Cisco Nexus Dashboard Release Notes, Release 2.0.2

Contents

Cisco Nexus Dashboard is the next generation of the Application Services Engine and provides a common platform for deploying Cisco Data Center applications. These applications provide real time analytics, visibility, and assurance for policy and infrastructure.

This document describes the features, issues, and limitations for the Cisco Nexus Dashboard software.

For more information, see the “Related Content” section of this document.

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
August 1, 2022	Updated the recommended CIMC version.
March 15, 2021	Additional open issue CSCwb18594.
December 14, 2021	Additional open issue CSCwa47299.
September 30, 2021	Additional open issue CSCvz54281.
September 9, 2021	Open issue CSCvx86223 previously listed for both 2.0.2g and 2.0.2h was resolved prior to the 2.0.2g release, so it’d been removed from this document.
August 25, 2021	Open issues CSCvw78716 and CSCvy31733 previously listed for both 2.0.2g and 2.0.2h releases are resolved in 2.0.2h release.
July 28, 2021	Additional known issue CSCvy62110.
June 9, 2021	Additional open issue CSCvx65764.
May 31, 2021	Release 2.0.2h became available.
April 27, 2021	Release 2.0.2g became available.

New Software Features

This release adds the following new features:

Feature	Description
Persistent IP addresses for application services	You can now provide persistent IP addresses for applications that require to retain the same IP addresses even in case it is relocated to a different Nexus Dashboard node. Nexus Insights requires some services such as software telemetry and hardware telemetry collectors to have persistent IP. This feature is supported for Nexus Insights, Release 5.1 with DCNM fabrics only. For more information, see Cisco Nexus Dashboard User Guide.
Support for virtual (VMware ESX) and cloud (AWS and Azure) cluster form factors	Starting with Release 2.0.2h, you can deploy Nexus Dashboard in VMware ESX, Amazon Web Services (AWS), or Microsoft Azure.

Feature	Description
	For more information, see Cisco Nexus Dashboard Deployment Guide.

Changes in Behavior

If you are installing or upgrading to this release, you must consider the following:

- When upgrading to Release 2.0.2, you must disable any applications installed in your cluster before the upgrade and re-enable them after the upgrade completes successfully.
- If you are running Nexus Insights application, you must delete the application before upgrading to Nexus Dashboard, Release 2.0.2 and then install Nexus Insights, Release 5.1 after the Nexus Dashboard upgrade is complete.

  Note that uninstalling the application will delete any collected application data, such as software and hardware telemetry.
- After upgrading to Release 2.0.2, we recommend upgrading all the applications to their latest versions.
- If you are deploying Multi-Site Orchestrator, Nexus Insights, and Network Assurance Engine in the same cluster, you must ensure that Nexus Insights and Network Assurance Engine are installed and enabled first before enabling the Multi-Site Orchestrator application.
- If you are running Multi-Site Orchestrator and Nexus Insights in your cluster and you want to install or upgrade Network Assurance Engine application, you must follow the following order of steps:
  - Disable Multi-Site Orchestrator application.
  - Disable Network Assurance Engine application if already installed.
  - Install or upgrade Network Assurance Engine application.
  - Enable Network Assurance Engine application.
  - Re-enable Multi-Site Orchestrator application.

  If you are not running Nexus Insights in your cluster, you can install Network Assurance Engine normally.
- Downgrading from Release 2.0.2 is not supported.

Open Issues

This section lists the open issues. Click the bug ID to access the Bug Search Tool and see additional information about the issue. The " Exists In" column of the table specifies the releases in which the issue exists.

Bug ID	Description	Exists in
CSCvy09409	Internal database system experienced out of memory. Streaming data will not be retrieved or saved after and during the time internal database component recovers completely and becomes stable.	2.0.2g
CSCvw78716	After importing configuration, REST API calls from DeviceConnector are failing with auth errors.	2.0.2g

Bug ID	Description	Exists in
CSCvy31733	Sites will shown in down status. This can happen for all the sites are imported.	2.0.2g
CSCvt78295	API shows active status for all the nodes, even though one node is down.	2.0.2g and later
CSCvu21304	Intersight device connector connects to the Intersight over the Cisco Application Services Engine Out-Of-Band Management.	2.0.2g and later
CSCvw39822	After a power cycle, system lvm initialization may fail due to disk latency.	2.0.2g and later
CSCvw57953	When the system is being recovered with a clean reboot of all nodes, the admin login password will be reset to the day0 password that is entered during the bootstrap of the cluster.	2.0.2g and later
CSCvv71205	Docker registry is not cleaned up after deletion of apps.	2.0.2g and later
CSCvw63887	On upgrade of NAE with a larger profile, the NAE elastic search pods do not reflect the right profile values for memory and CPU.	2.0.2g and later
CSCvw78729	Register link is greyed out for worker nodes and user is not able to register from UI.	2.0.2g and later
CSCvw83241	Firmware activation fails with atomix-active failure as the error in the UI.	2.0.2g and later
CSCvx89368	After ND upgrade, there will be still pods belonging to the older version running on the cluster. For example, in this case upgrade was from 2.0.1.27 to 2.0.1.36. After the upgrade, running following command gives: node1# kubectl get pods -n kube-system -o yaml | grep image: | grep 2.0.1.27 image: infra/ui:nd-2.0.1.27-e881b96b5 image: infra/ui:nd-2.0.1.27-e881b96b5 image: infra/ui:nd-2.0.1.27-e881b96b5 image: infra/ui:nd-2.0.1.27-e881b96b5 image: infra/ui:nd-2.0.1.27-e881b96b5 image: infra/ui:nd-2.0.1.27-e881b96b5 node1# acs version Nexus Dashboard 2.0.1.36 Clearly the ND nodes have completed upgrade, but some services are showing older version.	2.0.2g and later
CSCvy19785	On KVM form factor if the first master is clean rebooted, the node will not recover as the certificates on the virtual device are not re-generated.	2.0.2g and later
CSCvx93124	You may see the following message: [2021-04-13 13:48:20,170] ERROR Error while appending records to stats-6 in dir /data/services/kafka/data/0 (kafka.server.LogDirFailureChannel) java.io.IOException: No space left on device	2.0.2g and later
CSCvx65764	On second and third node OVA deployment, selecting " Download config from peers" does not grey out the cluster configuration fields. You do not need to fill out these fields and even if filled out, they will be ignored.	2.0.2g and later

Bug ID	Description	Exists in
CSCvz54281	All pods on node1 down. Node went into not-ready state, due to kubelet stopped pasting node status.	2.0.2g and later
CSCwa47299	This bug has been filed to evaluate the product against the following vulnerability in the Apache Log4j Java library disclosed on December 9, 2021 CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. Cisco is currently investigating impact. For more information, see Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021.	2.0.2g and later
CSCwb18594	When trying to add a site into Nexus Dashboard, if the password has an '&' the addition of the site fails and stays in an uknown state. With the following error message: " Site not available, Verify input:Response error:401 Unauthorized {\" totalCount\" :\" 1\" ,\" imdata\" :[{\" error\" :{\" attributes\" :{\" code\" :\" 401\" ,\" text\" :\" User credential is incorrect - FAILED local authentication\" }}}]}"	2.0.2g and later

Resolved Issues

This section lists the resolved issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The " Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvv61564	Accepting the user agreement does not start the app download.	2.0.2g
CSCvw67144	CX telemetry data for sites added via APIC out of band management IP is not supported.	2.0.2g
CSCvy04829	Unable to install a different version of the app on ND platform after upgrade.	2.0.2h
CSCvy12504	Kafka pod restarts a few times under heavy IO load. This may lead to a few pods that depends on healthy kafka to restart as well.	2.0.2h
CSCvy14081	The site manager and event manager pods are in a continuous crash. The logs will show a panic message that says " an inserted document is too large" . This indicates that there are too many audit objects in the database.	2.0.2h
CSCvy09409	Internal database system experienced out of memory. Streaming data will not be retrieved or saved after and during the time internal database component recovers completely and becomes stable.	2.0.2h
CSCvw78716	After importing configuration, REST API calls from DeviceConnector are failing with auth errors.	2.0.2h

Known Issues

This section lists known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the issue.

Bug ID	Description
CSCvw52468	When you upgrade the cluster from 1.1.3d to 2.0.1b, the proxy details configured in the DeviceConnector are overwritten by the proxy configuration present in Cluster Configuration. If there is no proxy configuration set in cluster config policy, the previously set proxy details were overwritten and unset.
CSCvw70476	When bringing up ND cluster for the first time, all three master nodes need to join Kafka cluster before any master node can be rebooted. Failing to do so, 2 node cluster does not become healthy as Kafka cluster requires 3 nodes to be in the cluster at once.
CSCvy62110	For Nexus Dashboard nodes connected to Catalyst switches packets are tagged with vlan0 even though no VLAN is specified. This causes no reachability over the data network. In this case, 'switchport voice vlan dot1p' command must be added to the switch interfaces where the nodes are connected.

Compatibility

For Cisco Nexus Dashboard applications compatibility information, see the Cisco Data Center Networking Applications Compatibility Matrix.

For Cisco Nexus Dashboard cluster sizing guidelines, see the Nexus Dashboard Cluster Sizing tool.

Physical Nexus Dashboard nodes must be running a supported version of Cisco Integrated Management Controller (CIMC).
CIMC, Release 4.2(2a) is the recommended version; CIMC, Release 4.0(1a) is the minimum supported version.

Related Content

Document	Description
Cisco Nexus Dashboard Release Notes	This document. Provides release information for the Cisco Nexus Dashboard product.
Cisco Nexus Dashboard Hardware Setup Guide	Provides information on physical server specifications and installation.
Cisco Nexus Dashboard Deployment Guide	Provides information on Cisco Nexus Dashboard software deployment.
Cisco Nexus Dashboard User Guide	Describes how to use Cisco Nexus Dashboard.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to ciscodcnapps-docfeedback@cisco.com. We appreciate your feedback.

Legal Information