



# **Upgrade considerations**

## **ONTAP System Manager**

NetApp  
April 02, 2021

# Table of Contents

- Upgrade considerations ..... 1
- Network features by release ..... 1
- Verify your network configuration after upgrading ..... 6

# Upgrade considerations

## Network features by release

Analyze the impact of network features available with each ONTAP 9 release.

Available beginning	Feature	Description
ONTAP 9.8	Auto port placement	<p>ONTAP can automatically configure broadcast domains, select ports, and help configure network interfaces (LIFs), virtual LANs (VLANs), and link aggregation groups (LAGs) based on reachability and network topology detection.</p> <p>When you first create a cluster, ONTAP automatically discovers the networks connected to ports and configures the needed broadcast domains based on layer 2 reachability. You no longer have to configure broadcast domains manually.</p> <p>A new cluster will continue to be created with two IPspaces:</p> <p><b>Cluster IPspace:</b> Containing one broadcast domain for the cluster interconnect. You should never touch this configuration.</p> <p><b>Default IPspace:</b> Containing one or more broadcast domains for the remaining ports. Depending on your network topology, ONTAP configures additional broadcast domains as needed: Default-1, Default-2, and so on. You can rename these broadcast domains if desired, but do not modify which ports are configured in these broadcast domains.</p> <p>When you configure network interfaces, the home port selection is optional. If you do not manually select a home port, ONTAP will attempt to assign an appropriate home port in the same broadcast domain as other network interfaces in the same subnet.</p> <p>When creating a VLAN or adding the first port to a newly created LAG, ONTAP will attempt to automatically assign the VLAN or LAG to the appropriate broadcast domain based on its layer 2 reachability.</p> <p>By automatically configuring broadcast domains and ports, ONTAP helps to ensure that clients maintain access to their data during failover to another port or node in the cluster.</p> <p>Finally, ONTAP sends EMS messages when it detects that the port reachability is incorrect and provides the "network port reachability repair" command to automatically repair common misconfigurations.</p>

Available beginning	Feature	Description
ONTAP 9.8	Internet Protocol security (IPsec) over wire encryption	<p>To ensure data is continuously secure and encrypted, even while in transit, ONTAP uses the IPsec protocol in transport mode. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.</p> <p>Once IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.</p> <p><a href="#">Configure IP security (IPsec) over wire encryption</a></p>
ONTAP 9.8	Virtual IP (VIP) expansion	<p>New fields have been added to the <code>network bgp peer-group</code> command. This expansion allows you to configure two additional Border Gateway Protocol (BGP) attributes for Virtual IP (VIP).</p> <p><b>AS path prepend:</b> Other factors being equal, BGP prefers to select the route with shortest AS (autonomous system) Path. You can use the optional AS path prepend attribute to repeat an autonomous system number (ASN), which increases the length of the AS path attribute. The route update with the shortest AS path will be selected by the receiver.</p> <p><b>BGP community:</b> The BGP community attribute is a 32-bit tag that can be assigned to the route updates. Each route update can have one or more BGP community tags. The neighbors receiving the prefix can examine the community value and take actions like filtering or applying specific routing policies for redistribution.</p>
ONTAP 9.8	Switch CLI simplification	<p>To simplify switch commands, the cluster and storage switch CLIs are consolidated. The consolidated switch CLIs include Ethernet switches, FC switches, and ATTO protocol bridges.</p> <p>Instead of using separate "system cluster-switch" and "system storage-switch" commands, you now use "system switch". For the ATTO protocol bridge, instead of using "storage bridge", use "system bridge".</p> <p>Switch health monitoring has similarly expanded to monitor the storage switches as well as the cluster interconnect switch. You can view health information for the cluster interconnect under "cluster_network" in the "client_device" table. You can view health information for a storage switch under "storage_network" in the "client_device" table.</p>

Available beginning	Feature	Description
ONTAP 9.8	IPv6 variable length	<p>The supported IPv6 variable prefix length range has increased from 64 to 1 through 127 bits. A value of bit 128 remains reserved for virtual IP (VIP).</p> <p>When upgrading, non-VIP LIF lengths other than 64 bits are blocked until the last node is updated.</p> <p>When reverting an upgrade, the revert checks any non-VIP LIFs for any prefix other than 64 bits. If found, the check blocks the revert until you delete or modify the offending LIF. VIP LIFs are not checked.</p>
ONTAP 9.7	Automatic portmap service	<p>The portmap service maps RPC services to the ports on which they listen.</p> <p>The portmap service is always accessible in ONTAP 9.3 and earlier, is configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically starting in ONTAP 9.7.</p> <p><b>In ONTAP 9.3 and earlier:</b> The portmap service (rpcbind) is always accessible on port 111 in network configurations that rely on the built-in ONTAP firewall rather than a third-party firewall.</p> <p><b>From ONTAP 9.4 through ONTAP 9.6:</b> You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.</p> <p><b>Starting in ONTAP 9.7:</b> The portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.</p> <p><a href="#">Portmap service configuration</a></p>
ONTAP 9.7	Cache search	<p>You can cache NIS <code>netgroup.byhost</code> entries using the <code>vserver services name-service nis-domain netgroup-database</code> commands.</p>
ONTAP 9.6	CUBIC	<p>CUBIC is the default TCP congestion control algorithm for ONTAP hardware. CUBIC replaced the ONTAP 9.5 and earlier default TCP congestion control algorithm, NewReno.</p> <p>CUBIC addresses the problems of long, fat networks (LFNs), including high round trip times (RTTs). CUBIC detects and avoids congestion. CUBIC improves performance for most environments.</p>

Available beginning	Feature	Description
ONTAP 9.6	LIF service policies replace LIF roles	<p>You can assign service policies (instead of LIF roles) 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.</p> <p>ONTAP supports service policies starting with ONTAP 9.5; however, service policies can only be used to configure a limited number of services. Starting with ONTAP 9.6, LIF roles are deprecated and service policies are supported for all types of services.</p> <p><a href="#">LIFs and service policies</a></p>
ONTAP 9.5	NTPv3 support	<p>Network Time Protocol (NTP) version 3 includes symmetric authentication using SHA-1 keys, which increases network security.</p>
ONTAP 9.5	SSH login security alerts	<p>When you log in as a Secure Shell (SSH) admin user, you can view information about previous logins, unsuccessful attempts to log in, and changes to your role and privileges since your last successful login.</p>
ONTAP 9.5	LIF service policies	<p>You can create new service policies or use a built-in policy. 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.</p> <p><a href="#">LIFs and service policies</a></p>
ONTAP 9.5	VIP LIFs and BGP support	<p>A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a border gateway protocol (BGP) LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces.</p> <p><a href="#">Create a virtual IP (VIP) data LIF</a></p>
ONTAP 9.5	Multipath routing	<p>Multipath routing provides load balancing by utilizing all the available routes to a destination.</p> <p><a href="#">Enable multipath routing</a></p>
ONTAP 9.4	Portmap service	<p>The portmap service maps remote procedure call (RPC) services to the ports on which they listen.</p> <p>The portmap service is always accessible in ONTAP 9.3 and earlier. Starting in ONTAP 9.4, the portmap service is configurable.</p> <p>You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.</p> <p><a href="#">Portmap service configuration</a></p>

Available beginning	Feature	Description
ONTAP 9.4	SSH MFA for LDAP or NIS	SSH multi-factor authentication (MFA) for LDAP or NIS uses a public key and nsswitch to authenticate remote users.
ONTAP 9.3	SSH MFA	SSH MFA for local administrator accounts use a public key and a password to authenticate local users.
ONTAP 9.3	SAML authentication	You can use Security Assertion Markup Language (SAML) authentication to configure MFA for web services such as Service Processor Infrastructure (spi), ONTAP APIs, and OnCommand System Manager.
ONTAP 9.2	SSH login attempts	You can configure the maximum number of unsuccessful SSH login attempts to protect against brute force attacks.
ONTAP 9.2	Digital security certificates	ONTAP provides enhanced support for digital certificate security with Online Certificate Status Protocol (OCSP) and pre-installed default security certificates.
ONTAP 9.2	Fastpath	<p>As part of a networking stack update for improved performance and resiliency, fast path routing support was removed in ONTAP 9.2 and later releases because it made it difficult to identify problems with improper routing tables. Therefore, it is no longer possible to set the following option in the nodeshell, and existing fast path configurations are disabled when upgrading to ONTAP 9.2 and later:</p> <pre>ip.fastpath.enable</pre> <p><a href="#">Network traffic not sent or sent out of an unexpected interface after upgrade to 9.2 due to elimination of IP Fastpath</a></p>
ONTAP 9.1	Security with SNMPv3 traphosts	<p>You can configure SNMPv3 traphosts with the User-based Security Model (USM) security. With this enhancement, SNMPv3 traps can be generated by using a predefined USM user's authentication and privacy credentials.</p> <p><a href="#">Configure traphosts to receive SNMP notifications</a></p>
ONTAP 9.0	IPv6	<p>Dynamic DNS (DDNS) name service is available on IPv6 LIFs.</p> <p><a href="#">Create a LIF</a></p>
ONTAP 9.0	LIFs per node	<p>The supported number of LIFs per node has increased for some systems. See the Hardware Universe for the number of LIFs supported on each platform for a specified ONTAP release.</p> <p><a href="#">Create a LIF</a></p> <p><a href="#">NetApp hardware universe</a></p>
ONTAP 9.0	LIF management	<p>ONTAP and System Manager automatically detect and isolate network port failures. LIFs are automatically migrated from degraded ports to healthy ports.</p> <p><a href="#">Monitor the health of network ports</a></p>

Available beginning	Feature	Description
ONTAP 9.0	LLDP	<p>Link Layer Discovery Protocol (LLDP) provides a vendor-neutral interface for verifying and troubleshooting cabling between an ONTAP system and a switch or router. It is an alternative to Cisco Discovery Protocol (CDP), a proprietary link layer protocol developed by Cisco Systems.</p> <p><a href="#">Enable or Disable LLDP</a></p>
ONTAP 9.0	UC compliance with DSCP marking	<p>Unified Capability (UC) compliance with Differentiated Services Code Point (DSCP) marking.</p> <p>Differentiated Services Code Point (DSCP) marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance. You can enable DSCP marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code.</p> <p>If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:</p> <p><b>0x0A (10):</b> The default value for data protocols/traffic.</p> <p><b>0x30 (48):</b> The default value for control protocols/traffic.</p> <p><a href="#">DSCP marking for US compliance</a></p>
ONTAP 9.0	SHA-2 password hash function	<p>To enhance password security, ONTAP 9 supports the SHA-2 password hash function and uses SHA-512 by default for hashing newly created or changed passwords.</p> <p>Existing user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to ONTAP 9 or later, and users can continue to access their accounts. However, it is strongly recommended that you migrate MD5 accounts to SHA-512 by having users change their passwords.</p>
ONTAP 9.0	FIPS 140-2 support	<p>You can enable the Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.</p> <p>By default, the FIPS 140-2 only mode is disabled.</p> <p><a href="#">Configure network security using Federal Information Processing Standards (FIPS)</a></p>

## Verify your network configuration after upgrading

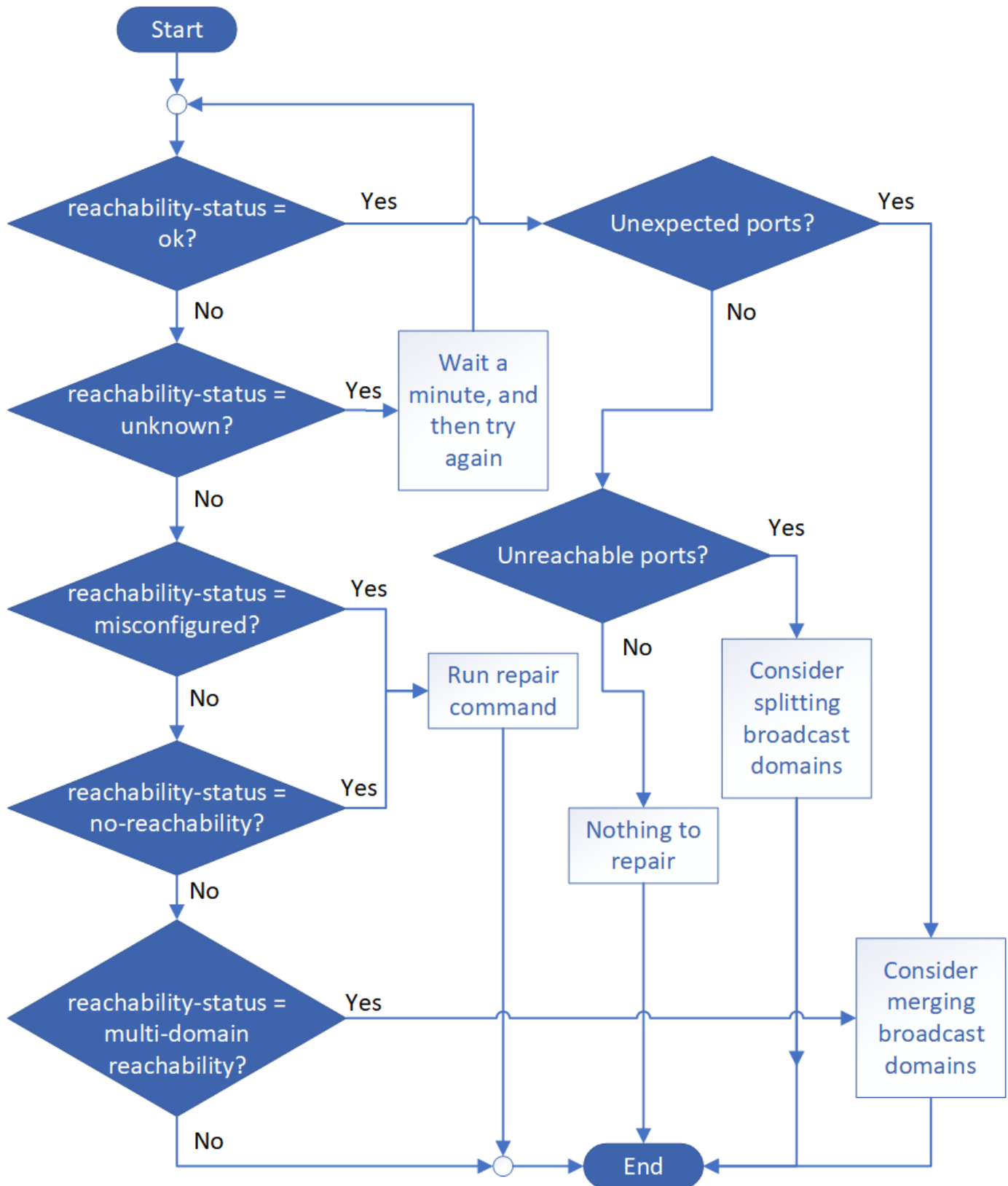
After an upgrade to ONTAP 9.8, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

Use the following command to verify each port has reachability to its expected broadcast domain:



```
network port reachability show -detail
```

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.



reachability-status	Description
ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see <a href="#">Merge broadcast domains</a>.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see <a href="#">Split broadcast domains</a>.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre data-bbox="475 804 1211 831">network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre data-bbox="475 1140 1211 1167">network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a> or <a href="#">Repair port reachability</a>.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

## Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.