



Cisco Nexus Data Broker, Release 3.3, Release Notes

This document describes the features, caveats, and limitations for the Cisco Nexus Data Broker software, Release 3.3.

Additional product documentation is listed in the “Related Documentation” section.

Release notes are updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
June 01, 2017	Created the release notes for the 3.3 release.
January 8, 2018	Updated the supported APIC versions.
January 9, 2018	Updated the support for NX-OS versions.

Contents

This document includes the following sections:

- **CONTENTS**
- **INTRODUCTION**
- **COMPATIBILITY INFORMATION**
- **USAGE GUIDELINES**
- **VERIFIED SCALABILITY LIMITS**
- **NEW AND CHANGED INFORMATION**
- **CAVEATS**
- **RELATED DOCUMENTATION**

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 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 Nexus Data Broker also provides management support for multiple disjointed Cisco Nexus Data Broker networks. You can manage multiple Cisco Nexus Data Broker topologies that may be disjointed using the same application instance. For example, if you have five data centers and want to deploy an independent Cisco Nexus Data Broker solution for each data center, you can manage all five independent deployments using a single application instance by creating a logical partition (network slice) for each monitored network.

Compatibility Information

The 3.3 release supports the following operating systems for the full visibility software sensors:

Device Model	Cisco Nexus Data Broker Minimum version	Deployment Mode Supported	Supported Use Cases
Cisco Nexus 3000 Series	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 3100 platform	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation and In-line redirection
Cisco Nexus 3164Q Switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 3500 Series	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9300	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation

Device Model	Cisco Nexus Data Broker Minimum version	Deployment Mode Supported	Supported Use Cases
platform	later	ded	and In-line redirection
Cisco Nexus 9500 platform	Cisco Nexus Data Broker 3.0 or later	Centralized only	Tap/SPAN aggregation only
Cisco Nexus 3200 switch	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9200 switch	Cisco Nexus Data Broker 3.1 or later	Centralized and Embedded	Tap/SPAN aggregation only
Cisco Nexus 9300-EX switch	Cisco Nexus Data Broker 3.1 or later	Centralized and Embedded	Tap/SPAN aggregation only

Usage Guidelines and Limitations

This section lists the usage guidelines and limitations for the Cisco Nexus Data Broker. You must use the Google Chrome browser version 45.x or later to access the web-based user interface.

- Export and import NDB Configuration feature is supported only for NDB embedded deployment. This feature is not supported for Port Group, Advance, UDF Filters, Production, and APIC SPAN session.
- By default, NDB cluster URL is <https://<NDBIP>:8443>.
- The browser supported by NDB is Google Chrome, version 45.x and later and FireFox version 45.x and later.
- APIC versions supported are 1.1, 1.2, 2.0 & 3.0 series.
- The **switchport mode trunk** command should be enabled on all the Nexus Data Broker managed interfaces.
- The **spanning-tree bpduguard enable** command should be enabled for all the inter-switch ports for all the platform series.
- Cisco Nexus Data Broker Embedded is supported on NXOS 7.0(I4).1 onwards, and 7.0(3)I6.1 onwards.
- The following features will not be supported in embedded mode deployment of Cisco Nexus Data Broker
 - Configuring SPAN session
 - Configuring copy device
 - Configuring copy sessions
 - Scheduling Configuration Backup

- Adding another NDB device
- Adding APIC for ACI SPAN Session
- Adding production device for SPAN session
- HTTP access on port 8080 is disabled by default. Only HTTPS access on port 8443 is enabled. You can enable HTTP access by editing the tomcat.xml file. For more details, refer to *Cisco Nexus Data Broker Configuration Guide*.
- The Cisco Nexus Data Broker assumes inter-switch link interfaces are configured to be layer 2 switch ports, and these interfaces are set to 'switchport trunk' by default.
- Before installing or upgrading to Cisco NDB, Release 3.3, you need to configure TCAM region for IPv6 ACL in all devices that are going to be managed by NDB 3.3.
- Use minimum JRE version 1.8.0_45 for latest security fixes.
- Cisco Nexus 9000 switches managed by Cisco Nexus Data Broker must have LLDP features enabled. Disabling LLDP may cause inconsistencies and require devices to be deleted and re-added.
- When removing devices from the Cisco Nexus Data Broker, the device associated port definitions and connections should be removed first. Otherwise, the device might contain stale configurations created by the Cisco Nexus Data Broker.
- For Cisco NX-API devices, there is a 3 minute wait after reload for the Cisco Nexus Data Broker configuration operations to begin (port definitions, connection creation/deletion and stats). This is to avoid any inconsistencies between Cisco Nexus Data Broker and device during the reload operation.
- For secured communication between Nexus Data Broker and Device through HTTPS, start Nexus Data Broker in 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
```
- A Cisco Nexus Data Broker instance can support either the OpenFlow or NX-API configuration mode, it does not support both configuration modes at an instance.
- VLAN based IP filtering is not supported for Nexus Series switch with NxOS version 7.0(3)I6.1. Hence, the filtering fails when you filter the traffic for the following series of switches: 92160YC-X Switch, 92300YC Swicth, 9272Q switch, 92304Q Switch, 9236C Switch.
- For the NDB cluster deployment, the round trip delay across the various servers participating in the cluster should be less than 50 milliseconds. If the round trip delay is more, the NDB cluster behaves unexpectedly. The NDB server round trip delay should be less than 50 ms. If anything above that will have issue in NDB sync up with member servers.
- For Cisco NDB Release 3.3, Cisco NX-OS Release versions 7.0(3)I5(1) and 7.0(3)I5(2) are not recommended for NXAPI or OpenFlow deployments.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Nexus Data Broker for Centralized Deployment

Table 2 Scalability Limits for Cisco Nexus Data Broker

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

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- [New Software Features](#)

New Software Features

Following new software features are available in this release:

- Advanced Filtering support for TCP and UDP flags. The following flags are supported:
 - IPv4 = DSCP, Fragments, Precedence, TTL
 - IPv6 = DSCP, Fragments
 - IPv4 + UDP = DSCP, Fragments, Precedence, TTL
 - IPv6 + UDP = DSCP, Fragments
 - IPv4 + TCP = Ack, DSCP, Fragments, FIN, Precedence, PSH, RST, SYN, TTL
 - IPv6 + TCP = Ack, DSCP, Fragments, FIN, Fragment, PSH, RST, SYN
- User Defined Filtering (UDF) support on Nexus 9000 series switch allows user to filter based on any parameter within the first 128 bytes of the packet.
- Support for Default Match-all filter that includes filtering MPLS traffic.
- Default UDF filter to match inner vlan in a QinQ environment.
- Export NDB Configuration to replicate the configuration on other devices. Configuration replication includes copying the information about port definitions, monitor devices, connections, service nodes and redirections corresponding to the exported devices.
 - Using the exported configuration, you can import the same configuration to another NDB.
 - This feature is supported for both the Open Flow and NXAPI devices.
 - This feature is currently supported only for NDB Embedded deployment.
- LDAP support for Role Based Access Control (RBAC) using external AAA server for both authentication and authorization.
- Support for Automatic Overlapping Filters Connection installation for both NXAPI and OpenFlow.
- Cisco NDB Embedded installation support for NXOS 7.0(3)I6.1 release on Cisco Nexus 9000 switches for NXAPI device type.
- NDB centralized application comes bundled with JRE. User don't need to download and install JRE in NDB server.

Feature Limitations:

The following feature limitation apply for the Cisco Nexus Data Broker, Release 3.3:

- NDB Embedded Installation for OpenFlow device is not supported for 7.0(3)I5.1 and 7.0(3)I6.1 NxOS release trains.
- NDB embedded is not supported on Cisco Nexus 3000 series switches running 7.0(3)I5.1 and 7.0(3)I6.1 NXOS image.

Caveats

This section contains lists of open and resolved caveats and known behaviors.

Caveats

- Open Caveats
- Resolved Caveats
- Known Caveats

Open Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Open Caveats in the 3.3 Release

Bug ID	Description
CSCuy81365	After a successful node configuration for symmetric load balancing on a port channel, the configured load balancing method in the label shows sporadically for some devices.
CSCvd61295	OpenFlow ports are in admin down state in the switch when the NDB restarts.
CSCuy81389	Cisco Nexus 9000 devices do not have an error pop up message for the connection installation of VLAN + Layer 3 filters.
CSCvc27514	Connection source ports are not listed on the Open Flow device.
CSCvc41941	Node Id of the device group is not updated after upgrading from NDB release 3.X to 3.2 and above.
CSCvc87978	Upgrading to Cisco Nexus Data Broker 3.2 with an Cisco Nexus 9000 NX-API switch needs the IPv6 hardware CLI command on the switch.
CSCve63563	When Custom Configuration Import operation is under progress, user should use NDB in View only mode till the import operation is completed.
CSCvh04723	Unable to remove MAC ACE using sequence number in Cisco NXOS I7(2) release.

Resolved Caveats

This section lists the resolved caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Resolved Caveats in the 3.3 Release

Bug ID	Description
CSCve06636	NDB 3.2 does not discover ISL if single LLDP neigh on Cisco Nexus 9000 Series switch.

Known Caveats

This section lists the known caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Known Caveats in the 3.3 Release

Bug ID	Description
CSCve58719	Module Serial number instead of Switch serial number in OF statistics.
CSCve57428	Unable to attach VLAN access list entry to the interface in NXOS Release 7.0(3)I6.1.
CSCve44700	Flows are not installing in switch with simple IPv6 match criteria.
CSCvd89813	NXAPI w/TACACS authentication failing.
CSCvd87975	Reconnecting the switch with NXOS I5.2 from NDB periodically.
CSCve60078	Device in NDB becomes suddenly disconnected - nginx_f crash.
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.

Related Documentation

The Cisco Nexus Data Broker documentation can be accessed from the following websites:

Nexus Data Broker Datasheet http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/nexus-data-broker/data_sheet_c78-729452.html?cachemode=refresh

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

The documentation includes installation information and release notes.

Table 3 Installation Documentation

Document	Description
<i>Cisco Nexus Data Broker Embedded Deployment Guide</i>	Describes the deployment Nexus Data Broker on NxOS devices either as a separate NDB virtual service or as an application along with GuestShell+ virtual service
<i>Cisco Nexus Data Broker Centralized Deployment Guide</i>	Describes the deployment of Nexus Data Broker in a Linux VM that be used to manage multiple NxOS device for SPAN configuration

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.

© 2017 Cisco Systems, Inc. All rights reserved.