Telemetry and Visibility with Cisco Nexus Dashboard



© 2025 Cisco and/or its affiliates. All rights reserved.

Overview

Q. What do the telemetry capabilities of Cisco Nexus® Dashboard offer?

A. The telemetry capabilities of Cisco Nexus Dashboard provide customers the ability to pre-empt unintentional errors, monitor and analyze networks in real time to identify anomalies, and provide root-cause analysis, with issue correlation, capacity planning, and accelerated troubleshooting. Previously a part of Nexus Dashboard Insights (NDI) in versions prior to Nexus Dashboard 4.1, these capabilities are now fully integrated into the base image of Nexus Dashboard, offering a unified solution.

Key features include:

- Real-time anomaly detection and root-cause analysis
- Historical context tracking for capacity planning and troubleshooting
- Correlation of telemetry data with Cisco best practices for proactive issue resolution

Q. Does the Cisco Nexus Dashboard support telemetry for both Cisco ACI® and Cisco NX-OS–based deployments?

A. Yes, Cisco Nexus Dashboard supports telemetry for both Cisco ACI and Cisco NX-OS environments with a single software image. It serves as

- Fabric controller for NX-OS environments
- Telemetry solution for Cisco ACI deployments, where a Cisco® APIC cluster is onboarded to Nexus Dashboard through a multicluster connectivity workflow

Q. What is the difference between telemetry features for Cisco ACI and Cisco NX-OS deployments?

A. The differences are minimal and continue to diminish with each release. While some capabilities remain specific to the fabric type (Cisco ACI or Cisco NX-OS), the goal is feature parity across the two fabric types. See the Cisco Data Center Networking Subscription page for details on supported features, license tiers, and fabric types.

Q. Which platforms support software telemetry?

A. As of Nexus Dashboard 4.1, software telemetry is supported on the Cisco Nexus 9000, Nexus 7000, and Nexus 3000 support software telemetry. Please refer to the release notes for detailed platform support.

Q. Which platforms support hardware telemetry?

A. Hardware telemetry is supported on

- Cisco Nexus 9000 EX/FX/FX2/GX/FX3/GX/GX2/H1/H2 platforms
- All future platforms based on cloud scale silicon

Q. What is the data-retention period for telemetry capabilities in Cisco Nexus Dashboard?

A. The following data is retained for 7 days:

- Endpoint history
- Switch status
- L3 neighbor information
- vPC domain stats
- Flow records (Flow Telemetry and Traffic Analytics)

© 2025 Cisco and/or its affiliates. All rights reserved.

The following data is retained for 30 days:

- Anomalies and advisories (Active alerts are always shown; cleared alerts are cleared after a 30-day period.)
- Interface and operational stats
- External traffic metrics

Q. How does the capacity planning in Nexus Dashboard differ from APIC's capacity dashboard?

A. While APIC provides a capacity dashboard; the data is not historical and is not correlated. Cisco Nexus Dashboard offers resource utilization and shows the utilization, trends, and anomalies when thresholds are exceeded or a sudden change from normal behavior (that is, the rate of change) is observed.

Q. Which types of data-center network deployments support telemetry with Cisco Nexus Dashboard?

A. The telemetry capabilities of Nexus Dashboard support Cisco ACI fabrics and Cisco NX-OS fabric topologies, including Classic LAN (including enhanced classic LAN), DC-routed/VXLAN EVPN, AI fabrics (routed and VXLAN-based), and external fabric types.

Q. How do the learning models in Cisco Nexus Dashboard get updated (for example, bug signatures, software image compatibility etc.)? Are such updates automatic, or do they have to be manually updated?

A. Metadata is updated automatically when Nexus Dashboard is connected to Cisco through the built-in Cisco Intersight® device connector. There is no additional cost for claiming Nexus Dashboard on Intersight. For more details please see Working with Cisco Intersight.

Q. What are the functionalities of the telemetry correlation engine in Cisco Nexus Dashboard?

A. The correlation engine is used to dynamically correlate raw telemetry data across the network from each node to provide actionable insights.

Key capabilities include:

- Root-cause analysis across Layers 1 to 3
- End-to-end flow-path visualization, with latency and ingress/egress details
- Packet-drop analysis pinpointing the exact locations and reasons for drops

The correlation engine is one of the most important microservices in Cisco Nexus Dashboard.

Q. What kind of advisories does Nexus Dashboard generate?

A. Nexus Dashboard generates advisories based on:

- Field notices, EOL/EOS updates, PSIRTs, and known bugs
- Correlation with enabled features, hardware, and software in the network.
- Recommendations for fixes, such as software upgrades, with details on disruptive vs. nondisruptive upgrade paths

Q. What kind of data does a software upgrade advisory provide with Nexus Dashboard?

A. A software upgrade advisory may be provided as a recommendation to fix an issue observed by Nexus Dashboard (for example: a PSIRT, a known caveat, or an EOL of software used in a switch, etc.). The advisory will then show what release is recommended upgrading to that will resolve the issue. It also shows intermittent releases to upgrade to, which may be needed to get to the destination software, and whether each of these upgrades will be disruptive or nondisruptive.

© 2025 Cisco and/or its affiliates. All rights reserved.

Q. Can Nexus Dashboard track changes in infrastructure or predict configuration changes due to software upgrades?

A. Nexus Dashboard proactively checks to prevent compliance violations and enable continuous assurance to address compliance posture, thus ensuring business services continuity. It accelerates troubleshooting and evaluates the impact of configuration changes with pre-change analysis, to minimize the risk of unintended consequences.

Deployment guidelines

Q. Are telemetry capabilities supported on both physical and virtual Cisco Nexus Dashboard form factors?

A. Yes, the telemetry function is supported for both physical and virtual form factors of Nexus Dashboard. For scaling and sizing details, please refer to the Nexus Dashboard Capacity Planning tool.

Q. Is there any difference in feature and scale when Nexus Dashboard is hosted on virtual vs. Physical appliances?

A. Full feature parity is available on with both virtual and physical factors of Nexus Dashboard. Verified scale is different and details can be found in the Nexus Dashboard Capacity Planning tool.

Q. Do I need to deploy separate Nexus Dashboard instances to enable telemetry for Cisco ACI- and Cisco NX-OS-based fabrics?

A. No, a single instance of Nexus Dashboard can provide telemetry for both ACI and NX-OS based fabrics, starting with Nexus Dashboard 2.1. Please see the Nexus Dashboard Capacity Planning tool for scalability considerations.

Q. How is the telemetry configuration deployed to Cisco ACI or Cisco NX-OS-based fabrics?

A. For ACI and NX-OS-managed fabrics, Nexus Dashboard will automatically push the required configurations for enabling telemetry data collection from the switches. For un-managed fabrics (NX-OS fabrics configured with fabric-monitor mode), the telemetry configuration must be manually configured on the corresponding switches. Nexus Dashboard provides a template of the required configurations needing to be applied to each switch.

For manual telemetry configuration of devices, use the traffic analytics compatibility mode. Please see https://www.cisco.com/c/en/us/td/docs/dcn/nd/4x/articles-411/analyzing-and-troubleshooting-your-network.html to learn more about the traffic analytics compatibility mode configuration.

Q. Can custom thresholds for anomalies be set for telemetry in Nexus Dashboard?

A. Yes, you can configure global rules for anomalies that allow you to define the severity threshold levels of each anomaly.

Q. How does Nexus Dashboard's flow telemetry differ from traffic analytics with flow analytics?

A. Flow Telemetry (FT) collects raw flow records, thus providing per-flow visibility from the switch ASIC. Nexus Dashboard collects hardware flow records (no CPU punt) on a timer through front-panel ports and can display flow paths and counters; it also triggers flow-telemetry events for anomalies (ACL/QoS drops, latency, etc.), which is ideal for packet-path troubleshooting and RCA on specific flows. Flow telemetry scale is based on the number of flows per second and is dependent on the cluster form factor.

Traffic Analytics (TA) provides service-level analytics built on top of flows. Nexus Dashboard auto-discovers services (by well-known L4 ports or user-defined custom categories), baselines them, and tracks latency, congestion, and drops over time with thresholds. Traffic analytics collapses flow records into conversations (between unique client and service endpoint pairings), which allows greater scale compared to flow telemetry.

© 2025 Cisco and/or its affiliates. All rights reserved.

Traffic analytics scale is based on conversations per minute and is dependent on the cluster form factor.

Q. What does a hardware flow record consist of?

A. A hardware flow record consists of the following:

- 5-tuple flow information
- Interface/queue information
- Time stamp
- Flow latency
- Additional flags

Q. What encoding and transports are supported for telemetry data in Nexus Dashboard?

A. Encoding and transports that are supported for telemetry data in Nexus Dashboard are as follows:

- Software telemetry: encoded in GPB/JSON and transported over TCP and gRPC
- Hardware telemetry: not encoded and transported over UDP

Q. What data lake does Cisco Nexus Dashboard use?

A. It uses elastic search to store data in a time-series database.

Q. How can I get more details if customers want to build their own stack to consume telemetry data?

A. If the customer wishes to build their own receiver, we publish the prototype file on GitHub; we have an integration with Telegraf for TCP/ gRPC telemetry. See the following link: https://github.com/influxdata/telegraf/tree/master/plugins/inputs/cisco_telemetry_mdt.

We also have integrations with Telegraf through gNMI. This is for direct consumption of telemetry data through gNMI for Cisco NX-OS–based environments without any analysis by Nexus Dashboard. Visit the following for more information about the gNMI input plug-in https://github.com/influxdata/telegraf/blob/release-1.19/plugins/inputs/gnmi/README.md.

Q. How does Cisco Nexus Dashboard detect known caveats, and what does it do next?

A. Cisco Nexus Dashboard performs as follows:

- Collects tech-support logs for each switch and matches with the digital signatures of known digitized Customer-Found Defects (CFDs)/bugs.
- It then generates an advisory with the recommended fix.
- If the fix is to upgrade the software, Nexus Dashboard will inform you about the bugs that will be fixed when you upgrade to the recommended release.
- Users can also measure the upgrade impact from within Nexus Dashboard, which runs pre- and post-checks and measures if the upgrade will be disruptive or nondisruptive.

Q. Is either multi-pod or multi-site supported in Cisco Nexus Dashboard for Cisco ACI?

A. Multi-pod and multi-site are both supported, including the ability to onboard and monitor the inter-pod and inter-site networks.

Q. How is data collected from switches?

A. Telemetry data can be collected through an in-band network or an out-of-band management network.

© 2025 Cisco and/or its affiliates. All rights reserved.

Q. As part of flow analytics and flow anomalies, can we see the packet path of the flow through the data center network? Is the packet path shown only on Nexus 9000 switches, or can it be shown on other platforms as well?

A. As part of flow analytics and flow anomalies, the packet path of the flow through the data-center network is shown, with drops and the reasons for the drops. This is currently supported for Nexus 9000 cloud-scale platforms. If there are other platforms along the path that do not support flow telemetry, Nexus Dashboard will try to find intermittent node or interface details using LLDP. Please check the user guide for Nexus Dashboard on supported topologies for Cisco ACI / Cisco NX-OS.

Q. If Precision Time Protocol (PTP) is needed, do we need a PTP grand master clock?

A. In order to provide accurate latency measurement, for multi-pod and multi-site fabrics it is highly recommended to leverage an external device to function as a PTP grandmaster. Nexus Dashboard only needs usec-level accuracy; therefore, this external PTP grandmaster device can also be a switch, a router, or a Linux server.

For Cisco NX-OS fabrics, Precision Time Protocol (PTP) must be configured on all switches that you want to support with Nexus Dashboard flow telemetry or traffic analytics. The user must ensure that PTP is correctly configured on all nodes in the fabric.

Precision Time Protocol (PTP) must be enabled on the Cisco APIC. On the Cisco APIC, navigate to System > System Settings > Precision Time Protocol > Admin State to enable PTP. For more information, please refer to the Cisco Nexus Insights Release 5.1(0) for Cisco Application Centric Infrastructure user guide.

For more information, please refer to the Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights.

Q. Can customers access Cisco Nexus Dashboard telemetry data and events using other tools?

A. Yes, there are multiple ways to access the telemetry data. The REST-API can be leveraged to pull telemetry data from Nexus Dashboard. Additionally, Kafka message bus and syslog are also supported to export post-processed software telemetry.

Q. Does Nexus Dashboard leverage Flow Table Events (FTEs) for telemetry functions?

A. Yes, FTE has been leveraged from Nexus Dashboard 2.0 with Cisco ACI and Cisco NX-OS fabrics utilizing Nexus cloud-scale-based platforms. Please refer to Nexus Dashboard release notes for platform version dependencies.

Q. Do we have any information on what different metrics are collected by Cisco Nexus Dashboard depending on the Cisco Nexus model? For example, what is the information that a Cisco Nexus 9300-FX can get that an EX cannot? Or what is the difference between FX2 and FX?

A. You are able to get control-plane information using software telemetry, and flows or ASIC counters using hardware telemetry. Cisco Nexus Dashboard will collect this data, store it in a time-series database, and correlate it to give users much more relevant data compared to the raw data from the switches – that is the power of Cisco Nexus Dashboard.

© 2025 Cisco and/or its affiliates. All rights reserved.

Tables 1 and 2 list the capabilities per platform. For supported features in particular release, please refer to the release notes.

Table 1. Platform capabilities

Cisco Nexus platform	DME	NX-API
3000 with 8GB+ DRAM	Yes	Yes
9200/9300	Yes	Yes
9500	Yes	Yes
5000/5500/6000	No	No
7000/7700	No	Yes

Table 2. Telemetry capabilities

Platform	FT	FTE	SSX
9300/9500-EX	Yes	No	No
9300/9500-FX	Yes	Yes	No
9364C	No	No	Yes
9300/9500-FX2	Yes	Yes	Yes
9300/9500-FX3	Yes	Yes	Yes
9300/9500-GX/GX2	Yes	Yes	Yes
9300-H1/H2	Yes	Yes	Yes

© 2025 Cisco and/or its affiliates. All rights reserved.

Q. Does the Cisco Nexus Dashboard application use remote storage?

A. Starting with Nexus Dashboard 3.0, an external NAS destination can be configured for the purpose of exporting flow telemetry records. These exported records are intended for archival purposes or for third-party tool processing and do not extend the retention period of the solution.

Q. What are the latency requirements for Cisco Nexus Dashboard?

A. The latency requirements for Nexus Dashboard are as follows:

- Between the Cisco Nexus Dashboard Cluster and APIC controllers, the latency tolerance is up to 150 ms.
- Between the Cisco Nexus Dashboard Cluster and fabric switches, the latency tolerance is up to 150 ms.
- Between the nodes of a Cisco Nexus Dashboard cluster, the latency tolerance is up to 50 ms.
- Between connected multiple Nexus Dashboard clusters, the latency tolerance is up to 500 ms.
- Between Cisco Nexus Dashboard cluster and AppDynamics®, the latency tolerance is up to 500 ms.
- Between Cisco Nexus Dashboard and Cisco Intersight, the latency tolerance is up to 500 ms.

Q. What are the bandwidth requirements for telemetry data?

A. The telemetry data bandwidth requirements are a combination of two factors:

- Software telemetry – 500 Kbps per switch
- Hardware telemetry:
  - Flow telemetry – 10 Mbps for 10,000 flows/s
  - Traffic analytics – 5 Mbps for 100,000 conversations/min

Please refer to the Nexus Dashboard Capacity Planning tool for information on the scale supported for specific Nexus Dashboard cluster sizes and form factors.

Q. How frequently is the flow telemetry data exported from the switches?

A. Data is exported at 1 second intervals.

Q. What is the typical volume of data generated by a single leaf per day for software telemetry?

A. The typical volume is as follows:

- Software telemetry: ~600 MB per leaf per day
- Flow analytics (10,000 flows/day): ~1.2 TB

How to buy

Q. What licenses are required for telemetry capabilities in Cisco Nexus Dashboard?

A. Licenses are required for each device (leaf switch only). Please refer to the ordering guide for more details.

Q. Is there an evaluation version of the Cisco Nexus Dashboard software?

A. Yes, the software is available in try-and-buy mode. Customers can download and use the Cisco Nexus Dashboard in lab or test environments without a purchasing license for a maximum of 180 days. For production deployments, purchase of licenses is required.

© 2025 Cisco and/or its affiliates. All rights reserved. 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)