Cisco Nexus 9000 Series NX-OS Release Notes, Release 9.3(6)

This document describes the features, issues, and exceptions of Cisco NX-OS Release 9.3(6) software for use on Cisco Nexus 9000 Series switches.

For more information, see Related Content.

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.

Date	Description
November 10, 2020	Cisco NX-OS Release 9.3(6) became available.
May 13, 2021	Added information about 93108TC-FX3P.
April 25, 2024	Added CSCwh50989 to Open Issues.

Contents

New and Enhanced Software Features

The enhanced features listed below are existing features introduced in earlier releases but enhanced to support new platforms in Cisco NX-OS Release 9.3(6).

New Features	
Feature	**Description**
VXLAN and IP-in-IP Tunneling	Added support for the coexistence of these features for Cisco Nexus 9300-FX2 platform switches. Coexistence of these features requires isolating IP-in-IP tunnels and VXLAN within their own VRFs. By isolating the VRFs, both VXLAN and the tunnels operate independently. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Enhanced Features	
Feature	**Description**
SVI Interfaces for BGP Interface Peering	Added support for Cisco Nexus 9000 Series switches. For more information, see the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x).
PBR over VXLAN	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
Proportional Multipath for VNF	Added support for Cisco Nexus 9500 platform switches with the N9K-C9508-FM-2 fabric module. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN EVPN Multi-Site Storm Control	Added enhancements to optimize rate granularity and accuracy. Bandwidth is calculated based on the accumulated DCI uplink bandwidth, and only interfaces tagged with DCI tracking are considered. In addition, granularity is enhanced by supporting two digits after the decimal point. These enhancements apply to Cisco Nexus 9300-EX, 9300-FX/FXP/FX2/FX3, and 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN Flood and Learn	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
VXLAN with IPv6 in the Underlay (VXLANv6)	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).

New Features	
Feature	Description
Proportional Multipath for VNF with Multi-Site	Introduced this feature for Cisco Nexus 9364C, 9300-EX, and 9300-FX/FX2/FX3 platform switches and Cisco Nexus 9500 platform switches with the N9K-C9508-FM-E2 fabric module and an -EX or -FX line card. This feature allows traffic to be sent across sites if a local VNF is not available. For more information, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x).
SVI Unnumbered	Added support for Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x).
Multicast Network Load Balancing	Added Multicast Network Load Balancing support on Cisco Nexus 9300-GX platform switches. For more information, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x).
Service exclude-bootconfig	Support added for the service exclude-bootconfig command to exclude the boot nxos image configuration from show and copy configuration commands. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).
PTPv1 Forwarding	Support added for the ptp forward-version1 command which forwards all PTPv1 packets based on the forwarding rule and prevents these packets from being dropped. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x).

New Hardware Features

No new hardware features are introduced for Cisco NX-OS Release 9.3(6).

Release Versioning Strategy

Cisco Nexus 9000 Series switches and the Cisco Nexus 3000 Series switches, use the same NX-OS binary image also called the "unified" image. The binary image covers all variations of the Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. Cisco NX-OS Release 9.2(1) was the first release that adopted unified version numbering. With unified version numbering, the platform designator is obsolete.

Moving forward for the previously identified platforms, we will be adopting the simplified 3-letter versioning scheme. For example, a release with X.Y(Z) would mean:

X - Unified release major

Y - Major / Minor release

Z - Maintenance release (MR)

Where the Z = 1 is always the first FCS release of a Major/Minor release.

An example of a previous release number is: 7.0(3)I7(4). In this format, **the 'I'** is the platform designator.

Note: In order to accommodate upgrade compatibility from an older software version that is expecting a platform designator, when the install all command is entered or the show install all impact command is entered, the version string appears as 9.3(6)I9(1). The "I9(1)" portion of the string can be safely ignored. It will later appear as 9.3(6).

Note: The Cisco Nexus 34180YC and 3464C platform switches are not supported in Cisco NX-OS Release 9.3(6).

Open Issues

Bug ID	Description
CSCvq33024	Headline: TRM Multisite: traffic drop on BGW after restarting ngmvpn Symptoms: TRM traffic loss for 1-2 seconds. Workarounds: None
CSCvw38210	Headline: FX2: ipfib crash post ND-ISSU when multicast global-span-tx Symptoms: On 9300-EX/FX2 switches, ipfib crash is observed post non-disruptive install (ND ISSU) in the presence of the configuration 'hardware multicast global-span-**tx'.** Workarounds: Disable by "no hardware multicast global-span-tx", copy run start or chose disruptive install upgrade. The "hardware multicast global-span-tx" command can be enabled post upgrade.
CSCvq15147	Headline: Interface BW not accounting unicast BW after SSO switchover Symptoms: After a switchover, the unicast fabric bandwidth does not get reserved on fabric links. Workarounds: Flapping the fabric interface should fix it.
CSCvw42172	Headline: grpc core seeing with the command grpc use-vrf default and no feature grpc/feature grpc Symptoms: The grpc process crashes when trying to unconfigure grpc ("no feature grpc") when the base grpc config has "grpc use-vrf default" already configured. After this feature grpc cannot be re-enabled. Workarounds: 1. Go to bash prompt by doing "run bash sudo su" . 2. Kill the grpc process 3 times by doing "kill \`pidof grpc". 3. Check that the process doesn't exist by doing "ps aux | grep grpc". 4. Come back to CLI from bash shell by running "exit". 5. The grpc feature can be enabled now if needed.

Bug ID	Description
CSCwh50989	Headline: Custom COPP causing transit traffic to be punted to the CPU on Nexus 9300-GX2
	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.
	Workarounds: Custom COPP policy using src/dst match mitigates punt for transit traffic.

Resolved Issues

Bug ID	Description
CSCvv04779	Headline: FEX 2248 is dropping multicast during IGMP update from client on a different FEX
	Symptoms: FEX N2K-C2248TP-E-1GE with a Nexus 5000 parent switch is intermittently dropping a small number of multicast packets during IGMP updates coming to the parent switch.
	Workarounds: Replace the FEX with a switch.
CSCvo04435	Headline: FEX port running FCoE goes into ErrDisabled (Pause Frame) without RX pause frames
	Symptoms: FCoE Ethernet ports are repeatedly going into error disabled state with the reason of excessive Rx pause frames.
	The message is:
	%ETHPORT-5-IF_DOWN_ERROR_DISABLED: Interface Ethernet162/1/2 is down (Error disabled. Reason:error)
	show interface eth162/1/2 Ethernet162/1/2 is down (ErrDisabled(Pause Frame))
	This occurs without any Rx pause frames being received at the time.
	There was Rx pause frames previously and eventually but when the port is error disabled there are no pause frames being received.
	Workarounds: A reload of the FEX allows the port to function for an undetermined amount of time. Once the port goes error disabled each time it is shutdown/no shutdown it immediately fails within a few seconds.
	Use Ethernet ports on the upstream switch.
CSCvo30537	Headline: VXLAN Multi-Site storm control
	Symptoms: When the storm control level is configured in EVPN Multi-Site for broadcast and unknown unicast, the reference used is the total aggregate bandwidth available on the DCI links and the fabric links.
	This bug documents a change in behavior for EVPN Multi-Site storm control where this feature only uses the bandwidth available on the DCI links.
	Workarounds: None

Bug ID	Description
CSCvu01334	Headline: Unable to delete PBR under Physical Interface Symptoms: This was on a N9K-C9336C-FX2 running 9.3(3). [+] Unable to remove the PBR configured under Physical interface. [+] Getting Following Error message when tried to remove it. switch(config)# interface ethernet 1/5 switch(config-if)# no ip policy route-map rm_webcache4 There are no ip policy configured on this interface <<< switch(config-if)# end switch# sh accounting log Fri Apr 17 07:03:37 2020:type=update:id=10.10.10.49@pts/0:user=test.s:cmd=configure terminal ; interface Ethernet1/5 (REDIRECT) Fri Apr 17 07:03:37 2020:type=update:id=10.10.10.49@pts/0:user=test.s:cmd=configure terminal ; interface Ethernet1/5 (SUCCESS) Fri Apr 17 07:03:49 2020:type=update:id=10.10.10.49@pts/0:user=test.s:cmd=configure terminal ; interface Ethernet1/5 ; no ip policy route-map rm_webcache4 (REDIRECT) Fri Apr 17 07:03:49 2020:type=update:id=10.10.10.49@pts/0:user=test.s:cmd=configure terminal ; interface Ethernet1/5 ; no ip policy route-map rm_webcache4 (FAILURE) Nothing shown up in logging log and nvram : switch# sh logging nvram last 20 2020 Apr 14 10:12:07 switch %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online 2020 Apr 14 10:12:05 switch %$ VDC-1 %$ %CARDCLIENT-2-FPGA_BOOT_PRIMARY: MIFPGA booted from Primary switch# sh logging last 20 2020 Apr 17 06:56:08 switch %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 10.10.10.49 - login 2020 Apr 17 07:03:52 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by test.s on 10.10.10.49@pts/0 2020 Apr 17 07:06:35 switch last message repeated 1 time Workarounds: reload ascii binary reload might not help
CSCvu47516	Headline: With QinVNI enabled, VXLAN packets in fabric carry .1q tag in outer header Symptoms: *VXLAN MCAST encapsulated BUM traffic dropped on transit spine node. Workarounds: *Removing the "nv overlay feature" on the spine node resolves the issue. (no feature nv overlay)

Bug ID	Description
CSCvu48458	Headline: EVPN: BGW reload in a square topology causes packet loss Symptoms: 200+sec of traffic loss with BGW reload and doesn't perform encap/decap until NVE loopbacks are up. Workarounds: None
CSCvu57731	Headline: N9K: DHCP Relay ACLs not programmed into TCAM after FEX fabric port-channel member comes up Symptoms: A Cisco Nexus 9500 platform switch with FEX fabric port-channel members spread across multiple line cards might fail to program DHCP Relay ACLs into TCAM if a FEX fabric port-channel member is administratively bounced before and after a module reload. Workarounds: This issue can be proactively mitigated by not administratively shutting down FEX fabric port-channel members prior to module reloads. This issue can be reactively worked around by reloading the Cisco Nexus 9500 platform switch without modifying the administrative state of FEX fabric port-channel members.

CSCvu69850	Headline: CPU-PG stuck after port flapping
	
	Symptoms: Port flapping cause the cpu-pg stuck and trigger the port-channel member port-suspend
	
	<pre>|--|
	| Output Pool-Group Buffer Utilization (cells/desc) |
	| Drop-PG No-drop CPU--PG LCPU-PG RCPU-PG SPAN-PG |
	|--|
	Total Instant Usage (cells) 76636 0 1361 0 0 0 |</pre>
	Workarounds: shutdown / no shutdown the issue port. This will release the cpu-pg and the issue clears.

Bug ID	Description
CSCvu76284	Headline: N9K Service "tahusd" crashed without intervention Symptoms: N9K-C9348GC-FXP/9.2(3) reload because of tahusd crashed without intervention. 2020 May 20 22:27:21 %$ VDC-1 %$ May 20 22:27:21 %KERN-2-SYSTEM_MSG: [7496306.170307] usd process 29349, uuid 1356 (0x54c) failed to send heartbeat - kernel 2020 May 20 22:27:23 %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 29349) hasn't caught signal 6 (core will be saved). 2020 May 20 22:27:25 %$ VDC-1 %$ %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "tahusd" in vdc 1 has had a hap failure 2020 May 20 22:27:25 %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 17386 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) . 2020 May 20 22:28:36 %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: core_client_main: PID 21120 with message filename = 0x102_tahusd_log.29349.tar.gz . 2020 May 20 22:28:37 %$ VDC-1 %$ %MODULE-2-MOD_DIAG_FAIL: Module 1 (Serial number: FDO234503GW) reported failure due to Service on linecard had a hap-reset in device DEV_SYSMGR (device error 0x54c) Workarounds: none
CSCvu78592	Headline: N9K-C93180YC-FX3S/N9K-C93108TC-FX3P: Unknown System-reset on write-erase and powercycle Symptoms: After below mentioned sequence, we see reset caused as Unknown for show system reset-reason CLI. Workarounds: We can check the reset-reason read by fpga read, via show system internal cardclient logs | i "crdcl_get_board_reset_reason: reason:" for example: show system internal cardclient logs | i "crdcl_get_board_reset_reason: reason:" [102] crdcl_get_board_reset_reason: reason:0x00000070 for power-cycle the reason number is 0x70(112). an alternative CLI to see reset-reason history is also present: show logging onboard internal reset-reason

Bug ID	Description
CSCvu80471	Headline: VXLAN vPC VTEP - Extended traffic loss when vPC peer reloads before NVE source hold timer expiry Symptoms: Traffic loss for hosts behind vPC in a VXLAN setup. NVE interface remains down after source hold-down timer expiry: # show nve interface nve1 det <> Source Interface hold-down-time: 180 >>> default time Source Interface hold-up-time: 30 Remaining hold-down time: 67 seconds. <<< after countdown finishes, goes to 0 From the same device, we can see the following in the log: %ETHPORT-5-IF_DOWN_NONE: Interface port-channel1 is down (None) <<< Virtual peer-link goes down %USER-2-SYSTEM_MSG: NVE: send reinit to bring down nve1 - nve <<< NVE goes down %NVE-5-NVE_INTF_STATE: nve1: NVE Interface state changed to down From here, VXLAN traffic stops and all the devices behind the vPC will have traffic blocked for an extended duration Workarounds: Do not upgrade/reload on the vPC peer switch (SW2) before the NVE source hold-down timer has expired on SW1.

Bug ID	Description
CSCvu82331	Headline: N9K: Native VLAN is not programmed correctly for Port-channels once re-configured Symptoms: After reload, if the portchannel, that has native VLAN configured, is re-configured to have new native VLAN, before this particular port channel goes to link UP state first time, the new native VLAN is not programmed correctly. LEAF3-FX# show int Po101 port-channel101 is down (No operational members) admin state is up, LEAF3-FX# sh run int Po101 | i native switchport trunk native vlan 666 LEAF3-FX# show sys int eltm info interface Po101 | grep -A 1 Operation Operational VLAN's (1): 666 LEAF3-FX# show hard int tah int Po101 | i default info_default_vlan : 666 LEAF3-FX# conf t LEAF3-FX(config)# int Po101 LEAF3-FX(config-if)# switchport trunk native vlan 1158 LEAF3-FX(config-if)# switchport trunk allowed vlan 1158 LEAF3-FX# sh run int Po101 | i native switchport trunk native vlan 1158 LEAF3-FX# show sys int eltm info interface Po101 | grep -A 1 Operation Operational VLAN's (1): 666 LEAF3-FX# show hard int tah int Po101 | i default info_default_vlan : 666 Workarounds: Bounce affected port channel.

Bug ID	Description
CSCvu82659	Headline: L2ACLREDIRECT diagnostic test fails for module N9K-X9732C-EX Symptoms: The L2ACLRedirect Gold diagnostics may fail for a Cisco Nexus 9732C-EX line card. The Cisco Nexus 9500 platform switch reports the following in the log: 2020 May 16 05:27:00.314 %DIAGCLIENT-2-EEM_ACTION_HM_SHUTDOWN: Test <L2ACLRedirect> has been disabled as a part of default EEM action 2020 May 16 05:27:00.314 %DIAG_PORT_LB-2-L2ACLREDIRECT_LOOPBACK_TEST_FAIL: Module:2 Test:L2ACLRedirect Loopback failed 10 consecutive times. Faulty module: affected ports:1,33,65,97 Error:Loopback test failed. Packets lost on the SUP in the receive direction 2020 May 16 05:27:00.323 %MODULE-4-MOD_WARNING: Module 2 (Serial number: FOC2413300R) reported warning due to Loopback test failed. Packets lost on the SUP in the receive direction in device DEV_SUPERVISOR_CTRL (device error 0x41830059) Workarounds: The workaround is to set the values of the following regions to non-zero values or set the values of these regions to the default configuration as shown below: no hardware access-list tcam region ing-racl 0 no hardware access-list tcam region ing-l2-qos 0 no hardware access-list tcam region ing-l3-vlan-qos 0
CSCvu84153	Headline: N9500-R acting as non-DR stops bridging mcast traffic after sg-expiry-timer expires Symptoms: Mcast traffic not reaching receiver connected to non-DR 9500-R device. Workarounds: Use vPC PL between DR and non-DR 9500-R.
CSCvu89271	Headline: usdk_sse: retry_count:3 mts_rcv failed Symptoms: %KERN-3-SYSTEM_MSG: [10800222.648254] usdk_sse: retry_count:3 mts_rcv failed:-4 rcvind from 0x102.594 errno 0 calling_pid 20997 stv:1591733785:216349 etv:1591733785:216374 - kernel Workarounds: None
CSCvu90939	Headline: N9K - Mgmt0 sending out signals when force admin Shut Symptoms: 93108TC-FX Ethernet port shows Up when remote mgmt0 of Cisco Nexus 9364C is admin down. Workarounds: No workaround
CSCvv00690	Headline: N9K - Mgmt0 RJ45 copper port goes down, once SFP is inserted on SFP port **Symptoms: Mgmt0 port on a Cisco Nexus 9000 Series switch goes down and doesn't come back up.** During the problem state, we have seen both RJ45 and SFP ports going down and stuck in down state. Workarounds: Setting the speed to 100 fixes the problem or removing the SFP from the SFP mgmt0 port brings up the RJ-45 port.

Bug ID	Description
CSCvv09729	Headline: Cisco Nexus 92348 back pressure results in PSU fan spinning wrong direction Symptoms: The power supply exhaust fan may spin in the wrong direction on the Cisco Nexus 92348. Workarounds: None
CSCvv09753	Headline: BGP mass prefix withdrawal causing high CPU spikes for event_manager and policyelem Symptoms: # # sh processes cpu | exclude 0.00 PID Runtime(ms) Invoked uSecs 1Sec Process ----- ----------- -------- ----- ------ ----------- 52 229124253 317691941 721 1.00% ksmd 28182 1027 290 3543 31.25% event_manager 28183 1948 523 3726 8.75% policyelem 28341 1286455 10566658 121 1.50% vman 28389 263 208 1266 0.50% confelem 28466 12223331 12799864 954 0.50% diagmgr 28531 183686 9203510 19 0.50% nginx 28535 290028 5637064 51 15.75% device_test 28689 275 123 2240 0.50% adjmgr 30088 231051 4497027 51 0.50% l2rib 30269 2085655 7006841 297 0.50% diag_port_lb 30270 79629350 558705133 142 1.50% ethpm 30409 365 364 1004 5.00% BGP 30429 353 284 1245 0.50% ospf 31735 183889131 2147483647 16 1.50% mts-sync-thr PID Runtime(ms) Invoked uSecs 1Sec Process ----- ----------- -------- ----- ------ ----------- 11833 187091199 2147483647 17 2.00% mts-sync-thr 27844 996 282 3532 30.25% event_manager 27845 1928 541 3564 8.75% policyelem PID Runtime(ms) Invoked uSecs 1Sec Process ----- ----------- -------- ----- ------ ----------- 27844 996 282 3532 34.25% event_manager 27845 1928 541 3564 23.00% policyelem 28048 287 921 311 2.00% confelem Workarounds: NA
CSCvv10145	Headline: nginx process memory leak while polling device via NXAPI Symptoms: A Cisco Nexus switch may experience a memory leak in the nginix process while polling the device via NXAPI. Workarounds: 1. Disable and then enable nxapi feature to restore the memory. N9K#(config)# no feature nxapi N9K#(config)# feature nxapi 2. Reload the box.

Bug ID	Description
CSCvv10248	Headline: N9K-C9372PX - Ports Fail to Come Up after upgrade from Cisco NX-OS 7.0(3)I4(7) to 7.0(3)I7(7) Symptoms: N9K-C9372PX - Ports Fail to Come Up after upgrade from Cisco NX-OS 7.0(3)I4(7) to 7.0(3)I7(7) Workarounds: No, only downgrade to Cisco NX-OS 7.0(3)I4(7) brings the link up.

Bug ID	Description
CSCvv12119	Headline: N9K EOR / N9K-SUP-A+ / Acl-mgr crash Symptoms: --- Reason: Reset triggered due to HA policy of Reset Service: aclmgr hap reset Version: 9.3(1) --- Crash Decode: --- #0 0xf7708bf0 in __kernel_vsyscall () #1 0xf60dfcd6 in __bsd_signal (sig=-166843161, handler=0x6) at ../sysdeps/posix/signal.c:32 #2 0xffb34b14 in ?? () #3 0xf7056106 in mts_is_reject (msg_ref=0xffb350fb) at ../infra/mts/lib//mts_common.c:503 #4 0xf64f1ca9 in mpmts_is_mpmts (mts_q=8, msg_ref_p=0xffb350fb) at ../utils/libmpmts/mpmts.c:1253 #5 0xf64efd9d in mpmts_drop (mts_q=8, msg_ref_p=0xffb350fb) at ../utils/libmpmts/mpmts.c:402 #6 0x103c4017 in aclmgr_stat_ha_sync_send_update (client=2248147310, rootnode=71303717, msg=0x11f8c7ac " ", len=96) at ../feature/acl_mgr/server/aclmgr_stat.c:1528 #7 0x103ab85b in aclmgr_stat_update (client=2248147310, rootnode=71303717, msg=0x11f8c7ac " ", len=96) at ../feature/acl_mgr/server/aclmgr_stat.c:297 #8 0x1020daf8 in aclmgr_ppf_rdy_ntf_fun (ses_handle=0xcbb8a31f, session_id=18374969612505979315, statustype=Ddb_srv_ses_sts_rqst_done, nstatus=19, usr_data_ptr=0x0) at ../feature/acl_mgr/server/aclmgr_ppfsess.c:1665 #9 0xf65edaee in ddb_srv_ses_ntf (srv_ses=0x11e1c4fc, ntf_sts=Ddb_srv_ses_sts_rqst_done) at ../utils/libddb/server/ddb_srv_ses.c:4475 #10 0xf65edd02 in ddb_srv_ses_cl_done_action (srv_ses=0x11e1c4fc) at ../utils/libddb/server/ddb_srv_ses.c:4543 #11 0xf65e404c in ddb_srv_ses_state_change_exe (new_state_fun=0xf65edb69 <ddb_srv_ses_cl_done_action>, srv_ses=0x11e1c4fc) at ../utils/libddb/server/ddb_srv_ses.c:726 #12 0xf65e423c in ddb_srv_ses_state_change_no_flush (new_state=Ddb_srv_ses_state_rqst_done, next_fun=0xf65edb69 <ddb_srv_ses_cl_done_action>, srv_ses=0x11e1c4fc) at ../utils/libddb/server/ddb_srv_ses.c:787 #13 0xf65ede9b in ddb_srv_ses_status_ready (srv_ses=0x11e1c4fc, next_state=Ddb_srv_ses_state_rqst_done) at ../utils/libddb/server/ddb_srv_ses.c:4616 #14 0xf65ee061 in ddb_srv_ses_status_ready_chk (clgrp=0x11e1c794, srv_ses=0x11e1c4fc, next_state=Ddb_srv_ses_state_rqst_done, state_change=0x0) at ../utils/libddb/server/ddb_srv_ses.c:4645 #15 0xf65eecd6 in ddb_srv_ses_msg_status (expected_state=Ddb_srv_ses_state_rqst, msg=0x11d96474, srv_db=0x11c7684c, msg_process_status=0xffb35f40) at ../utils/libddb/server/ddb_srv_ses.c:4913 #16 0xf65e18b9 in ddb_srv_process_msg (msg=0x11d96474, db=0x11c0b26c, usr_data_ptr=0x0, msg_process_status=0xffb35f40) at ../utils/libddb/server/ddb_srv_msg.c:106 #17 0xf6632b25 in ddb_process_msg (db_handle=0xcb99d697, mts_msg_ref=0x1214f8a8, usr_data_ptr=0x0, msg_processing_status=0xffb36308) at ../utils/libddb/common/ddb_intf.c:1947 #18 0xf65bea7c in ppf_process_msg (db_handle=0xcb99d697, mts_msg_ref=0x1214f8a8, usr_data_ptr=0x0, msg_processing_status=0xffb36308) at ../utils/libppf/common/ppf_intf.c:871 #19 0x10163863 in aclmgr_hdl_ppf_msg (event_p=0x1214f89c, ret_fsm_event_list_pp=0xffb36c1c) at ../feature/acl_mgr/server/aclmgr_msg_handlers.c:312 #20 0x10151c37 in aclmgr_demux (event=0x1214f89c, ret_fsm_event_list=0xffb36c1c) at ../feature/acl_mgr/server/aclmgr_fu.c:1580 #21 0xf6ed023d in fu_fsm_engine_process_app_ev (event=0x1214f89c, new_ev=0x1214f93c, fsm_event_list_ref=0xffb36c1c, demux_ev_ref=0xffb36c18) at ../utils/fsmutils/fsm.c:2205 #22 0xf6ed1c6a in fu_fsm_engine () at ../utils/fsmutils/fsm.c:2536 #23 0x101020cd in main (argc=1, argv=0xffb372e4) at ../feature/acl_mgr/server/aclmgr_main.c:449--- Workarounds: N/A

Bug ID	Description

CSCvv13718	Headline: Service aclmgr crashing with hap failure in Nexus9K
	
	Symptoms: The 'aclmgr' process crashes several times and caused switch to be in boot loop.
	
	<pre>
	2020 Jun 17 15:01:02 s1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service 'aclmgr' (PID 26533) hasn't caught signal 11 (core will be saved).
	2020 Jun 17 15:01:03 s1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service 'aclmgr' (PID 26899) hasn't caught signal 11 (core will be saved).
	2020 Jun 17 15:01:03 s1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service 'aclmgr' (PID 27049) hasn't caught signal 11 (core will be saved).
	2020 Jun 17 15:01:04 s1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service 'aclmgr' (PID 27314) hasn't caught signal 11 (core will be saved).
	2020 Jun 17 15:01:04 s1 %$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service 'aclmgr' in vdc 1 has had a hap failure
	</pre>
	
	And the core file is found with the 'show cores'
	
	</pre>
	
	Workarounds: This is an enhancement.

CSCvv14030	Headline: IPV6 Multihop BFD still uses single hop mode even when directly connected interface is shut down Symptoms: Source interface is Vlan300 instead the one set in bgp update source. Type is SH instead of MH OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int. Vrf Type fa00:1::1 fc00:1::3. 1090519042/0 Down N/A(3) Down Vlan300 default SH On Wireshark capture the device does receives the BFD with lo0: 2020-06-29 12:53:30.805031 fc00:1::3 -> fa00:1::1 BFD Control Diag: No Diagnostic, State: Down, Flags: 0x00 Workarounds: None
CSCvv17486	Headline: N9K-C93216TC-FX2 - Some ports fail to come up after having cable inserted Symptoms: Some ports (typically groups of 4) will fail to come up on N9K-C93216TC-FX2 after having a cable installed Workarounds: Reload the impacted switch

Bug ID	Description
CSCvv20329	Headline: Cisco Nexus 9000 reloads due to "NVE" process Symptoms: Cisco Nexus 9000 reloads with "NVE" core files generated atomic250-lsw03-1 %$ VDC-1 %$ %VPC-2-PEER_KEEP_ALIVE_RECV_FAIL: In domain 1, VPC peer keep-alive receive has failed atomic250-lsw03-1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nve" (PID 29875) hasn't caught signal 6 (core will be saved). atomic250-lsw03-1 %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay Done. atomic250-lsw03-1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready atomic250-lsw03-1 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nve" (PID 31970) hasn't caught signal 6 (core will be saved). Workarounds: Before upgrading, reduce the scale of VNIs to less than 3000, preferably to the supported number of VNIs on that release and then upgrade the switch.
CSCvv21551	Headline: Memory leak in "ascii-cfg" process due to "write-memory" command in archive config Symptoms: There is a memory leak in the "ascii-cfg" process. It happens when customers use the archive feature with the "write-memory" command. The leak happens when entering the "copy run start" command which also triggers the archive to automatically run in parallel and backup will be performed. Workarounds: -> Remove the "write-memory" command.

Bug ID	Description

CSCvv22452	Headline: Cisco NX-OS HSRP stuck in "Initial" state after reload with static HSRP MAC configured
	
	Symptoms: - - For Nexus we see broken VLAN 2251 with static HSRP MAC configured, after reload HSRP gets stuck in "Initial" state, but should move to next states as seen for working VLAN 2250.
	
	<pre>
	N3K-C3172PQ-2# show run int vlan 2250-2251
	
	!Command: show running-config interface Vlan2250-2251
	!Running configuration last done at: Sat Aug 1 10:23:49 2020
	!Time: Sat Aug 1 10:47:27 2020
	
	version 7.0(3)I7(6) Bios:version 5.3.1
	
	interface Vlan2250
	 no shutdown
	 ip address 10.1.1.3/24
	 hsrp version 2
	 hsrp 2250
	  preempt
	  priority 120
	  ip 10.1.1.1
	
	interface Vlan2251
	 no shutdown
	 ip address 10.231.240.2/29
	 hsrp version 2
	 hsrp 2251
	  mac-address 0000.0C9F.0014
	  preempt
	  priority 120
	  ip 10.231.240.1
	</pre>
	
	- Reload both switches (Broken VLAN 2251 doesn't come up, Working VLAN 2250 does come up):
	- Expectation is for both VLANs to come up:
	
	<pre>
	N3K-C3172PQ-1# show hsrp brief
	*:IPv6 group #:group belongs to a bundle
	              P indicates configured to preempt.
	                |
	 Interface Grp Prio P State Active addr Standby addr Group addr
	  Vlan2250 2250 100 Listen unknown 10.1.1.3 10.1.1.1 (conf) <--- This is expected.
	  Vlan2251 2251 100 Initial unknown unknown 10.231.240.1 (conf) <--- This is unexpected.
	
	N3K-C3172PQ-2# show hsrp brief
	*:IPv6 group #:group belongs to a bundle
	              P indicates configured to preempt.
	                |
	 Interface Grp Prio P State Active addr Standby addr Group addr
	  Vlan2250 2250 120 P Active local 10.1.1.2 10.1.1.1 (conf) <--- This is expected.
	  Vlan2251 2251 120 P Initial unknown unknown 10.231.240.1 (conf) <--- This is unexpected.
	</pre>
	
	Workarounds: -Shutdown/no shutdown SVI VLAN 2251 (or impacted HSRP VLAN) will move the HSRP state

18

Bug ID	Description
CSCvv23532	Headline: show run all - delay printing output for SAP 296 CLIS Symptoms: A delay may occur when printing out the configuration of a Nexus device using `show running-config all` The delay may be up to a 60 seconds. Workarounds: There is no operational impact but just a delay in printing out the output. Do not use the "show run" command with the 'all' parameter which prints all default config.
CSCvv25573	Headline: DHCP request sent towards the server has router ID in option 54 instead of server ID Symptoms: Host doesn't receive IP address from DHCP server Workarounds: SMU available in software download page for permanent fix.
CSCvv26271	Headline: TCAM carving rejected with hw-telemetry 128 after upgrade to Cisco NX-OS 9.3(5) Symptoms: `hardware access-list tcam region hw-telemetry 128 `ERROR: INN: Tcam carving rejected. Aggregate TCAM region configuration exceeded the available Egress TCAM space. Please re-configure. Workarounds: Write erase and reload. Another option is to do reload ASCII

CSCvv26464	Headline: N9k - IGMP report destined to 224.0.0.x sent back on same port it is received on
	
	Symptoms: MAC flaps on downstream switches connected behind Cisco Nexus switches, intermittent connectivity issues.
	Traffic is reflected back on same interface it was received on
	Duplicate IGMP reports seen in the VLAN.
	
	Workarounds: Suppress such IGMP reports which are destined to link local multicast range.
	On Cisco Nexus 9000 port ACLs can be used to suppress such traffic provided TCAM is carved for PACL region example:
	 sh ip access-lists block-igmp-link-local
	
	IP access list block-igmp-link-local
	   statistics per-entry
	   10 deny igmp any 224.0.0.252/32 [match=300]
	   20 deny igmp any 224.0.0.22/32 [match=0]
	   100 permit ip any any [match=557]

Bug ID	Description
CSCvv28528	Headline: nfm crashes with flow monitor scale and flow scale Symptoms: The Netflow (nfm) process may crash. The following will be reported in the log: 2020 Sep 16 20:53:58 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nfm" (PID 31961) hasn't caught signal 6 (core will be saved). 2020 Sep 16 20:55:00 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nfm" (PID 3656) hasn't caught signal 6 (core will be saved). 2020 Sep 16 20:56:01 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nfm" (PID 7427) hasn't caught signal 6 (core will be saved). 2020 Sep 16 20:57:02 %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "nfm" (PID 8834) hasn't caught signal 6 (core will be saved). 2020 Sep 16 20:57:02 %$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service "nfm" in vdc 1 has had a hap failure Workarounds: None
CSCvv28681	Headline: Cisco Nexus 9500-R heavy RPF failure traffic congesting CPU pipeline causing IGMP drops Symptoms: IGMP groups time out due to dropping of IGMP packets in CoPP. Workarounds: Fixing the RPF failure causing congestion.
CSCvv29453	Headline: Line card PFM going out of sync, extraneous "Module is undergoing ISSU" in XML output Symptoms: One, or more, line cards on a Cisco Nexus 9500 may become stuck in 'initializing' or 'powered-dn' state after switch boots up. The following messages may be reported in the log for the affected module(s): 2020 Jul 28 03:46:45 %ETHPORT-5-IF_SEQ_ERROR: Error ("sequence timeout") communicating with MTS_SAP_VLAN_MGR for opcode MTS_OPC_VLAN_MGR_GET_PORT_TRUNKING_MEMBERSHIP_2 (RID_MODULE: 5) 2020 Jul 28 03:47:05 %VMM-2-VMM_SERVICE_ERR: VDC1: Service SAP Ethpm SAP for slot 5 returned error 0x408c0008 (sequence timeout) in if_bind sequence Workarounds: Power cycle/Reload the line card.
CSCvv31955	Headline: Multicast IP PIM register not sent and data packet got punted to CPU. Symptoms: S,G never built even though the data packet is hitting the L2 interface. IP PIM register is never generated by CPU due to data packet getting dropped inside CPU. Workarounds: Flapping the corresponding SVI M will fix the issue or use static OIL. Applying static OIL makes it work. Even after static OIL removal, the working state still remains. The issue will trigger once again, after the sender stops sending packets for a while and the S,G timed out.

Bug ID	Description
CSCvv32676	Headline: After upgrade from 9.2(3) to 9.3(4), the interface using QSFP-100G-PSM4-S doesn't detect the SFP Symptoms: switch# sh int e x/y trans details Ethernetx/y transceiver is not present switch # sh int eth x/y Ethernetx/y is down (XCVR not inserted) Workarounds: None
CSCvv35193	Headline: avl_iterator does not get initialized in l2fm_send_smac_dump Symptoms: Crash in the L2FM Daemon process. A "l2fm" core file will be generated before the device reloads and the process log will show the cause of death due to "SYSMGR_DEATH_REASON_FAILURE_SIGNAL" like below: Service: l2fm Description: L2FM Daemon Executable: /isan/bin/l2fm Started at Fri Apr 24 17:35:19 2020 (737325 us) Stopped at Thu Aug 6 16:19:44 2020 (774441 us) Uptime: 103 days 22 hours 44 minutes 25 seconds Start type: SRV_OPTION_RESTART_STATELESS (23) Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2) Last heartbeat 0.52 secs ago System image name: System image version: 9.2(4) PID: 30215 SAP: 221 UUID: 410 -Traceback:librsw.so+0x65f86 librsw.so+0x65f86 librsw.so+0x66f67 l2fm+0x10195cce l2fm+0x10197b3b l2fm+0x1076743d l2fm+0x10469a7b l2fm+0x1031f390 libfsrv.so+0x2170d libfsrv.so+0x2394c Active Patches: Workarounds: There are no known workarounds at this time.

Bug ID	Description
CSCvv36175	Headline: N9K global cmd system dot1q-tunnel transit causes double dot1q tag on egress to server Symptoms: With the global command "system dot1q-tunnel transit" present in a vxlan enabled N9K switch the switch will not remove the incoming dot1q tag (VXLAN Encap) but add another, dot1q tag to the frame (VXLAN Decap) on the egress port (trunk) towards the end systems. These frames then get subsequently dropped by the end systems which is causing loss of service on the end systems. Workarounds: Remove the global command 'system dot1q-tunnel transit' if it is not in use. Or toggle the command: # no system dot1q-tunnel transit # system dot1q-tunnel transit

Bug ID	Description
CSCvv37188	Headline: Port profile refresh does not remove DHCP relay address from interface Symptoms: A Cisco Nexus 9000 Series switch configured with port profiles will not correctly remove old DHCP relay server addresses from an interface when the interface's applied port profile is refreshed with the "refresh profile" command. For example, consider a Nexus 9000 device where the SVI for VLAN 10 is configured with DHCP relay servers 198.51.100.10 and 198.51.100.20. N9K# show running-config | section VLAN10 <snip> configure profile VLAN10 interface Vlan10 vrf member example-1 no ip redirects no ipv6 redirects ip address 192.0.2.1/24 tag 12345 ip dhcp relay address 198.51.100.10 use-vrf example-1 ip dhcp relay address 198.51.100.20 use-vrf example-1 mtu 9216 fabric forwarding mode anycast-gateway no shutdown apply profile VLAN10 N9K# show running-config interface vlan 10 expand-port-profile <snip> interface Vlan10 no shutdown mtu 9216 vrf member example-1 no ip redirects ip address 192.0.2.1/24 tag 12345 no ipv6 redirects fabric forwarding mode anycast-gateway ip dhcp relay address 198.51.100.10 ip dhcp relay address 198.51.100.20 A new port profile is created that updates the DHCP relay server 198.51.100.20 to be 198.51.100.30 instead. N9K# show running-config | section VLAN10_new configure profile VLAN10_new interface Vlan10 vrf member example-1 no ip redirects no ipv6 redirects ip address 192.0.2.1/24 tag 12345 ip dhcp relay address 198.51.100.10 use-vrf example-1 ip dhcp relay address 198.51.100.30 use-vrf example-1 mtu 9216 fabric forwarding mode anycast-gateway no shutdown Finally, the existing VLAN10 port profile is refreshed with the contents of the VLAN10_new port profile using the "profile refresh" command. N9K# configure terminal N9K(config)# refresh profile VLAN10 VLAN10_new overwrite The old "ip dhcp relay address 198.51.100.20" configuration will still appear in the VLAN10 SVI's

Bug ID	Description
CSCvv44146	Headline: ARP request cannot pass through peer-link after changing default reserved VLAN Symptoms: 1/ system vlan 3800 reserve # show system vlan reserved system current running vlan reservation: 3800-3927 2/ N9K-1 and N9K-2 build vpc, N9K-3 is used to simulate the server. We shut down the connection between N9K-1 and N9K-3. After that, we find this problem: N9K-3 ping svi 4000 ip of N9K-1, fail ethanalyzer shows that packet is not sent out of N9K-2 Workarounds: Use other VLAN
CSCvv48289	Headline: Unable to upgrade from 9.3.2 to 9.3.5 via install all for N9K-C92348GC-X Symptoms: Upgrade from 9.3.2 to 9.3.5 fails via ISSU with the below error switch# install all nxos bootflash:nxos.9.3.5.bin Installer will perform compatibility check first. Please wait. Installer is forced disruptive Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos". [##################] 100% -- SUCCESS Verifying image type. [##################] 100% -- SUCCESS Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin. [##################] 100% -- SUCCESS Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin. [##################] 100% -- SUCCESS 2020 Aug 13 01:52:01 switch %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: confcheck status indicates error, error no: 2. - new_installer [##################] 100% -- FAIL. Return code 0x40930028 (Compatibility checks with running-config failed). Pre-upgrade check failed. Return code 0x40930066 (SRG processing failed). switch# 2020 Aug 13 01:52:03 switch %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: srg processing failed (0x 40930028) - new_installer 2020 Aug 13 01:52:03 switch %$ VDC-1 %$ %FW_APP-2-FIRMWARE_IMAGE_LOAD_SUCCESS: sysmgrcb_system_upg_done Workarounds: NA

Bug ID	Description

CSCvv48780	Headline: Nexus 9K reboots with "evms hap reset" when evms debug is run and eem is configured at the same time
	
	Symptoms: evms core generated
	
	`show cores`
	VDC Module Instance Process-name PID Date(Year-Month-Day Time)
	--- ------ -------- --------------- -------- -------------------------
	1 1 1 evms 27713 2020-08-20 20:16:51
	1 1 1 evms 2103 2020-08-20 20:16:51
	
	`show version`
	Last reset at 604555 usecs after Thu Aug 20 20:14:44 2020
	 Reason: Reset triggered due to HA policy of Reset
	 System version: 9.3(3)
	 Service: evms hap reset <<<<<<<<<<<
	
	`show logging nvram`
	%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "evms" (PID 2103) hasn't caught signal 11 (core will be saved).
	%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "evms" (PID 27246) hasn't caught signal 11 (core will be saved).
	%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "evms" (PID 27713) hasn't caught signal 11 (core will be saved).
	%$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "evms" (PID 27296) hasn't caught signal 11 (core will be saved).
	%$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service "evms" in vdc 1 has had a hap failure <<<<<<<<<<<
	
	`show logging onboard exception-log`
	
	exception information --- exception instance 1 ----
	Module Slot Number: 0
	Device Id : 134
	Device Name : System Manager
	Device Errorcode : 0x0000019b
	Device ID : 00 (0x00)
	Device Instance : 00 (0x00)
	Dev Type (HW/SW) : 01 (0x01)
	ErrNum (devInfo) : 155 (0x9b)
	System Errorcode : 0x401e0089 Service in VDC has had a hap-reset
	Error Type : FATAL error
	PhyPortLayer : 0x0
	Port(s) Affected : none
	Error Description : evms hap reset <<<<<<<<<<<<<<<<
	DSAP : 0 (0x0)
	UUID : 1 (0x1)
	Time : Thu Aug 20 20:14:44 2020
	            (Ticks: 5F3ED9B4 jiffies)
	
	switch# show system reset-reason
	
	----- reset reason for module 1 (from Supervisor in slot 1) ---
	1) At 604555 usecs after Thu Aug 20 20:14:44 2020
	   Reason: Reset triggered due to HA policy of Reset
	   Service: evms hap reset 25 <<<<<<<<<<<<<<<<
	   Version: 9.3(3)
	
	Workarounds: NA

Bug ID	Description
CSCvv49105	Headline: Control-Plane Tx will get dropped due to incorrect namespace ID Symptoms: ICMP Tx will get dropped due to incorrect namespace ID Workarounds: 1. Kill KIM process using kill -6 <process ID> and Delete the interface VLAN/recreate it. 2. Reload of the switch - Preferred way
CSCvv49936	Headline: VXLAN "VNI range entered is invalid" returned for "no member vni xxxxx" after ISSU Symptoms: After the ISSU upgrade from Cisco NX-OS 7.0(3)I7(6) to 9.3(5) it is not possible to un-configure a member VNI from the nve1 interface. The command "no member vni xxxxx" returns an error " VNI range entered is invalid". In the case of vPC, the same error is returned on both switches. Workarounds: There are no known workarounds.
CSCvv50051	Headline: After ISSU from 7.0(3)I7.7 to 9.3(5) QoS network inconsistency in vPC even config is consistent Symptoms: After a non-disruptive ISSU from Cisco NX-OS 7.0(3)I7.7 to 9.3(5) vPC consistently failing due to inconsistency in network QoS (MTU). This is a false positive. Configuration is consistent. Workarounds: Two possible workarounds: Workaround 1: - Copy default network QOS config to custom network qos profile - apply custom profile - remove customer profile Workaround 2: Reload

Bug ID	Description
CSCvv57560	Headline: Traceback: SNMPd crash when cache entry is deleted
	Symptoms: The affected device reports through the system logs that SNMP crashes due to signal 11:
	%SYSMGR-2-SERVICE_CRASHED: Service "snmpd" (PID 27822) hasn't caught signal 11 (core will be saved).
	Core files are generated in some events, use the 'show process log' command to see if a core was created or not:
	# show processes log

	<pre>VDC Process PID Normal-exit Stack Core Log-create-time
	--- --------------- ------ ----------- ----- ----- ---------------
	  1 snmpd ##### N Y Y <Date>
	  1 snmpd ##### N N N <Date></pre>

	Use the 'show cores vdc-all' command to check for core files.
	If a core file is present engage TAC to assist with core retrieval, decode, analysis and to identify if this software bug impacts the device:
	# show cores vdc-all

	<pre>VDC Module Instance Process-name PID Date(Year-Month-Day Time)
	--- ------ -------- --------------- -------- -------------------------
	# # # snmpd ##### <Date></pre>

	Workarounds: Disable SNMP.
CSCvv58281	Headline: Issues with QinQ Tags after upgrade to Cisco NX-OS 9.3(5)
	Symptoms: After an NX-OS upgrade or reload of Cisco Nexus 9000 Series switches configured for selective Q-in-Q, to Cisco NX-OS 9.3(5), the feature might not work as expected.
	Workarounds: Enter "system dot1q-tunnel transit"
CSCvv60665	Headline: ISSU ports with QSFP-100G40G-BIDI remain not connected after a flap
	Symptoms: Port remains stuck in (Link not connected) after port flap or admin shut/no shut.
	Workarounds: Reloading the switch clears the issue.
CSCvv63802	Headline: Cisco NX-OS Incorrect RFC 5424 format after configuring logging rfc-strict 5424
	Symptoms: NX-OS could follow RFC 5424 by the following command:
	switch# logging rfc-strict 5424
	But compared with the RFC 5424, there is an extra half-width space between <PRI> and VERSION in our syslog.
	Workarounds: N/A

Bug ID	Description
CSCvv68826	Headline: LDAP search-filter config breaks in Cisco NX-OS 9.3.x Symptoms: After upgrading to Cisco NX-OS 9.3(5) from 7.0(3)I4(8), LDAP search-filter config got changed. Before upgrade: userprofile attribute-name "xxxx" search-filter "110charactersString" base-DN "xxxx" After upgrade: userprofile attribute-name "xxxx" search-filter "63charactersString" base-DN "xxxx" * Problem is: Not able to use all 128 characters in search filter. N9k(config)#ldap search-map <searchMapName> N9k(config-ldap-search-map)# userprofile attribute-name "xxxx" search-filter "110charactersString" base-DN "xxxx" ERROR: value of property searchFilter is out of range: N9k(config-ldap-search-map)# userprofile attribute-name "xxxx" search-filter ? WORD Search Map search-filter (Max Size 128) * This search-filter only has 110 characters and it still not accepted. Whereas, we have a limit of 128. Workarounds: * Tested in lab. Could use only 63 character in search filter: N9k(config-ldap-search-map)# userprofile attribute-name "xxxx" search-filter "63charactersString" base-DN "xxxx" N9k(config-ldap-search-map)#
CSCvv72527	Headline: Port-channel gets added as a SPAN destination in monitor session for EX/FX based LC in EOR Symptoms: So basically there is a limitation, FEX and SPAN port-channel destinations are not supported on the Cisco Nexus 9500 platform switches with -EX or -FX line cards. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_011011.html However, when you configure the interface first with "switchport monitor" and then put it in a channel-group the config is getting imported from the interface to the port-channel and allowing it in the SPAN destination port EX based LC. This needs to be blocked. Workarounds: NA
CSCvw00090	Headline: N9K upgrade/SSO > causing policy elem continuous cores > whole box reloaded Symptoms: EOR Chassis reload due to policy elem process crash2020 Oct 12 02:08:59 N9K-2-CX %$ VDC-1 %$ %SYSMGR-2-SERVICE_CRASHED: Service "policy elem" (PID 31293) hasn't caught signal 6 (core will be saved). Workarounds: None

Bug ID	Description

CSCvt86036	Headline: VXLAN - Traffic to IP x.x.137.2 is wrongly intercepted by OAM Sup ACL
	
	Symptoms: ARPs with Target IP x.x.137.2 in VXLAN Fabric on Decap side are lost. Other IP is same VLAN/VNI works well.
	This traffic is hitting Sup ACL entry:
	# show system internal access-list sup-redirect-stats | inc ig OAM
	  3076 VxLAN OAM 2 >>>
	<>
	  3076 VxLAN OAM 10 >>>
	
	Workarounds: Avoid using IP's in range x.x.137.2.

CSCvv54636	Headline: Cisco Nexus 9000 EOR NLB IGMP multicast on a stick: traffic blackholed if ingress Port-channel split across ASICs Symptoms: Traffic may be blackholed and some load-balancing combinations may work. Workarounds: If on a stick NLB deployment, ensure all port-channel members belong to the same physical ASIC (hence the same module). (show interface hardware-mapping) or Do not use "on a stick" port-channel deployment.

Bug ID	Description

CSCvv54693	Headline: Segment routing: route not properly installed on FIB when switch is reloaded
	
	Symptoms: Network topology configured with MPLS+segment-routing has FIB routes pointing to Null0 interface and the traffic is blackholed.
	
	Workarounds:
	On the PE segment-routing configuration:
	
	PE-router# show run segment-routing
	
	segment-routing
	
	 mpls
	
	  global-block 16000 25000
	
	  connected-prefix-sid-map
	
	   address-family ipv4
	
	    1.1.1.1/32 index 7
	
	remove and re-apply the index:
	
	PE-router(config)# segment-routing
	
	PE-router(config-sr)# mpls
	
	PE-router(config-sr-mpls)# connected-prefix-sid-map
	
	PE-router(config-sr-mpls-conn-pfxsid)# address-family ipv4
	
	PE-router(config-sr-mpls-conn-pfxsid-af)# no 1.1.1.1/32 index 7
	
	PE-router(config-sr-mpls-conn-pfxsid-af)# 1.1.1.1/32 index 7

CSCvv95278	Headline: Ports stay in "connected/UP" state when the Distributed Services Card is down Symptoms: Nexus switch can't detect that the server is connected to the interface is shut down and port on Nexus shows connected. Workarounds: Enter shut or no shut.
CSCvw07604	Headline: NVE source Interface flaps every 3 minutes Symptoms: NVE source Interface flaps every 3 minutes(or time equal to the delay restore timer expiry) Workarounds: As of now, only the disruptive workaround of Removing feature vPC and re-applying the configurations for vPC will help to fix. Note that removing the feature vPC will remove all the vPC associated configurations and so this is a disruptive Change.

Bug ID	Description
CSCvv50588	Headline: Mismatch in bucket reassignment when active and standby nodes are down with no fail action Symptoms: ITD redirects flows from failed primary nodes with failed node level standbys towards other active primary nodes, even when fail action is not configured for the service. Workarounds: 1. Having services with fail-action node per bucket/node re-assign/node least-bucket (not recommended for vpc scenarios) will still redirect flows of failed nodes towards other active nodes but will allow for correct redirection back to the original primary nodes once they recover and avoid the problem of skewed load-balancing when all nodes are active. 2. Based on the topology and load distribution, if using hot-standby nodes instead of node level standbys is a possibility, the problem would not be encountered. For migration to 9.3.6 once the issue is hit in an older release, user would need to use the default install option (disruptive) to upgrade and allow for the incorrect policies to be fixed. Alternatively, the services would need to be shut down and unshut after a non-disruptive upgrade to fix the incorrect policies.
CSCvv64248	Headline: DHCP Relay DHCP OFFER broadcast loop/bounce in EVPN Fabric Symptoms: DHCP offers (broadcast) may bounce back between VTEPs in VXLAN Fabric environment MAC flaps on downstream switches as DHCP offers are reflected back towards the client. Workarounds: • Disable DHCP relay if not in use for given SVI • Remove DHCP server from vlan that has configured DHCP relay
CSCvw08685	Headline: BGP core dumped when running show tech-support Symptoms: BGP core is dumped when running "show tech-support xxx". See "show cores". The reset reason might not be recorded upon the reload. Workarounds: None
CSCvv04821	Headline: Cloud Scale ASIC switches Egress RACL not blocking/filtering traffic Symptoms: • Egress RACL configured on ACL does not block traffic • Egress RACL is not programmed for one or more forwarding blocks/slices Workarounds: Remove and re-configure egress RACL under the VLAN interface/SVI.
CSCvv64626	Headline: Cisco Nexus 9000/Cloud Scale ASICs ELAM ERROR: FLOP ELAM must be triggered Symptoms: ELAM report on Cisco Nexus 9000 may give false results for the captured/triggered packet. Workarounds: Reset, re-trigger and start the ELAM. In most cases the 2nd attempt for same packet trigger results in correct results.

Bug ID	Description
CSCvv64935	Headline: Port-security feature may not restrict traffic on the VPC port-channel Symptoms: In the scenario where the port-security vPC port-channel is configured with violation restrict all source-miss traffic may be allowed by the hardware (due to misprogramming). This can be triggered by re-moving the port-security feature globally and reconfiguring it afresh. Workarounds: Port-channel flap may resolve this issue.
CSCvv82316	Headline: VXLAN - RIB failing to update after tracked static route is suspended. Symptoms: The wrong route is installed in the RIB instead of the routes from the spine after the tracked static route is suspended. Workarounds: A possible workaround would be to increase the weight of the two other routes received from the spines.
CSCvv99134	Headline: Crash after copy r s if any line of banner has characters "% In" at beginning. Symptoms: Cisco Nexus 9000 device will crash if the beginning of the banner line contains: % In Workarounds: Do not contain "% In" at beginning of any line. For example: % In Replace with: # In
CSCvv22414	Headline: Cisco Nexus 9508/9516 with 4k VLAN scale modules go to powered-dn state when upgrading to Cisco NX-OS Release 9.3(3) and above. Symptoms: In Cisco Nexus 9508/9516 switches modules go to powered down state when upgrading to Cisco NX-OS Release 9.3(3) and above. Workarounds: Perform the following: 1. Power up one module at a time 2. Reduce VLAN prior to upgrade and re-configure back once up in Cisco NX-OS Release 9.3(3) 3. Downgrade to any release below Cisco NX-OS Release 9.3(3)
CSCvv40314	Headline: Suppress constant new Mac learn notification due to L2/L3 bind failures. Symptoms: A Nexus switch may experience high cpu utilization and a high volume of MTS messages when learning a large number of MAC addresses in a burst. Workarounds: None
CSCvv76073	Headline: N3K-C36180YC-R: STS LED on the back of the chassis does not light up Symptoms: On N3K-C36180YC-R, STS LED on the back of the chassis does not light up. No functional im-pact has been reported by this symptom. Workarounds: No workaround. As described, no functional impact has been reported by this symptom.

Bug ID	Description
CSCvw05137	Headline: Cisco Nexus Cloudscale VxLAN-TRM - MFDM prime oiflist leak with high number of IGMP Join/Leave Symptoms: Multicast traffic is not received by receivers due to resource allocation failure. Workarounds: None
CSCvv29703	Headline: Error occurred while trying to read database when recreating an object-group Symptoms: When attempting to recreate or modify an object-group on the Cisco Nexus 9000 the following error gets displayed: "Error occured while trying to read database" Workarounds: None
CSCvv68241	Headline: Once a user connected via NXAPI, user can't delete/modify username Symptoms: You may not be able to remove a user who logged under NXAPI in the past. Workarounds: To remove unwanted user following can be done: 1. Backup NXAPI configuration 2. Remove NXAPI feature 3. Remove user in question after changing the assigned role. 4. Reconfigure NXAPI
CSCvv71176	Headline: Supervisor isolated from chassis after system controllers not responding on EPC&EOBC path Symptoms: Output only shows the supervisor in the chassis. Workarounds: Reload the supervisor to restore connectivity to the chassis.
CSCvv60794	Headline: Multicast routing over GRE in VRF fails. Symptoms: When configuring multicast routing over a GRE tunnel, and the tunnel is placed into a different VRF than underlay (e.g. "vrf member" is set, but tunnel destination is reachable via global routing table), the GRE tunnel will be seen in the OIL, but actual traffic won't be replicated. Workarounds: None.

Bug ID	Description
CSCvv80116	Headline: LACP vpc-convergence + switchport trunk allowed vlan none - Interface Error Disable Symptoms: Following error messages could be observed with N9k/3k switches: %ETHPORT-5-IF_SEQ_ERROR: Error ("invalid argument to function call") communicating with MTS_SAP_PIXM_LOCAL for opcode MTS_OPC_PIXM_SET_MULT_CBL_VLAN_PORT_STATE (RID_PORT: Ethernet1/10) %ETHPORT-5-IF_DOWN_ERROR_DISABLED: Interface Ethernet1/10 is down (Error disabled. Reason:invalid argument to function call) Interface is marked as error disabled due to internal error: # show int eth1/10 Ethernet1/10 is down (Internal-Fail errDisable) # show int eth1/10 brief -- Ethernet VLAN Type Mode Status Reason Speed Port Interface Ch # -- Eth1/10 1 eth trunk down Internal-Fail errDisabl auto(D) 5 Workarounds: Allow at least one VLAN under port-channel interface with "lacp vpc-convergence" configured: Example: Switch# switchport trunk allowed vlan 2
CSCvv84849	Headline: Cisco Nexus 9000 experience a Crash due to Fatal Module Error Symptoms: Nexus N9K may experience a software crash due to Fatal Module Error. This can be seen either in "show version" or "show system reset-reason". Workarounds: Unknown
CSCvw03925	Headline: Cisco Nexus 9000, Release 9.3(3) OSPF non-0 FA when redistributing the OSPF route from VRF to default Symptoms: OSPF receives type-5 LSA with a non-0 FA pointing to unreachable address. It prevents OSPF installing the prefix into the RIB since FA is unreachable. Workarounds: N/A
CSCvw01364	Headline: Locally originated control packets to directly connected host sent towards EVPN fabric instead Symptoms: • the LEAF A while originating the IPv6 BGP packets towards directly connected FW, sends it across EVPN fabric instead of directly • the remote LEAVES (C/D) bounces the packet back and then it's correctly forwarded towards Fire-wall. • capture of packets (eg. ethanalyzer) originated by LEAF A shows that the packet gets VxLAN en-capsulated and sent towards the VIP of leaves C/D Workarounds: None

Bug ID	Description
CSCvw16965	Headline: Nexus 9500 forwards traffic after TTL expires Symptoms: Nexus 9500 with modules N9K-X9732C-EX and N9K-X97160YC-EX. Packets received with a TTL=1 on this Nexus are forwarded instead of dropped, also we generate a reply back to the source with an ICMPv4 Type 11, Code 0 Time Exceeded message, last part is correct, however, we should drop these packets. Issue is seen only when packet is received on one module and we need to forward it on a different module, therefore, FM is on the path and we see packets with TTL=0 or TT=1 being forwarded, this issue is not seen when ingress and egress module are the same. Workarounds: None
CSCvw27405	Headline: Tahusd crash due to link flapping Symptoms: 2020 Oct 28 04:22:12 STLD1-630-01-03-N9K-RU28 %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "tahusd" (PID 11733) hasn't caught signal 6 (core will be saved). 2020 Oct 28 04:22:15 STLD1-630-01-03-N9K-RU28 %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "tahusd" in vdc 1 has had a hap failure 2020 Oct 28 04:22:15 STLD1-630-01-03-N9K-RU28 %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 30279 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) . 2020 Oct 28 04:22:51 STLD1-630-01-03-N9K-RU28 %KERN-2-SYSTEM_MSG: [147094.667915] usd process 11733, uuid 1356 (0x54c) tahusd failed to send heartbeat - kernel # show system reset-reason ----- reset reason for module 1 (from Supervisor in slot 1) --- 1) At 81613 usecs after Wed Oct 28 04:25:29 2020 Reason: Reset Requested due to Fatal Module Error Service: tahusd hap reset Version: 9.3(5) Workarounds: None
CSCvw08018	Headline: BFD rate-limiter resources exhausted for transit traffic with udp port 6784 Symptoms: BFD rate-limiter resources may be consumed by transit traffic with udp destination port 6784. This is the same port that micro bfd uses (bfd per-link). Any BFD session passing through this hardware rate-limiter may be impacted randomly 9.3(5) if the resources are exhausted. Workarounds: Use an ACL at the edge of the network to block udp 6784.
CSCvw12553	Headline: aclqos core dump generated when removing an ACE from the access list Symptoms: When negating a sequence of an ACE in the ACL, the switch crashes in aclqos service. Workarounds: Find the destination where there is a mismatch of the ACEs and remove/add policy from that destination.

Bug ID	Description
CSCvw19844	Headline: VLAN shown in show interface status is incorrect Symptoms: VLAN shown in "show interface status" command output is wrong. Workarounds: None
CSCvw16095	Headline: Multicast Frame Error did not mark in "drop info" in ELAM summary Symptoms: Multicast packet got frame error on packet size or the multicast group member is missing. ELAM summary failed to show the correct drop information but the ELAM report detail does drop info. Workarounds: do (TAH-elam-insel6)# report detail | sec STA_rwb_drop_vector_capture_access Instead Following output can be seen sun[0].rwx[0].STA_rwb_drop_vector_capture_access: 0x000000800. <<< DROP CAPTURED info: 0x000000800 ... ... info.eoferr_first_cell: 0x1 <<< Frame error
CSCvv98749	Headline: config-replace adds "switchport vlan mapping all dot1q-tunnel" in checkpoint causing CR failure Symptoms: While MACSec config replacement is done it was discovered that other areas of config-replace were also broken. The. attached base (test1-base.conf), target (test1-target.conf) configs and the failed log file will allow the issue to be reproduced consistently. Workarounds: N/A
CSCvv73708	Headline: FX2/MLD: IGMP/MLD crash on secondary VPC peer due to missing null check for group header Symptoms: MLD and IGMP crash Workarounds: None
CSCvw17562	Headline: Configure replace fails with hostname change for VDC Symptoms: Configure replace will fail with an error when used with verify-only option. Workarounds: Do show running-config and copy paste the below line and add it to the top of the Config-replace file: Lab# sh running-config !Command: show running-config !Running configuration last done at: Tue Oct 20 16:27:49 2020 !Time: Tue Oct 20 16:29:58 2020 version 9.3(2) Bios:version 07.67 <<<<<<<<

Bug ID	Description
CSCvw03356	Headline: Crash in ipqosmgr service after QoS policy change and show startup-config" CLI Symptoms: QoS policy configuration change leads to crashes once saved and loaded from startup configuration. "show startup-config" is a known trigger. Workarounds: None
CSCvw10137	Headline: DHCPv6 relay - High CPU DHCP snooping Symptoms: High CPU in DHCP snooping process. High MTS build up for DHCP snooping UDP sockets. Workarounds: None
CSCvw12977	Headline: Cisco Nexus 9000 EOR "hardware access-list tcam region ing-netflow 512" not working after upgrade Symptoms: For EOR N9K, after upgrade, access-list tcam size of ing-netflow shows 0 "Hardware access-list tcam region ing-netflow 512" not working (no warning, running config does not change) Workarounds: Config the tcam size to one value higher than 512 (such as 1024) than config to 512 again.
CSCvv26058	Headline: SNMPD core on N3K-C3408-S running longevity with Cisco NX-OS Release 9.3(3) CCO for 47 days Symptoms: The snmpd process may crash after running for a long time. Workarounds: None
CSCvv91239	Headline: Cisco Nexus 9000 could not learn MAC address of silent hosts after multiple TCN occurrence Symptoms: The MAC addresses of the silent hosts might not be learnt by N9K after continuous TCN occurrence. Workarounds: 1. Clear ip arp of the affected host clear ip arp x.x.x.x vrf XXXX 2. Configure "ip arp delete-adj-on-mac-delete" under SVI (gateway). Cisco Nexus 9000 will delete all ARPs of this vlan after receiving TCN. The re-learning of ARP will be triggered by traffic.
CSCvw13710	Headline: Reload: Kernel Panic triggered by nxpython process Symptoms: nxpython process repeatedly crashed and then kernel panic Workarounds: The root cause is that nxpython process crashes repeatedly. If a process crashes repeatedly before it hits kernel panic, it might try to stop/remove the process from the system.

Bug ID	Description
CSCvw22417	Headline: IGMPV0 leave is re-generated across the peer-link when mrouter port is auto-renewed without querier. Symptoms: External V2 querier did not send in the membership query but constantly sent to PIM Join. This will cause the querier absent from transition device but the mrouter port still presented. At the same time, receiver is promoting v3 membership report with link-local mcast group along with other groups. Based on these prequisition, the end result is the device (device that got the IGMP signalling) across the peer-link (the one that have mrouter port towards external querier) start re-generating the IGMP leave with IGMPV0. Workarounds: Manual configure igmp v2 querier on Local Nexus.
CSCvw15785	Headline: Nexus9000 C93180YC-FX3S-Fan PID needs to be changed from NXA-FAN-30CFM-B to NXA-FAN-35CFM-PI Symptoms: Wrong FAN PID outputs with "show inventory", and PID needs to be changed from NXA-FAN-30CFM-B to NXA-FAN-35CFM-PI Workarounds: N/A
CSCvw21655	Headline: Port-Security secure learn for non-vPC vlan incorrectly synced to vPC peer on Peer-Link Symptoms: -Secure learn for non vPC vlan end device on the peer-link -Loss of connectivity from end host with incorrect secure mac learn on peer-link to remote vPC peer switch because of the active mac learn on an interface where the vlan is not allowed. -MACDB entries for ignoring correct dynamic learn because of bad existing secure learn "IGN_NL_SEC_MAC_PRESE" sh system internal l2fm l2dbg macdb add maca.maca.maca Month Day xx:xx:xx 2020 0x16000001 0 IGN_NL_SEC_MAC_PRESE 3 0 0x2 Workarounds: Allow non vPC vlans with secure mac learns on the peer-link where the overriding secure learn is seen.
CSCvw30171	Headline: DHCP snooping binding not refresh Symptoms: If have approximate 2000 dhcp snooping entries in N9K after reloading the dhcp snooping binding will not refresh. Workarounds: None
CSCvs20871	Headline: N9K-C92348GC-X: ND ISSU Control Plane Downtime is High Symptoms: ND ISSU Control Plane downtime might be higher than 120sec on certain N9K-C92348GC-X switches. This can cause protocol flaps resulting traffic loss. Workarounds: N/A

Bug ID	Description
CSCvw36505	Headline: Macsec ports in Auth-pending state with addition of valid keychain from Empty keychain Symptoms: Ports will be in 'Auth Pending' when policies are changed using empty keychain. Workarounds: Reload.
CSCvv54511	Headline: Nexus 9348GC-FXP with half duplex sees Rx Frm Rcv Errors Symptoms: Collisions/CRC will be seen on half duplex links with bidirectional traffic. Performance impact will be seen for the hosts that are connected on half duplex links. Workarounds: None

Known Issues

Behavior Changes for Cisco Nexus 9504 and 9508 Switches with -R Line Cards

Bug ID	Description
N/A	Interface: The output format for the exec command CLI show vpc orphan-ports has changed from the 7.0(3)F3(4) release to the 9.3(6) release.
N/A	FEX: MTU 9216 is the default value for FEX fabric ports-channels.
N/A	FEX: MTU 9216 is the only allowed value to be configured on FEX fabric port-channels. Configuring any other value will throw an error.
CSCvp87914	FEX: If the MTU value on a FEX fabric port-channel was set to 9216 before upgrading to Cisco NX-OS Release 9.3(6), the show running config command will not display the MTU config as it is the new default in Cisco NX-OS Release 9.3(6). Due to this, the show running-config diff command displays the difference which is expected.
N/A	Programmability: Release 9.3(6) brings in a new kernel and new processes.
N/A	Programmability: Interface counter statistics are grouped together in the XML/JSON output. The output for the show interface-counters command in JSON format has changed.
N/A	Programmability: NX-API does not support insecure HTTP by default.
N/A	Programmability: NX-API does not support weak TLSv1 protocol by default.
N/A	Security: Stronger ciphers are used in this release.
N/A	Security: A new command, no service password-recovery is supported.
N/A	Security: Only one version out of v4 and v6 versions of the uRPF command can be configured on an interface. If one version is configured, all the mode changes must be done by the same version. The other version is blocked on that interface. Cisco Nexus 9300-EX, 9300-FX, and 9300-FX2 platform switches do not have this limitation and you can configure v4 and v6 version of urpf cmd individually.

General Known Issues

Bug ID	Description
CSCvt99828	Setting the value of "none" for the property authName, basically stands for a zero value, which is not allowed, and shouldn't be used. Allowable values other than "none" should be used as inputs to this property.
CSCvt99859	The allocate-label option-b command is disabled and not shown in the configuration unless MPLS Layer 3 VPN is enabled. This is achieved by entering the feature mpls l3vpn command.
CSCvt93823	An NVE interface is required to be in shut state before making changes to the source-interface for NVE. Trying to do the default operation on NVE interface brings it out of the shut state as it performs a no shut first. This causes the operation to fail as there is an attempt to modify the source-interface in the no shut mode. Fixing this might require changes to how the default keyword behaves fundamentally. This can affect other types of interfaces, as well, as they too can be operated on using the default keyword. For this reason, if there is a need to remove the configuration for the NVE interface, enter the shut command on the NVE interface. Then enter the no interface nve 1 command, followed by reconfiguring the NVE interface with the new configuration.
CSCvu48474	Due to an ASIC limitation, FC-FEC cannot be configured on the native (non-retimer) ports (ports 25-36) of N9K-C93600CD-GX when broken out to 2x50G. Only RS-FEC and FEC off are supported. To be consistent, the retimer port (ports 1-24) capabilities are also being limited to RS-FEC and FEC off when broken out to 2x50G. There is no plan to enable FC-FEC on the retimer ports for this reason, so this CDET is being closed.
CSCvu02712	Intermittent CRC errors are seen on Cisco Nexus N9K-C9236C retimer ports (1-8 and 29-36), when connected to Cisco Nexus N9K-C93600CD-GX 100G native ports (25-28) and broken out to 4x25G. The issue is not seen in non-breakout 100G mode. Workarounds: Avoid these connections. Ports 9-28 on the Cisco Nexus N9K-C9236C can be used instead.
CSCvt41915	ISIS route is deleted from kernel when ip unnumbered config is deleted and added back in quick succession (within say 30 seconds) Recovery: ip unnumbered config deletion and addition should be done within the 60-second window to be safe. If issue is hit, recovery is to flap the interface with the shut command followed by the no shut command.

Bug ID	Description

CSCvr20128	The issue happens for pinned static routes only. These routes don't get installed in the kernel. So, BGP sessions over these routes might not work. A ping from Bash will not work.
	
	 Recovery:
	
	 If the issue is seen, pinned static routes can be deleted and added back.
	
	 Also, entering the clear ip route vrf *<vrf-name>* command can be done to recover from the issue.
	
	 Further Problem Description:
	
	 1. The issue happens for pinned static routes only. Pinned static routes is a feature borrowed from Catalyst 6000 IOS platforms and not many customers use it on Cisco Nexus 9000.
	
	 2. There are 3 flavors of the issue
	
	     a. Pinned static route could have a next hop which is not in the subnet of the IP address configured on the interface.
	
	     In this case, the kernel cannot install the route irrespective of when Netstack sends the route programming request because, the next hop is not in the same subnet of the interface IP address.
	
	     b. Pinned static route could have some next hops. But on the interface, there is no global IPv6 address configured. It has only a link-local address configured.
	
	     In this case also, the kernel cannot install the route irrespective of when Netstack sends the route programming request because the next hop is not in the same subnet of the interface IP address.
	
	     c. Pinned static route could have a next hop which is in the same subnet of the IP address configured on the interface.
	
	     In this case, the kernel can install the route only if Netstack sends a route programming request after it programs the IP address to the kernel. While programming the route, the kernel determines that the next hop is already programmed. This is a very specific case of pinned static routes.

CSCvc95008	On Cisco Nexus 9300-EX, 9348GC-FXP, 93108TC-FX, 93180YC-FX, 9336C-FX2, 93216TC-FX2, 93360YC-FX2, 93240YC-FX2, 92348GC-X, C93108TC-EX-24, C93108TC-FX-24, C93180YC-EX-24, C93180YC-FX-24, 9316D-GX, 9364C-GX, and 93600CD-GX switches, when 802.1q EtherType has changed on an interface, the EtherType of all interfaces on the same slice will be changed to the configured value. This change is not persistent after a reload of the switch and will revert to the EtherType value of the last port on the slice.
CSCvr92708	CoPP violations can be seen under class-map copp-system-p-class-l2-default and access-group copp-system-p-acl-mac-undesirable in an MVPN setup on a PE device. This can cause an impact to MVPN control plane functionality for packets such as MSDP and PIM register messages, in case of a large number of MVPN PE devices and MDT groups. You can create a custom CoPP policy with an increased "cir" value until no CoPP violation is seen for that class.

Bug ID	Description
CSCvr95514	Per-VRF Configuration of MDT MTU size is not supported on MVPN PE devices on N9K-X9636C-R/RX, N3K-C36180YC-R, N3K-C3636C-R platforms. While, Tunnel MTU size is not configurable interface MTU for the core facing interface can be configured to control port-level MTU. MDT tunnel is capable of carrying up to jumbo MTU size of 9192 (excluding tunnel header), provided interface MTU for the core-facing interface also supports jumbo MTU.
CSCvr92710	CMIS standards prescribe delays at each state as mentioned by the QSFP-DD firmware on those optics. If you are using those optics with delays, you will see a higher link-up time.
CSCvr14625	CMIS standards prescribe delays at each state as mentioned by the QSFP-DD firmware on those optics. If you are using those optics with delays, you will see a higher link-up time.
CSCvr13930	The Cisco Nexus 9300-GX ASIC does not support FC-FEC on the second lane of 50x2 breakout port. This is due to an ASIC limitation. The second link cannot come up when 50x2 breakout is done. Workarounds: You must configure RS-FEC with 50x2 breakout.
CSCvr11900	Multicast routes used by Data MDT are not deleted immediately on MVPN PE (where Encapsulation takes place) after all the customer (VRF) traffic stops which use the same Data MDT. They may stay up for 15 minutes and then get deleted.

N/A	When large files, for example NX-OS, images are copied to USB, the following message is printed:
	
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [`
	`8032.291555] INFO: task vsh.bin:9418 blocked for more than 120 seconds. – kernel`
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [`
	`8032.291560]     Tainted: P        O    4.1.21-WR8.0.0.28-standard #1 –`
	`kernel`
	`2019 Jul  2 15:49:47 Molti_A %$ VDC-1 %$ Jul  2 15:49:46 %KERN-3-SYSTEM_MSG: [`
	`8032.291561] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this`
	`message. – kernel`
	
	As long as these messages correspond to a copy operation to USB, this message can be ignored.

N/A	In the NX-API sandbox, whenever XML or JSON output is generated for the show run command or the show startup command, the output contains additional characters. For example, `</nf:source>        <============nf: is extra` `<namespace>` : extra characters are seen with XML and JSON from NX-API.
N/A	When you upgrade a Cisco Nexus 9000 device to Cisco NX-OS Release 9.3(6), if a QSFP port is configured with the manual breakout command and is using a QSA, the configuration of the interface Ethernet 1/50/1 is no longer supported and will need to be removed. To restore the configuration, you must manually configure the interface Ethernet 1/50 on the device.
N/A	Due to the airflow design, back-to-front fans require the fan to be run at full speed all the time. You might also see fan speeds increase from 40% to 70% post-upgrade. This applies to the following PIDs: N9K-C9272Q, N9K-C9236C, N9K-C93180YC-FX, N9K-C93180TC-FX, N9K-C9364C, N9K-C9336C-FX2, N9K-C9332C. This change is made as of Cisco NX-OS Release 7.0(3)I7(3). If your PID is not listed, please contact Cisco TAC for additional verification.
N/A	PTP is not supported on the 96136YC-R line card or for line cards on the Cisco Nexus 9504 switch.

Bug ID	Description
N/A	The following features are not supported on the Cisco Nexus 9364C switch. ■ 100 G port cannot support breakout (HW limitation) ■ FEX ■ ISSU ■ Segment routing ■ Tetration (HW limitation)
N/A	■ The following feature is not supported on the Cisco Nexus 9332C: o uRPF
N/A	Only the following switches support QSFP+ with the QSFP to SFP/SFP+ adapter (40 Gb to 10 Gb): ■ N9K-C93120TX ■ N9K-C93128TX ■ N9K-C9332PQ ■ N9K-C9372PX ■ N9K-C9372PX-E ■ N9K-C9372TX ■ N9K-C9396PX ■ N9K-C93108TC-EX ■ N9K-C93108TC-FX ■ N9K-C93180YC-EX ■ N9K-C93180YC-FX
N/A	The Cisco Nexus 9300 platforms support for the QSFP+ breakout has the following limitations: ■ 1 Gb and 10 Gb can be supported using the QSFP-to-SFP Adapter on 40-Gb uplink ports on Cisco Nexus 9300 platform switches in NX-OS. ■ For the Cisco Nexus 9332PQ switch, all ports except 13-14 and 27-32 can support breakout.

Bug ID	Description
N/A	The following switches and line cards support the breakout cable (40 Gb ports to 4x10-Gb ports): ■ N9K-C9332PQ ■ N9K-X9436PQ line card ■ N9K-X9536PQ line card ■ N9K-C93180LC-EX-–last four ports are breakout capable (10x4, 24x4, 50x2) ■ N9K-C93180YC-EX ■ N9K-C93108TC-EX ■ N9K-X9732C-EX line card ■ N9K-X9732C-FX line card ■ N9K-X97160YC-EX line card ■ N9K-C93180YC-EX ■ N9K-C93108TC-EX ■ N9K-C93180YC-FX ■ N9K-C93108TC-FX ■ N9K-C9348GC-FXP
N/A	Limitations for ALE (Application Link Engine) uplink ports are listed at the following location: Limitations for ALE 40G Uplink Ports on Cisco Nexus 9000 Series Switches
N/A	Converting Type-6 encrypted passwords back to original state is not supported on MACSec chain.
CSCvx88757	After updating the syslog server address, the "This server is temporarily unreachable" message/text is provided as an output. This will continue until the source interface is reconfigured. The workaround is to delete and reconfigure the source interface settings.
CSCwi99525	On Cisco Nexus N2K-C2348TQ HIFs fail to utilize redundant Port-Channel links, to NIF, during link failover events.

Device Hardware

The following tables list the Cisco Nexus 9000 Series hardware that Cisco NX-OS Release 9.3(6) supports. For additional information about the supported hardware, see the *Hardware Installation Guide* for your Cisco Nexus 9000 Series device.

Table 1 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 2 Cisco Nexus 9500 Cloud Scale Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
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-EX	Cisco Nexus 9500 32-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-X9736C-EX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16
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 and 4-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	16

Table 3 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

Table 4 Cisco Nexus 9500 Classic Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9408C-CFP2	Line card with 8 100 Gigabit CFP2 ports	4	8	16
N9K-X9432C-S	Cisco Nexus 9500 32-port 40/100 Gigabit Ethernet QSFP28 line card	4	8	N/A
N9K-X9432PQ	Cisco Nexus 9500 32-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9636PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	N/A
N9K-X9464PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9464TX2	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4-port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9536PQ	Cisco Nexus 9500 36-port 40 Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564PX	Cisco Nexus 9500 48 1/10-Gigabit SFP+ and 4 port 40-Gigabit Ethernet QSFP+ line card	4	8	16
N9K-X9564TX	Cisco Nexus 9500 48 port 1/10-Gigabit BASE-T Ethernet and 4 port 40-Gigabit Ethernet QSFP+ line card	4	8	16

Table 5 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-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-C9516-FM-E	Cisco Nexus 9516 50-Gigabit cloud scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 100-Gigabit cloud scale fabric module	4	5

Table 6 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

Table 7 Cisco Nexus 9500 Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9504-FM	Cisco Nexus 9504 40-Gigabit fabric module	3	6
N9K-C9508-FM	Cisco Nexus 9508 40-Gigabit fabric module	3	6
N9K-C9516-FM	Cisco Nexus 9516 40-Gigabit fabric module	3	6
N9K-C9504-FM-S	Cisco Nexus 9504 100-Gigabit fabric module	4	4
N9K-C9508-FM-S	Cisco Nexus 9508 100-Gigabit fabric module	4	4

Table 8 Cisco Nexus 9500 Fabric Module Blanks with Power Connector

Product ID	Description	Minimum	Maximum
N9K-C9508-FM-Z	Cisco Nexus 9508 Fabric blank with Fan Tray Power Connector module	N/A	2
N9K-C9516-FM-Z	Cisco Nexus 9516 Fabric blank with Fan Tray Power Connector module	N/A	2

Table 9 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
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 10 Cisco Nexus 9500 System Controller

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

Table 11 Cisco Nexus 9500 Fans and Fan Trays

Product ID	Description	Quantity
N9K-C9504-FAN	Fan tray for 4-slot modular chassis	3
N9K-C9508-FAN	Fan tray for 8-slot modular chassis	3
N9K-C9516-FAN	Fan tray for 16-slot modular chassis	3

Table 12 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 13 Cisco Nexus 9200 and 9300 Fans and Fan Trays

Product ID	Description	Quantity	Cisco Nexus Switches
N9K-C9300-FAN1	Fan 1 module with port-side intake airflow (burgundy coloring)	3	9396PX (early versions)
N9K-C9300-FAN1-B	Fan 1 module with port-side exhaust airflow (blue coloring)	3	9396PX (early versions)

Product ID	Description	Quantity	Cisco Nexus Switches	
N9K-C9300-FAN2	Fan 2 module with port-side intake airflow (burgundy coloring)	3	93128TX	9396PX 9396TX
N9K-C9300-FAN2-B	Fan 2 module with port-side exhaust airflow (blue coloring)	3	93128TX	9396PX 9396TX
N9K-C9300-FAN3	Fan 3 module with port-side intake airflow (burgundy coloring)	3	92304QC 9272Q[1]	93120TX
N9K-C9300-FAN3-B	Fan 3 module with port-side exhaust airflow (blue coloring)	3	92304QC 9272Q[1]	93120TX
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	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP[1]
NXA-FAN-30CFM-F	Fan module with port-side exhaust airflow (blue coloring)	3	92160YC-X 9236C[1] 93108TC-EX 93108TC-FX[1] 93180LC-EX[1] 93180YC-EX 93180YC-FX[1]	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9348GC-FXP

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

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

[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.

Table 14 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 93180LC-EX	93180YC-EX 93180YC-FX
NXA-PAC-500W-PI	500-W AC power supply with port-side intake airflow (burgundy coloring)	2	93108TC-EX 93180LC-EX	93180YC-EX 93180YC-FX
N9K-PAC-650W	650-W AC power supply with port-side intake (burgundy coloring)	2	9332PQ 9372PX 9372PX-E 9372TX	9372TX-E 9396PX 9396TX

Product ID	Description	Quantity	Cisco Nexus Switches	
N9K-PAC-650W-B	650-W AC power supply with port-side exhaust (blue coloring)	2	9332PQ 9372PX 9372PX-E 9372TX	9372TX-E 9396PX 9396TX
NXA-PAC-650W-PE	650-W power supply with port-side exhaust (blue coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S	92304QC 93108TC-EX 93180YC-EX
NXA-PAC-650W-PI	650-W power supply with port-side intake (burgundy coloring)	2	92160YC-X 9236C 92300YC 93180YC-FX3S	92304QC 93108TC-EX 93180YC-EX
NXA-PAC-750W-PE	750-W AC power supply with port-side exhaust airflow (blue coloring) [1]	2	9336C-FX2 93240YC-FX2	9332C 9336C-FX2
NXA-PAC-750W-PI	750-W AC power supply with port-side exhaust airflow (burgundy coloring) [1]	2	9336C-FX2 93240YC-FX2	9332C 9336C-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 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 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	
N9K-PAC-1200W	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	93120TX	

Product ID	Description	Quantity	Cisco Nexus Switches	
N9K-PAC-1200W-B	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	93120TX	
NXA-PAC-1200W-PE	1200-W AC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93360YC-FX2	9364C
NXA-PAC-1200W-PI	1200-W AC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93360YC-FX2	9364C
N9K-PUV-1200W	1200-W Universal AC/DC power supply with bidirectional airflow (white coloring)	2	92160YC-X 9236C 92300YC 92304QC 9272Q[1] 93108TC-EX 93108TC-FX 93360YC-FX2 93180YC-FX3S	93120TX 93128TX 93180LC-EX 93180YC-EX 93180YC-FX 9364C
NXA-PDC-930W-PE	930-W DC power supply with port-side exhaust airflow (blue coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S	93120TX 93180YC-FX 9364C 92160YC-X
NXA-PDC-930W-PI	930-W DC power supply with port-side intake airflow (burgundy coloring)	2	9272Q 93108TC-EX 93180YC-EX 93360YC-FX2 93180YC-FX3S	93120TX 93180YC-FX 9364C 92160YC-X
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
NXA-PDC-1100W-PI	1100-W DC power supply with port-side intake airflow (burgundy coloring)	2	93240YC-FX2 93600CD-	9332C 9336C-FX2

Product ID	Description	Quantity	Cisco Nexus Switches	
			GX 9316D-GX	
UCSC-PSU-930WDC	930-W DC power supply with port-side intake (green coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX 93120TX 93128TX 93180YC-EX	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
UCS-PSU-6332-DC	930-W DC power supply with port-side exhaust (gray coloring)	2	92160YC-X 9236C 92304QC 9272Q 93108TC-EX 93120TX 93128TX 93180YC-EX	9332PQ 9372PX 9372PX-E 9372TX 9372TX-E 9396PX 9396TX
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 airflow (blue coloring)	2	9364C-GX	
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	

[1] Compatible with Cisco NX-OS Release 9.3(3) and later.

Table 15 Cisco Nexus 9200 and 9300 Switches

Cisco Nexus Switch	Description
N9K-C92160YC-X	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports (4 of these ports support 100-Gigabit QSFP28 optics).
N9K-C92300YC	1.5-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 ports and 18 fixed 40-/100-Gigabit QSFP28 ports.
N9K-C92304QC	2-RU Top-of-Rack switch with 56 40-Gigabit Ethernet QSFP+ ports (16 of these ports support 4x10 breakout cables) and 8 100-Gigabit QSFP28 ports.
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-C9236C	1-RU Top-of-Rack switch with 36 40-/100-Gigabit QSFP28 ports (144 10-/25-Gigabit ports when using breakout cables)
N9K-C9272Q	2-RU Top-of-Rack switch with 72 40-Gigabit Ethernet QSFP+ ports (35 of these ports also support 4x10 breakout cables for 140 10-Gigabit 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.
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-C93120TX	2-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports
N9K-C93128TX	3-RU Top-of-Rack switch with 96 1/10GBASE-T (copper) ports and an uplink module up to 8 40-Gigabit QSFP+ ports
N9K-C9316D-GX	1-RU switch with 16x400/100/40-Gbps ports.
N9K-C93180LC-EX	1-RU Top-of-Rack switch with 24 40-/50-Gigabit QSFP+ downlink ports and 6 40/100-Gigabit uplink ports. You can configure 18 downlink ports as 100-Gigabit QSFP28 ports or as 10-Gigabit SFP+ ports (using breakout cables).
N9K-C93180YC-EX	1-RU Top-of-Rack switch with 48 10-/25-Gigabit SFP28 fiber ports and 6 40-/100-Gigabit QSFP28 ports

Cisco Nexus Switch	Description
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-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-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-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-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-C9332C	1-RU fixed switch with 32 40/100-Gigabit QSFP28 ports and 2 fixed 1/10-Gigabit SFP+ ports.
N9K-C9332PQ	1-RU switch with 32 40-Gigabit Ethernet QSFP+ ports (26 ports support 4x10 breakout cables and 6 ports support QSFP-to-SFP adapters)
N9K-C93360YC-FX2	2-RU switch with 96 10-/25-Gigabit SFP28 ports and 12 40/100-Gigabit QSFP28 ports
N9K-C9336C-FX2	1-RU switch with 36 40-/100-Gb Ethernet QSFP28 ports.
N9K-C9348GC-FXP	Nexus 9300 with 48p 100M/1 G, 4p 10/25 G SFP+ and 2p 100 G QSFP
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. Ports 65 and 66 support 1/10 Gigabit speeds.
N9K-C9364C-GX	2-RU fixed-port switch with 64 100-Gigabit SFP28 ports.
N9K-C9372PX	1-RU Top-of-Rack switch with 48 1-/10-Gigabit SFP+ ports and 6 40-Gigabit QSFP+ ports
N9K-C9372PX-E	An enhanced version of the Cisco Nexus 9372PX-E switch.

Cisco Nexus Switch	Description
N9K-C9372TX	1-RU Top-of-Rack switch with 48 1-/10GBASE-T (copper) ports and 6 40-Gigabit QSFP+ ports
N9K-C9372TX-E	An enhanced version of the Cisco Nexus 9372TX-E switch.
N9K-C9396PX	2-RU Top-of-Rack switch with 48 1-/10-Gigabit Ethernet SFP+ ports and an uplink module with up to 12 40-Gigabit QSFP+ ports
N9K-C9396TX	2-RU Top-of-Rack switch with 48 1/10GBASE-T (copper) ports and an uplink module with up to 12 40-Gigabit QSFP+ ports

Table 16 Cisco Nexus 9000 Series Uplink Modules

Product ID	Description
N9K-M4PC-CFP2	Cisco Nexus 9300 uplink module with 4 100-Gigabit Ethernet CFP2 ports. For the Cisco Nexus 93128TX switch, only two of the ports are active. For the Cisco Nexus 9396PX and 9396TX switches, all four ports are active.
N9K-M6PQ	Cisco Nexus 9300 uplink module with 6 40-Gigabit Ethernet QSFP+ ports for the Cisco Nexus 9396PX, 9396TX, and 93128TX switches.
N9K-M6PQ-E	An enhanced version of the Cisco Nexus N9K-M6PQ uplink module.
N9K-M12PQ	Cisco Nexus 9300 uplink module with 12 40-Gigabit Ethernet QSPF+ ports.

Optics

To determine which transceivers and cables are supported by a switch, see the [Transceiver Module (TMG) Compatibility Matrix](#).

To see the transceiver specifications and installation information, see the [Install and Upgrade Guides](#).

Cisco Network Insights for Data Center

Cisco NX-OS Release 9.3(6) supports the Cisco Network Insights Advisor (NIA) and Cisco Network Insights for Resources (NIR) on Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches and 9500 platform switches with -EX/FX line cards.

For more information, see the [Cisco Network 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 9.3(x)](#).

For information about an In Service Software Upgrade (ISSU), see the [Cisco NX-OS ISSU Support Matrix](#).

Exceptions

- [Cisco Nexus 9200, 9300-EX, and 9300-FX Platform Switches](#)

- [Cisco Nexus 9300-FX3 Platform Switches](#)

- [Cisco Nexus 9300-GX Platform Switches](#)

- [Cisco Nexus 9500 Platform N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches](#)

- [FEX Modules](#)

- [N9K-X96136YC-R Line Card](#)

- [N9K-X9736C-FX Line Card](#)

- [Nexus 9500 Cloud Scale](#)

Cisco Nexus 9200, 9300-EX, and 9300-FX Platform Switches

The following features are not supported for the Cisco Nexus 9200, 9300-EX, and 9300-FX platform switches:

- 64-bit ALPM routing mode

- Cisco Nexus 9272PQ and Cisco Nexus 92160YC platforms do not support the PXE boot of the Cisco NX-OS image from the loader.

- ACL filters to span subinterface traffic on the parent interface

- Egress port ACLs

- Egress QoS policer (not supported for Cisco Nexus 9200 platform switches). The only policer action supported is drop. Remark action is not supported on the egress policer.

- FEX (not supported for Cisco Nexus 9200 platform switches)

- GRE v4 payload over v6 tunnels

- IP length-based matches

- IP-in-IP (not supported on the Cisco Nexus 92160 switch)

- Maximum Transmission Unit (MTU) checks for packets received with an MPLS header

- NetFlow (not supported on Cisco Nexus 9200 platform switches)

- Packet-based statistics for Traffic Storm Control (only byte-based statistics are supported)

- PVLANs (not supported on Cisco Nexus 9200 platform switches)

- PXE boot of the Cisco NX-OS image from the loader (not supported for Cisco Nexus 9272PQ and 92160YC switches)

- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)

- Q-in-Q for VXLAN (not supported on Cisco Nexus 9200 and 9300-EX platform switches)

- Q-in-VNI (not supported on Cisco Nexus 9200 platform switches)

- Resilient hashing for port channels

- Rx SPAN for multicast if the SPAN source and destination are on the same slice and no forwarding interface is on the slice

- SVI uplinks with Q-in-VNI (not supported for Cisco Nexus 9300-EX platform switches)

- Traffic Storm Control for copy-to-CPU packets

- Traffic Storm Control with unknown multicast traffic

- Tx SPAN for multicast, unknown multicast, and broadcast traffic

- VACL redirects for TAP aggregation

Cisco Nexus 9300-FX3 Platform Switches

The following features are not supported for the Cisco Nexus 9300-FX3 Platform switches:

- ACL with DSCP Wildcard Mask

- ARP Suppression with Reflective Relay

- Dynamic ACL - Named ACL support for applying blacklist/limited VLAN access for devices

- ECMP Hashing based on GRE Inner IP Header

- Enhanced ISSU

- Enhanced Policy-Based Routing (ePBR)

- ePBR Multi-Hop

- ePBR with Probes

- ePBR with User-Defined Probes

- IPv6 MIB support (IP-MIB)

- Multicast Service Reflection (Ingress, PIM-border, Egress)

- Multiple LLDP neighbors per physical interface

- Secure VXLAN EVPN Multi-Site using CloudSec

- Selective Q-in-VNI + Advertise PIP on a VTEP

- Selective Q-in-VNI + VXLAN VLAN on the same port

- Standard ISSU

- Symmetric Hashing - ECMP (Inner DA)

- Unidirectional Ethernet (UDE)

- VXLAN EVPN with downstream VNI

- VXLAN over parent interface that also carries sub-interfaces

Cisco Nexus 9300-GX Platform Switches

The following features are not supported for the Cisco Nexus 9300-GX platform switches:

■ 802.1x with VXLAN

■ Asymmetric PFC

■ Autonegotiation on all ports

■ Enhanced ISSU

■ FC-FEC for Cisco Nexus 9316D-GX and 93600CD-GX switches is not supported on the second lane of the 50x2 breakout port.

■ FEX

■ FTE

■ TRM + Multi-Site

■ ITD with VXLAN

■ Multi Auth with COA

■ Multicast over GRE

■ RTP Monitoring

■ Standard ISSU

■ VRF Aware FT

Cisco Nexus N9K-X9408PC-CFP2 Line Card and 9300 Platform Switches

The following features are not supported for Cisco Nexus 9500 platform switches with the N9K-X9408PC-CFP2 line card and Cisco Nexus 9300 platform switches with generic expansion modules (N9K-M4PC-CFP2):

■ 802.3x

■ Breakout ports

■ FEX (supported on some Cisco Nexus 9300 platform switches)

■ Flows other than 40G

■ Multichassis EtherChannel Trunk (MCT)

■ NetFlow

■ Port-channel (No LACP)

■ PFC/LLFC

■ Precision Time Protocol (PTP)

■ PVLAN (supported on Cisco Nexus 9300 platform switches)

- Shaping support on 100g port is limited

- SPAN destination/ERSPAN destination IP

- Traffic Storm Control

- vPC

- VXLAN access port

FEX Modules

The following features are not supported for FEX modules:

- Active-Active FEX and straight-through FEX are not supported on the Cisco Nexus 92348GC switch.

- For Cisco Nexus 9500 platform switches, 4x10-Gb breakout for FEX connectivity is not supported.

Cisco Nexus N9K-X96136YC-R Line Card

The following features are not supported for Cisco Nexus 9500 platform switches with the N9K-X96136YC-R line card:

- Breakout

- PTP and gPTP

Cisco Nexus N9K-X9736C-FX Line Card

The following feature is not supported for Cisco Nexus 9500 platform switches with the N9K-X9736C-FX line card:

- Ports 29-36 do not support 1 Gbps speed.

Cisco Nexus 9500 Cloud Scale (EX/FX) Line Cards

The following features are not supported for Cisco Nexus 9500 platform switches with -EX/FX line cards:

- FEX

- IPv6 support for policy-based routing

- LPM dual-host mode

- SPAN port-channel destinations

Related Content

Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference: Cisco Nexus NX-API Reference

Cisco Nexus 9000 Series documentation: Cisco Nexus 9000 Series Switches

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 9.3(x)**

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes: Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 9.3(6)

Cisco Nexus OpenConfig YANG Reference, Release 9.3(x): Cisco Nexus OpenConfig YANG Reference, Release 9.3(x)

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

When you downgrade from Cisco NX-OS Release 9.3(6) 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.

For more information, 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: www.cisco.com/go/trademarks. 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. (1110R)

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.