Cisco Nexus Data Broker Release Notes, Release 3.9

This document describes the features, caveats, and limitations on Cisco Nexus Data Broker for Release 3.9.

Use this document with documents listed in *Related Documentation*.

Online History Change Table

Date	Description
April 3, 2020	Initial release of the document.
April 13, 2020	Added CSCvt75433, CSCvt75421, CSCvt75405, CSCVo98675, CSCvt62492 to the list of NDB Open Caveats.
April 23, 2020	Added CSCvt92735 to the list of NX-OS Known Caveats.
May 12, 2020	Added CSCvu17887, CSCvu16131 to the list of NDB Open Caveats.
August 17, 2020	Added CSCvv22414 to the list of NX-OS Known Caveats.
March 21, 2021	Added CSCvx45678,CSCvx32214 to the list of NX-OS Known Caveats.
April 19, 2021	Added CSCvx79293 to the list of NX-OS Known Caveats. Modified the Interoperability Matrix table with support for NX-OS 9.3(7).
May 14, 2021	Added CSCvy16218 to the list of NX-OS Known Caveats.
September 7, 2021	Added CSCvz21072 to the list of NX-OS Known Caveats.
September 20, 2021	Updated the Interoperability Matrix table to indicate support for NX-OS Release 10.1(2).
October 20, 2021	Added CSCvz99026 to the list of Open Caveats.
December 10, 2021	Updated to indicate 93180LC-EX is not supported on NX-OS Release 10.1(2).
July 1, 2022	Updated the Interoperability table to indicate support of NX-OS releases, 9.3(5), 9.3(7a), 9.3(8), for Cisco Nexus 3548 switch.
July 18, 2022	Updated the Interoperability Matrix table to indicate support for NX-OS release 9.3(9).

Contents

Introduction

Visibility into application traffic is important for infrastructure operations to maintain security and compliance, and to perform resource planning and troubleshooting. With the technological advances and growth in cloud-based applications, it has become imperative to gain increased visibility into the network traffic. Traditional approaches to gain visibility into network traffic are expensive and rigid, making it difficult for managers of large-scale deployments.

Cisco Nexus Data Broker (NDB) with Cisco Nexus Switches provides a software-defined, programmable solution to aggregate copies of network traffic using SPAN or network taps for monitoring and visibility. As opposed to traditional network taps and monitoring solutions, this packet-brokering approach offers a simple, scalable and cost-effective solution well-suited for customers who need to monitor higher-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

Cisco NDB also provides a software-defined, programmable solution to perform inline inspection of the network traffic for monitoring and visibility purpose. Inline traffic inspection is performed on specific traffic by redirecting it through multiple security tools before it enters or exits a network.

New Software Features

Details of all the features listed here are available in the Cisco Nexus data Broker Configuration Guide, Release 3.9

Feature	Description
Show tech for NX-API Devices	Enables the user to collect information from one or more switches in one attempt, instead of collecting data separately from each switch. NDB logs can also be downloaded.
Span Destination with ER-SPAN Enhancements	From NDB, ER-SPAN based session(s) can be created.
Cluster Topology	The topology for all the nodes of the NDB cluster are in sync.
Slice Support for NX-API/ SPAN and AUX Devices	All types of devices are placed in different slices based on the requirement.
Restore Configuration	Enables the user to select the option of restoring the configuration and the port admin state in the NDB switch.
Connection Status Updates	Session staus is added to the list of parameters that determine the status of a connection. The green band indicating the success of the connection turns pink or yellow if the session has failed.
Software-based UDE for Block Rx	NDB to push port configurations for software unidirectional ethernet for send-only. This is supported on N9K 95xx switches with 97160YC-EX line card for NX-OS 9.3(3) onwards.
JSON Import/ Export Enhancement	Enables all configurations to be exported and imported in JSON format.
JRE Version updates	JRE version was updated to 1.8.221.
Device Reload Updates	The reload of NX-API devices is detected based on the state of the ethernet modules.
Multiple Port	The time taken to configure certain ports has been reduced.

Feature	Description
Configuration Updates	

Unsupported Features

The following features are not supported in the embedded deployment mode of Cisco Nexus Data Broker:

- Adding another NDB device

- Adding APIC for ACI SPAN session

- Adding production device for the SPAN session

- Configuring SPAN session

- Configuring copy device

- Configuring copy sessions

- Scheduling Configuration Backup

- NDB High availability

Compatibility Information

Cisco Nexus Data Broker, Release 3.9 supports the following Cisco Nexus platforms:

Device Model	Cisco Nexus Data Broker Minimum Version	Supported Deployment Mode	Supported Use Cases
Cisco Nexus 3000 Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 3100 Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 3164Q Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 3200 Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only In-line redirection
Cisco Nexus 3500 Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9200 Series Switch	Cisco Nexus Data Broker 3.1 or later	Centralized and Embedded Note: Cisco Nexus 9200 Series switches support only one switch deployment.	Tap/SPAN aggregation only
Cisco Nexus 9300 Series Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 9300-EX Series Switch	Cisco Nexus Data Broker 3.1 or later	Centralized and Embedded	Tap/SPAN aggregation only

Cisco Nexus 9300-FX Series Switch	Cisco Nexus Data Broker 3.5 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9332C Series Switch	Cisco Nexus Data Broker 3.8 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9364C Series Switch	Cisco Nexus Data Broker 3.8 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9500 Series Switch Supported Modules: ▪ N9K-X9464TX	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9500-EX Series Switch Supported Modules: ▪ N9K-X97160YC-EX ▪ N9K-X9732C-EX	Cisco Nexus Data Broker 3.5 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9500-FX Series Switch	Cisco Nexus Data Broker 3.5 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 31100 Series Switch	Cisco Nexus Data Broker 3.7 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 9300-FX2 Series Switch	Cisco Nexus Data Broker 3.7 or later	Centralized and Embedded	Tap/SPAN aggregation only

Cisco NDB Hardware and Software Interoperability Matrix

The following table lists the hardware and software interoperability matrix for Cisco NDB, Release 3.9:

Nexus Switch Model(s)	Implementation Type	Supported NX-OS Versions	OpenFlow Agent
3048/3064/3172	OpenFlow	6.0(2)U6(x), I2(x), and I3(x)	1.1.5

3048/3064/3172	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8), 9.3(9).	2.14
3046/3064	NX-API	6.0(2)U6(x), 7.0(3)I4(1) to 7.0(3)I4(8b)	Not supported
3172	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to, 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9).	Not applicable
3164	OpenFlow	Not supported	Not supported
3164	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9).	Not applicable
3232	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9).	2.14
3232	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9).	Not applicable

3548	OpenFlow	6.0(2)A6(x) and 6.0(2)A8(x). I7(5) and I7(5a), and 9.3(1) to 9.3(5), 9.3(7a), 9.3(8) , 9.3(9). (OF agent is not required) 7.0(3)I7(2) to 7.0(3)I7(9)	1.1.5
3548	NX-API	Not supported	Not supported
92160/92304	OpenFlow	Not supported	Not supported
92160/92304[1]	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8), 10.1(2) , 9.3(9).	Not applicable
9372/9396[1]/93128[1]	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8),10.1(2) , 9.3(9).	2.14
9372/9396[1]/93128[1]	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9), 10.1(2).	Not applicable
9364C/9332C	NX-API	9.2(3) to 9.2(4) and 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8), 9.3(9), 10.1(2).	NA
9364C/9332C	OpenFlow	Not supported	Not supported
93180LC-EX[1] / 93108TC-EX / 93180YC-EX	OpenFlow	Not supported	Not supported

93180LC-EX[1]/ 93108TC-EX / 93180YC-EX	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8), 9.3(9), 10.1(2).	NA
93108TC-FX / 93180YC-FX	OpenFlow	Not supported	Not supported
93108TC-FX / 93180YC-FX	NX-API	7.0(3)I7(1) to 7.0(3)I7(6), 7.0(3)I7(8), 7.0(3)I7(9), 9.2(1) to 9.2(4) , 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8), 9.3(9), 10.1(2).	Not applicable
9504/9508/9516	OpenFlow	Not supported	Not supported
9504/9508/9516	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7), 9.3(7a), 9.3(8), 9.3(9).	Not applicable
31108TC-V / 31108PC-V	NX-API	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9), 10.1(2).	Not applicable
31108TC-V / 31108PC-V	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9), 10.1(2).	Not applicable
9336C-FX2 / 93240YC-FX2	NX-API	7.0(3)I7(5), 7.0(3)I7(5a), 7.0(3)I7(6) to 7.0(3)I7(9), 9.2(1) to 9.2(4), 9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9),10.1(2).	Not applicable

N9K-C93360YC-FX2	NX-API	9.3(1) to 9.3(5), 9.3(7) , 9.3(7a), 9.3(8) , 9.3(9),10.1(2).	Not applicable

[1-] NX-OS Release 10.1(2) is not supported on these platforms.

Supported APIC Versions

The following table lists the APIC versions supported on Cisco NDB for Release 3.9:

APIC Version	Cisco NDB (Minimium Version)	Supported Deployment Mode
1.1, 1.2 and 2.0	NDB 3.0	Centralized only
2.x	NDB 3.1 and above	Centralized only
4.x	NDB 3.7 and above	Centralized only

Verified Scalability Limits

The following table lists the scalability limits for centralized deployment on Cisco:

Description	Small	Medium	Large
Number of switches used for Tap and SPAN aggregation	25	50	75

Licensing Information

For details about NDB Licensing, see the Cisco Nexus Data Broker Licensing section in the Ordering guide.

Guidelines and Limitations

This section lists guidelines and limitations for features in Cisco Nexus Data Broker Release 3.9:

- Cisco NDB Openflow embedded is not supported on Cisco Nexus 3000/9000 series switches running 7.0(3)I6.1 and 7.0(3)I7.1 NXOS image.

- Dry Run feature is disabled by default. To enable this feature, see Cisco NDB Configuration Guide.

- Default deny ACL on all ports and Default ISL deny ACL on ISL ports is enabled by default for Cisco NDB ,Release 3.6 and later releases. To disable this feature, refer the *Cisco Nexus Data Broker Configuration Guide, Release 3.9*

- By default, NDB cluster URL is https://<NDBIP>:8443

- NDB supports Google Chrome version 45.x and later, FireFox version 45.x and later, and Internet Explorer version 11 and later.

- The switchport mode trunk and spanning-tree bpdufilter enable command should be enabled for all switch ports on all Cisco NDB managed switches.

- Cisco Nexus switches managed by Cisco NDB in NX-API mode must have LLDP feature enabled. Disabling LLDP may cause inconsistencies and require switch rediscovery for NX-API switches

- For secured communication between Cisco NDB and switch through HTTPS, start Cisco NXB in TLS mode for the first time only. Subsequent Cisco NDB restarts does not require TLS mode. For more details, refer to Cisco Nexus Data Broker Configuration Guide.

- The TLS KeyStore and TrustStore passwords are sent to the Cisco Nexus Data Broker so it can read the password-protected TLS KeyStore and TrustStore files only through HTTPS.

  ./xnc config-keystore-passwords [--user {user} --password {password} --url {url} --verbose --prompt --keystore-password {keystore_password} --truststore-password {truststore_password}.

  Here default URL to be - https://Nexus_Data_Broker_IP:8443

- Cisco Nexus 92XX devices does not support the QnQ, you cannot use this switch in the Multi switch environment.

11

- A Cisco NDB instance can support either the OpenFlow or NX-API configuration mode, it does not support both configuration modes in the same Cisco NDB instance.

- VLAN based IP filtering is not supported for Nexus Series switch with NX-OS Release 7.0(3)I6.1. Hence, the filtering fails when you filter the traffic for the following series of switches: 92160YC-X,92300YC, 9272Q, 92304Q, and 9236C.

- Do not configure TACACS on the Cisco NDB switches. You can configure it only for authentication and authorization. It is not to be used for accounting.

- Cisco NX-OS Release 7.0(3)I5(1), 7.0(3)I5(2), and 7.0(3)I7(2) are not recommended for OpenFlow and NX-API deployments.

- Cisco NDB Embedded will be supported on NX-OS 7.0(I4).1 onwards, and 7.0(3)I6.1 onwards. For more information, see the *Nexus Data Broker Hardware and Software Interoperability Matrix* section.

Caveats

Note: All caveats listed in this document are those that were reported against the Cisco NDB.

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Note: All caveats listed in this document are those that were reported against the Cisco NDB.

This section includes the following topics:

- NDB Resolved Caveats

- NDB Open Caveats

- NX-OS Known Caveats

NDB Resolved Caveats

The following table lists the Resolved Caveat in Release 3.9. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Bug ID	Description
CSCvi33830	Unable to configure ports/connections after creating slice user.
CSCvs34338	Slice is not compatible with Auxiliary devices, Swagger APIs, and Span Management (ACI/PS)

CSCvk47961	Port configuration fails while importing the json file with unsupported characters in the description.
CSCvg26989	Export operation does not retrieve Node specific configuration.
CSCvs06129	Connection in failed state post upgrading NDB from 2.x, 3.0 and 3.1 to 3.8.1 and above.

NDB Open Caveats

The following table lists the open caveats in the Cisco Release 3.9. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Bug ID	Description
CSCvm65172	Direction change should be supported while editing span session.
CSCvg29188	Limitations in uploading a configuration that has redirections (bi-directional).
CSCvg10351	NDB Server backup entries are not shown in the UI after the upgrade.
CSCvk39789	**"Could not commit transaction" exception thrown at NDB.**
CSCvs65911	Port Channel Configuration is not getting exported.
CSCvt75405	Layout of Connection Table is not proper in 3.9.
CSCvt75421	Upgrade failed with Remote Source configuration from 3.8 to 3.9 in a sequence.
CSCvo98675	Upgrade is not happening on doing any operations on second session.
CSCvt75433	Search by Description field in NDB Connections tab is not working.
CSCvt62492	Port-channel operations on ISL links results in failure of Link discovery.
CSCvu16131	N9K-C93180YC-FX can't connect to NDB after upgrade to 3.9.0.
CSCvu17887	Process Thread-15 takes 97% of CPU in NDB 3.9.0.
CSCvz99026	Not able to install connection with filter having IPv6/IPV4+VLAN in 10.1(2) NXOS.

NX-OS Known Caveats

The following table lists the known caveats from previous releases. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Bug ID	Description
CSCvo85210	Can't match MAC address in IP packet, it will hit deny any any in IP ACLs.
CSCvq61822	Need Error handling for feature SFLOW with ERSPAN destination since they are mutually exclusive.
CSCvt15642	Can't match MAC address in IP packet, it will hit deny any any in IP ACLs.
CSCvo21059	MPLS tapagg should allow deny ace without redirection option.
CSCvd15455	Openflow - Portchannel links are not seen on NDB, Release 2.1.
CSCvc87992	Connections are not matched with the VLAN ID of source ports on ISL links with an IPv6 filter.
CSCvt15877	Not able to use ipv6 + vlan on the ISL link.

CSCvs50998	IP ACL with UDF match removes internal VLAN tag in Cisco NX-OS Release 9.3(2).
CSCvr01876	Re-direct STP, CDP packets similar to LLDP port for Openflow.
CSCvs59353	After device reload guestshell activation fails due to low memory on devices for NXOS 9.x.x version.
CSCvs75586	IP/GRE traffic not matching TapAgg ACL in 9.2(3).
CSCvs79485	After an upgrade the odd vlan-id numbers are written incorrectly in TCAM 9.3(3).
CSCvt14639	Not able to convert Layer 2 ports to layer 3 in 9.3(3).
CSCvt03231	ACL with HTTP tcp-option-length redirect statement are not matching traffic correctly in 9.3(3).
CSCvt37799	ERSPAN Dest doesn't work when L2 port with mode tap-aggregation is converted to L3 port in 9.3(3).
CSCvt92735	After reloading switch N9372PX-118 in GS it takes more time to send interface details to NDB server.
CSCvv22414	9508/9516-with 4k VLAN scale modules go to powered down state when upgrading to 9.3.3 and above.
CSCvx45678	After device reload guestshell activation fails due to low memory on devices for NXOS 9.3(5) version.
CSCvx32214	Dot1q-tunnel(QinQ) is not programmed correctly for port-channel members in NXOS 9.3(5).
CSCvx79293	Not seeing timestamptag on interface after configuring the cmds on C9504 platform in nxos 9.3.7.
CSCvy16218	Username is shown as 'guestshell' irrespective of user executes the guestshell.
CSCvz21072	NDB throws NumberFormatException error with NX-OS 9.3(7a) devices.

Related Documentation

The entire Cisco NDB documentation set is available at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-data-broker/tsd-products-support-series-home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

https://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Open a service request online at:

https://tools.cisco.com/ServiceRequestTool/create/launch.do

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.