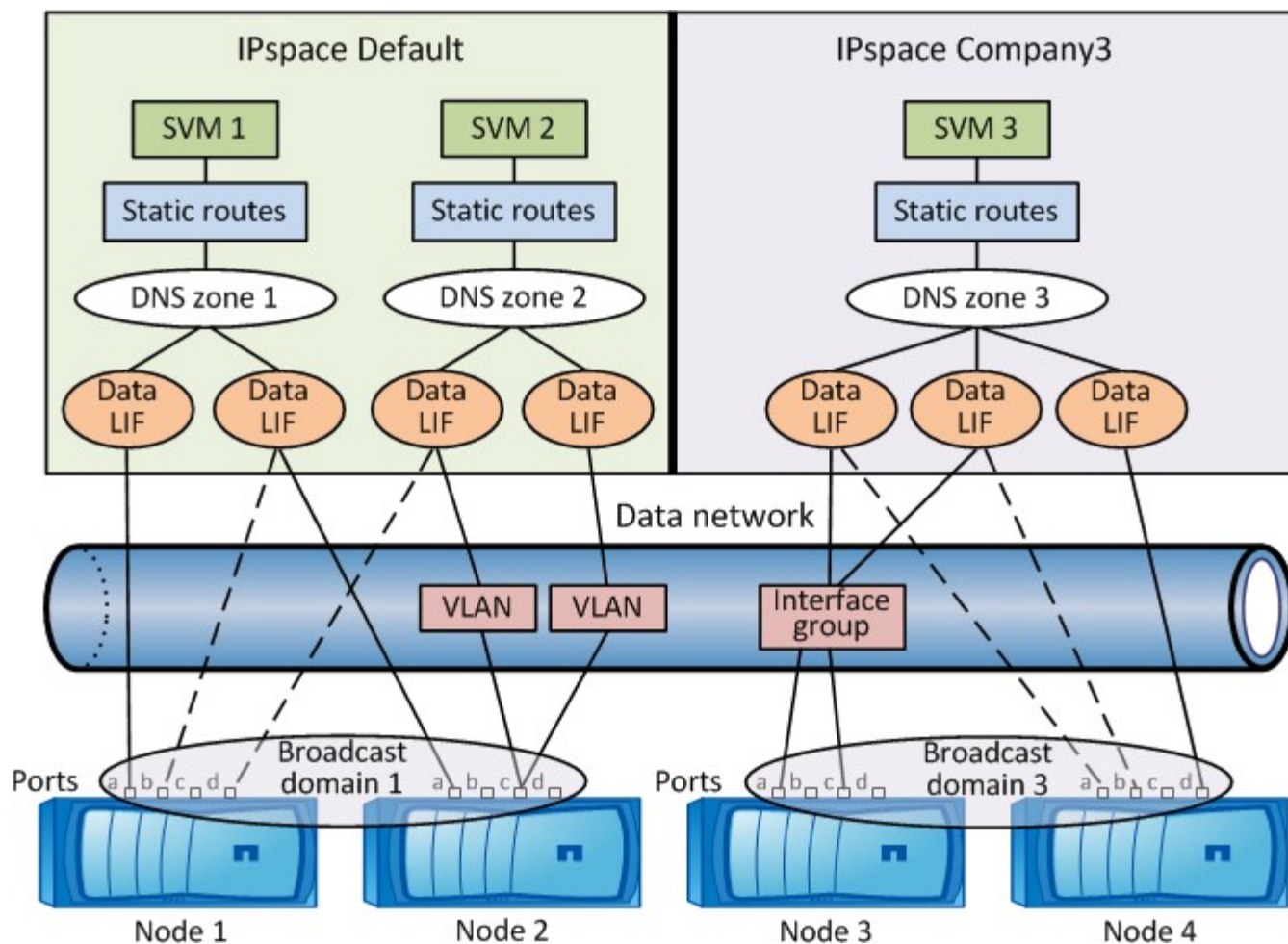
DNS zone can be specified during the LIF creation, providing a name for the LIF to be exported through the cluster's DNS server. Multiple LIFs can share the same name, allowing the DNS load balancing feature to distribute IP addresses for the name according to load.

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:

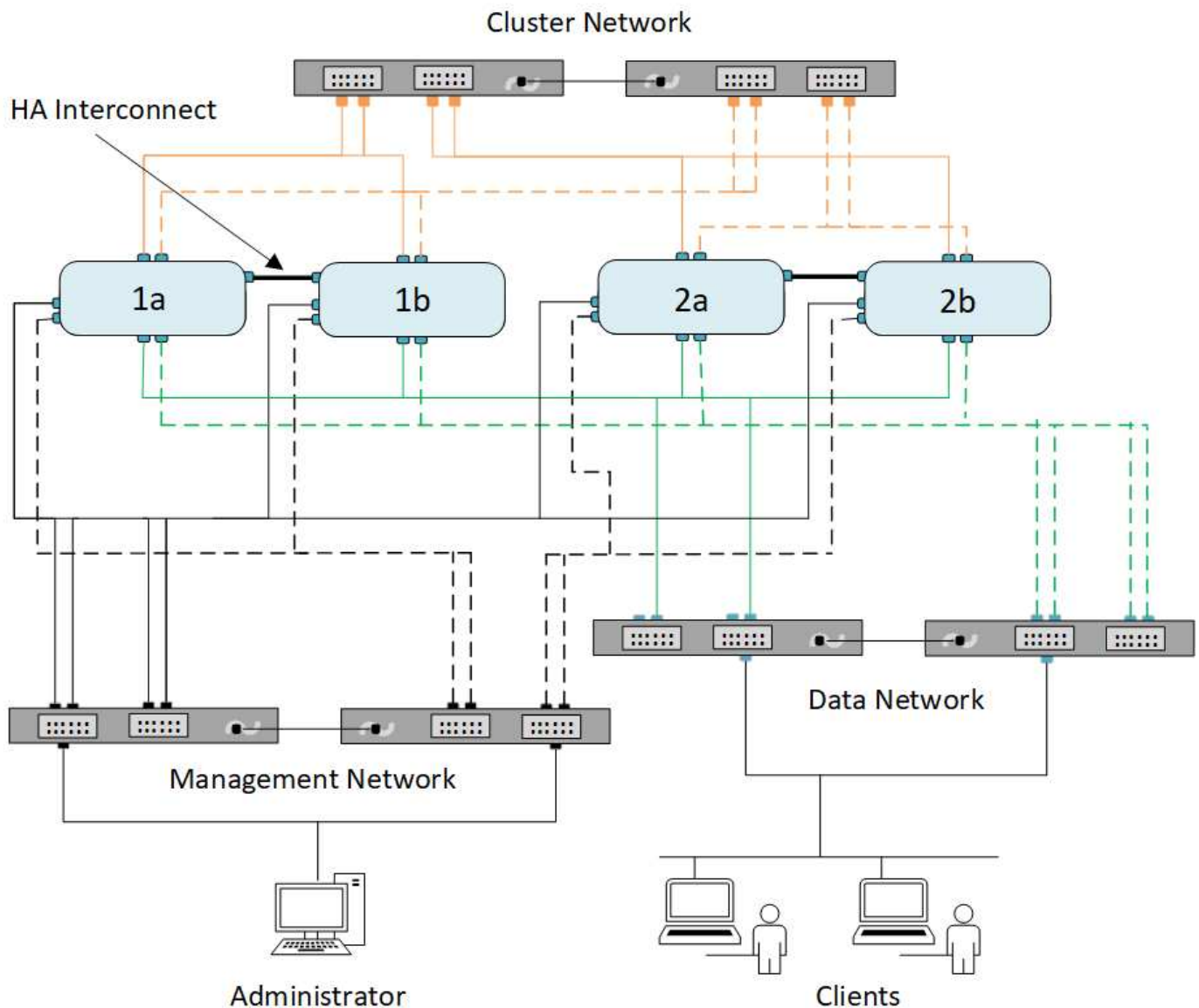


Best practices for ONTAP network cabling

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 intracuster 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.

For more information on network cabling, see the [AFF and FAS System Documentation Center](#) and the [Hardware Universe](#).

Determine which LIF failover policy to use in an ONTAP network

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:

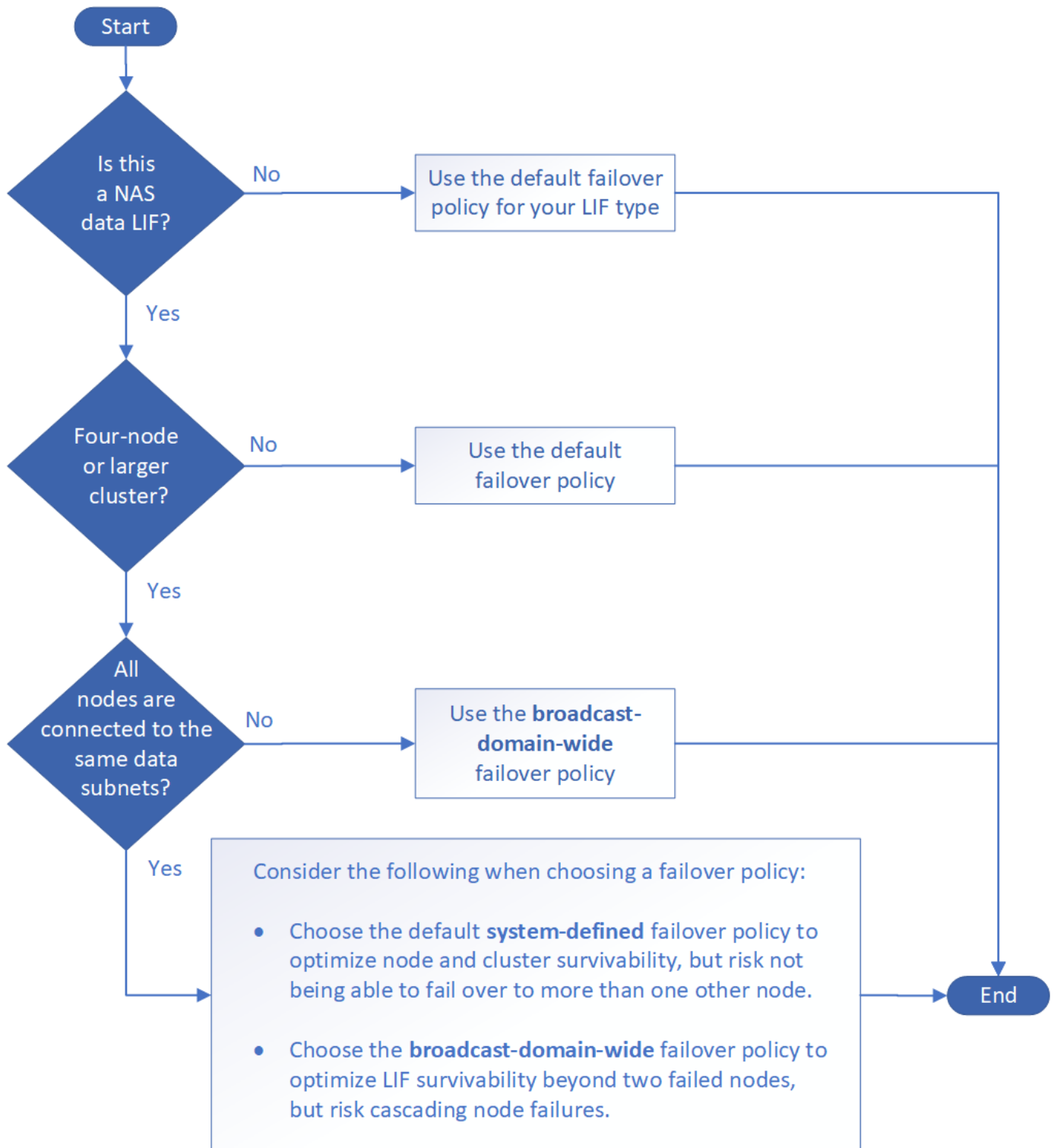
```
network interface show -failover
```

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



Default failover policies by LIF type

LIF type	Default failover policy	Description
BGP LIFs	disabled	LIF does not fail over to another port.
Cluster LIFs	local-only	LIF fails over to ports on the same node only.
Cluster-mgmt LIF	broadcast-domain-wide	LIF fails over to ports in the same broadcast domain, on any and every node in the cluster.

Intercluster LIFs	local-only	LIF fails over to ports on the same node only.
NAS data LIFs	system-defined	LIF fails over to one other node that is not the HA partner.
Node management LIFs	local-only	LIF fails over to ports on the same node only.
SAN data LIFs	disabled	LIF does not fail over to another port.

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.

Related information

- [network interface 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—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.