Cisco Nexus Data Broker Release Notes, Release 2.1

This document describes the features, system requirements, limitations, and caveats in the Cisco Nexus Data Broker Release 2.1.

Online History Change

Date	Description
June 17 2015	Created the release notes for Cisco Nexus Data Broker Release 2.1
October 19, 2015	Added supported NXOS versions.

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 2.1 provides the following:

- Support for entry of a VLAN range when creating a filter.
- Ability to clone filters and rules.
- Ability to assign multiple filters to a rule.
- Ability to configure both allow and deny filters for the same rule.
- 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 rule and per device per rule.
- Inter-switch link (ISL) utilization information available in the topology diagram and in the rule path.
- Enable packet truncation on input ports on Cisco Nexus 3500 Series switches.
- Support for Cisco Nexus 3500 series switches.
- Embedded application support for Cisco Nexus 3500 Series switches
- Scalable topology for Test Access Point (TAP) and Switched Port Analyzer (SPAN) port aggregation.
- Support for Q-in-Q to tag input source TAP and SPAN ports.
- Symmetric load balancing.
- Rules for matching monitoring traffic based on Layer 1 through Layer 4 information.
- The ability to replicate and forward traffic to multiple monitoring tools.
- Time stamp tagging using Precision Time Protocol (PTP).

- 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 and Cisco One Platform Kit (onePK), version 1.3.0.
- Embedded application support for Cisco Nexus 3000 and 3100 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.
- Connect to Cisco onePK agents for which Cisco onePK devices have been configured.
- Configure these additional features, depending on the type of switch:
  - Set VLAN ID on Cisco Nexus 3000 and 3100 Series switches.
  - Enable symmetric load balancing on Cisco Nexus 3000 Series switches.
  - Enable Q-in-Q on Cisco Nexus 3000 and 3100 Series switches.

Supported NXOS Versions

- All 6.0(2)XX(X) Cisco Nexus 3000 NXOS versions are supported in OpenFlow mode.
- 7.0(3)|1(2) is supported in NXAPI mode.

New Features

Cisco Nexus Data Broker 2.1 provides the following new features:

- Cisco Nexus 9300 and Cisco Nexus 9500 platform support with the NX-OS 7.0(3)I1(2) release.
- Informational messages are displayed when users set up any-to-multipoint connections.
- Topologies display the number of connections and connection names that a particular monitoring device is a part of.
- When starting the Nexus Data Broker process, if the Java version is lower than 1.8.0_45, a warning message is displayed.

Usage Guidelines

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

- 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 2.1* 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 recommended to use JRE version 1.8.0_45 for latest security fixes.
- Nexus 9000 switches managed by Cisco Nexus Data Broker 2.1 must have LLDP features enabled. Disabling LLDP may cause inconsistencies and require devices to be deleted and re-added.
- When removing devices from the Nexus Data Broker, the device associated port definitions and connections should be removed first. Otherwise, the device might contain stale configurations created by the Nexus Data Broker.
- For Cisco NX-API devices, there is a 2 minute or more wait after the Nexus Data Broker configuration operations (port definitions, connections creation/deletion, and stats) to reload the device and avoid any inconsistency between the 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 Nexus Data Broker instance can support either the OpenFlow or NX-API configuration mode, but not both.
- Nexus 9000 devices do not support VLAN ID for Edge-SPAN and Edge-TAP interfaces.

Scale Information

Table 1 lists the scale limits for Cisco Nexus Data Broker.

Table 1 Scale Limits

Description	Small	Medium	Large
Number of devices	100	300	500
Number of slices	25	100	200
Number of proactive flows	10,000	50,000	100,000

System Requirements

Table 2 lists the system requirements for Cisco Nexus Data Broker 2.1.

Table 2 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	24 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 2.1:

- Firefox 18.x and later
- Chrome 24.x and later

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

Upgrading to Release 2.1

This section explains the supported method for upgrading your release.

From	Supported Method
2.0 or later	Direct upgrade is supported
Earlier than 2.0	Perform the following procedure: 1. Upgrade to 2.0 2. Upgrade to 2.1

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 3 lists the descriptions of resolved caveats in Cisco Nexus Data Broker Release 2.1. You can use the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 3 Resolved Bugs in Cisco Nexus Data Broker Release 2.1

Bug ID	Description
CSCuu52437	In Add Filter Pop up, when a user enters input in the Source IP and Destination IP address fields in the format of IP address/mask and installs the connection, the connection is installed in the device with the address and a subnet mask of /32 in the device.

Open Bugs for this Release

Table 4 lists the descriptions of open bugs in Cisco Nexus Data Broker Release 2.1. You can use the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 4 Open Bugs in Cisco Nexus Data Broker Release 2.1

Bug ID	Description
CSCuu41674	When a user tries to remove a connection, the attempt will fail. A pop-up window will appear to inform the user about connection inconsistency and tell the user to fix the problem through the Troubleshooting tab. After fixing the connection through the Troubleshooting tab, the connection status is green, and the connection is not removed from the NX-API plugin or from the device. The user will still see connection statistics reported for the connection.
CSCuu73817	Sometimes NX-API connection is reset periodically between the Nexus Data Broker and Nexus 9000 switches. Nexus Data Broker automatically reconnects within few seconds.
CSCuu87271	In a topology with two Nexus 9000 switches interconnected with only a single link, and these two switches are not connected to any other neighbors, Nexus Data Broker does not display the topology link because NX-API provides the LLDP neighbor output in a different format. This issue does not impact Nexus 3xxx series switches in OpenFlow mode.

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

This section lists the new Cisco APIC product documents for this release.

- *Cisco Nexus Data Broker Configuration Guide, Release 2.1*

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.