Upgrade considerations

ONTAP 9

NetApp
December 14, 2022

Table of Contents

Upgrade considerations

Network features by release

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

Available beginning	Feature	Description
ONTAP 9.12.1	LIF Services	You can use the `management-log-forwarding` service to control which LIFs are used to forward audit logs to a remote syslog server. For more information on the log forwarding feature, see Manage audit log destinations. LIFs and service policies in ONTAP 9.6 and later
ONTAP 9.12.1	System Manager networking enhancements	System Manager offers more control over the subnet and home port selection during network interface creation. System Manager also supports the configuration of NFS/RDMA connections. Create SVMs

ONTAP 9.12.0	System Manager networking enhancements	System Manager offers more control over networking functions, including the following: • Link Aggregation Groups (LAGs) • VLANs • Broadcast domains • Subnets • Network interfaces Combine physical ports to create interface groups Configure VLANs over physical ports Add a broadcast domain Delete a broadcast domain Display subnets Create a subnet Delete a subnet Add or remove IP addresses from a subnet Change subnet properties Create a LIF Modify a LIF Migrate a LIF Revert a LIF to its home port Viewing and managing your network
ONTAP 9.11.1	iSCSI LIF Failover	The new iSCSI LIF failover feature supports automatic and manual migration of iSCSI LIFs in an SFO partner failover and in a local failover. It is available for All SAN Array (ASA) platforms. iSCSI LIF failover for ASA platforms
ONTAP 9.11.1	LIF Services	New client-side LIF services provide more control over which LIFs are used for outbound AD, DNS, LDAP, and NIS requests. LIFs and service policies in ONTAP 9.6 and later

ONTAP 9.11.1	Link Layer Discovery Protocol (LLDP)	The cluster network supports LLDP to allow ONTAP to work with cluster switches that do not support Cisco Discovery Protocol (CDP). Display network connectivity with neighbor discovery protocols
ONTAP 9.10.1	Automatic detection and repair recommendations for network wiring issues	ONTAP can automatically detect and recommend corrections for network wiring issues based on a broadcast domain constituent's (ethernet ports) layer-2 reachability. When a port reachability issue is detected, System Manager recommends a repair operation to resolve the issue. Automatic detection and repair recommendations for network wiring issues
ONTAP 9.10.1	Internet Protocol security (IPsec) certificate authentication	IPsec policies now support pre-shared keys (PSKs) and certificates for authentication. • Policies configured with PSKs require sharing of the key among all clients in the policy. • Policies configured with certificates do not require sharing of the key among clients because each client can have its own unique certificate for authentication. Configure IP security (IPsec) over wire encryption
ONTAP 9.10.1	LIF services	Firewall policies are deprecated and wholly replaced with LIF service policies. A new NTP LIF service provides more control over which LIFs are used for outbound NTP requests. LIFs and service policies in ONTAP 9.6 and later
ONTAP 9.10.1	NFS over RDMA	ONTAP offers support for NFS over RDMA, a higher performance realization of NFSv4.0 for customers with the NVIDIA GDX ecosystem. Utilizing RDMA adapters allows memory to be copied directly from storage to the GPU, circumventing the CPU overhead. NFS over RDMA

ONTAP 9.9.1	Cluster resiliency	The following cluster resiliency and diagnostic improvements improve the customer experience: • Port monitoring and avoidance: ◦ In two-node switchless cluster configurations, the system avoids ports that experience total packet loss (connectivity loss). Previously this functionality was only available in switched configurations. • Automatic node failover: ◦ If a node cannot serve data across its cluster network, that node should not own any disks. Instead its HA partner should take over, if the partner is healthy. • Commands to analyze connectivity issues: ◦ Use the following command to display which cluster paths are experiencing packet loss: `network interface check cluster-connectivity show`

ONTAP 9.9.1	VIP LIF enhancements	The following fields have been added to extend virtual IP (VIP) border gateway protocol (BGP) functionality: • -asn or -peer-asn (4-byte value) The attribute itself is not new, but it now uses a 4-byte integer. • -med • -use-peer-as-next-hop The `asn_integer` parameter specifies the autonomous system number (ASN) or peer ASN. • Beginning with ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (0 - 64511 available values). • Beginning with ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (65536 - 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability. You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred. VIP BGP provides default route automation using BGP peer grouping to simplify configuration. ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the `-use-peer-as-next-hop` attribute to `true`. By default, this attribute is `false`. Configure virtual IP (VIP) LIFs

ONTAP 9.8	Auto port placement	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. 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. A new cluster will continue to be created with two IPspaces: **Cluster IPspace**: Containing one broadcast domain for the cluster interconnect. You should never touch this configuration. **Default IPspace**: 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. 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. 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. 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. 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.
ONTAP 9.8	Internet Protocol security (IPsec) over wire encryption	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 protocols. IPsec provides the only encryption in flight option for iSCSI traffic. 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. Configure IP security (IPsec) over wire encryption

ONTAP 9.8	Virtual IP (VIP) expansion	New fields have been added to the `network bgp peer-group` command. This expansion allows you to configure two additional Border Gateway Protocol (BGP) attributes for Virtual IP (VIP). **AS path prepend**: 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. **BGP community**: 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.
ONTAP 9.8	Switch CLI simplification	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. 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". 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.
ONTAP 9.8	IPv6 variable length	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). When upgrading, non-VIP LIF lengths other than 64 bits are blocked until the last node is updated. 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.

ONTAP 9.7	Automatic portmap service	The portmap service maps RPC services to the ports on which they listen. 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 beginning with ONTAP 9.7. **In ONTAP 9.3 and earlier**: 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. **From ONTAP 9.4 through ONTAP 9.6**: You can modify firewall policies to control whether the portmap service is accessible on particular LIFs. **Beginning with ONTAP 9.7**: The portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service. Portmap service configuration
ONTAP 9.7	Cache search	You can cache NIS `netgroup.byhost` entries using the `vserver services name-service nis-domain netgroup-database` commands.
ONTAP 9.6	CUBIC	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. 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.
ONTAP 9.6	LIF service policies replace LIF roles	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. ONTAP supports service policies beginning with ONTAP 9.5; however, service policies can only be used to configure a limited number of services. Beginning with with ONTAP 9.6, LIF roles are deprecated and service policies are supported for all types of services. LIFs and service policies
ONTAP 9.5	NTPv3 support	Network Time Protocol (NTP) version 3 includes symmetric authentication using SHA-1 keys, which increases network security.

ONTAP 9.5	SSH login security alerts	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.
ONTAP 9.5	LIF service policies	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. LIFs and service policies
ONTAP 9.5	VIP LIFs and BGP support	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. Create a virtual IP (VIP) data LIF
ONTAP 9.5	Multipath routing	Multipath routing provides load balancing by utilizing all the available routes to a destination. Enable multipath routing
ONTAP 9.4	Portmap service	The portmap service maps remote procedure call (RPC) services to the ports on which they listen. The portmap service is always accessible in ONTAP 9.3 and earlier. Beginning with ONTAP 9.4, the portmap service is configurable. You can modify firewall policies to control whether the portmap service is accessible on particular LIFs. Portmap service configuration
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	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: `ip.fastpath.enable` Network traffic not sent or sent out of an unexpected interface after upgrade to 9.2 due to elimination of IP Fastpath
ONTAP 9.1	Security with SNMPv3 traphosts	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. Configure traphosts to receive SNMP notifications
ONTAP 9.0	IPv6	Dynamic DNS (DDNS) name service is available on IPv6 LIFs. Create a LIF
ONTAP 9.0	LIFs per node	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. Create a LIF NetApp hardware universe
ONTAP 9.0	LIF management	ONTAP and System Manager automatically detect and isolate network port failures. LIFs are automatically migrated from degraded ports to healthy ports. Monitor the health of network ports
ONTAP 9.0	LLDP	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. Enable or Disable LLDP

ONTAP 9.0	UC compliance with DSCP marking	Unified Capability (UC) compliance with Differentiated Services Code Point (DSCP) marking. 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. If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used: **0x0A (10)**: The default value for data protocols/traffic. **0x30 (48)**: The default value for control protocols/traffic. DSCP marking for US compliance
ONTAP 9.0	SHA-2 password hash function	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. 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.
ONTAP 9.0	FIPS 140-2 support	You can enable the Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces. By default, the FIPS 140-2 only mode is disabled. Configure network security using Federal Information Processing Standards (FIPS)

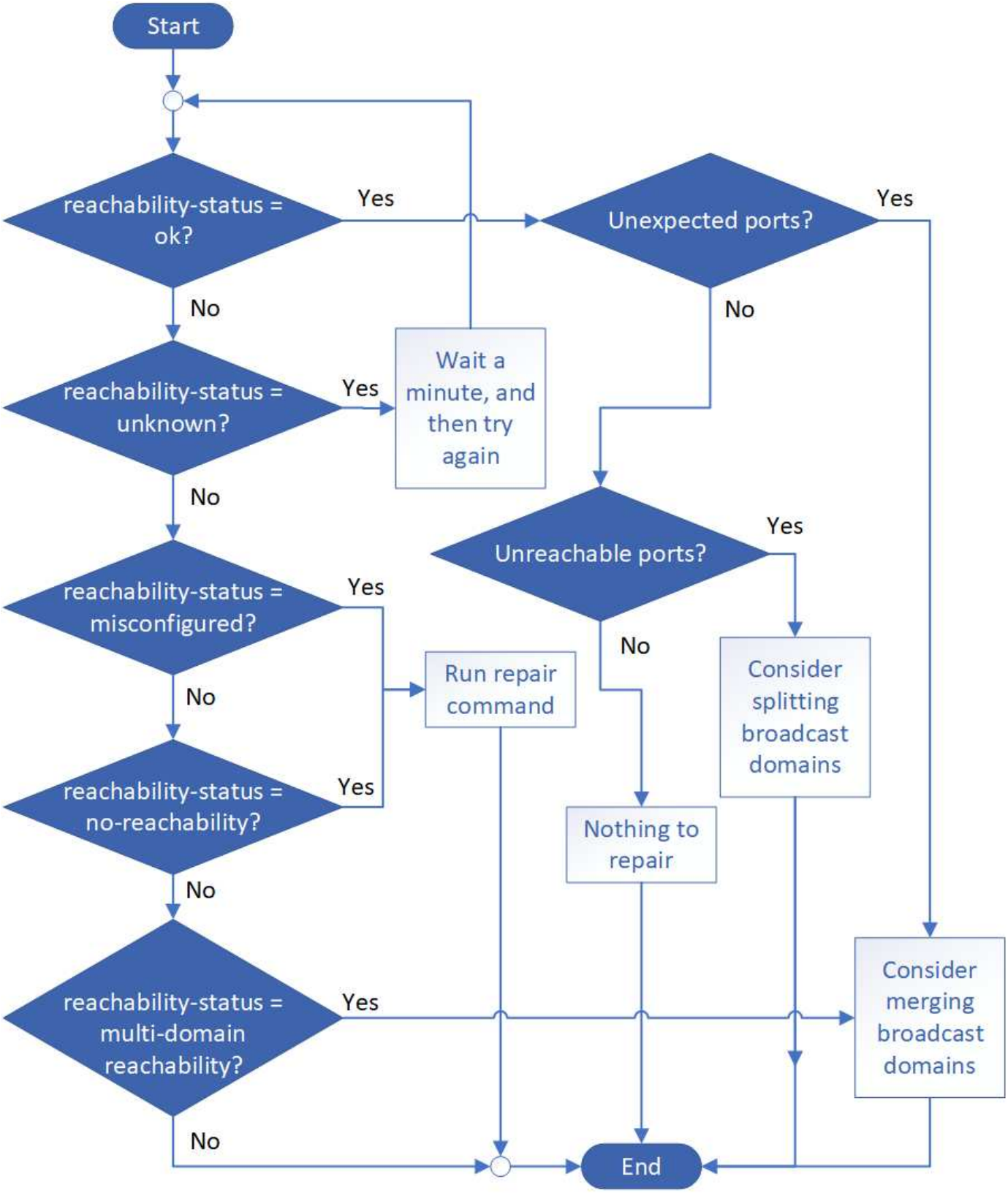
Verify your networking configuration after upgrading to ONTAP 9.8 or later

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	The port has layer 2 reachability to its assigned broadcast domain. If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see Merge broadcast domains. If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see Split broadcast domains. If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.
misconfigured-reachability	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. 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: `network port reachability repair -node -port` For more information, see Repair port reachability.
no-reachability	The port does not have layer 2 reachability to any existing broadcast domain. 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: `network port reachability repair -node -port` For more information, see Repair port reachability.
multi-domain-reachability	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. 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. For more information, see Merge broadcast domains or Repair port reachability.
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

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

Trademark information