CISCO

Cisco Nexus Insights Release Notes, Release 5.0.1 – For Cisco DCNM

Contents

Cisco Nexus Insights (NI) application consist of a pair of monitoring utilities that can be added to the Cisco Data Center Network Manager (DCNM).

This document describes the features, issues, and limitations for Cisco NI app on the Cisco DCNM.

For more information, see Related Content

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
January 29, 2021	Added switch freeform limitation to the section, Usage Guidelines and Limitations.
January 8, 2021	Updated Flow Telemetry support for Cisco Nexus 9300-GX platform.
December 22, 2020	Release 5.0(1) became available.

New Software Features

Feature	Description
Multi-Site	Monitor multiple sites with single instance of Cisco Nexus Insights.
UI enhancements	Improved design with a streamlined tabbed layout, enhanced options for selecting a time range, centralized summary of sites with All Sites Dashboard, detect and indicate when features are not supported by a node.
Cisco NI app unification	Integrating Cisco NIR and Cisco NIA apps into Cisco NI app to get anomalies, advisories, and functionalities such as scheduling log collection jobs, scheduling bug scan and compliance jobs, connectivity analysis jobs, firmware upgrade impact and upgrade paths, recommendations for upgrade versions, and RPM updates. It also includes in-depth analysis work flows for advisories and anomalies.
Topology View	Visualize logical constructs such as Tenant, VRF, EPG and more on top of physical topology. Perform rapid troubleshooting using filters to focus on problematics nodes.
Cisco Nexus Insights Independence	Cisco NI app collects the node capabilities to determine and display the features supported and features not supported for each node on the site.
Micro-Burst detection	Expose and locate invisible microbursts. Know the congestion hot spots and protect application performance.
Flow Telemetry Events	Use flow table events to minimize troubleshooting time through automated root-cause analysis of data plane anomalies, such as routing issues, ACL drops, buffer drops and more.
Host flow overlay technologies support	Packet visibility and flow telemetry support for overlay technologies such as host flow overlay. The host flow overlay technologies include NSX-V flow monitoring.
Kafka messaging support	Share Cisco Nexus Insights enriched value-added output with application ecosystem. Build synergetic workflows with third party IT applications.

Feature	Description
Email notification support	Get offline alerts about network health using email notification facility. Pick and choose which issues you need to be alerted about.
PSIRT notification and Defect notification	Detect vulnerability exposure with PSIRT scan. Detect exposure to known defects with defect scan.
Resources	Monitor capacity utilization changes and threshold violation with resource anomalies.
Statistics	View control plane, data plane statistics, detect control plane and data plane anomalies.
AppDynamics Integration	AppDynamics provides the required metrics for monitoring, identifying, and analyzing the applications that are instrumented with AppDynamics agents. Cisco NIR provides flow analytics, statistics analytics, and topology view on these metrics to identify anomalies.
Support for Cisco Nexus 9300-GX series switches	Monitor high performance, scalable data center with support for Cisco Nexus 9300-GX series 400 GE platform switches.

Note: For Cisco NI Release 5.0(1), you must install the latest software maintenance update on Cisco DCNM Release 11.4(1). See Installing Software Maintenance Update on Cisco DCNM 11.4(1) for more information.

Open Issues

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

Bug ID	Description	Exists In
CSCvu69962	Logical fabrics may show up in Cisco Nexus Insights.	5.0(1)
CSCvu81560	Upgrade from DCNM 11.3.1 to 11.4.1.32 hangs in standby mode.	5.0(1)
CSCvu84489	Stopping a recurrent bug scan in log collection phase does not stop the job immediately.	5.0(1)
CSCvt77736	When there is no data coming from switches, topNodes API returns all nodes into the list as healthy with endpoint count as 0.	5.0(1)
CSCvv47086	Retry to push configuration does not work if flow telemetry is in enabled state but software telemetry has failed.	5.0(1)
CSCvv58470	Advisories are displayed for devices removed from the Site or Fabric.	5.0(1)
CSCvv58497	In Cisco Nexus Insights app, log collection fails on some nodes.	5.0(1)
CSCvv75635	fabricName is not mandatory in the add integrations API.	5.0(1)
CSCvv87562	Email notifications does not include compliance advisories.	5.0(1)
CSCvv89866	Endpoint data is displayed for unsupported devices.	5.0(1)
CSCvv98827	When fabric is disabled, corresponding collection from AppD is not disabled.	5.0(1)

Bug ID	Description	Exists In
CSCvw00525	Fabrics with HW flow telemetry in disabled failed is cannot be upgraded.	5.0(1)
CSCvw05118	After downgrading the switch to 7.0(3)I7(8) version from 9.3.5 or above, telemetry is only partially configured on the switch.	5.0(1)
CSCvw07745	In Cisco Nexus Insights only top 100 flows are displayed in the flow events anomaly analyze page. You are unable to view the remaining flow events.	5.0(1)
CSCvw11350	MAC duplication endpoint anomaly does not get cleared.	5.0(1)
CSCvw12315	Cisco Nexus Insights generated flow anomalies on DCNM cannot be streamed to remote Kafka broker.	5.0(1)
CSCvt66683	When a switch is removed from a fabric, flows records originating from that switch is displayed in Nexus Insights unless analytics feature configurations are removed.	5.0(1)
CSCvv75183	Flow resource type anomalies are not exported to external kafka server.	5.0(1)
CSCvv82571	FTE events show up as anomaly when the switch with large network configuration is configured for telemetry with Cisco Nexus Insights.	5.0(1)
CSCvu74237	Under scale condition, when some of the flow records are either dropped in the switch or dropped in processing, partial paths will be displayed.	5.0(1)
CSCvw12315	Cisco Nexus Insights generated flow anomalies on Cisco DCNM cannot be streamed to remote Kafka broker.	5.0(1)
CSCvv96466	EP records shows incorrect status.	5.0(1)
CSCvw52303	When NX-OS version is upgraded, FTE configurations are not be pushed even if the upgraded NX-OS version supports FTE.	5.0(1)
CSCvw82970	It takes more than 10 mins for VRF updates to be reflected in the Cisco NI app.	5.0(1)

Resolved Issues

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

Bug ID	Description	Fixed In
CSCvs28382	Flow path may not be able to display all the drops when there is continuous link flaps causing packet loss at more than one node. But the Anomalies section will capture the errors.	5.0(1)
CSCvu15103	IPv4 host route and IPv6 host route graphs show empty data in Diagnostics Report.	5.0(1)
CSCvu76228	After adding a switch to the fabric in Monitored mode, the status may not be updated to Enabling in the GUI.	5.0(1)

Bug ID	Description	Fixed In
CSCvu92352	Empty BD and EPG chart are displayed for anomalies on a node from DCNM fabric for IPv4 or IPv6 host routes and Longest Prefix Match (LPM) threshold anomalies.	5.0(1)
CSCvu89501	EP anomalies are not generated after reloading a switch.	5.0(1)
CSCvu60874	After a switch is upgraded or downgraded, configuration for unsupported switch is displayed.	5.0(1)

Known Issues

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

Bug ID	Description	Exists In
CSCvu74237	Under scale condition, when some of the flow records are either dropped in the switch or dropped in processing, partial paths will be displayed.	5.0(1)
CSCvw31279	VRF that is associated with the NSX-V flow may not be the correct VRF the NSX-V flow is taking in the fabric.	5.0(1)

Hardware Requirements

The Cisco NI application supports Cisco DCNM 11.4(1) release. It is recommended to use the latest Cisco DCNM release. It is recommended to have a native HA (DCNM primary/secondary) + 3 Compute node deployment for Cisco DCNM when you want to run Cisco NI but not mandatory.

Table 1.   Hardware Requirements for Deployments up to 80 Switches and 2000 Flows

Node	Deployment Mode	Logical CPU*	Memory	Storage	Network
Cisco DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes (x3)	OVA/ISO	32 vCPUs	64G	500G HDD	3xNIC

Table 2.   Hardware Requirements for Deployments from 81 to 350 Switches and 12000 Flows

Node	Deployment Mode	Logical CPU*	Memory	Storage	Network
Cisco DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes (SE-CL-L3 5 SE Nodes)	ISO	NA	NA	NA	NA

* A logical CPU is a Virtual CPU in a virtual hypervisor based environment and is a hyperthread in a baremetal environment.

Compatibility Information

For Cisco NI on Cisco DCNM compatibility with Day-2 Operations apps, see the [Cisco Data Center Networking Applications Compatibility Matrix](#).

Software/Hardware	Release
Minimum Cisco NXOS version required for Software Telemetry	7.0(3)I7(6), 7.0(3)I7(7), 8.4(2)
Minimum Cisco NX-OS version required for Software and Hardware Telemetry	9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 7.0(3)I7(8)
Minimum Cisco NX-OS version required for Host Flow Overlay	9.3(4), 7.0(3)I7(8)
Minimum Cisco NX-OS version required for Micro-Burst, Endpoint Analytics, and Multicast Protocols	9.3(4)
Minimum Cisco NX-OS version required for Modular Hardware Telemetry	9.3(4)
Minimum Intersight Device Connector version on Cisco DCNM	1.0.9-644
Minimum Cisco NX-OS version required for Connectivity Analysis	9.3(3)
Cisco Device supported for Host Flow Overlay	Cisco Nexus 9000 -FX, -FX2, and -GX platform switches
Cisco Devices supported for Flow Telemetry Events	Cisco Nexus 9000 -FX, -FX2, and -GX platform switches and 9700 -FX line cards
Cisco Device supported for Flow Telemetry	Cisco Nexus 9300-EX, -FX, -FX2, and -GX platform switches and 9500-EX and FX
Cisco Device supported for Software Telemetry	- Cisco Cloud Scale ASIC devices - Cisco Nexus 7000 series switches: N77-C7710 or N77XX, N7K-C7009, N7K-C7010 or 70XX - Cisco Nexus 3000 series switches: Nexus 3100-XL series, Nexus 3100-V series, Nexus 3200 series, Nexus 3400 series, Nexus 3500-XL series - Cisco Nexus 9504 and 9508 with -R and -RX lines cards: - N9K-X96136YC-R, N9K-C9508-FM-R, N9K-C9504-FM-R, N9K-X9636C-R, N9K-X9636C-RX - Cisco Nexus 3600 platform switches: N3K-C3636C-R, N3K-C36480LD-R2, N3K-C36180YC-R

Software/Hardware	Release
Cisco Device not supported for Software Telemetry	• Cisco Nexus 9300-GX platform switches • Cisco Nexus 9300-FX3, 9700-GX, and 9700-FX3 platform switches • Cisco N3K-C3408-S, N3K-C3432D-S, N3K-C34200YC-SM, N3K-34180YC, and N3K-3464C switches • Cisco N3K-C3464C, N3K-C34180YC, N3K-C3408S, N3K-C34200YC-SM, N3K-C3432D-I • Cisco N9K-C93180YC-FX3, N9K-C93108TC-FX3, N9K-C93360YC-FX3
Micro-Burst support	See Supported Platforms for details.
Arista EOS	4.21
Arista Device Supported	Arista 7050SX and 7280SR platform switches

Note: Flow Telemetry data will consume 6MB for 10K IPv4 flows per node. Flow Telemetry data will consume 12MB for 10K IPv6 flows per node.

Verified Scalability Limits

Software/Hardware	Scale Limits
Number of flows supported for Hardware Telemetry	12000
Maximum number of nodes supported in a fabric in managed mode	150
Maximum number of nodes supported across all fabrics	350

Note: For fabrics greater than 150 nodes, monitored mode is recommended.

Usage Guidelines and Limitations

This section lists the usage guidelines and limitations for Cisco NI app:

• The Cisco NI application requires that physical servers hosting Cisco DCNM computes as VMs are at least Cisco C220-M4 category. It is also required that a compute be hosted on a data store with a dedicated hard disk of atleast 500GB. See Hardware Requirements.

• The Cisco NI application installation on Cisco DCNM requires that the DNS server is valid and reachable.

• Telemetry for hardware TCAM utilization, such as forwarding TCAM and ACL TCAM are not supported on Cisco Nexus C9504, C9508, and C9516 platform switches.

- Cisco NI app does not support software telemetry and flow telemetry data from switches to the flow collector running on Cisco DCNM compute nodes over IPv6.

- Software Telemetry telemetry should be enabled before enabling Hardware Telemetry.

- Cisco NI app checks for metadata update every hour. However, there may not be an update every time.

- After metadata update you need to run manual bug scan to reflect PSIRTs.

- User initiated upload to Cisco Intersight Cloud fails if the Log Collector job completed prior to Cisco DCNM HA failover. It is recommended to start a new Log Collector job after Cisco DCNM HA failover.

- The Hardware Resources tab in System Resource Utilization Dashboard is not supported for Cisco Nexus 7000 series switches. The hardware resources do not have a direct mapping to the objects that show in Cisco NI app. The command that shows hardware details does not provide the percentage of entries used and the maximum number of entries allocated for a particular feature. The Cisco NI application does not raise the anomalies and details page for any resource in Hardware Resources tab for Cisco Nexus 7000 series switches.

- The features supported on Cisco Nexus 7000 series switches includes Environmental, Statistics, and Resources.

- The features not supported on Cisco Nexus 7000 series switches includes Endpoint Analytics, Multicast, Microburst, CDP statistics protocol, and harware resource statistics such as COPP, HRT, LPM, QoS, and ACL.

- The features supported on Cisco Nexus 3000 series switches includes Enviromental, Statistics, and Resources.

- The features not supported on Cisco Nexus 3000 series includes Endpoint Analytics, Multicast, and Microburst.

- The IGMP and IGMP Snoop multicast statistics protocols are supported only on Cisco Nexus 9000 series switches.

- The IGMP and IGMP Snoop multicast statistics protocols are not supported for the following:

  ◦ Cisco Nexus 3000 and 7000 series switches.

  ◦ Cisco N9K-X9636C-R, N9K-X9636Q-R, N9K-X96136YC-R, and N3K-C3636C-R line cards.

- Cisco NI app does not support BGP PrefixSaved statistics on the following:

  ◦ Cisco Nexus 3000, 7000, and 9000 platform switches.

  ◦ Cisco N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636Q-R, and N3K-C3636C-R line cards.

- Classic fabric type is supported for host flow overlay monitoring. VXLAN fabric type is not supported for host overlay flow monitoring.

- Cisco DCNM allows network-admin and network-operator roles to assign read or write access for fabrics. Cisco NI app displays all the fabrics even though you do not have permission to modify. Any operation on a fabric fails without read or write access to the fabric. Cisco NI app does not enforce the RBAC roles configured in Cisco DCNM, the operations that telemetry manager generates are filtered/enforced by Cisco DCNM according to the RBAC rules configured.

- In switch add cases, the software or the hardware fabric state might show the final state as Enable-failed. Under this condition the GUI might not refresh the Configuration setup page. Even though the fabric has reached a final state, the failed switch retry might be happening. In order to view the correct fabric and switch states, exit the Configuration Setup page and return back to the Setup page. Click the pending or failed switches to determine if the status has been updated from "Processing" to "Failure" or "Success" states.

- After enabling Cisco NI on a fabric and adding a group of switches together to the fabric, DCNM sends notification for the newly added switches. When NI tries to program the newly added switches, DCNM can be potentially finishing the switch discovery for these switches. In this case, the NI operation fails on the switches. The failed NI operations should be retried with retry facility in Cisco NI.

- Enabling Flow collection on NI 5.0 deployed on DCNM 11.5(1) with Cisco NX-OS version 9.3(5), results in OUT_OF_SYNC issue in DCNM. This issue is applicable to -FX2 platform switches only. To resolve this issue, perform the following steps:

  ◦ After enabling Flow collection, create a switch freeform intent from DCNM for FX2 switches with the following configuration.

  flow event telemetryFlowEvent

    group drop-events

      flow-count 500

  ◦ Remove the intent whenever Flow collection is disabled from NI to avoid fabric OUT_OF_SYNC issue observed in DCNM.

  To disable Flow collection, choose Settings > Data Management > Flows >. In the Flows Rules Configuration page, click the Flow Collection slider.

  See Enabling Freeform Configurations on Fabric Switches for more information.

- If NI 5.0 is enabled, you will not be able to enable Cisco Network Insights Base app on DCNM.

Related Content

The Cisco NI documentation can be accessed from the following website:

https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-insights/series.html

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, and release notes, as well as other documentation.

Document	Description
Cisco Nexus Insights Release Notes for Cisco DCNM	This document.
Cisco Nexus Insights User Guide for Cisco DCNM	Describes how to download, install, and set up Cisco NI app.

Documentation Feedback

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

Legal Information

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.