



Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.3(4a)M

Introduction

This document describes the features, issues, and exceptions of Cisco NX-OS Release 10.3(4a)M software for use on Cisco Nexus 9000 Series switches.

The [Cisco NX-OS Software Strategy and Lifecycle Guide](#) provides details about the new Cisco NX-OS Software Release and Image-naming Convention.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

The following table lists the changes to this document:

Date	Description
June 28, 2024	Added CSCwi92006 to the Open Issues section.
April 25, 2024	Added CSCwh50989 to the Resolved Issues section.
November 14, 2023	Added CSCwf34104 to the Resolved Issues section.
November 2, 2023	Cisco NX-OS Release 10.3(4a)M became available

New and Enhanced Software Features

There are no new software features introduced in Cisco NX-OS Release 10.3(4a)M.

The enhanced features listed below are existing features introduced in earlier releases, but enhanced to support new platforms in Cisco NX-OS Release 10.3(4a)M.

Enhanced Features		
Product Impact	Feature	Description
Feature Set	Support for Enhanced ISSU on N9K-C9408	Enhanced ISSU is now supported on Cisco N9K-C9408 platform switch. See Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.3(x).
Scalability	vPC port channel scale enhancements	The vPC port channel scale is enhanced from 80 to 98 on Cisco Nexus 9300-FX2 switch and from 80 to 128 on Cisco Nexus 9300-GX2 switch. See Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.3(4a)M.

Note: Beginning with Cisco NX-OS Release 10.3(4a)M, the existing logging rfc-strict 5424 command (optional) that enables the syslog protocol RFC 5424 is enhanced by adding a new keyword (full) as follows: **logging rfc-strict 5424 full**. The addition of this keyword ensures complete compliance with the RFC 5424 standard for Syslog Protocol. However, if the values are not available for the [APP-NAME] [PROCID] [MSG-ID] [STRUCTURED-DATA] fields, then the nil value is indicated by a dash (-). See Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands), and Cisco Nexus 9000 Series NX-OS System Messages Reference, Release 10.3(x).

Hardware Features

There are no new hardware features introduced in Cisco NX-OS Release 10.3(4a)M.

For details about transceivers and cables that are supported on a switch, see the [Transceiver Module \(TMG\) Compatibility Matrix](#).

Unsupported Features on N9K-C92348GC

Beginning with Cisco NX-OS Release 10.1(1), the following features are not supported on N9K-C92348GC:

- VXLAN
- SW/HW Telemetry
- NetFlow/Analytics
- iCAM
- PTP
- NX-SDK
- DME, Device YANG, OpenConfig YANG, gRPC, NETCONF, and RESTCONF

Note: NXAPI CLI and XML Agent (NETCONF over SSH) are supported on this platform.

Release Image

In Cisco NX-OS Release 10.3(4a)M, the following two 64-bit images are supported:

- The 64-bit Cisco NX-OS image filename with "nxos64-cs" as the prefix (for example, nxos64-cs.10.3.4a.M.bin) is supported on all Cisco Nexus 9000 series switches except Cisco Nexus 9500 -R and -R2 switches and cards.
- The 64-bit Cisco NX-OS image filename with "nxos64-msll" as the prefix (for example, nxos64-msll.10.3.4a.M.bin) is supported on Cisco Nexus 9000 -R and -R2 series modular switches.

The 32-bit image is no longer supported.

Open Issues

Bug ID	Description
CSCwh76275	Headline: Nexus 9364-GX2A - Slice 0 discards Multicast traffic after RTP Flow Monitor is enabled. Symptoms: Nexus 9364-GX2A discards Multicast traffic after RTP Flow Monitor is enabled and continues to discard it even after RTP Flow Monitor is disabled. Workarounds: None.
CSCwh88428	Headline: On Nexus 9000 switch, SNMP trap is not sent when Storm Control traffic falls below the threshold. Symptoms: A Cisco Nexus 9000 device can fail to send an SNMP trap when Storm Control traffic falls below the threshold and the following syslog is seen. However, trap is not seen. %ETHPORT-5-STORM_CONTROL_BELOW_THRESHOLD: Traffic in port Ethernet1/1 has fallen

Bug ID	Description
	below the configured threshold, action - Trap. Workarounds: None.
CSCwi92006	Headline: all interfaces shown input/output rate as 0pps on N9K FX2 platform Symptoms: all interfaces shown input/output rate as 0pps on N9K-FX2 platform without any operations. Impact is on N9K-FX2 switches and does not impact the N3K. Workarounds: None.

Resolved Issues

Bug ID	Description
CSCwf34104	<p>Headline: SMU not installed after switch reload/panic/smu-install reload</p> <p>Symptoms: The symptoms are as follows:</p> <ol style="list-style-type: none"> Nexus 9000 Switch is running 10.3(3) and has any SMUs committed. Example: Swich_Name# show install committed Boot Image: NXOS Image: bootflash:///nxos64-cs.10.3.3.F.bin Committed Packages: nxos64-cs.CSCwf61602-1.0.0-10.3.3.lib32_64_n9000 committed Committed SMUs may not be activated after reload due to power-cycle, software reload. Below command will show the SMU will be Inactive Committed (wrong signature) Switch_Name# show install patches Boot Image: NXOS Image: bootflash:///nxos64-cs.10.3.3.F.bin nxos64-cs.CSCwf61602-1.0.0-10.3.3.lib32_64_n9000 Inactive Committed (wrong signature) <p>Workarounds: When Inactive Committed (wrong signature) is present, reload again to re-commit the SMU.</p>
CSCwv16064	<p>Headline: NX-OS to be conformed with RFC 5424 (NILVALUE for STRUCTURED-DATA and MSGID fields)</p> <p>Symptoms: In all Cisco NX-OS versions, the implementation of syslog does not follow RFC 5424 leading to following problems:</p> <ul style="list-style-type: none"> Adding NILVALUE for STRUCTURED-DATA field as we don't have structured data currently in syslog messages. RFC 5424:6.3. STRUCTURED-DATA In case of zero structured data elements, the STRUCTURED-DATA field MUST contain the NILVALUE. Adding NILVALUE for MSGID in syslog header as this must be there if no data is available for MSGID. For the rest fields like APP-NAME, PROCID NILVALUE is not mandatory. <p>Workarounds: None</p>

Bug ID	Description
CSCvz06811	<p>Headline: Nexus Data Broker switch floods IGMPv3 membership queries out of all input ports.</p> <p>Symptoms: IGMP membership queries are flooded out of monitoring ports. IGMP storms (due to queries) are forwarded from Nexus Data Broker Switch to production network.</p> <p>Workarounds: Filter the IGMP with an access list.</p>
CSCwd75778	<p>Headline: Unable to connect to gRPC port 50051 in non-default vrf.</p> <p>Symptoms: Unable to connect to gRPC port 50051 in non-default vrf with MPLS path. Telnet to port 50051 also fails.</p> <p>Workarounds: None</p>
CSCwd75851	<p>Headline: /nxos/xlog is filled 100% with repeated copy run start and log files are not rolled over.</p> <p>Symptoms: When configuration changes are automated and multiple sessions try to save the configuration changes simultaneously and repeatedly, a syslog is seen.</p> <p>Workarounds: Avoid simultaneous configuration sessions and excessive/repeated config save operation.</p>
CSCwd41247	<p>Headline: samcproxy is deadlocked with multiple Instances.</p> <p>Symptoms: Configuration or simple tasks such as turning on a locator LED do not complete. Multiple instances of samcproxy running are seen, and one is in a deadlocked state. There may also be other miscellaneous faults on the domain, due to samcproxy being in a bad state.</p> <p>Workarounds: Contact Cisco TAC for a workaround as this requires debug shell access.</p>
CSCwd77505	<p>Headline: MAC Address Not Learned on Peer 6332 FI.</p> <p>Symptoms: The host experiences a failover event or the VM is migrated to a different host, and the network connectivity to that VM is lost.</p> <p>Workarounds: Contact Cisco TAC for workarounds.</p>
CSCwe20605	<p>Headline: Encrypted tunnel (VXLAN Cloudsec) traffic is getting dropped on Cisco Nexus 9300-FX3 switch.</p> <p>Symptoms: After upgrading Cisco Nexus 9300-FX3 switch to Cisco NX-OS Release 10.3(2)F image, few or all encrypted tunnel traffic is dropped. VXLAN Cloudsec or tunnel encryption statistics do not update.</p> <p>Workarounds: The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Remove tunnel-encryption from DCI uplinks. 2. Copy running-config startup-config. 3. Reload the switch. <p>Post reloading, configure tunnel-encryption on DCI uplinks.</p>
CSCwe43450	<p>Headline: Unexpected Kernel panic post ISSU from Cisco NX-OS Release 9.3(6) to 9.3(9).</p> <p>Symptoms: After ND-ISSU from Cisco NX-OS Release 9.3(6) to 9.3(9), an unexpected reload due to kernel panic is noticed in POE devices. This symptom can be verified by running either the sh logging onboard internal reset-reason command or the sh system reset-reason command. The output shows Reset Requested due to Fatal Module Error.</p> <p>Workarounds: None</p>
CSCwe81696	<p>Headline: 100M links with the use of GLC-T/GLC-TE transceivers do not come up in Cisco NX-OS Release 10.2(4), 10.2(5), and 10.3(2).</p>

Bug ID	Description
	<p>Symptoms: Links with 100M speed do not come up and remain in a Link not connected status.</p> <p>Workarounds: None</p>
CSCwf12345	<p>Headline: Seeing intermittent traffic drops during ND_ISSU for 4-5 seconds for FCoE hosts.</p> <p>Symptoms: During non-disruptive upgrade from Cisco NX-OS Release 10.3(1) or 10.3(2) to 10.3(3), intermittent traffic disruption is seen on FCoE hosts. Traffic switches over to available alternate path and then switches back.</p> <p>Workarounds: For upgrades from Cisco NX-OS Release 10.3(1)F or 10.3(2)F to 10.3(3)F, you can configure the holdtimer in LLDP to be of 255 (max value) using the following global command and then initiate upgrade: lldp holdtime 255.</p>
CSCwf21754	<p>Headline: After the reload ascii command, VRF ID always points to default when traffic flow is through the SVI interface.</p> <p>Symptoms: When the Cisco Nexus 9500 switch is reloaded with the reload ascii command, the NetFlow export sends ingressVRF-id as default VRF-id (1)</p> <p>Workarounds: Reload the switch.</p>
CSCwf24420	<p>Headline: Need to disable PIE feature and command from Cisco Nexus 9808 switches.</p> <p>Symptoms: PIE commands do not show right output for fan, power supply, and optics.</p> <p>Workarounds: None</p>
CSCwf34708	<p>Headline: Nexus 9000 OS installation with no-reload option can cause BFD to go down.</p> <p>Symptoms: BFD cannot go up after upgrading OS as follows:</p> <ol style="list-style-type: none"> 1. Run install all nxos [os image] no-reload on all switches. 2. Reload one of switches. 3. BFD neighbor down and cannot come up until reload the opposite switch. Besides, OSPF neighbor with BFD is still in full state even though BFD is down. <p>Workarounds: Reload other switches.</p>
CSCwf52916	<p>Headline: Improve telemetry trace tm-error " failure reason:Value too large" .</p> <p>Symptoms: " failed reason:Value too large" from " show system internal telemetry trace tm-errors" .</p> <p>Workarounds: None.</p>
CSCwf72985	<p>Headline: Telemetry subscription of DME path sys/ptp/correction as an event is not working.</p> <p>Symptoms: Telemetry subscription with DME path sys/ptp/correction as an event is not working. The Nexus 9000 switch is not generating push packets for the subscription of DME path sys/ptp/correction as an event while the PTP clock correction falls into a configured correction range.</p> <ol style="list-style-type: none"> 1. DME does not list the event-driven telemetry subscription. 2. Event count is empty for the sensor-group of interest. <p>Workarounds: Perform the following workaround:</p> <ol style="list-style-type: none"> 1. Under the affected telemetry sensor-group, reconfigure the DME path EXAMPLE - sensor group 302 with DME path sys/ptp/correction conf t

Bug ID	Description
	<pre> sensor-group 302 no path sys/ptp/correction depth unbounded path sys/ptp/correction depth unbounded end </pre> <p>2. Configure different sensor-groups for the additional subscription to use for the same path.</p> <p>Do this for each new subscription to prevent the same sensor-group to be used in more than 1 subscription.</p>
CSCwf74305	<p>Headline: Logging 2.0: reduce number of instances that autocollect run to reduce load on CLI/vsh.</p> <p>Symptoms: Slow CLI execution in EXEC mode or CONF mode for period of the time when high rate of severity 0,1,2 unique syslog messages are logged by nxos (high rate is more than 100 messages per second).</p> <p>Workarounds: Disable autocollect feature: event manager applet syslog_trigger override __syslog_trigger_default event policy-default count 65000 time 1 action 1.0 collect disable</p> <p>NOTE: Do not add any other action in the EEM applet as that will prevent autocollect to be disabled. Only single action can be present in this applet.</p> <p>Ensure policy-default count is configured to prevent default EEM action to run.</p>
CSCwf75437	<p>Headline: N9K-C9504 after system switchover, static route(configured static route BFD) will disappear.</p> <p>Symptoms: Initially, Static Route associated with a BFD session that is up is present in the routing table before switchover. After switchover, static route associated with the BFD session that is up is not present in the routing table (this doesn't occur always).</p> <p>Workarounds: None.</p>
CSCwv35496	<p>Headline: Nexus 9508 MACsec - interface stuck in Authorization pending state due to one way traffic.</p> <p>Symptoms: Nexus 9508 with N9K-X9732C-EXM doesn't establish MACsec session on random ports with port status in Authorization pending. The interface on the switch shows TX counters but no RX counters increment because of which the session is stuck in Authorization pending.</p> <p>N9508# show int eth1/14Ethernet1/14 is down (Authorization pending)</p> <p>Workarounds: Reload of the affected card may help to bring up the stuck sessions. If the ports again go back into Authorization pending state, replacing the line card may help to bring up affected MACsec sessions.</p>
CSCwe43450	<p>Headline: Kernel panic due to Fatal Module Error after nondisruptive(ND) ISSU on N9K-C9348GC-FXP.</p> <p>Symptoms: After ND-ISSU, an unexpected reload due to kernel panic is noticed in N9K-C9348GC-FXP switches. This symptom can be verified by running either the show logging onboard internal reset-reason command or the show system reset-reason command. The output shows Reset Requested due to Fatal Module Error.</p> <p>Workarounds: Use disruptive/normal upgrade procedure.</p>
CSCwe50502	<p>Headline: Nexus 9000 - Unexpected reload due to Watchdog with high ktah_nl_asic_isr Interrupts.</p> <p>Symptoms: A Nexus 9000 running Cisco NX-OS 9.3(9) can reload unexpectedly with a reason of Watchdog Timeout due to a high amount of ktah_nl_asic_isr hardware interrupt events seen in a kernel panic log.</p>

Bug ID	Description																												
	Workarounds: None.																												
CSCwe74517	<p>Headline: eBGP-Removing template peer-policy under L2VPN EVPN address-family deletes prefixes,</p> <p>Symptoms: In a scenario where eBGP for L2VPN EVPN with rewrite-asn is used along with template peer-policy for L2VPN EVPN neighbor on Nexus 9000 or Nexus 3000 switches running Cisco NX-OS Release 10.2(4)F, after removing the template peer-policy under the L2VPN neighbor configuration, the Nexus deletes the rewrite-asn from BGP neighbor even though it is hardcoded under the neighbor config.</p> <p>Workarounds: Reconfigure affected neighbor. Note: Avoid restarting the BGP as this process is disruptive and all the BGP neighbors/BGP routes will bounce. Hence, it is recommended to reconfigure the affected BGP neighbor.</p>																												
CSCwe92797	<p>Headline: Nexus 9000 prunes VLANs even when VTP Pruning is not enabled.</p> <p>Symptoms: Nexus 93180YC-EX in vPC running on Cisco NX-OS release 10.2(4) prunes all VLANs in the normal VLAN range of 1-1001 after reload. The output of the show int port-channel 1 trunk command shows that VLANs in the range of 1-1001 are pruned.</p> <p>Workarounds: Re-enable feature VTP as follows: no feature vtp feature vtp vtp domain <domain-name></p>																												
CSCwf03457	<p>Headline: Auto-complete for VRF name can cause unexpected config changes.</p> <p>Symptoms: When the first letter of a VRF is typed and enter key is pressed, if there is only one VRF starting with that letter, the switch may or may not try to auto-complete the VRF name this depending on the command that is used. For commands such as show run vrf or vrf member, the auto-complete feature doesn't work but for the no vrf context command, the auto-complete feature works. This means that the switch deletes the VRF starting with that letter instead of showing a message that the VRF doesn't exist. This behavior can lead the user to delete a VRF by mistake causing network disruptions.</p> <ol style="list-style-type: none"> Starting with the following VRFs created: SWITCH(config-if)# show vrf <table border="0"> <thead> <tr> <th>VRF-Name</th> <th>VRF-ID</th> <th>State</th> <th>Reason</th> </tr> </thead> <tbody> <tr> <td>ANOTHERTEST</td> <td>6</td> <td>Up</td> <td>-- <<<</td> </tr> <tr> <td>default</td> <td>1</td> <td>Up</td> <td>--</td> </tr> <tr> <td>management</td> <td>2</td> <td>Up</td> <td></td> </tr> </tbody> </table> Delete none-existing VRF "A" SWITCH(config-if)# no vrf context A <<< "A" vrf doesn't exist but the switch will auto-complete and will delete vrf "ANOTHERTEST" SWITCH(config)# show vrf <table border="0"> <thead> <tr> <th>VRF-Name</th> <th>VRF-ID</th> <th>State</th> <th>Reason</th> </tr> </thead> <tbody> <tr> <td>default</td> <td>1</td> <td>Up</td> <td>--</td> </tr> <tr> <td>management</td> <td>2</td> <td>Up</td> <td>--</td> </tr> </tbody> </table> No message was shown for the not existing VRF and due to auto-complete feature, the VRF starting with the letter A was deleted. <p>Workarounds: Make sure to write all the VRF names while deleting a VRF. Use TAB key to auto-complete. However, this option is not possible in a few scenarios, for example, when using scripts for automation.</p>	VRF-Name	VRF-ID	State	Reason	ANOTHERTEST	6	Up	-- <<<	default	1	Up	--	management	2	Up		VRF-Name	VRF-ID	State	Reason	default	1	Up	--	management	2	Up	--
VRF-Name	VRF-ID	State	Reason																										
ANOTHERTEST	6	Up	-- <<<																										
default	1	Up	--																										
management	2	Up																											
VRF-Name	VRF-ID	State	Reason																										
default	1	Up	--																										
management	2	Up	--																										
CSCwf08452	<p>Headline: Lag in entering commands on N9K-93360YC-FX2.</p> <p>Symptoms: Most of the ports on the N9K-93360YC-FX2 switch are populated with GLC-TE Transceivers. Any changes to the port configurations usually cause very long delays (minutes).</p>																												

Bug ID	Description
	<p>This could be from a switchport or shut/no shut command. Issues recur even after running spanning-tree port type edge command and explicitly setting the speed on the port. The switch also seems to take a very long time to recognize a new physical connection or GLC-TE reset. GLC-TEs are supported on this model according to the matrix page.</p> <p>Workarounds: Apply the no QOS statistics command.</p>
CSCwf09490	<p>Headline: Nexus 9000/DNS - DNS resp is rejected when lookup is done in different VRF for smart license callhome transport.</p> <p>Symptoms: Smart license connection fails when transport mode is used - callhome with source interface non default VRF. DNS reply from server is rejected on the switch (example from inband capture) timestamp: x.x.x.x # y.y.y.y ICMP 120 Destination unreachable (Port unreachable) Where x.x.x.x is switch source interface IP and y.y.y.y is dns server IP Due to this smart license fails to reach license server.</p> <p>Workarounds: Have DNS and callhome in default VRF or do not specify specific source interface.</p>
CSCwf13179	<p>Headline: VLAN Filter Allows an ACL with the 'log' keyword to be used when applied to a non-existent VLAN.</p> <p>Symptoms:</p> <ul style="list-style-type: none"> • VLANs are suspended on interfaces after a VLAN Filter is applied. • At first the only VLANs affected are the ones identified by the 'vlan-list' component of the VLAN Filter. • If the affected interfaces are flapped, the suspension will spread to all VLANs currently hosted on the interfaces that were flapped. • The switch generates logs similar to: <ul style="list-style-type: none"> ◦ %ETHPORT-3-IF_ERROR_VLANS_SUSPENDEDED: VLANs 2707 on Interface Ethernet1/2 are being suspended. (Reason: ACL Logging is not supported in egress direction.) ◦ %ETHPORT-5-IF_SEQ_ERROR: Error (" ACL Logging is not supported in egress direction.") communicating with MTS_SAP_SPM for opcode MTS_OPC_ETHPM_PORT_LOGICAL_BRINGUP (RID_PORT: Ethernet1/2) <p>Workarounds: Perform the following workaround:</p> <ol style="list-style-type: none"> 1. Remove the VLAN Filter configuration or remove the log keyword from the ACL used by the VACL. 2. Flap all the affected interfaces by performing shutdown and then no shutdown.
CSCwf17674	<p>Headline: Nexus 9300-GX2 - Unexpected Reboot due to CSUSD HAP Reset.</p> <p>Symptoms: Nexus 9300-GX2 switches may reboot unexpectedly due to csusd process crash and a log is generated.</p> <p>Workarounds: None.</p>
CSCwf17839	<p>Headline: BGP core and traceback generated when showing received paths with soft-reconfig.</p> <p>Symptoms: There are two issues that the DDTs resolves:</p> <ol style="list-style-type: none"> 1. BGP core file is generated on Nexus 9000 after using the show l2vpn vpn route x.x.x.x command. 2. Asserts seen when displaying BGP routes. <p>The symptoms are visible when:</p> <ul style="list-style-type: none"> • Soft-reconfig is enabled • A route advertisement is dropped using route-map in. • You are specifically trying to view the route that was dropped.

Bug ID	Description
	Workarounds: None; do not run the show command to view the route.
CSCwf19968	<p>Headline: vsh.bin fails after setting a SPAN capture with thousands of source VLANs in a single session.</p> <p>Symptoms: When configuring thousands of source VLANs the device becomes unresponsive, the switch hangs and closes the ssh session, then the vsh.bin process reloads unexpectedly. For example, switch(config-monitor)# source vlan 31-3967 Warning: Tx Vlan Span is not supported 2023 Mar 8 10:10:07 switch %SYSMGR-2-LAST_CORE_BASIC_TRACE: : PID 19845 with message vsh.bin(non-sysmgr) crashed, core will be saved. switch# show cores VDC Module Instance Process-name PID Date(Year-Month-Day Time) ----- 1 1 1 vsh.bin 19845 2023-03-08 10:10:07</p> <p>Workarounds: Avoid setting a higher number of source VLANs as a single SPAN session can support a total of 32 source VLANs.</p>
CSCwf21554	<p>Headline: On NX-OS, special character ">" causes issues with clear-text key-string in key chain.</p> <p>Symptoms: Using a key-string with ">" character causes the parser to not capture the string, resulting in an empty string and missing configuration.</p> <p>Workarounds: Avoid using the ">" character in a clear-text (pre encrypted) key-string configuration.</p>
CSCwf30217	<p>Headline: RTP flows traffic creation generates nfm core dump.</p> <p>Symptoms: When RTP flow monitoring is configured and RTP traffic is received, NetFlow crashes and generates a crash file.</p> <p>Workarounds: None. However, removing the RTP Flow monitoring ACL can resolve the issue.</p>
CSCwf32021	<p>Headline: PTP process crash.</p> <p>Symptoms: When the PTP profile mode is 8275.1 on Nexus 9300-FX3 platform, PTP process crashes.</p> <p>Workarounds: Disable PTP using the no feature ptp command.</p>
CSCwf33807	<p>Headline: Kernel logs are saved in the tmp_logs directory.</p> <p>Symptoms: After a crash in the FEX, the kernel traces are not saved in the platform after a reload, but in the tmp_logs directory.</p> <p>Workarounds: None.</p>
CSCwf34104	<p>Headline: RPMDDB inconsistency gpg-pubkey is not installed - seen after image REL key is enabled.</p> <p>Symptoms: The following symptoms are seen:</p> <ol style="list-style-type: none"> 1. Nexus 9000 Switch running on Cisco NX-OS Release 10.3(3) has one more SMU committed. 2. Sometimes, after a power-on, power-cycle or reload of the switch takes place, there are no SMUs committed. <p>Workarounds: Remove and re-add the SMU.</p>

Bug ID	Description
CSCwf34746	<p>Headline: Configuring track in role-interface mode can cause vsh crash.</p> <p>Symptoms: Configuring track in role-interface mode as below can cause vsh crash. N9K# conf t N9K(config)# role name eem-role N9K(config-role)# interface policy deny N9K(config-role-interface)# permit interface Ethernet1/8 N9K(config-role-interface)# track 8 interface Ethernet1/8 line-protocol->ssh crashed</p> <p>Workarounds: Configure track in global configuration mode.</p>
CSCwf36120	<p>Headline: Unable to configure specific sFlow settings on N9K-C92348GC-X in Cisco NX-OS Release 10.3(2)F.</p> <p>Symptoms: When configuring sFlow on the Nexus 93248GC-X switch, the collector-port and agent-ip show the following error message: "ERROR: sflow configuration failed." Other sFlow configurations such as the counter-poll-interval can be configured.</p> <p>Workarounds: The issue is due to collector-ip configuration, so keep the collector-ip configuration at last among other sFlow configuration.</p>
CSCwf36533	<p>Headline: Nexus 9000 - vPC ports stuck into STP BLK state on secondary vPC after vPC Fabric Peering sync is recovered.</p> <p>Symptoms: The symptoms are as follows:</p> <ul style="list-style-type: none"> • When Spine drop the vPC peer communication, Nexus vPC peer-link detected BPDU receive timeout, and will block vPC port-channel. • After vPC peer communication is restored, vPC port-channel stuck into STP BLK state on secondary vPC. <p>Workarounds: To recover, shut/no shut the port that is on BLK state.</p>
CSCwf37901	<p>Headline: VXLAN VLANs suspended by vPC consistency checker due to different replication mode and VNI type.</p> <p>Symptoms: VXLAN VLANs get suspended due to different replication modes, but configuration shows that replication mode is the same on both vPC switches.</p> <p>Workarounds: Remove the affected VNI and then add again.</p>
CSCwf39373	<p>Headline: OSPFv3 is adding a link-local forwarding address for NSSA type 7 originated routes.</p> <p>Symptoms: While a user redistributes a static route into the device in the Not-so-stubby Area (NSSA) [NSSA is an OSPF Stub Area, which can carry routes learned by other protocols such as BGP or RIP and Static in this case] and making the current OSPF router as a border router, the user observes in the database that the forwarding address is link local and not any of the available global addresses on ospfv3 enabled interfaces in the area. Link local address is used instead of Global IPv6 address in the forwarding address.</p> <p>Workarounds: Configure a loopback with a global ipv6 address in the NSSA area to pick a global address from.</p>
CSCwf42887	<p>Headline: On Nexus 9300-FX3 switch, VXLAN storm-control policer fabric bandwidth does not update after fabric link flap.</p> <p>Symptoms: On Nexus 9300-FX3 switch, VXLAN storm-control policer fabric bandwidth does not update after fabric link flap.</p> <p>Workarounds: Perform Shut/No-shut multi-site loopback. This will reset the policer but not stop the behavior. Then disable evpn storm-control.</p>
CSCwf47425	<p>Headline: Ports of N9K-C93600CD-GX with QSA (10G) don't forward traffic.</p> <p>Symptoms: Although the 10G port with QSA adapter is in the up state, it doesn't forward traffic.</p>

Bug ID	Description
	Workarounds: None.
CSCwf48266	<p>Headline: Debug hardware internal command on N9K-C93360YC-FX2 causes tahusd crash.</p> <p>Symptoms: N9K-C93360YC crashes after entering debug commands while in the module shell, generating a tahusd core.</p> <p>Workarounds: For any debugging in the module shell, contact TAC.</p>
CSCwf48692	<p>Headline: Nexus 9300-FX3S/FX3 may randomly time out syncE peer.</p> <p>Symptoms: Random syncE peer timeouts.</p> <p>Workarounds: None.</p>
CSCwf50388	<p>Headline: tahusd crash due to InPhi retimer quad port dead lock.</p> <p>Symptoms: The following symptoms are seen: tahusd reloaded due to software mutex lock. Last reset at 22466 usecs after Sat May 20 11:29:29 2023 Reason: Reset Requested due to Fatal Module Error System version: 9.3(9) Service: tahusd hap reset</p> <p>Workarounds: None. However, the chassis silently reloads and recovers post reload. To avoid this issue, keep all links that are unused in admin shut state.</p>
CSCwf54392	<p>Headline: On a Nexus 9000 switch, radius-server key <> is missing after ND ISSU.</p> <p>Symptoms: When upgrading a Nexus 9000 switch from a code where LXC boot mode is not the default mode, to one where it is, using non-disruptive ISSU, the radius-server key 7 <string> configuration can go missing. This is due to the change in default boot mode.</p> <p>Workarounds: Remove and reapply the missing CLI string to reconfigure and ensure it is consistent between the configuration and the DME.</p>
CSCwf56529	<p>Headline: Nexus 9000: Attempting to delete an ACE from Custom CoPP ACL will fail.</p> <p>Symptoms: When attempted to delete an ACE from a custom CoPP policy ACL, the operation fails and the configuration remains. This is confirmed by the accounting log failure and show running-config.</p> <p>Workarounds: None.</p>
CSCwf57648	<p>Headline: Nexus 9500-R modules incorrect outer DMAC after initialization.</p> <p>Symptoms: Nexus 9500 with -R line cards to perform an MPLS to VXLAN handoff. The Nexus 9500 acting as the PE device adds an incorrect DMAC to the outer VXLAN header, which causes the downstream VXLAN leaf to drop the packet. The incorrect MAC observed is "00:DO:00:00:88". Similar issue is also possible in non MPLS to VXLAN handoff scenario after initialization of the switch.</p> <p>Workarounds: If the switch is found to be in this state, a "reload ascii" will fix the mis-programming. Another workaround is to poweroff module <> and no poweroff module <> of the problematic line cards to recover from the issue.</p>
CSCwf58507	<p>Headline: FEX 2348UPQ brings hosts link too fast after powercycle causes traffic blackholing for around 1 min.</p> <p>Symptoms: When FEX 2348TQ power-cycles all hosts using GLC-T, GLC-T-C, SFP-H10GB-CU3M, SFP-H10GB-CU3M, SFPs link up while the FEX is down. After 5 seconds links go up for around 1 minute, although FEX and its FIs are down from the perspective of Nexus 9000.</p> <p>Workarounds: Use LACP or any other SFP or upgrade the version.</p>
CSCwf61588	Headline: %NFM-1-RTP_FLOW_ERROR_DETECTED - CLI execution slowness is seen.

Bug ID	Description
	<p>Symptoms: General slowness in command execution in CLI is seen if multiple %NFM-1-RTP_FLOW_ERROR_DETECTED: syslogs are generated. One of the reasons for multiple syslog generation is when large unique flows are present, for every flow that becomes lossless to lossy, a new syslog is logged. Same is true for lossy to lossless.</p> <p>Workarounds: None.</p>
CSCwf61602	<p>Headline: Duplicate bia is seen on 9300-GX switch.</p> <p>Symptoms: On the N9K-93600CD-GX switch, BIA block is reused after port 1/25. So, there will be duplicate bia mac. This is shown in the output.</p> <p>Workarounds: None.</p>
CSCwf63078	<p>Headline: The ip dhcp relay commands are not retained on SVI after changing VRF membership.</p> <p>Symptoms: The ip dhcp relay address commands are no longer present in the SVI after changing the VRF membership, even though the system vrf-member-change retain-l3-config command is globally configured.</p> <p>Workarounds: Re-apply the missing ip dhcp relay address commands to the affected SVI.</p>
CSCwf64467	<p>Headline: Incorrect config-profile configuration cannot remove corresponding entry in vsh config.</p> <p>Symptoms: When entering a command with an incorrect network in a config profile and applying the profile to the main configuration, the profile cannot be unapplied. For example, when applying a config profile with a line such as ip prefix-list PL-1 permit 10.0.0.10/24 => the correct network address would be 10.0.0.0/24 in the "show run", the address that will configure correctly will be ip prefix-list PL-1 permit 10.0.0.0/24, but the config profile cannot be unapplied.</p> <p>Workarounds: None.</p>
CSCwf67122	<p>Headline: MSDP instability if VRF not enabled for BGP.</p> <p>Symptoms: MSDP performance issues may be observed if it's running in a VRF that's not enabled in BGP while BGP is configured globally.</p> <ul style="list-style-type: none"> • Adjacencies may flap due to keepalives expiring, while packet captures indicate no drops. • SA propagation may be significantly delayed, or SAs may never be received. • The receive queue for MSDP TCP sockets in "show sockets connection" would be full. <p>Workarounds: Enable the MSDP VRF under the BGP process. No additional configuration such as address families or neighbors is required. router bgp 65500 vrf MSDP-VRF Alternatively, disable BGP entirely using the no router bgp 65500 command.</p>
CSCwf67313	<p>Headline: ENV LED light as amber while FAN and PSU are operational.</p> <p>Symptoms: ENV LED lit as amber even if all the FAN and PSU are operational. All fans and PSUs are shown as OK in the output of the show environment command. In the output of the show system internal platform all command, the LED status are as follows. All fans are running in normal speed shown in `show env fan detail` ChassisLEDs: TOR=Green, Env=Amber, PS=Green, Fan=Amber TORLEDs: Status=Green</p> <p>Workarounds: None.</p>
CSCwf67373	<p>Headline: The copy r s command is aborted after ND-ISSU from older releases to Cisco NX-OS Release 10.2.1 and beyond with FEX.</p> <p>Symptoms: The copy r s command is aborted after ND-ISSU from older releases to 10.4(1)F with FEX. The layer for FEX ports is inconsistent across DME and backend. As DME has layer 2 for FEX ports, it was trying to configure VLANs and in backend vlan_mgr was rejecting the config as it was layer 3 in the backend. The correct layer was layer 3. AS NXAPI retries happen in a continuous loop, the copy r s command gets aborted.</p>

Bug ID	Description
	<p>Workarounds: Configuring switchport/no switchport on all affected interfaces should recover the switch from issue scenario.</p>
<p>CSCwf69556</p>	<p>Headline: Nexus 9000: Interface description including string "%n" or "%ln" crash Service "port-profile" .</p> <p>Symptoms: An error occurs when we put the string "%n" or "%ln" as interface description.</p> <pre>----- switch(config-if)# interface Ethernet1/5 switch(config-if)# description % Inter XXXX-1001-XX % 2023 Jun 8 14:44:58 switch %\$ VDC-1 %\$ %SYSMGR-2-SERVICE_CrXSHED: Service "port-profile" (PID 16609) hasn't caught signal 11 (core will be saved). 2023 Jun 8 14:44:58 switch %\$ VDC-1 %\$ %USER-2-SYSTEM_MSG: ssnmgr_app_init called on ssnmgr up - aclmgr -----</pre> <p>Similar issue is noticed with following strings too:</p> <pre>description %ln description % ln description %n description % n</pre> <p>After repeating to configure description with these strings several times, NX-OS is reloaded.</p> <p>Workarounds: Do not use "%n" or "%ln" in interface description.</p>
<p>CSCwf70688</p>	<p>Headline: Nexus 9000: NX-API ospfAdjEp.json cannot retrieve OSPF neighbors correctly after interface flapping.</p> <p>Symptoms: NX-API ospfAdjEp.json cannot retrieve OSPF neighbors correctly after interface flapping. For example, when the OSPF processes have 10 neighbors and the response from the show ip ospf neighbors vrf all command always lists 10 neighbors, but the request through ospfAdjEp.json lists only 9 neighbors.</p> <p>Workarounds: Use /api/mo/sys/ospf.json?query-target=subtree&target-subtree-class=ospfAdjEp instead of /api/class/ospfAdjEp.json.</p>
<p>CSCwf73133</p>	<p>Headline: Nexus 9300-FX3P reports high correction during GM failover and holdover in PHY PTP mode.</p> <p>Symptoms: High corrections reported by PTP clients during GM failover.</p> <p>Workarounds: None.</p>
<p>CSCwf75767</p>	<p>Headline: Syslog to enable layer3 peer-router seen, even with no routing enabled on vPC VLANs.</p> <p>Symptoms: Below log is being seen in # show logging log, even if no routing is enabled on vPC VLANs. Suppressing syslog by "no layer3 peer-router syslog" has no impact.</p> <p>ipfib: Routing adjacency over vPC detected without required configuration. Please configure layer3 peer-router under the vPC domain. See https://cisco.com/go/l3pr for more information.</p> <p>Workarounds: Enable layer3 peer-router under vPC configuration on both vPC peers.</p>
<p>CSCwf75862</p>	<p>Headline: Bi-dir traffic received on DF winner interface is dropped towards the RPF (RP).</p> <p>Symptoms: Bi-dir traffic received on DF winner interface is dropped towards the RPF (RP). All consistency checkers are clean. Elam summary shows forward. Elam detail shows RPF failure.</p> <p>Workarounds: None.</p>
<p>CSCwf79132</p>	<p>Headline: After ISSU upgrade performed with maintenance mode, SVIs stay down.</p> <p>Symptoms: On Nexus 9000 all SVIs remain down after exiting maintenance mode post ISSU upgrade. Example of VLAN interface in problematic state:</p> <pre>nexus9000# show interface vlan 3600 Vlan3600 is down (suspended), line protocol is down, autostate enabled</pre>

Bug ID	Description
	<p>nexus9000# show system internal eltm event-history vxlan-error 2023-06-26T06:27:59.067882000+00:00 [M 1] [eltm] E_DEBUG Outer Bd Alloc failed Nve ifx 0x1a005e00, Overlay state = Up v4/v6 tid (0x1 80000001 1 0) en (0 0) 2023-06-23T13:39:01.222605000+00:00 [M 1] [eltm] E_DEBUG Failed to force alloc outer_bd 16 for vxlan infra vlan 3600</p> <p>Workarounds: Rebooting the switch restores the SVIs.</p>
CSCwf84373	<p>Headline: Admin shut the interface mgmt0, other end port remains up/flapping.</p> <p>Symptoms: With admin-shut SFP management port on Cisco Nexus 9300-FX2 switches, the peer link reports UP and DOWN flapping.</p> <p>Workarounds: None.</p>
CSCwf86821	<p>Headline: ACL not programming in hardware with udp-relay config on Nexus 9000.</p> <p>Symptoms: ACL entries not programming in hardware with udp-relay config on Nexus 9000 when adding under the SVI. slot 1=====ERROR: no ACL related hardware resources for vdc [1], vlan [210]</p> <p>Workarounds: Perform the following commands in the following sequence under the SVI: switch #(config-if) no ip udp relay addrgroup <object-group name> switch #(config-if) ip udp relay addrgroup <object-group name></p>
CSCwf88604	<p>Headline: ePBR crash @iscm_parse_ipv6_ace on epbr ipv6 policy configuration with object groups.</p> <p>Symptoms: The ePBR process crashes are observed on configuring an eBPR IPv6 policy on an interface on a Nexus 9000 switch. The process crash triggers a reload of the Nexus 9000 switch. This problem is observed on a Nexus switch running on Cisco NX-OS Release 10.3(3)F. The epbr ipv6 policy <policy-name> configuration command is applied on a Layer 3 interface and IPv6 object-group is/are used as ePBR policy match condition.</p> <p>Workarounds: Do not use IPv6 object-group in ePBR policy ACL match condition. Replace the object-group with standard ACE entry in the IPv6 access-list configuration.</p>
CSCwf94763	<p>Headline: Telemetry GPB Event paths starting with a forward slash (/) are not working.</p> <p>Symptoms: On a switch that is configured with feature telemetry, the GPB destination does not send all data for a YANG path if the path starts with a forward slash (/).</p> <p>Workarounds: Remove the forward slash (/).</p>
CSCwf98148	<p>Headline: Port-security static binding gets stuck if the interface is converted to Layer 3 before deleting the configuration.</p> <p>Symptoms: If the interface is configured with a port-security static binding and then shut down before converting it to Layer 3 using the no switchport command, the static entry continues to be shown statically associated to the interface. The only way to remove this static entry is to disable the port-security feature using the no feature port-security command. If the static binding is removed before converting the interface to Layer 3, or if the default interface command is entered, the issue is not seen.</p> <p>Workarounds: Perform the following workaround:</p> <ol style="list-style-type: none"> 1. Do not shut down the interface before converting it to Layer 2. 2. Default the interface before converting it to Layer 3. 3. Remove the static entry with the no feature port-security command before converting the interface to Layer 3.

Bug ID	Description
	<p>4. If the entry is stuck, disable and re-enable the port-security feature.</p>
CSCwf98194	<p>Headline: PBR in combination with a NULL 0 route not working properly, we see drops (UC_PC_CFG_TABLE_DROP).</p> <p>Symptoms: The issue is seen when we have a NULL 0 route present for the destination in combination with PBR which is causing the traffic to be dropped.</p> <p>Workarounds: If the NULL 0 route to the destination is removed no drop is seen.</p>
CSCwf98268	<p>Headline: Static MAC binding with dynamic MAC learnt on the same interface with PVLAN and port security issue.</p> <p>Symptoms: On Nexus 9000 switch, port-security and PVLAN static MAC binding with dynamic MAC learnt on the same interface is causing disproportionate maximum values to the configured MAC under the interface.</p> <p>Workarounds: To configure the port-security static MAC again, default interface to ethernet x/y.</p>
CSCwf98753	<p>Headline: Nexus 9000: Redistributed Routes Are Not Removed from Routing Protocol when deleted from URIB.</p> <p>Symptoms: A prefix that is redistributed into a routing protocol is stuck in its database even though the route is no longer in URIB.</p> <p>Workarounds: Configure a Null0 route for the affected prefix and then remove it. ip route 0.0.0.0/0 null0 no ip route 0.0.0.0/0 null0</p>
CSCwh01493	<p>Headline: Nexus 9300-FX3/GX random-detect threshold burst-optimized is causing packet drop.</p> <p>Symptoms: " random-detect threshold burst-optimized" configured under class type queuing c-out-8q-q-default" is causing drops on the interface where this service policy is applied. " random-detect threshold burst-optimized ecn" will cause the same issue.</p> <p>Workarounds: Remove " random-detect threshold burst-optimized" .</p>
CSCwh04496	<p>Headline: SNMP reloads unexpectedly without collecting the main thread on the core file.</p> <p>Symptoms: The issue was seen for the first time on a Nexus N9K-C9508 running on Cisco NX-OS Release 10.3(2)F. The failure was reported by SNMP, the device did not reload but the process .%SYSMGR-2-SERVICE_CRASHED: Service "snmpd" (PID 3678) hasn't caught signal 6 (core will be saved).</p> <p>Workarounds: Disable SNMP using the no snmp-server protocol enable command.</p>
CSCwh11140	<p>Headline: Remote Address not sent in TACACS Authorization packet when using NETCONF over SSH.</p> <p>Symptoms: Remote Address not sent in TACACS Authorization packet when using NETCONF over SSH.</p> <p>Workarounds: None.</p>
CSCwh12084	<p>Headline: Trustpoint should present the entire certificate chain instead of just leaf certificate.</p> <p>Symptoms: When the user imports the identity certificate with the entire certificate chain to the switch, the switch only presents the end/leaf certificate which causes the peer end hard to verify the certificate.</p> <p>For example, trustpoint server has 3 certificates: grpc server cert ----- intermediate CA ----- root CA When grpc agent uses trustpoint server as server certificate, it can only provide the grpc server cert in the above chain to the client.</p> <p>Workarounds: When the client needs to verify the identity of the switch, make sure to include the</p>

Bug ID	Description
	intermediate CA that signed the end certificate.
CSCwh14712	<p>Headline: N9K-C93240YC-FX2 - URIB core observed when flapping interfaces continuously.</p> <p>Symptoms: On a Cisco Nexus C93240YC-FX2 running Cisco NX-OS Release 10.3(3)F, URIB core is observed during continuous link shut/no shut.</p> <p>Workarounds: None.</p>
CSCwh17302	<p>Headline: Attached HMM /32 vrf leaking not working with maximum-paths mixed.</p> <p>Symptoms: The following symptoms are seen when leaking a /32 prefix from source VRF-A to target VRF-B on a pair of Nexus 9000s:</p> <ul style="list-style-type: none"> • Source-vrf sees the /32 prefix locally from HMM. • Target VRF does not leak the /32 prefix. • While looking for the /32 prefix on the RIB only less specific route is leaked (less specific prefix is coming redistribute-direct of SVI subnet where /32 is attached). • While checking on target VRF, /32 prefix is not seen, and only leakage of the /27 prefix (from the SVI/direct redistribution) is seen. <p>Workarounds: Perform any one of the following workarounds:</p> <ul style="list-style-type: none"> • Clearing the less specific prefix on the target VRF. • Remove <maximum-paths mixed> from the source VRF.
CSCwh18918	<p>Headline: On Nexus 9000 switches, python3 crashes are observed after upgrade.</p> <p>Symptoms: Several python3 core files are created after upgrading to 10.2(x) and higher releases from 9.3(x). To see the generated cores, use the show cores command.</p> <p>Additional issue that can be seen on upgrade from Cisco NX-OS Release 10.2(x) and higher is that the displayed timezone in the output of the show clock command may not match the configuration.</p> <p>Workarounds: Perform the following workaround:</p> <ol style="list-style-type: none"> 1. Configure clock timezone from the device: <pre>conf t clock timezone PST -8 0 end</pre> 2. After completing this configuration, go back and check from shell that localtime file has been populated. 3. The clock timezone config can also be removed, if needed, after verifying the file.
CSCwh19743	<p>Headline: Nexus 9000 - 'flowcontrol send on' is configured on Port-channel after removing FEX HIF member ports.</p> <p>Symptoms: The flowcontrol send on configuration is added automatically to Port-channel interface.</p> <pre>interface port-channel63 switchport switchport mode trunk switchport trunk allowed vlan 2506 spanning-tree port type edge trunk flowcontrol send on</pre> <p><<<Flowcontrol configuration added this way cannot be modified.</p> <p>Workarounds: Perform the no interface port-channel X command to manually remove the port-channel interface then re-create the port-channel.</p>
CSCwh22483	<p>Headline: Nexus 9000 is not encapsulating MACsec traffic properly into VXLAN.</p> <p>Symptoms: In the scenario where a MACsec packet's size exceeds 344-byte and needs to be</p>

Bug ID	Description
	<p>sent over a VXLAN fabric, it will be encapsulated. However, the information contained in Total Length field in the IP header is not properly set, this behavior is also seen for the length field in the UDP datagram header.</p> <p>Workarounds: None.</p>
CSCwh26273	<p>Headline: Moving the vPC Port-channel mode from access to PVLAN, brings the Po INACTIVE and wrong VLAN association.</p> <p>Symptoms: When we change the existing vPC Port-channel mode from access to PVLAN, it puts Po into INACTIVE on one of the vPC switches and VLAN association is also wrong.</p> <p>Workarounds: If we first remove access VLAN X association under vPC Po, then configure it with PVLAN mode and associate primary and secondary VLAN, it works properly.</p> <pre>conf t interface Po1 no switchport access vlan 218 switchport private-vlan host-association 99 9 switchport mode private-vlan host</pre>
CSCwh27705	<p>Headline: Nexus 9000 NBM: OIL is missing from the output of the show ip mroute command for a static NBM flows.</p> <p>Symptoms: The egress interface is not seen for few random flows in the outgoing interface list in multicast routing table though the egress interface is seen in NBM.</p> <p>Workarounds: None.</p>
CSCwh27987	<p>Headline: Nexus 9000: The power inline auto command does not seem to work for class 4 powered devices.</p> <p>Symptoms: On a Nexus 9000 switch running in POE mode facing issues with auto negotiation on, PoE power is to be used on a powered device.</p> <p>Workarounds: Powered device works with power inline static max xxxx.</p>
CSCwh28126	<p>Headline: Flapping a member of the peer-link causes BUM traffic to be sent back via the port channel we received on.</p> <p>Symptoms: In vPC back to back deployment, a BUM traffic received by the vPC port-channel between the two vPC domains might loop back if the vPC domain that received the traffic during that time had a member of the peer-link flapping.</p> <p>Workarounds: None.</p>
CSCwh29918	<p>Headline: CLI snmp oid supportlist to drop oid branches 1.3.6.1.4.1.9.9.221.1.1.2 and 1.3.6.1.4.1.9.9.221.1.1.3.</p> <p>Symptoms: Even though SNMP OIDs are not supported, CLI shows these as supported.</p> <p>Workarounds: While running snmpwalk, disregard the supported oid list.</p>
CSCwh30104	<p>Headline: Nexus 9000 - icam system monitor - history does not have all entries present.</p> <p>Symptoms: The icam monitoring system misses history values for few processes. The output of the show icam system <...> history XXX command does not show history for all processes.</p> <p>Workarounds: Manually collect the output of the show icam system command and save on external NMS or monitor processes memory by using the show CLI.</p>
CSCwh30962	<p>Headline: NX-OS - BGP Graceful Restart Helper ignores BFD down event when TCP FIN is received from restarting peer.</p> <p>Symptoms: When IOS-XE has BGP+BFD peering with NX-OS, and ASR1K is reloaded, NX-OS continues to send traffic to ASR1K for up to 2 minutes. However, the expected behavior for NX-OS is to re-converge to a different path sooner than that.</p>

Bug ID	Description
	Workarounds: Shutdown BGP neighbor prior to reload.
CSCwh32362	<p>Headline: Evora crash when incorrect evora register is given.</p> <p>Symptoms: the N9K-9732C-EXM card may reload when collecting data.</p> <p>Workarounds: Ensure the correct register is issued by using the show command.</p>
CSCwh37778	<p>Headline: Block the link loopback command on unsupported Nexus 9000 switches.</p> <p>Symptoms: When the link loopback command is configured on an unsupported Nexus 9000 switch, tah_usd or similar crash is seen. SSH session hangs when connecting to a box and configuring this CLI. Reload occurs after the crash.</p> <p>Workarounds: Avoid using this command on unsupported switches.</p>
CSCwh42160	<p>Headline: IPv6 ECMP is not working after GIR isolation and moving back to non-GIR.</p> <p>Symptoms: The symptoms are as follows:</p> <ol style="list-style-type: none"> 1. Before GIR, all IPv6 traffic have ECMP and traffic is distributed. 2. After GIR, IPv6 traffic goes over one path as ECMP programming goes wrong and no ECMPs exist anymore. Traffic drop for IPv6 as well as IPv4 is seen as the corresponding port gets oversubscribed. <p>Workarounds: None. However, the condition can be avoided by not changing the metric on any next hop in an ECMP to a lower value.</p>
CSCwh43960	<p>Headline: BGP Neighbor scale is incorrect in iCAM for Nexus 9500-R cards.</p> <p>Symptoms: On Nexus 9500 switches with -R line cards, iCAM utilization messages are displayed when device is still well within scalability limits for BGP neighbors. %iCAM-4-SCALE_THRESHOLD_EXCEEDED_WARN: Utilization of 94 percent for feature BGP Neighbors is over the warning threshold. show icam scale thresholds - displays incorrect value of 272 instead of 960</p> <p>Workarounds: Logging message can be safely ignored if within scale limits.</p>
CSCwh46028	<p>Headline: ePBR policy name of 31 characters - no error message printed.</p> <p>Symptoms: An ePBR policy name of 31 characters long can be configured but when applying this policy to an interface, the corresponding dynamic access-list is never created and no ingress RACL TCAM is used.</p> <p>Workarounds: Configure an ePBR policy-name of less than 30 characters maximum.</p>
CSCwh46613	<p>Headline: Client Link-Layer Address Length Value 6.</p> <p>Symptoms: In DHCPv6 environment with Nexus 9000 as a DHCP relay, the client link-layer address option 79 is only showing a value of length 6 as follows:</p> <pre>Client Link-Layer Address Option: Client Link-Layer Address (79) Length: 6 Value: b8cef69dedf7</pre> <p>This is not compliant with RFC: https://www.rfc-editor.org/rfc/rfc6939. The value should be of length 8 as shown below from the RFC:</p> <pre>option-code: OPTION_CLIENT_LINKLAYER_ADDR (79) option-length: 2 + length of link-layer address</pre> <p>Workarounds: None.</p>
CSCwh49061	<p>Headline: VLAN Mapping - strict incompatibility during downgrade from Cisco NX-OS Release 10.3.x to 9.3.x.</p>

Bug ID	Description
	<p>Symptoms: VLAN Mapping commands need to be removed when downgrading from Cisco NX-OS Release 10.3.x to 9.3.x version.</p> <p>Workarounds: Remove switchport vlan mapping command and re-add after downgrade.</p>
CSCwh50989	<p>Headline: Custom COPP causing transit traffic to be punted to the CPU on Nexus 9300-GX2</p> <p>Symptoms: When custom-COPP policy contains ACL rules which match on Layer 4 destination or source port, transit traffic also hits the COPP and the packets are copied to CPU. This causes duplication of traffic as CPU also routes the copied packets to the destination.</p> <p>Workarounds: Custom COPP policy using src/dst match mitigates punt for transit traffic.</p>
CSCwh51356	<p>Headline: Nexus 9300 shows incorrect PTP source port ID in the show command output.</p> <p>Symptoms: Nexus 9300 displays incorrect PTP source port ID in the output of the show ptp port interface <> command. When the displayed PTP port number is used in ethanalyzer display-filter, no traffic is displayed.</p> <p>Workarounds: Add 1 to displayed PTP source port number when it is used in ethanalyzer display-filter.</p>
CSCwh51709	<p>Headline: netif_queue EDMA hang on N9K-C9364D-GX2A does not reset system (GOLD test hangs).</p> <p>Symptoms: Inband control-plane protocols go down.</p> <p>Workarounds: Reset the system.</p>
CSCwh52964	<p>Headline: Unable to remove switchport private-vlan mapping trunk from port-channel.</p> <p>Symptoms: Unable to remove switchport private-vlan mapping trunk from port-channel.</p> <p>Workarounds: Perform the following workaround:</p> <ol style="list-style-type: none"> 1. Remove the port-channel. 2. Default the interfaces and Configure private VLAN in the following order: <pre> int eth 1/x1 switchport channel-group x mode active int po x switchport mode private-vlan trunk promiscuous switchport private-vlan trunk allowed vlan <> switchport private-vlan mapping trunk <> <>-<> int eth 1/x2 switchport switchport mode private-vlan trunk promiscuous switchport private-vlan trunk allowed vlan <> switchport private-vlan mapping trunk <> <>-<> channel-group x mode active.</pre>
CSCwh55354	<p>Headline: On Nexus 9000 EoR,-R/R2 Line Cards, module ejector interrupt storm fix is missing in -R/R2 Line Cards.</p> <p>Symptoms: Marginal seating of IO module can lead to ejector button driven interrupt storm which causes platform manager to crash.</p> <p>Workarounds: Reset module to verify good connection, verify chassis grounding, etc. Use the no hardware ejector enable command to disable the ejector interrupts on the switch.</p>

Bug ID	Description
CSCwh56979	<p>Headline: Nexus 9000 - High CPU due to nxpython3 process when multiple LLDP neighbors are detected on single interface.</p> <p>Symptoms: High CPU on Nexus 9000 due to nxpython3 process. The output of the show system internal process cpu 1 command (or "top" from bash) is as follows:</p> <pre><snip> PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND 13834 root 20 0 406612 57924 42228 R 100.0 0.2 0:00.45 nxpython3 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND 13862 root 20 0 416732 66004 44820 R 100.0 0.3 0:00.53 nxpython3 13871 root 20 0 123608 23284 19156 R 75.0 0.1 0:00.12 nxpython3 78 root 25 5 0 0 0 S 6.2 0.0 461:10.37 ksmd 13867 admin 20 0 3704 2728 1992 R 6.2 0.0 0:00.01 top </snip></pre> <p>show logging log prints the following:</p> <pre><snip> F340.05.22-N9K-C93180YC-FX-3EC# sh logg las 2 2023 Sep 13 19:34:10 F340.05.22-N9K-C93180YC-FX-3EC %LLDP-2- DETECT_MULTIPLE_PEERS: Multiple peers detected on Eth1/9 2023 Sep 13 19:34:41 F340.05.22-N9K-C93180YC-FX-3EC %LLDP-2- DETECT_MULTIPLE_PEERS: Multiple peers detected on Eth1/9 (message repeated 31 times) </snip></pre> <p>Workarounds: Configure the logging level lldp 0 or logging level lldp 1 command.</p>
CSCwh57443	<p>Headline: Missing Syslog Messages for GM change notification.</p> <p>Symptoms: On PTP enabled Nexus devices, GM clock failover takes place. All PTP-enabled Nexus devices update/failover to new GM, but, sometimes, syslog is not generated as expected on few devices.</p> <p>Workarounds: None.</p>
CSCwh60227	<p>Headline: Interface on Nexus 9000 remains in OSPF passive state post reload, despite configured to be non-passive.</p> <p>Symptoms: After a standard reload or reload ascii when the switch boots, the interface remains in the OSPF passive state although it is configured not to be so.</p> <p>Workarounds: Toggle no ip ospf passive-interface on and then off again as follows:</p> <pre>conf t interface port-channel 99 ip ospf passive-interface no ip ospf passive-interface</pre> <p>The interface shows a hello/dead timer, which means it is sending OSPF hello.</p>
CSCwh61136	<p>Headline: Fatal Upgrade Error HW reset reason printed without more information.</p> <p>Symptoms: In the output of the show logging onboard int reset-reason command, reload reason is saved as Fatal Upgrade Error.</p> <p>Reset Reason for this card:</p> <pre>Image Version : 9.3(9) Reset Reason (LCM): Unknown (0) at time Sun Sep 10 12:17:13 2023 Reset Reason (SW): Reset due to patch install (132) at time Sat Apr 1 03:15:23 2023 Reset Reason (HW): Reset Requested due to Fatal Upgrade Error (8) at time Sun Sep 10 12:17:13 2023 Last log in OBFL was written at time Sun Sep 10 12:02:45 2023</pre> <p>And no extra information is saved as core, kernel, stack traces, or logs.</p> <p>Workarounds: None.</p>
CSCwh67379	<p>Headline: On N9K-C93180YC-FX3, ingress QoS Classification of MPLS EXP is incorrect.</p> <p>Symptoms: Interfaces with MPLS packets coming with EXP bit set to 4/5 are classifying the</p>

Bug ID	Description
	<p>packets in another class-map that matches mpls exp top 1-3.</p> <p>Workarounds: Modify the class-map to match individual MPLS EXP bit instead of range.</p>
CSCwh68013	<p>Headline: User roles are not showing correctly after NX-OS upgrade.</p> <p>Symptoms: After the upgrading the switch to Cisco NX-OS Release 10.2(5), the role assigned to the user is incorrect, for example, assigned as network operator instead of network admin. However, attributes shared by the Radius server contains admin role VSA.</p> <p>Workarounds: Use correct VSA syntax to be sent.</p>
CSCwh68484	<p>Headline: Power supplies SHUT/NO SHUT for no reason.</p> <p>Symptoms: Some power supplies on a pair of nexus switches shut/no shut abnormally without causing any impact on the working on the switches.</p> <p>Workarounds: The power supplies recover without any manual intervention.</p>
CSCwh72248	<p>Headline: The vPC port-channel with switchport monitor configuration causes inconsistencies after reload.</p> <p>Symptoms: The following symptoms are seen:</p> <ol style="list-style-type: none"> 1. If port-channel is not vPC port-channel but configured with switchport monitor then you cannot add vPC configuration to it. 2. If port-channel is already vPC port-channel then you can configure " switchport monitor" under it. 3. If vPC port-channel is configured with " switchport monitor" and switch is reloaded, then, after reload, configuration cannot be saved. <p>Workarounds: Remove switchport monitor from the vPC port-channel.</p>
CSCwh74734	<p>Headline: tahusd crash on N9K-93108TC-FX3P.</p> <p>Symptoms: When the switch goes through a rare thermal sensor failure hardware issue, tahusd fails to deserialize client request in the protobuf_c_rpc third-party FOSS library. The error is triggered due to a bug in the error code path handling of this library. The error code path takes in a file-descriptor as an unsigned value and converts it into a signed one; and the fd value is used to decide the amount of memory to malloc. As the unsigned to signed conversion results in a huge value, tahusd code tries to malloc it and runs into SIGABRT being raised from libc resulting in the crash.</p> <p>Workarounds: None.</p>

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 10.3(4a)M supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 9000 Series device.

Table 1. Cisco Nexus 9400 Switches

Product ID	Description
N9K-C9408	4-rack unit (RU) 8-slot LEM-based modular chassis switch, which is configurable with up to 128 200-Gigabit QSFP56 (256 100-Gigabit by breakout) ports or 64 400-Gigabit ports.
N9K-C9400-SUP-A	Cisco Nexus 9400 Supervisor Card
N9K-C9400-SW-GX2A	Cisco Nexus 9400 25.6Tbps Switch Card
N9K-X9400-8D	Cisco Nexus 9400 8p 400G QSFP-DD LEM

Product ID	Description
N9K-X9400-16W	Cisco Nexus 9400 16p 200G QSFP56 LEM

Note: N9K-C9400-SW-GX2A Sup card ports 2xSFP Eth10/1-2 are not supported in Cisco NX-OS Release 10.3(x).

Table 2. Cisco Nexus 9800 Switches

Product ID	Description
N9K-C9808	16-RU modular switch with slots for up to 8 Line Cards in addition to two supervisors, 8 fabric modules, 4 fan trays, and 3 power trays.

Table 3. Cisco Nexus 9800 Series Line Cards

Product ID	Description
N9K-X9836DM-A	Cisco Nexus 9800 36-port 400G QSFP-DD Line Card with MACsec.

Table 4. Cisco Nexus 9800 Series Fabric Modules

Product ID	Description
N9K-C9808-FM-A	Cisco Nexus 9800 Fabric Module with for 8-slot Chassis

Table 5. Cisco Nexus 9800 Supervisor Module

Product ID	Description	Quantity
N9K-C9800-SUP-A	Cisco Nexus 9800 Platform Supervisor Module	*

Table 6. Cisco Nexus 9800 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9808-FAN-A	Cisco Nexus 9800 8-slot chassis fan tray (1 st Generation)	4

Table 7. Cisco Nexus 9800 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
NXK-HV6.3KW20A-A	Cisco Nexus 9800 6,300W 20A AC and HV Power Supply	9 (3 per tray)	Cisco Nexus 9808

Table 8. Cisco Nexus 9500 Switches

Product ID	Description
N9K-C9504	7.1-RU modular switch with slots for up to 4 Line Cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 4 power supplies.
N9K-C9508	13-RU modular switch with slots for up to 8 Line Cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 8 power supplies.
N9K-C9516	21-RU modular switch with slots for up to 16 Line Cards in addition to two supervisors, 2 system controllers, 3 to 6 fabric modules, 3 fan trays, and up to 10 power supplies.

Table 9. Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9716D-GX	Cisco Nexus 9500 16-port 400G QSFP-DD Line Card	4	8	N/A
N9K-X9736C-FX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8	16
N9K-X9788TC-FX	Cisco Nexus 9500 48-port 1/10-G BASE-T Ethernet	4	8	16

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
	and 4-port 40/100 Gigabit Ethernet QSFP28 Line Card			
N9K-X97160YC-EX	Cisco Nexus 9500 48-port 10/25-Gigabit Ethernet SFP28 and 4-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8	16
N9K-X9732C-FX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8	16
N9K-X9732C-EX	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8	16
N9K-X9736C-EX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8	16

Table 10. Cisco Nexus 9500 R-Series Line Cards

Product ID	Description	Maximum Quantity	
		Cisco Nexus 9504	Cisco Nexus 9508
N9K-X9636C-R	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8
N9K-X9636C-RX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 Line Card	4	8
N9K-X9636Q-R	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP Line Card	4	8
N9K-X96136YC-R	Cisco Nexus 9500 16-port 1/10 Gigabit, 32-port 10/25 Gigabit, and 4-port 40/100 Gigabit Ethernet Line Card	4	8
N9K-X9624D-R2	Cisco Nexus 9500 24-port 400 Gigabit QDD Line Card	Not supported	8

Table 11. Cisco Nexus 9500 Cloud Scale Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM-E	Cisco Nexus 9504 100-Gigabit cloud scale fabric module	4	5
N9K-C9504-FM-G	Cisco Nexus 9500 4-slot 1.6Tbps cloud scale fabric module	4	5
N9K-C9508-FM-E	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9508-FM-E2	Cisco Nexus 9508 100-Gigabit cloud scale fabric module	4	5
N9K-C9508-FM-G	Cisco Nexus 9500 8-slot 1.6Tbps cloud-scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 12. Cisco Nexus 9500 R-Series Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM-R	Cisco Nexus 9504 100-Gigabit R-Series fabric module	4	6
N9K-C9508-FM-R	Cisco Nexus 9508 100-Gigabit R-Series fabric module	4	6
N9K-C9508-FM-R2	Cisco Nexus 9508 400-Gigabit R-Series fabric module	4	6

Table 13. Cisco Nexus 9500 Supervisor Modules

Supervisor	Description	Quantity
N9K-SUP-A	1.8-GHz supervisor module with 4 cores, 4 threads, and 16 GB of memory	2

Supervisor	Description	Quantity
N9K-SUP-A+	1.8-GHz supervisor module with 4 cores, 8 threads, and 16 GB of memory	2
N9K-SUP-B	2.2-GHz supervisor module with 6 cores, 12 threads, and 24 GB of memory	2
N9K-SUP-B+	1.9-GHz supervisor module with 6 cores, 12 threads, and 32 GB of memory	2

Note: N9K-SUP-A and N9K-SUP-A+ are not supported on Cisco Nexus 9504 and 9508 switches with -R Line Cards.

Table 14. Cisco Nexus 9500 System Controller

Product ID	Description	Quantity
N9K-SC-A	Cisco Nexus 9500 Platform System Controller Module	2

Table 15. Cisco Nexus 9500 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3
N9K-C9504-FAN2	Fan tray that supports the Cisco N9K-C9504-FM-G fabric module	3
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3
N9K-C9508-FAN2	Fan tray that supports the Cisco N9K-C9508-FM-G fabric module	3
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3

Table 16. Cisco Nexus 9500 Fabric Module Blanks with Power Connector

Product ID	Description	Minimum	Maximum
N9K-C9504-FAN-PWR	Nexus 9500 4-slot chassis 400G cloud scale fan tray power connector	1	2
N9K-C9508-FAN-PWR	Nexus 9500 4-slot chassis 400G cloud scale fan tray power connector	1	2

Table 17. Cisco Nexus 9500 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
N9K-PAC-3000W-B	3 KW AC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PDC-3000W-B	3 KW DC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PUV-3000W-B	3 KW Universal AC/DC power supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516
N9K-PUV2-3000W-B	3.15-KW Dual Input Universal AC/DC Power Supply	Up to 4 Up to 8 Up to 10	Cisco Nexus 9504 Cisco Nexus 9508 Cisco Nexus 9516

Table 18. Cisco Nexus 9200 and 9300 Switches

Cisco Nexus Switch	Description
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.
N9K-C9364C-GX	2-RU fixed-port switch with 64 100-Gigabit SFP28 ports.
N9K-C93600CD-GX	1-RU fixed-port switch with 28 10/40/100-Gigabit QSFP28 ports (ports 1-28), 8 10/40/100/400-Gigabit QSFP-DD ports (ports 29-36)
N9K-C9364C	2-RU Top-of-Rack switch with 64 40-/100-Gigabit QSFP28 ports and 2 1-/10-Gigabit SFP+ ports. - Ports 1 to 64 support 40/100-Gigabit speeds. - Ports 49 to 64 support MACsec encryption.

Cisco Nexus Switch	Description
	Ports 65 and 66 support 1/10 Gigabit speeds.
N9K-C9332C	1-RU fixed switch with 32 40/100-Gigabit QSFP28 ports and 2 fixed 1/10-Gigabit SFP+ ports.
N9K-C9332D-GX2B	1-Rack-unit (1RU) spine switch with 32p 400/100-Gbps QSFP-DD ports and 2p 1/10 SFP+ ports.
N9K-C9348D-GX2A	48p 40/100/400-Gigabit QSFP-DD ports and 2p 1/10G/10G SFP+ ports
N9K-C9364D-GX2A	64p 400/100-Gigabit QSFP-DD ports and 2p 1/10 SFP+ ports
N9K-C93180YC-FX3	48 1/10/25 Gigabit Ethernet SFP28 ports (ports 1-48) 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54)
N9K-C93180YC-FX3S	48 1/10/25 Gigabit Ethernet SFP28 ports (ports 1-48) 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54)
N9K-C9336C-FX2-E	1- RU switch with 36 40-/100-Gb QSFP28 ports
N9K-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports
N9K-C93360YC-FX2	2-RU switch with 96 10-/25-Gigabit SFP28 ports and 12 40/100-Gigabit QSFP28 ports
N9K-C93240YC-FX2	1.2-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 12 40-/100-Gigabit Ethernet QSFP28 ports.
N9K-C93216TC-FX2	2-RU switch with 96 100M/1G/10G RJ45 ports, 12 40/100-Gigabit QSFP28 ports, 2 management ports (one RJ-45 and one SFP port), 1 console, port, and 1 USB port.
N9K-C93180YC-FX	1-RU Top-of-Rack switch with 10-/25-/32-Gigabit Ethernet/FC ports and 6 40-/100-Gigabit QSFP28 ports. You can configure the 48 ports as 1/10/25-Gigabit Ethernet ports or as FCoE ports or as 8-/16-/32-Gigabit Fibre Channel ports.
N9K-C93180YC-FX-24	1-RU 24 1/10/25-Gigabit Ethernet SFP28 front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. The SFP28 ports support 1-, 10-, and 25-Gigabit Ethernet connections and 8-, 16-, and 32-Gigabit Fibre Channel connections.
N9K-C93108TC-FX	1-RU Top-of-Rack switch with 48 100M/1/10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-FX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports.
N9K-C93108TC-FX3P	1-RU fixed-port switch with 48 100M/1/2.5/5/10GBASE-T ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C9348GC-FXP	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP
N9K-C92348GC-X	The Cisco Nexus 92348GC-X switch (N9K-C92348GC-X) is a 1RU switch that supports 696 Gbps of bandwidth and over 250 mpps. The 1GBASE-T downlink ports on the 92348GC-X can be configured to work as 100-Mbps, 1-Gbps ports. The 4 ports of SFP28 can be configured as 1/10/25-Gbps and the 2 ports of QSFP28 can be configured as 40- and 100-Gbps ports. The Cisco Nexus 92348GC-X is ideal for big data customers that require a Gigabit Ethernet ToR switch with local switching.
N9K-C93180YC-EX	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93180YC-EX-24	1-RU 24 1/10/25-Gigabit front panel ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports
N9K-C93108TC-EX	1-RU Top-of-Rack switch with 48 10GBASE-T (copper) ports and 6 40-/100-Gigabit QSFP28 ports
N9K-C93108TC-EX-24	1-RU 24 1/10GBASE-T (copper) front panel ports and 6 40/100-Gigabit QSFP28 spine facing ports.

Table 19. Cisco Nexus 9200 and 9300 Fans and Fan Trays

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-FAN-160CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	9364C ^[1] 93360YC-FX2
NXA-FAN-160CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	3	9364C ^[1] 93360YC-FX2
NXA-FAN-160CFM2-PE	Fan module with port-side exhaust airflow (blue coloring)	4	9364C-GX
NXA-FAN-160CFM2-PI	Fan module with port-side intake airflow (burgundy coloring)	4	9364C-GX
NXA-FAN-30CFM-B	Fan module with port-side intake airflow (burgundy coloring)	3	93108TC-EX 93108TC-FX ^[1] 93180YC-EX

¹ For specific fan speeds see the Overview section of the Hardware Installation Guide.

Product ID	Description	Quantity	Cisco Nexus Switches
			93180YC-FX [1] 9348GC-FXP [1]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	93108TC-EX 93108TC-FX [1] 93180YC-EX 93180YC-FX [1] 9348GC-FXP
NXA-FAN-35CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	4	92300YC [1] 9332C [1] 93180YC-FX3S [2] 93180YC-FX3 93108TC-FX3P
		6	9336C-FX2-E 9316D-GX 93600CD-GX
NXA-FAN-35CFM-PI	Fan module with port-side intake airflow (burgundy coloring)	4	92300YC [1] 9332C [1] 93180YC-FX3S [2] 93180YC-FX3 93108TC-FX3P
	Fan module with port-side exhaust airflow (blue coloring)	6	9316D-GX 93600CD-GX
	Fan module with port-side exhaust airflow (blue coloring)	6	9336C-FX2-E
NXA-FAN-65CFM-PE	Fan module with port-side exhaust airflow (blue coloring)	3	93240YC-FX2 [1] 9336C-FX2 [1]
NXA-FAN-65CFM-PI	Fan module with port-side exhaust airflow (burgundy coloring)	3	93240YC-FX2 9336C-FX2 [1]

Table 20. Cisco Nexus 9200 and 9300 Power Supplies

Product ID	Description	Quantity	Cisco Nexus Switches
NXA-PAC-500W-PE	500-W AC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180YC-EX 93180YC-FX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180YC-EX 93180YC-FX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92300YC 93180YC-FX3S 93108TC-EX 93180YC-EX 93180YC-FX3
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92300YC 93180YC-FX3S 93108TC-EX 93180YC-EX 93180YC-FX3
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) 1	2	9336C-FX2 9336C-FX2-E 9332C 93240YC-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side intake airflow	2	9336C-FX2

² This switch runs with +1 redundancy mode so that if one fan fails, the switch can sustain operation. But if a second fan fails, this switch is not designed to sustain operation. Hence before waiting for the major threshold temperature to be hit, the switch will power down due to entering the fan policy trigger command.

Product ID	Description	Quantity	Cisco Nexus Switches
	(burgundy coloring) 1		9336C-FX2-E 9332C 93240YC-FX2
NXA-PAC-1100W-PE2	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9332C 9316D-GX 9336C-FX2 9336C-FX2-E 93600CD-GX
NXA-PAC-1100W-PI2	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 9332C 9316D-GX 9336C-FX2 9336C-FX2-E 93600CD-GX
NXA-PAC-1100W-PI	Cisco Nexus 9000 PoE 1100W AC PS, port-side intake	2	93108TC-FX3P
NXA-PAC-1100W-PE	Cisco Nexus 9000 PoE 1100W AC PS, port-side exhaust	2	93108TC-FX3P
NXA-PAC-1900W-PI	Cisco Nexus 9000 PoE 1900W AC PS, port-side intake	2	93108TC-FX3P
NXA-PAC-1200W-PE	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	93360YC-FX2 9364C
NXA-PAC-1200W-PI	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	93360YC-FX2 9364C
N9K-PUV-1200W	1200-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92300YC 93108TC-EX 93108TC-FX 93360YC-FX2 93180YC-FX3S 93180YC-EX 93180YC-FX 9364C
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93180YC-FX 9364C
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S 93180YC-FX 9364C
NXA-PDC-1100W-PE	1100-W DC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX 9332C 9336C-FX2 9336C-FX2-E
NXA-PDC-1100W-PI	1100-W DC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 93600CD-GX 9316D-GX 9332C 9336C-FX2 9336C-FX2-E
UCSC-PSU-930WDC	930-W DC power supply with port-side intake (green coloring)	2	93108TC-EX 93180YC-EX
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust (gray coloring)	2	93108TC-EX 93180YC-EX
NXA-PHV-1100W-PE	1100-W AC power supply with port-side exhaust airflow (blue coloring)	2	93240YC-FX2 9336C-FX2
NXA-PHV-1100W-PI	1100-W AC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 9336C-FX2
NXA-PAC-2KW-PE	2000-W AC power supply with port-side exhaust	2	9364C-GX

Product ID	Description	Quantity	Cisco Nexus Switches
	airflow (blue coloring)		
NXA-PAC-2KW-PI	2000-W AC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
NXA-PDC-2KW-PE	2000-W DC power supply with port-side exhaust airflow (blue coloring)	2	9364C-GX
NXA-PDC-2KW-PI	2000-W DC power supply with port-side intake airflow (burgundy coloring)	2	9364C-GX
N2200-PAC-400W	400-W AC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X
N2200-PAC-400W-B	400-W AC power supply with port-side intake airflow (burgundy coloring)	2	92348GC-X
N2200-PDC-350W-B	350-W DC power supply with port-side intake airflow	2	92348GC-X
N2200-PDC-400W	400-W DC power supply with port-side exhaust airflow (blue coloring)	2	92348GC-X

Compatibility Information

Fabric Module and Line Card compatibility details are listed below:

Table 21. Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	N9K-C9504-FM-G	N9K-C9508-FM-G	N9K-C9504-FM-E	N9K-C9508-FM-E	N9K-C9508-FM-E2	N9K-C9516-FM-E2
N9K-X9716D-GX	4	4	No	No	No	No
N9K-X9736C-FX	5	5	5	5	5	5
N9K-X97160YC-EX	4	4	4	4	4	4
N9K-X9788TC-FX	4	4	4	4	4	4
N9K-X9732C-EX	4	4	4	4	4	4
N9K-X9736C-EX	4	4	4	4	4	4
N9K-X9732C-FX	4	4	4	4	4	4
	5 (n+1 redundancy)	5 (n+1 redundancy)	5 (n+1 redundancy)	5 (n+1 redundancy)	5 (n+1 redundancy)	5 (n+1 redundancy)

Table 22. Cisco Nexus 9500 R-Series Line Cards

Product ID	N9K-C9504-FM-R	N9K-C9508-FM-R
N9K-X9636C-RX	6	6
N9K-X9636Q-R	4	4
	6 (n+2 redundancy)	6 (n+2 redundancy)
N9K-X9636C-R	5	5
	6 (n+1 redundancy)	6 (n+1 redundancy)
N9K-X96136YC-R	6	6

Table 23. Cisco Nexus 9500 R2-Series Line Cards

Product ID	N9K-C9508-FM-R2
N9K-X9624D-R2	6

Optics

For information about transceivers and cables supported on a switch, see the [Transceiver Module \(TMG\) Compatibility Matrix](#). For the transceiver specifications and installation information, see the [Install and Upgrade Guides](#).

Cisco Nexus Dashboard Insights for Data Center

Cisco NX-OS Release 10.3(4a)M supports the Nexus Dashboard Insights on Cisco Nexus 9200, 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, 9400, and 9800 platform switches and 9500 platform switches with - EX/FX/GX Line Cards. See the [Cisco Nexus Insights documentation](#).

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.3(x). For information about an In Service Software Upgrade (ISSU), see the [Cisco NX-OS ISSU Support Matrix](#).

Related Content

Cisco Nexus 9000 Series documentation: [Cisco Nexus 9000 Series Switches](#)

Cisco NX-OS Software Release and Image-naming Convention: [Cisco NX-OS Software Strategy and Lifecycle Guide](#)

Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator: [Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator](#)

Cisco Nexus 9000 Series Software Upgrade and Downgrade Guide: Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.3(x).

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes: Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 10.3(4a).

Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference: [Cisco Nexus NX-API Reference](#)

Cisco NX-OS Supported MIBs:
<ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html>

Supported FEX modules: [Cisco Nexus 9000 Series Switch FEX Support Matrix](#)

Licensing Information: [Cisco NX-OS Licensing Guide](#) and [Cisco Nexus Smart Licensing Using Policy User Guide](#)

When you downgrade from Cisco NX-OS Release 10.3(4a)M to an earlier release, the features that use the ACI+NX-OS Essentials, Advantage, and add-on licenses or the Hardware Streaming Telemetry license continue to work in honor mode in the downgraded version. In addition, the output of the show license usage command continues to include entries for these unsupported licenses.

See the [Cisco NX-OS Licensing Guide](#).

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2023 Cisco Systems, Inc. All rights reserved.