Cisco Nexus Data Broker Release Notes, Release 3.2

This document describes the features, system requirements, limitations, and caveats in the Cisco Nexus Data Broker Release 3.2.

Online History Change

Date	Description
December 14, 2016	Created the release notes for Cisco Nexus Data Broker Release 3.2
January 9, 2017	Specified that Cisco Nexus Data Broker will be supported on NX-OS Release 7.0(3)I4(1) and earlier
January 24, 2017	Added CSCvc87973, CSCvc87978, and CSCvc87992 to *Open Caveats*
February 3, 2017	Added to *Usage Guidelines*: unsupported features in embedded mode deployment, the supported Cisco APIC versions and a CLI command that should be configured for all inter-switch ports.

Table of Contents

Introduction

Visibility into application traffic has traditionally been important for infrastructure operations to maintain security, troubleshooting, and compliance, and to perform resource planning. 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.

Features

Cisco Nexus Data Broker 3.2 provides the features from the previous Cisco Nexus Data Broker releases listed below. For a list of newly added features specific to this release, see *New Features*:

- Support for entry of a VLAN range when creating a filter.
- Ability to clone filters and connections.
- Configure multiple ports for Edge span and Edge tap.
- Ability to assign multiple filters to a connection.
- Ability to configure both allow and deny filters for the same connection.
- Enable time stamp tagging using PTP on Cisco Nexus 3500 Series switches.
- Display flow and port statistics for devices in the Cisco Nexus Data Broker main user interface.
- Display flow statistics per connection and for each device within the connection.
- Inter-switch link (ISL) utilization information available in the topology diagram and in the connection path.
- Enable packet truncation on input ports on Cisco Nexus 3500 Series switches.
- Scalable topology for Test Access Point (TAP) and Switched Port Analyzer (SPAN) port aggregation.
  - Support for Cisco Nexus 3000 Series switches
  - Cisco Nexus 3100 Series switches
  - Cisco Nexus 3200 Series switches
  - Cisco Nexus 3500 Series switches
  - Cisco Nexus 9000 Series switches
- QinQ to tag input source TAP and SPAN ports.

- Symmetric load balancing.
- Support for MPLS tag stripping.
- Connections matching monitoring traffic based on Layer 1 through Layer 4 information.
- Support for Layer 7 filtering for HTTP traffic.
- The ability to replicate and forward traffic to multiple monitoring tools.
- Reaction to changes in the TAP/SPAN aggregation network.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory (AD) using RADIUS or TACACS for authentication, authorization, and accounting (AAA).
- End-to-end path visibility, including both port and flow level statistics for troubleshooting.
- Robust Representational State Transfer (REST) API and a web-based GUI for all functions.
- Support for Cisco Plug-in for OpenFlow, version 1.0.
- Device addition using Device name.
- Inline monitoring and redirection for security use cases.
- Limit Local Authentication Fallback.

The following features require NX-OS 7.0(3)|4(1) or later:

- Configure matching on HTTP methods and redirect traffic based on that with NX-API.
- MPLS tag striping on the following:
  - Cisco Nexus 3100 Series switches
  - Cisco Nexus 3200 Series switches
  - Cisco Nexus 9000 Series switches
- OpenFlow mode of support for Cisco Nexus 9300 Series switches
- Q-in-Q on the following:
  - Cisco Nexus 3000 Series switches
  - Cisco Nexus 3100 Series switches
  - Cisco Nexus 3200 Series switches
  - Cisco Nexus 9000 Series switches

Cisco Nexus Data Broker enables you to:

- Classify SPAN and TAP ports.
- Add monitoring devices to capture network traffic.
- Filter which traffic should be monitored.
- Redirect packets from a single or multiple SPAN or TAP ports to multiple monitoring devices through delivery ports.

- Restrict which users can view and modify the monitoring system.

Supported NX-OS Versions

NX-OS Releases supported in OpenFlow mode:

- 6.0(2)U6(X) and later on the following:
  - Cisco Nexus 3000 Series switches
  - Cisco Nexus 3100 Series switches
- 6.0(2)A6(5a) and later on the following:
  - Cisco Nexus 3500 Series switches
- 7.0(3)I4(1) and later on Cisco Nexus 9000 Series switches
- 7.0(3)I4(1) and later on the following:
  - Cisco Nexus 3200 Series switches
  - Cisco Nexus 9300 Series switches
- 7.0(3)I5(1) and later on Cisco Nexus 9200 Series switches
- 7.0(3)I5(1) and later on Cisco Nexus 9300-EX Series switches

NX-OS Versions supported in NX-API mode:

- 7.0(3)I4(1) and later on the following:
  - Cisco Nexus 9000 Series switches
  - Cisco Nexus 3200 Series switches
  - Cisco Nexus 3100 Series switches
  - Cisco Nexus 9300 Series switches
  - Cisco Nexus 9500 Series switches
- 7.0(3)I5(1) and later on the following:
  - Cisco Nexus 9200 Series switches
  - Cisco Nexus 9300-EX Series switches

New Features

Cisco Nexus Data Broker 3.2 contains the following new features:

- One-time setup required for Cisco Nexus Data Broker embedded by running a python script
- Cisco Nexus Data Broker as a service

- Cisco Nexus Data Broker configuration: Auto save
- Cisco Nexus Data Broker Resiliency: Auto restart
- IPv6 Support for filtering based on IPv6 address, protocol and ports when using Nexus Data Broker in NX-API mode
- Administration GUI page to periodically Backup and Restore Cisco Nexus Data Broker configuration
- Port definition page alignments
- Port Groups for TAP/SPAN ports
- Flexibility to clone from only one point for Inline redirection
- New Device type - Production switch (PS)
- Configure SPAN destination and session in Production Nexus 3000 series or Nexus 9000 series Switches (NX-API enabled)

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

This section includes the following topics:

- Resolved Bugs in this Release
- Open Bugs for this Release

Resolved Bugs in this Release

Table 1 lists the descriptions of resolved caveats in Cisco Nexus Data Broker Release 3.2. You can use the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 1 Resolved Bugs in Cisco Nexus Data Broker Release 3.2

Bug ID	Description
CSCux36587	Unable to connect to the Cisco Nexus Data Broker web GUI after terminating the JAVA process.
CSCuz38047	In NX-API mode of operation, Nexus Data Broker NX-API Device fails to reconnect after switch hostname is changed.
CSCuz38506	Transport layer security (TLS) with OpenFlow does not work with Cisco Nexus Data Broker.

CSCva22812	When Cisco Nexus Data Broker is in NX-API mode with Cisco Nexus 3172 switches and the device /var becomes full due to access.log, responses to NX-API requests fail and the Cisco Nexus Data Broker configuration is overwritten with a blank configuration when Save is chosen.
CSCva77683	Version check fails even with the upgraded version of Java.
CSCvb24185	Setting the port description for a Cisco Nexus 3548 switch running 6.0(2)A6(5a) displays “Error: Error in setting port description” and the port configures everything other than the port description.
CSCuz66487	A connection with a UDP filter cannot be installed when the source/dest port has a 5 digit value.

Open Bugs for this Release

Table 2 lists the descriptions of open bugs in Cisco Nexus Data Broker Release 3.2. You can use the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 2 Open Bugs in Cisco Nexus Data Broker Release 3.2

Bug ID	Description
CSCuu41674	Removing an existing connection fails and a pop-up window appears to inform the user about connection inconsistency and request the user to fix the problem through the Troubleshooting tab. After fixing the connection through the Troubleshooting tab, the connection status is displayed in green, and the connection is not removed from NDB and the device. This issue occurs occasionally only if NX-API device connection is lost at the exact time that the connection is being removed.
CSCuy81389	Cisco Nexus 9000 devices do not have an error pop up message for the connection installation of VLAN + Layer 3 filters.
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.
CSCvc27514	Ports are not listed when the connection on an OpenFlow device does not have a selected source port.
CSCvc41941	Device group node Ids are not updated after upgrading from 3.X to 3.2.
CSCvc46460	EPG Names in APIC SPAN sessions do not handle populated options with special characters.
CSCvc87973	The IPv6 hardware command should be configure in Cisco Nexus 9000 switches.
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.
CSCvc87992	Connections are not matched with the VLAN ID of source ports on ISL links with an IPv6 filter.
CSCvh04723	Unable to remove MAC ACE using sequence number in Cisco NXOS I7(2) release.

Usage Guidelines

This section lists the usage guidelines for the Cisco Nexus Data Broker.

- APIC version to be supported is 1.1 and 1.2 series
- The spanning-tree bpdufilter enable command should be configured for all inter-switch ports for all platform series.
- Cisco Nexus Data Broker Embedded will be supported on NX-OS Release 7.0(3)I4(1) and earlier.
- The following features will not be supported in embedded mode deployment of Cisco Nexus Data Broker
  - Adding SPAN session
  - Adding copy device
  - Adding copy sessions
  - Scheduling Configuration Backup
  - Backing Up or Restoring the Configuration
- HTTP access on port 8080 is disabled by default. Only HTTPS access on port 8443 is enabled. If required, HTTP can be enabled by editing the tomcat.xml file. Please refer to *Cisco Nexus Data Broker Configuration Guide, Release 3.2* for details.
- 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.
- It is required to use JRE version 1.8.0_45 for latest security fixes.
- Cisco Nexus 9000 switches managed by Cisco Nexus Data Broker 3.2 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.
- Before upgrading Cisco NDB, ensure that the domain name is not configured in the switch. If the domain name is configured, remove the domain name using the no ip domain-name *domain_name_string* command and save the configuration.
- The switch description should not start with a number and the only special characters allowed are an underscore (_) or a hyphen (-). If the switch descriptions start with a number or if it contains special characters that are not allowed, change the description and synchronize the changes to NDB.
- Before upgrading Cisco NDB, do not change the switch configuration on the port description. Change in switch configuration can result in failure during NDB version upgrade or downgrade.
- For Cisco NX-API devices, there is a 2 minute or more wait after the Cisco Nexus Data Broker configuration operations (port definitions, connections creation/deletion, and stats) to reload the device and avoid any inconsistency between the Cisco Nexus Data Broker and the device.
- 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

Limitations

- The same Cisco Nexus Data Broker instance can support either the OpenFlow or NX-API configuration mode, but it does not support both configuration modes.

Device Support Matrix

Table 4 lists the supported Cisco Nexus Data Broker software for the various Cisco Nexus switches.

Table 3 Cisco Nexus Data Broker Application Device Support Matrix

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 platform	Cisco Nexus Data Broker 3.0 or later	Centralized and Embedded	Tap/SPAN aggregation 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 Note: Cisco Nexus 9200 Series switches support only one switch deployment.	Tap/SPAN aggregation only
Cisco Nexus 9300-EX switch	Cisco Nexus Data Broker 3.1 or later	Centralized and Embedded	Tap/SPAN aggregation only

Scale Information

Table 4 lists the scale limits for Cisco Nexus Data Broker.

Table 4 Scale Limits

Description	Small	Medium	Large

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

System Requirements

Table 5 lists the system requirements for Cisco Nexus Data Broker 3.2.

Table 5 System Requirements per Deployment Size

Description	Small	Medium	Large
CPUs (virtual or physical)	6-core	12-core	18-core
Memory	8 GB RAM	16 GB RAM	32 GB RAM
Hard disk	Minimum of 40 GB of free space available on the partition on which the Cisco Nexus Data Broker software is installed.		
Operating system	A recent 64-bit Linux distribution that supports Java, preferably Ubuntu, Fedora, or Red Hat.		
Other	Java Virtual Machine 1.8 or later.		

Supported Web Browsers

The following web browsers are supported for Cisco Nexus Data Broker 3.2:

- Firefox 45.x and later
- Chrome 45.x and later

Note: Javascript 1.5 or a later version must be enabled in your browser.

Upgrading to Release 3.2

This section explains the supported method for upgrading your release.

From	Supported Method
3.0 or later	Direct upgrade is supported
Earlier than 3.0	Perform the following procedure: 1. Upgrade to 3.0 2. Upgrade to 3.2

Related Documentation

For more information, see the related documents at the following link:

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

New Documentation

There are no new documents for this release.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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.