Cisco Nexus Dashboard Release Notes, Release 2.0.1

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
March 15, 2021	Additional open issue CSCwb18594.
December 14, 2021	Additional open issue CSCwa47299.
July 28, 2021	Additional known issue CSCvy62110.
January 29, 2021	Release 2.0.1d became available.
December 22, 2020	Release 2.0.1b became available.

New Software Features

This release adds the following new features:

Feature	Description
GUI-based cluster deployment	Initial cluster configuration and deployment have been simplified using an intuitive GUI-based bootstrap process.
Common site management	You can now on-board Cisco ACI fabrics using the Nexus Dashboard UI and use these sites for all the applications running inside your cluster without the need for each application to manage the sites separately.
Common user management	You can now manage all users (local or remote) directly in the Nexus Dashboard without the need for each application to manage the users separately.
Single Sign-On (SSO)	Single sign-on allows you to configure user authentication and autherization once on a remote authentication server such as LDAP and then use the same users across all Nexus Dashboard applications and fabrics without having to log in every time you switch between them. This provides a seamless user experience across all operational services.
Separate admin and user dashboard views	Separate administrator and user dashboard views provide customizable, role-based access to the Nexus Dashboard UI and allow each user to focus on their specific operations and use cases by limiting overall access to the entire system.
Co-hosting of applications	You can now co-host multiple applications within the same Nexus Dashboard cluster.
Stanby master nodes	You can now configure and add standby master nodes to your Nexus Dashboard cluster to enable fast and easy failover in case of a primary master node failure.

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
CSCvw86325	This is socket leak in docker daemon hence it's possible that over the period of time docker gets to socket limit and kubelet fails to communicate with docker at all. In specific situation, impacted node will be moved to ?not-ready? state and will not recover automatically. As the node is marked as not-ready, usual pod eviction will be triggered. UI will show node status into error as well set of services into failed state.	2.0.1b
CSCvw96543	acs techsupport collect -> this command collects a tgz file under /techsupport directory. On inspecting the contents of this tgz, it will be missing logs.tgz and app_logs.tgz. This happens only for techsupport collected using acs command and not for the policy ts collected through UI.	2.0.1b
CSCvx02338	Device connector configuration on ND will fail if it is configured with a proxy that uses a username and password.	2.0.1b
CSCvx10853	Failed to download the application or firmware image.	2.0.1b
CSCvx07705	Post upgrade apigwmgr service restarts repeatedly	2.0.1b
CSCvx09316	App Store cannot establish connection ton DC Appcenter to download or check for updates.	2.0.1d
CSCvt78295	API shows active status for all the nodes, even though one node is down.	2.0.1b and later
CSCvu18725	DNS search domains are not updated until the Cisco Application Service Engine nodes are rebooted.	2.0.1b and later
CSCvu21304	Intersight device connector connects to the intersight over the Cisco Application Services Engine Out-Of-Band Management.	2.0.1b and later
CSCvw39822	After a power cycle, system lvm initialization may fail due to disk latency.	2.0.1b 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.	2.0.1b and later
CSCvv61564	Accepting the user agreement does not start the app download.	2.0.1b and later
CSCvv71205	Docker registry is not cleaned up after deletion of apps.	2.0.1b and later
CSCvw54286	401 error on Resource Utilization page for Internet Explorer browsers.	2.0.1b 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.	2.0.1b and later

Bug ID	Description	Exists in
CSCvw67144	CX telemetry data for sites added via APIC out of band management IP is not supported.	2.0.1b and later
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 doesn't become healthy as Kafka cluster requires 3 nodes to be in the cluster at once.	2.0.1b and later
CSCvw78716	After importing configuration, REST API calls from DeviceConnector are failing with auth errors.	2.0.1b and later
CSCvw78729	Register link is greyed out for worker nodes and user is not able to register from UI.	2.0.1b and later
CSCvw83241	Firmware activation fails with atomix-active failure as the error in the UI.	2.0.1b and later
CSCvw52468	When you upgrade the cluster from 1.1.3d to 2.0.1bb, 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.	2.0.1b 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.	2.0.1b 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\" }}}]}"	2.0.1b 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
CSCvu25186	After Cisco Application Services Engine session timeout, the app page shows " Authorization field missing" error upon refreshing the page.	2.0.1b
CSCvu13175	Upgrade GUI shows error when nodes are upgrading and upgrade status is not visible.	2.0.1b
CSCvt72554	Audit logs are not generated for Cisco Application Services Engine upgrade or downgrade.	2.0.1b
CSCvu28529	IP address of the NTP server is required during the first-boot setup.	2.0.1b
CSCvu81594	Intersight DeviceConnector in Cisco ASE 1.1.3 allows read-only user to view and configure its settings.	2.0.1b

Bug ID	Description	Fixed in
CSCvu86665	In certain conditions, pods are running ready but this is not reported at service level. This creates two issues: 1) Breaks the health check where we expect all the instances of a service running and ready and can eventually lead to upgrade failure. 2) As one of the endpoint is missing from service, it impacts API load balancing across all endpoints for a given service.	2.0.1b
CSCvq72219	NTP, DNS, Firmware, DC proxy over inband management is not supported.	2.0.1b
CSCvv75573	In Application Services Engine 1.1.3, upgrade fails with workers trying to upgrade before all primary nodes are upgraded.	2.0.1b
CSCvw86325	This is socket leak in docker daemon hence it's possible that over the period of time docker gets to socket limit and kubelet fails to communicate with docker at all. In specific situation, impacted node will be moved to ?not-ready? state and will not recover automatically. As the node is marked as not-ready, usual pod eviction will be triggered. UI will show node status into error as well set of services into failed state.	2.0.1d
CSCvw96543	acs techsupport collect -> this command collects a tgz file under /techsupport directory. On inspecting the contents of this tgz, it will be missing logs.tgz and app_logs.tgz. This happens only for techsupport collected using acs command and not for the policy ts collected through UI.	2.0.1d
CSCvx02338	Device connector configuration on ND will fail if it is configured with a proxy that uses a username and password.	2.0.1d
CSCvx10853	Failed to download the application or firmware image.	2.0.1d
CSCvx09316	App Store cannot establish connection ton DC Appcenter to download or check for updates.	2.0.1d
CSCvx07705	Post upgrade apigwmgr service restarts repeatedly	2.0.1d

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 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.

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