Cisco Nexus Dashboard and Services Release Notes, Release 3.2(2)

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

Contents

Cisco Nexus Dashboard and Services 3

New software features 4

New hardware features 4

Supported upgrade paths 5

Changes in behavior 5

Open issues 6

Resolved issues .... **Error! Bookmark not defined.**

Known issues 15

Compatibility information 20

Verified scalability limits 24

Rollup and retention numbers for Nexus Dashboard Insights telemetry 25

Related content 26

Documentation feedback 27

Legal information 27

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

Cisco Nexus Dashboard and Services

Cisco Nexus Dashboard is a central management console for multiple data center fabrics and a common platform for hosting Cisco data center operation services. These services are available for all the data center fabrics and provide real-time analytics, visibility, assurance for network policies and operations, as well as policy orchestration for the data center fabrics, such as Cisco Application Centric Infrastructure (ACI) or NX-OS deployments spanning LAN Fabric, SAN, and IP Fabric for Media (IPFM) networks. The services are as follows:

- Cisco Nexus Dashboard Fabric Controller (NDFC): A comprehensive management solution for all Cisco NX-OS deployments spanning LAN, SAN, and IP Fabric for Media (IPFM) networks in data centers powered by Cisco. Cisco NDFC also supports devices such as IOS XE switches, IOS XR routers, and third-party devices. Being a multi-fabric controller, Cisco NDFC manages multiple deployment models such as VXLAN EVPN, classic 3-tier, FabricPath, and routed fabrics for LAN while providing ready-to-use control, management, monitoring, and automation capabilities. In addition, when enabled as a SAN controller, NDFC automates Cisco Multilayer Director Switches (MDS) and Cisco Nexus-family infrastructure in NX-OS mode with a focus on storage-specific features and analytics.
- Cisco Nexus Dashboard Insights: Simplifies and automates visibility, troubleshooting, root-cause analysis, and remediation of network issues. By ingesting real-time streamed network telemetries from all devices, Nexus Dashboard Insights provides pervasive infrastructure visibility. It continuously verifies and validates the operational states of the network while proactively detecting any drifts from the operators' intent, detecting different types of anomalies throughout the network, analyzing the root cause of anomalies, and identifying remediation methods. It modernizes the operation of networks, helping the network team to reduce troubleshooting efforts, increase operation efficiency, and proactively prevent network outages.
- Cisco Nexus Dashboard Orchestrator: The intersite policy manager, which provides single-pane management that enables you to monitor the health of all interconnected fabrics. It also allows you to define centrally the intersite configurations and policies that can then be pushed to the different Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller, or DCNM fabrics, which in turn deploy them in those fabrics. This provides a high degree of control over when and where to deploy the configurations.

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

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

Table 1 New and changed information

Date	Description
July 16, 2025	Release 3.2(2m) became available. The image includes the following Nexus Dashboard services versions: • Nexus Dashboard Fabric Controller release 12.2(3) • Nexus Dashboard Orchestrator release 4.4(3) • Nexus Dashboard Insights release 6.5(2)

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

New software features

New software features for Nexus Dashboard

Table 2 New software features for Nexus Dashboard

Product Impact	Feature	Description
Base functionality	Support for EMEA region for Intersight claim.	Beginning with release 3.2(2), Nexus Dashboard can be claimed on US ('us-east-1') or EU regions ('eu-central-1').
Upgrade	Support for UCS server firmware 4.3(5.x)	Support for UCS server firmware 4.3(5.x). You must perform the upgrade in the following order: 1. Upgrade or Install ND to 3.2(2). 2. Upgrade the UCS server firmware 4.3(5.x). For more information, see the “Compatibility” section, Table 19 Supported UCS server firmware.

New software features for Orchestrator

There are no new features for Orchestrator.

New software features for Fabric Controller

There are no new features for Fabric Controller.

New software features for Insights

Insights for Cisco ACI

There are no new enhancements for Insights for Cisco ACI

Insights for Cisco NDFC or Standalone NX-OS enhancements

Table 3 Insights for Cisco NDFC or Standalone NX-OS enhancements

Product Impact	Feature	Description
Base functionality	Support for Traffic Analytics on Classic LAN fabrics	Beginning with NDI release 6.5(2), Traffic Analytics on Classic LAN fabrics is supported, but only over out-of-band (OOB) management ports. In addition, the two-tier Collapsed Core topology is supported, along with other validated topologies, if any. For more information, see the " Traffic Analytics" section in Cisco Nexus Dashboard Insights Analysis Hub, Release 6.5.x - For Cisco NDFC or Standalone NX-OS.

New hardware features

New hardware features for Fabric Controller

The following is the list of new hardware supported with this release.

Cisco Unified Computing System (Cisco UCS) for SAN deployments

- Cisco UCS 64108 108-Port Fabric Interconnect - 10/25/40/100 Gigabit Ethernet, FCoE and Fiber Channel switch offering up to 7.42 Tbps throughput and up to 108 ports

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

Note: To view UCS FI 64108 vFC traffic in NDFC, the UCS FI NX-OS version must be 4.3(4a) or 4.3(4b) or later.

Supported upgrade paths

For supported upgrade paths, see the *Cisco Nexus Dashboard and Services Deployment and Upgrade Guide, Release 3.2(x)*.

Changes in behavior

Changes in behavior for Nexus Dashboard

- Beginning with Nexus Dashboard release 3.2(2m), bugscan no longer detects Active bugs through CLI and device log analysis, but is limited to Susceptible Bug detection using platform and software version information only. This functionality will be re-introduced in a future release.
- Beginning with ND release 3.2(2), there are updates to the behavior when deploying in Linux KVM (for example, only CLI-based procedures are supported when creating the VMs for the nodes).

  For more information, see the " Deploying in Linux KVM (Release 3.2(2) and Later)" chapter in see Cisco Nexus Dashboard and Services Deployment and Upgrade Guide, Release 3.2.x.

Changes in behavior for Orchestrator

- There are no changes in behavior in this release.

Changes in behavior for Fabric Controller

Common enhancements to all personas

- Beginning with NDFC release 12.2(3), a behavior change is introduced where SSH host key verification is enforced in NDFC. This is similar to any SSH client behavior where a new key seen is trusted but a new key seen afterwards for a given host causes a key verification failure.

  For more information, see the section " Server Settings" in the Overview and Initial Setup of Cisco NDFC.

LAN controller enhancements

- The security groups feature is now supported on FX, FX2, H, and C9408 switches.

  For more information, see Configuring Security for VXLAN EVPN Fabrics.
- ToR switches in Data Center VXLAN EVPN fabrics will be out of sync with NX-API and SNMP trap configurations pending diffs after you upgrade to NDFC 12.2(2x) or later.
  - The old behavior: NX-API and SNMP trap host configurations are not generated for ToR switches.
  - The new behavior: NX-API and SNMP trap host configurations are generated for ToR switches.
- Beginning with NDFC release 12.2(3), for switches in Classic LAN or External Connectivity Network fabric types, a new Expected config/Generated config toggle switch is available, which displays the NDFC-generated configuration based on the intent in the NDFC policies.

For more information, see the section " Previewing Switches" in Add Switches for LAN Operational Mode.

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

- Beginning with NDFC release 12.2(3), when editing a network attachment in a VXLAN fabric on a switch with border or border gateway shown in the Switch Role column, you can also provide comma-separated route targets to import or export at the switch level in the Import Route Target and Export Route Target fields. This is supported for both Nexus 9000 and Catalyst 9000 switches.

  For more information, see the section " Network Attachments" in About Fabric Overview for LAN Operational Mode Setups.

- Beginning with NDFC release 12.2(3), support is available for Type 6 for BGP authentication key encryption type for VXLAN EVPN, Enhanced Classic LAN, and BGP fabrics.

  For more information, see:

  - BGP Fabric
  - Data Center VXLAN EVPN
  - Enhanced Classic LAN

- Beginning with NDFC release 12.2(3), a new **Set Allowed Vlan On Leaf-ToR Pairing** field is introduced when configuring ToR switches in Data Center VXLAN EVPN fabrics.

  For more information, see Configuring ToR Switches.

- Beginning with NDFC release 12.2(3), a new **Freeform** tab is introduced when creating or editing these fabric types:

  - BGP Fabric
  - Data Center VXLAN EVPN
  - Enhanced Classic LAN
  - IPFM and Classic IPFM

- Beginning with NDFC release 12.2(3), a new **VRF Lite** tab is introduced when creating or editing VRFs.

  For more information, see the “Creating a VRF” section in About Fabric Overview for LAN Operational Mode Setups.

SAN controller enhancements

- There are no changes in behavior in this release.

Changes in behavior for Insights

- There are no changes in behavior in this release.

Resolved issues

To see additional information about the caveats, click the bug ID to access the Bug Search Tool (BST). The “Exists In” column of the table specifies the releases in which the issue exists.

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

Resolved issues for Nexus Dashboard

Table 4 Resolved issues for Nexus Dashboard

Bug ID	Description	Fixed in
CSCwn00572	Nexus Dashboard CIMC console doesn't respond or is stuck Or When upgrading Nexus Dashboard, one or more nodes can fail on bootstrap, where there are no messages and CIMC console does not respond.	3.2(2m)
CSCwo61222	Nexus Dashboard Physical Appliance is unable to boot after updating the IMC firmware to version 4.3(5.x).	3.2(2m)
CSCwm83093	After the ND 3.0.1 version there is no longer an 'acs installer update xxx' command you can run from the CLI. When running the new command 'acs upgrade update file:/tmp/nd-dk9.3.2.1e.iso' it fails.	3.2(2m)
CSCwk86899	Post upgrade of an existing cluster with a standby to 3.1.x or when adding a new standby, the Kubernetes installation on the standby will fail. The other nodes' cluster health will show: " unable to get node health" of the standby node.	3.2(2m)
CSCwk82268	Day-1 issue with argo based service. Event monitoring is an argo-based service and in rare cases of a fresh install of ND, argo may fail to initialize its base DB collections, which in turn prevents event monitoring to post its alert policies into the DB.	3.2(2m)

Resolved issues for Fabric Controller

Table 5 Resolved issues for Fabric Controller

Bug ID	Description	Fixed in
CSCwm80127	NDFC IPFM fabric Nexus switches shows PTP data error “nexus not streaming PTP data” after time of working properly.	3.2(2m) (NDFC 12.2(3))
CSCwn31986	When discovery falls and there is a change in the AAA password, NDFC fails to discover the switches. You must restart the NDFC discovery pod to recover the discovery password.	3.2(2m) (NDFC 12.2(3))
CSCwk89345	In a Multi-Cluster fabric group, adding a child fabric fails when the child fabric that is being added has networks with DHCP relay configured. The addition fails with following error: " Invalid template config parameters: invalid character 'd' after object key:value pair"	3.2(2m) (NDFC 12.2(3))
CSCwi81474	When contract associations belonging to different VRFs reference the same contract (Filter and Action), the direction gets indirectly converted to policies and filter security CLIs. VRF creation happens implicitly as part of network creation. This means that VRFs are created and security groups/associations are also created for the VRF referencing the same contract. No switches are attached to the VRF yet. Switches are attached to the network, and NDFC implicitly creates the VRF and the security policies. The security group/associations are removed for multiple VRFs. When deployment is done from the Networks, Switches, or VRFs page, VRF deployment fails.	3.2(2m) (NDFC 12.2(3))

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

Bug ID	Description	Fixed in
CSCwj38937	The Nexus Dashboard Fabric Controller service fails to enable after an upgrade if a Domain Name System (DNS) server is unavailable.	3.2(2m) (NDFC 12.2(3))
CSCwm34299	After upgrading NDFC from version 12.2.1 to 12.2.2, topology view is no longer showing ISL san-port-channel interfaces, standalone ISL links are displayed. All ISLs are visible from **Manage > inventory > Links**.	3.2(2m) (NDFC 12.2(3))

Resolved issues for Orchestrator

Table 6 Resolved issues for Orchestrator

Bug ID	Description	Fixed in
CSCwk69595	Restore of backup config is shown as success in ND. Open the widget to see individual status of " Orchestrator" . If it is below 100%, it could be that the restore job is still running in the background but ND did not display its status to the user.	3.2(2m) (Orchestrator 4.4(3))
CSCwj20303	Template deployment fails with the following error message: " ...bulk write exception: write errors: [E11000 duplicate key error collection: ...."	3.2(2m) (Orchestrator 4.4(3))
CSCwj20287	When a new EPG that uses VRF from " common" tenant is added for shared service use case, the traffic from this EPG does not reach the other EPG.	3.2(2m) (Orchestrator 4.4(3))
CSCwi83171	When trying to do a preview deployment on a configuration with VRF->BD or BD->EPG references, the referenced object is not seen in the preview deploy screen.	3.2(2m) (Orchestrator 4.4(3))
CSCwi95494	Unable to deploy Fabric Resource Policy template with VPCI after modifying Node 1 and Node 2.	3.2(2m) (Orchestrator 4.4(3))
CSCwi82478	The issue occurs in the following scenario: 1. Deployed template version1 2. Modify the template to version2 3. Undeploy the template without first deploying version2. The undeployment happens on version1 but the UI displays the data from version2.	3.2(2m) (Orchestrator 4.4(3))
CSCwi30690	For a BD in NDO schema, only the linked L3Out name is populated, and the BD's L3Out reference field is empty even though the L3Out is managed by NDO. This behavior can be observed in the Reconcile Drift UI where the BD's L3Out reference is missing in the NDO schema tab, and only the name is displayed.	3.2(2m) (Orchestrator 4.4(3))

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

Resolved issues for Insights

Resolved issues for Insights for Cisco ACI

Table 7 Resolved issues for Insights for Cisco ACI

Bug ID	Description	Fixed in
CSCwk84891	Seeing Active Flow Config Anomaly for "Flows configuration failed for site: xxx." even though flows are collecting as expected on that site. Issue has been present since recent upgrade to ND 3.1.1l and NDI 6.4.1.45.	3.2(2m) (Insights 6.5(2))
CSCwk87837	When the flow has the RTO (TCP retransmission inside/outside) anomaly, the flow is marked unhealthy. However, the corresponding anomalies are not visible when you drill down to flow details anomaly page.	3.2(2m) (Insights 6.5(2))
CSCwj09007	Compliance Rules created in 6.2.2.x or 6.3.1.x are tagged as "Deleted" in Compliance Report page (Analyze -> Analysis Hub -> Compliance) after upgrading	3.2(2m) (Insights 6.5(2))

Resolved issues for Insights for Cisco NDFC or Standalone NX-OS

Table 8 Resolved issues for Insights for Cisco NDFC or Standalone NX-OS

Bug ID	Description	Fixed in
CSCwk84891	Seeing Active Flow Config Anomaly for "Flows configuration failed for site: xxx." even though flows are collecting as expected on that site. Issue has been present since recent upgrade to ND 3.1.1l and NDI 6.4.1.45.	3.2(2m) (Insights 6.5(2))
CSCwj10388	Congestion score detail graphs and queue details on "Trends & Statistics" page are not evenly plotted if you stay on the page for some time.	3.2(2m) (Insights 6.5(2))

Open issues

To see additional information about the caveats, click the bug ID to access the Bug Search Tool (BST). The "Exists In" column of the table specifies the releases in which the issue exists.

Open issues for Nexus Dashboard

Table 9 Open issues for Nexus Dashboard

Bug ID	Description	Exists in
CSCwo89719	When selecting fabric firmware version 6.1(3f), the node firmware options are not displayed as expected. The node firmware should list version 16.1(3f) (10+ the selected controller version). If the fabric firmware version is skipped, the node firmware should list version 16.1(2g) (10+ the current controller version 6.1(2g)). The issue is specific to environments with NX and ACI both fabrics added on ND.	3.2(2m) and later
CSCwk92046	Pre-upgrade validation appears to be fine for NTP health, but notification bell shows NTP server errors for at least one configured server. If the user continues with the upgrade, the cluster will report NTP errors upon coming up when calling "acs health" on the CLI, as well as on the system settings page on the UI, blocking apps from starting and eventually causing the upgrade to time out.	3.2(2m) and later

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

Bug ID	Description	Exists in
CSCwk98029	Backup restore fails when ND does the initial health checks of all apps in the system and the output of `kubectl get apps` contains one or both of the following: elasticsearch-6.8.4 elasticsearch-nir-6.8.4 Note that the system is healthy in this state; there will be no faults seen on the ND UI/acs health outputs.	3.2(2m) and later
CSCwk82268	Day-1 issue with argo based service. Event monitoring is an argo-based service and in rare cases of a fresh install of ND, argo may fail to initialize its base DB collections, which in turn prevents event monitoring to post its alert policies into the DB.	3.2(2m) and later
CSCwk87978	Use the History tab to view failed backup details. If you view the failed backup details in the backup list, you will see an empty drawer.	3.2(2m) and later
CSCwk40021	In the case of a full cluster outage, the alerting service itself will go unreachable and will not be able to track alerts. In this release, we do not store the failed state anywhere in cases of complete cluster outages that could be picked up as an alert later post cluster recovery.	3.2(2m) and later
CSCwi63356	High memory utilization on some but not all nodes after node failover.	3.2(2m) and later

Open issues for Fabric Controller

Table 10 Open issues for Fabric Controller

Bug ID	Description	Exists in
CSCwq23284	When you delete all the switches and fabrics from the NDFC and go to the fabric software page, the last fabric information will show up there as stale information.	3.2(2m) (NDFC 12.2(3))
CSCwp27571	When N9K-C9408 is added as VTEP to a ND/NDFC managed VXLAN fabric with IPv6 underlay and multicast replication mode, Recalculate & Deploy generates an error stating that the platform is not supported.	3.2(2m) (NDFC 12.2(3))
CSCwk79989	The service insertion of the Service As Default Gateway use case is enabled and attached. When you delete one Layer 2 network from the service insertion's associated Layer 2 network list, the intended configuration to clean up that Layer 2 network-related configuration on the service switch is not generated.	3.2(2m) (NDFC 12.2(3))
CSCwk81978	After a leaf-ToR unpairing was done, a Recalculate and Deploy operation only shows diffs on the ToR switch.	3.2(2m) (NDFC 12.2(3))
CSCwo59630	Security groups, contracts, associations, protocols pages are empty post fabric or MSD restore.	3.2(2m) (NDFC 12.2(3))
CSCwo62524	For IOS devices, when a VRF policy is created with template IOS_XE_VRF, generated pending config with VRF and network level deploy may have ordering issues with the VRT forwarding sub command deployed after IP related sub commands and result in removal of IP related sub commands.	3.2(2m) (NDFC 12.2(3))

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

Bug ID	Description	Exists in
CSCwo72314	NDI Cannot complete Bugscan, with Authorization request failing on the calls to Fabric Controller Cluster.	3.2(2m) (NDFC 12.2(3))
CSCwo67502	A new knob has been introduced on the switch preview side-by-side page for viewing Expected/Generated configurations in Nexus Dashboard Fabric Controller (NDFC) for LAN Classic and External Fabric. The Pending Config option, which is meant to display the same order of commands for the same operation, does not consistently show the correct order in some scenarios. Specifically: Incorrect Command Ordering: When there is a config diff (i.e., differences in configurations that need to be pushed), the Generated Config displays the commands in the wrong order. This is especially noticeable when comparing the configuration to the running config output in the same screen. The ordering mismatch can lead to confusion, even though there is no functional impact on the system. Display Gaps Between Configs: In some cases, there are visible gaps between configuration entries in the display, which further contributes to the confusion. These gaps may appear when comparing the Expected vs. Generated configurations, making it unclear whether there are missing configurations or misalignment in the data. While the issue does not affect the functionality of the system (i.e., the configuration will still be pushed and applied correctly), it could cause confusion for users who are relying on the previewed config order to verify changes before applying them.	3.2(2m) (NDFC 12.2(3))
CSCwo33001	The route-target field for the VRF definition and attachment is not validated in REST API calls.	3.2(2m) (NDFC 12.2(3))
CSCwo61400	If user updates the existing attached service insertion after NDFC upgrade to 12.2.2 or 12.2.3, NDFC generated pending configs will include both the existing and the new change triggered configs.	3.2(2m) (NDFC 12.2(3))
CSCwo48369	Security Groups Pre-provision is not enabled in the member fabrics even though its enabled in the parent MSD fabric.	3.2(2m) (NDFC 12.2(3))
CSCwk80157	When creating an active/standby physical service cluster using the Fabric Overview > Services > Service Clusters page, the vPC interface with the same name as the first service node attached to the switch interface is not shown during the second service node creation, even though two service nodes are attached to different vPC pairs.	3.2(2m) (NDFC 12.2(3))
CSCwk80282	There are policy-based routing (PBR) policies defined in NDFC 12.1.3 or 12.2.1. The PBR stats diagram in NDFC 12.2.1 or 12.1.3 shows the collected PBR stats for involved VRFs, networks, and routed WAN interfaces on the related switches. After an NDFC upgrade to 12.2.2, the PBR stats will only be shown for the involved VRFs.	3.2(2m) (NDFC 12.2(3))

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

Open issues for Orchestrator

Table 11 Open issues for Orchestrator

Bug ID	Description	Exists in
CSCwo90400	Static ports are removed from some sites during EPGs migration between templates.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCwk81460	Restore of backup config fails in NDO under certain conditions as described in the issue.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCwj55927	After moving a policy from one template to another template, the first template deployment is successful but the second template deployment fails with a "referenced policy cannot be deleted" message.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvo84218	When service graphs or devices are created on Cloud APIC by using the API and custom names are specified for AbsTermNodeProv and AbsTermNodeCons, a brownfield import to the Nexus Dashboard Orchestrator will fail.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvo20029	Contract is not created between shadow EPG and on-premises EPG when shared service is configured between Tenants.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvn98355	Inter-site shared service between VRF instances across different tenants will not work, unless the tenant is stretched explicitly to the cloud fabric with the correct provider credentials. That is, there will be no implicit tenant stretch by Nexus Dashboard Orchestrator.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvt00663	Deployment window may not show all the cloud related config values that have been modified.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvt41911	After brownfield import, the BD subnets are present in fabric local and not in the common template config	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvt44081	In shared services use case, if one VRF has preferred group enabled EPGs and another VRF has vzAny contracts, traffic drop is seen.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvt02480	The REST API call "/api/v1/execute/schema/5e43523f1100007b012b0fcd/template/Template_11?undeploy=all" can fail if the template being deployed has a large object count	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvt15312	Shared service traffic drops from external EPG to EPG in case of EPG provider and L3Out vzAny consumer	3.2(2m) (Orchestrator 4.4(3)) and later

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

Bug ID	Description	Exists in
CSCvw10432	Two cloud fabrics (with Private IP for CSRs) with the same InfraVNETPool on both fabrics can be added to NDO without any infraVNETPool validation.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCvy36810	Multiple Peering connections created for 2 set of cloud fabrics.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCwa37204	Username and password are not set properly in proxy configuration so a component in the container cannot connect properly to any fabric. In addition, external module pyaci is not handling the web socket configuration properly when user and password are provided for proxy configuration.	3.2(2m) (Orchestrator 4.4(3)) and later
CSCwm52983	After upgrade or configuration restore, you may see the following warning: " Configuration Inconsistencies detected.... BindingType is required for VMware VMM Domain..."	3.2(2m) (Orchestrator 4.4(3)) and later

Open issues for Insights

Open issues for Insights for Cisco ACI

Table 12 Open issues for Insights for Cisco ACI

Bug ID	Description	Exists in
CSCwq07846	When you try to create a prechange analysis, it does not move past the base epoch selection page. When you click Next in the General tab, the following error appears: " Unable to save or start Pre-Change Analysis. Contact TAC." The issue is seen regardless of snapshot fabric or online fabric. The issue is seen for both Manual and JSON/ XML changes.	3.2(2m) (Insights 6.5(2))
CSCwo45591	NDI reconnecting to APIC every minute, removing and adding subscriptions and flow exporters.	3.2(2m) (Insights 6.5(2))
CSCwo68025	In ND 3.2.2e, Insights Service is not supported N9K-C92348GC-FX3.	3.2(2m) (Insights 6.5(2)) and later
CSCwk78455	Arc between two EPGs may show indication as unhealthy but no anomalies are shown in the tables.	3.2(2m) (Insights 6.5(2)) and later
CSCwb28067	If same EPG name is used across tenants in ACI fabrics, then flow path stitching and its details could be incorrect. This could impact forward, and reverse path stitch shown in flow pages of Nexus Dashboard Insights.	3.2(2m) (Insights 6.5(2)) and later

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

Bug ID	Description	Exists in
CSCwd83293	A switch reloads with a core dump of dcgrpc, dc_nae, dc, or any combination of these processes.	3.2(2m) (Insights 6.5(2)) and later
CSCwh22018	Connectivity Analysis is supported on Cisco APIC release 6.0.(3e) and NICC release 3.0.0.546.	3.2(2m) (Insights 6.5(2)) and later
CSCwj33727	When you navigate to a cluster with no remote user defined for the radius domain, the NDI application remains in a loading state where you cannot navigate or access anything.	3.2(2m) (Insights 6.5(2)) and later
CSCwh45345	Anomalies in workflow such as NDO assurance, Delta Analysis, and Compliance may not be present in the main anomalies table due to the total number of anomalies generated hitting the maximum threshold.	3.2(2m) (Insights 6.5(2)) and later
CSCwj91960	Nexus Dashboard Insights does not detect the " Service Chain Redirect Policy Violation" anomaly on switches.	3.2(2m) (Insights 6.5(2)) and later
CSCwn80892	For BGP connections configured with loopback interfaces (or logical interfaces except SVI), if peer connectivity is lost, no anomaly is raised, and there is no RCA graph available.	3.2(2m) (Insights 6.5(2)) and later

Open issues for Insights for Cisco NDFC or Standalone NX-OS

Table 13 Open issues for Insights for Cisco NDFC or Standalone NX-OS

Bug ID	Description	Exists in
CSCwq07846	When you try to create a prechange analysis, it does not move past the base epoch selection page. When you click Next in the General tab, the following error appears: " Unable to save or start Pre-Change Analysis. Contact TAC." The issue is seen regardless of snapshot fabric or online fabric. The issue is seen for both Manual and JSON/ XML changes.	3.2(2m) (Insights 6.5(2))
CSCwo68025	In ND 3.2.2e, Insights Service is not supported N9K-C92348GC-FX3	3.2(2m) (Insights 6.5(2)) and later
CSCwo49038	The configuring FT with flow rule filters on a layer2 (switched) interface results in a failure, as these filters are only supported on Layer3 (routed) interfaces. The validation is missing and UI, and lets the user to go ahead with configuration which will eventually fail.	3.2(2m) (Insights 6.5(2)) and later
CSCwh45345	Anomalies in workflow such as NDO assurance, Delta Analysis, and Compliance may not be present in the main anomalies table due to the total number of anomalies generated hitting the maximum threshold.	3.2(2m) (Insights 6.5(2)) and

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

Bug ID	Description	Exists in
		later
CSCwi96511	NDI shows zero latency for flows that are sent to egress leaf over vPC link.	3.2(2m) (Insights 6.5(2)) and later
CSCwj07014	When fabric contains EoR spine in flow troubleshoot, paths shown are not accurate.	3.2(2m) (Insights 6.5(2)) and later
CSCwn80892	For BGP connections configured with loopback interfaces (or logical interfaces except SVI), if peer connectivity is lost, no anomaly is raised, and there is no RCA graph available.	3.2(2m) (Insights 6.5(2)) and later

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.

Known issues for Nexus Dashboard

Table 14 Known issues for Nexus Dashboard

Bug ID	Description
CSCwj24254	The issue occurs in the following scenario: 1) During bootstrap, add three nodes 2) Select the NDFC and NDI deployment mode 3) Go back to the previous page and delete two nodes 4) UI does not block bootstrap process afterwards. The API error appears after submitting the bootstrap configuration.
CSCwi08020	On some of the virtual setup we have seen DB we store for prometheus gets full and mond stops working. As a result, UI will fail to poll some of the metrics required for cluster health etc.
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.
CSCvw39822	On power cycle system lvm initialization may fail due to a slowness in the disks.
CSCvw48448	Upgrade fails and cluster is in diverged state with one or more nodes on the target version.
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.
CSCvw70476	When bringing up ND cluster first time, all three primary nodes need to join Kafka cluster before any primary node can be rebooted. Failing to do so, 2 node cluster doesn't become healthy as Kafka cluster requires 3 nodes to be in Kafka cluster first time.
CSCvx89368	After ND upgrade, there will be still pods belonging to the older version running on the cluster.

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

Bug ID	Description
CSCvx98282	Pods in pending state for a long period upon restart. These pods are usually stateful sets that require specific node placement and capacity must be available on the specific node they are first scheduled. This happens when multiple applications are installed on the same ND cluster and the ND capacity overloaded.
CSCvu21304	Intersight device connector connects to the Intersight over the Cisco Application Services Engine Out-Of-Band Management.
CSCwe04619	The 'acs health' command may show a service as unhealthy and kubectl (available in the Tech Support collection) shows the service is in ContainerCreateError state.
CSCwd84875	Two Nodes RMA requires manual intervention.
CSCwb31373	After node failover, kubernetes scheduling may be unable to find appropriate resources for the pods in an app. The symptom is that the app health will not converge and kubectl commands will show unhealthy pods.
CSCwj06781	If GUI-based upgrade workflow fails, the UI error message shows a documentation link for using a manual upgrade as a workaround, but the documentation link points to existing release's content which does not apply to the target release.
CSCwj44955	There may be an issue during the bootstrap process on 3-node vND (ESX) clusters which can cause the 'acs health' command to show the following error: 'k8s: services not in desired state - aaamgr,cisco-intersightdc,eventmonitoring,infra-kafka,kafka,mongodb,sm,statscollect'
CSCwd84563	Upgrade to v2.3 from v2.1.2d - No warning messages to disable old App/containers.
N/A	In the Nexus Dashboard in-product Help Center, the Release Notes link currently points to the incorrect version of Cisco Nexus Dashboard Release Notes. The link should point to the Cisco Nexus Dashboard 3.2(2) Release Notes instead.

Known issues for Orchestrator

Table 15 Known issues for Orchestrator

Bug ID	Description
CSCwk73141	When upgrading using NDO, the validation of the APIC image upgrade fails with timeout error. This can happen if the APIC takes more than 90 seconds to respond to the validation request from NDO or if the APIC has lots of faults, which need to be examined during the validation process.
CSCwi64894	Extra contract relationships seen in shadow objects when parent EPG consumes or provides to multiple contracts.
CSCwi12966	Implicit Filters and Contracts are not getting updated when the original policies are modified. Any small property changes in policies is not updating the implicit objects.
CSCvv67993	NDO will not update or delete VRF vzAny configuration which was directly created on APIC even though the VRF is managed by NDO.
CSCvo82001	Unable to download Nexus Dashboard Orchestrator report and debug logs when database and server logs are selected

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

Bug ID	Description
CSCvn90706	For hybrid cloud deployments, no validation is available for shared services scenarios
CSCvi61260	If an infra L3Out that is being managed by Cisco Multi-Site is modified locally in a Cisco APIC, Cisco Multi-Site might delete the objects not managed by Cisco Multi-Site in the Infra L3Out.
CSCvu71584	Routes are not programmed on CSR and the contract config is not pushed to the Cloud fabric.
CSCvw47022	Shadow of cloud VRF may be unexpectedly created or deleted on the on-premises fabric.
CSCvt47568	Let's say APIC has EPGs with some contract relationships. If this EPG and the relationships are imported into NDO and then the relationship was removed and deployed to APIC, NDO doesn't delete the contract relationship on the APIC.
CSCwa31774	When creating VRFs in infra tenant on a Google Cloud fabric, you may see them classified as internal VRF in NDO. If you then import these VRFs in NDO, the allowed routeleak configuration will be determined based on whether the VRF is used for external connectivity (external VRF) or not (internal VRF). This is because on cAPIC, VRFs in infra tenant can fall into 3 categories: internal, external and un-decided. NDO treats infra tenant VRFs as 2 categories for simplicity: internal and external. There is no usecase impacted because of this.
CSCwa47934	Removing fabric connectivity or changing the protocol is not allowed between two fabrics.
CSCwa52287	Template goes to approved state when the number of approvals is fewer than the required number of approvers.
CSCvy31532	After a fabric is re-registered, NDO may have connectivity issues with APIC or CAPIC
CSCwc62636	If cloud fabrics have EVPN-based connectivity with another cloud or on-premises fabric, then contract-based routing must be enabled for intersite traffic to work.
CSCwc59208	When APIC-owned L3Outs are deleted manually on APIC by the user, stretched and shadow InstP belonging to the L3Outs get deleted as expected. However, when deploying the template from NDO, only the stretched InstPs detected in config drift will get deployed.
CSCvz07639	NSG rules on Cloud EPG are removed right after applying service graph between Cloud EPG and on-premises EPG, which breaks communication between Cloud and on-premises.
CSCwa26712	Existing IPSec tunnel state may be affected after update of connectivity configuration with external device.
CSCwa40878	User can not withdraw the hubnetwork from a region if intersite connectivity is deployed.
CSCwa17852	BGP sessions from Google Cloud fabric to AWS/Azure fabric may be down due to CSRs being configured with a wrong ASN number.
CSCwi19857	APIC has GOTO and GOTHROUGH options when configuring an L3 device, but in NDO the GOTHROGH option is not exposed intentionally. Only the GOTO option is supported.
CSCwi95494	May be unable to deploy a template with VPCI after modifying Node 1 and Node 2. NDO will not delete a VPC peer group on APIC, because it may be shared by multiple other VPCs that are not managed by NDO, removing which may cause config issues.
CSCwi35916	After an upgrade to NDO 4.2.1 or later, the orchestrator raises configuration drifts that are not automatically reconciled, associated to the configuration objects for Service Devices and Service Graphs.

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

Bug ID	Description
N/A	The ipDPLearning configuration under EPG and BD subnets is available as an option through the NDO 4.4.3 REST API but is not supported.

Known issues for Fabric Controller

Table 16 Known issues for Fabric Controller

Bug ID	Description
CSCwq29875	A backup was taken in release 3.2.2 when telemetry was enabled for many fabrics (close to 10 fabrics). Now if a restore was done with a different cluster name. After the restore, the user manually does a resync from NDI. NDI deregisters all the fabrics. De-registration failed since some components had the old clustername in its DB/cache leading to inconsistency.
CSCwo43874	If you click on the Learn More link in the Fabric Software GUI page, it brings up the older Image Management article, when it should be bringing up the newer Fabric Software article.
CSCwd85885	Network creation error on upgraded setup.
CSCwe53978	Persistent configuration difference is observed for 'ip dhcp relay address' command.
CSCwf12259	For a SAN fabric, the timelines beneath the graph on Congestion Analysis are not accurately aligned for the interface graphs.
CSCwf14008	On SAN Insights for a host, the Rx/Tx graphs for a switch interface appear as truncated.
CSCwh30277	When you perform an install or upgrade using a Software Maintenance Upgrades (SMU) image, the upgrade status fails to change from out-of-sync to in-sync.

Known issues for Insights

Known issues for Insights for Cisco ACI

Table 17 Known issues for Insights for Cisco ACI

Bug ID	Description
CSCwh50022	Existing syslog export with SSL may be broken after Nexus Dashboard Insights (NDI) upgrade.
CSCvz52746	Tenant, VRF and EPG details will not be reported in Flow Browse or Details page if Q-in-Q flow is monitored using Netflow in Nexus Dashboard Insights.
CSCvv31284	External EPG name is not reported in Cisco Nexus Insights app even though the subnet is specified.
CSCvw11059	The EX tier-1 leaf switch is not stitched in the flow path.
CSCwb59463	In ACI platforms, with fast-link-fail over feature enabled, path summary will not have north bound or spine facing information in the flow path summary for FX2 based platforms.
CSCwb92508	When you click on Pre-Change Analysis rows in the table, if you navigate through them a bit faster without waiting for the sidebar to completely load, you may sometimes notice duplicated changes added in the

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

Bug ID	Description
	form.
CSCvr32097	LLDP transmit receive packets statistics graph displays the same values regardless of the selected time range.
CSCwa86961	When L4-L7 intra VRF traffic is going through spine switches, Nexus Dashboard Insights flow path summary might not show spine switch information like spine name and interface names.
CSCwb02805	In Nexus Dashboard Insights, flow path information for L4-L7 traffic does not show the L3Out service leaf switch information.
CSCwb66891	For L3Out to EPG intra-VRF L4-L7 traffic, some of leaf switches and spine switches might not exporting flow information. Flow path will not include those nodes in the path information.
CSCvz67522	Nexus Dashboard Insights does not model Endpoint Security Groups and related rules. Stale Policy CAM rules and Enforced VRF policy violation anomaly will be displayed in Nexus Dashboard Insights
CSCwb39004	Nexus Dashboard Orchestrator job schedule and Inter-Site view in the anomaly table usability issues
CSCwb43792	vCenter anomalies are not exported as part of email export, when basic or advanced option is selected.
CSCwb87579	Since Explore is designed to support max fabric wide rules of 150k, nae-policy-explorer pod would go OOM when Explore " Connectivity analysis " is run for completed epoch having a large policy scale.
CSCwh37988	Bug Scan status will be shown as Failed with reason " CPU/Memory metrics not available for the device" .
CSCwh29141	There will be an error thrown by config service if the exporters are created if the POST API is called using deprecated categories as input.
CSCvw03887	In flow analytics the health score on the flow records is displayed as healthy even when ingress flow records are not available.
CSCvw24739	In flow analytics page, PC and vPC interface ID are displayed instead of port name.
CSCwh42672	Once the online fabric is onboarded to NDI, you cannot edit the username or password from the NDI UI.
CSCwf98815	There is no option for enabling and disabling the NDO assurance for online fabrics.

Known issues for Insights for Cisco NDFC or Standalone NX-OS

Table 18 Known issues for Insights for Cisco NDFC or Standalone NX-OS

Bug ID	Description
CSCwh50022	Existing syslog export with SSL may be broken after Nexus Dashboard Insights (NDI) upgrade.
CSCvt77736	When there is no data coming from switches, topNodes API returns all nodes into the list as healthy with endpoint count as 0.
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.
CSCvv58470	Advisories are displayed for devices removed from the Site or Fabric.
CSCvv89866	Endpoint data is displayed for unsupported devices.

Bug ID	Description
CSCvw00525	Fabrics with hardware flow telemetry in disabled failed state cannot be upgraded.
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.
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.
CSCvx69082	Flow Telemetry configuration is not removed from FX3S switch if the switch was running NX-OS release 9.3.7 with Flow Telemetry enabled and then upgraded or downgraded to NX-OS release 10.1.
CSCwa19211	If external routes in the border leaf switch are filtered and only default route is advertised to other leaf switch via BGP EVPN VXLAN, assurance will raise anomalies for all external routes missing in the leaf switch per VRF.
CSCwa42157	OVERLAPPING_EXT_INT_PREFIX - extended support in NX-OS assurance
CSCwb43792	vCenter anomalies are not exported as part of email export, when basic or advanced option is selected.
CSCwh29141	There will be an error thrown by config service if the exporters are created if the POST API is called using deprecated categories as input.
CSCwh37988	Bug Scan status will be shown as Failed with reason " CPU/Memory metrics not available for the device" .
CSCwh42672	Once the online fabric is onboarded to NDI, you cannot edit the username or password from the NDI UI.
CSCwk28382	On a headless setup, the " switchport mode dot1q-tunnel" configuration is handled by users. If you have " switchport mode dot1q-tunnel" on any L2 interface, the command disable cdp creates an issue with topology.

Compatibility information

Compatibility information for Nexus Dashboard

Beginning with release 3.1(1), Nexus Dashboard software also includes the compatible services within the same image.

For Cisco Nexus Dashboard cluster sizing guidelines and the list of supported services for each cluster form factor, see the Nexus Dashboard Capacity Planning tool.

VMware vMotion is not supported for Nexus Dashboard nodes deployed in VMware ESX.

Beginning with release 3.2(2), Nexus Dashboard can be claimed on US ('us-east-1') or EU regions ('eu-central-1').

Supported UCS server firmware

Physical Nexus Dashboard nodes support Cisco UCS-220-M5 (SE-NODE-G2) and UCS-225-M6 (ND-NODE-L4) servers.

Physical Nexus Dashboard nodes must be running a supported version of UCS server firmware (which includes Cisco Integrated Management Controller (CIMC), BIOS, RAID controller, and disk and NIC adapter firmware).

Table 19 Supported UCS server firmware

Product ID	Supported Firmware Releases
SE-NODE-G2 (UCS-220-M5)	• 4.2(3b) • 4.2(3e) • 4.3(2.230207) • 4.3(2.240009) • 4.3(2.240077)
ND-NODE-L4 (UCS-225-M6)	• 4.3(4.240152) • 4.3(4.242066) • For firmware 4.3(5.x), you must upgrade or install ND to 3.2.2 and then upgrade your CIMC to one of the following versions: ○ 4.3(5.250030) ○ 4.3(5.250001)

Note: Though other firmware versions than those listed above may be supported on standard UCS C220/C225 servers, they are not supported on Nexus Dashboard appliances and could lead to issues.

Cisco UCS-C220-M3 and earlier servers are not supported for Virtual Nexus Dashboard clusters.

Browser Compatibility

The Cisco Nexus Dashboard and services UI is intended to be compatible with the most recent desktop version of most common browsers, including Chrome, Firefox, Edge, and Safari. In most cases, compatibility will extend one version behind their most recent release.

While not designed for compatibility with mobile devices, most mobile browsers are still able to render majority of Nexus Dashboard and services UI. However, using the above-listed browsers on a desktop or laptop is recommended. Mobile browsers aren’t officially supported by Cisco Nexus Dashboard and services.

Compatibility information for Orchestrator

This release supports the hardware listed in the “Prerequisites” section of the Cisco Nexus Dashboard Orchestrator Deployment Guide.

This release supports Nexus Dashboard Orchestrator deployments in Cisco Nexus Dashboard only.

Cisco Nexus Dashboard Orchestrator can be cohosted with other services in the same cluster. For cluster sizing guidelines, see the Nexus Dashboard Cluster Sizing tool.

Cisco Nexus Dashboard Orchestrator can manage fabrics managed by a variety of controller versions. For fabric compatibility information see the Nexus Dashboard and Services Compatibility Matrix.

Compatibility information for Fabric Controller

Cisco Nexus Dashboard Version Compatibility

NDFC 12.2.3 is bundled with the ND 3.2.2f image. There is no longer any separate option for upload of applications into the Nexus Dashboard. Nexus Dashboard is now a single unified product.

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

Supported Cisco Platforms and Software Versions

For compatibility of NDFC release 12.2.3 with various switches, applications, and other devices, see the Compatibility Matrix for Nexus Dashboard Fabric Controller.

For compatibility of NDFC release 12.2.3 with specific Nexus Dashboard, services, and fabric versions, see the Cisco Nexus Dashboard and Services Compatibility Matrix.

For information on cluster sizing guidelines, co-hosting scenarios, and supported form factors, see Nexus Dashboard Capacity Planning tool.

For the list of supported non-Nexus and third-party platforms in this release, see the Compatibility Matrix for Cisco NDFC.

Compatibility information for Insights

For Nexus Dashboard Insights compatibility information see the Services Compatibility Matrix.

Table 20 Compatibility information for Insights for Cisco ACI

Software	Release/PID
Cisco Device supported for Software Telemetry	Cisco Nexus 9300-EX, -FX, -FX2, -GX, and 9500 platform switches with EX, FX line cards Cisco Nexus 9000 FX3 and 9336C-FX2-E platform switches Cisco Nexus 9300-GX2 Platform Switches NOTE: Cisco Nexus 9300-GX2 platform switches support Flow Telemetry for the Cisco Nexus 9000 ACI-Mode Switches release 16.0(3) and later. Beginning with the Cisco APIC 16.1(1) release, FTE is supported.
Cisco Nexus Dashboard cluster	SE-CL-L3, ND-CLUSTER-L4
Minimum Intersight Device Connector version on Cisco Nexus Dashboard	1.0.9-828
Cisco Device supported for Flow Telemetry	Cisco Nexus 9300-EX, -FX, -FX2, -GX, and 9500 platform switches with EX, FX line cards Cisco Nexus 9000 FX3 and 9336C-FX2-E platform switches Cisco Nexus 9300-GX2 Platform Switches NOTE: Cisco Nexus 9300-GX2 platform switches support Flow Telemetry for the Cisco Nexus 9000 ACI-Mode Switches release 16.0(3) and later. Beginning with the Cisco APIC 16.1(1) release, FTE is supported.
Minimum Cisco APIC version required for FTE and Micro-Burst	5.1(1h)
AppDynamics APM	4.5

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

Table 21 Compatibility information for Insights for Cisco NDFC or Standalone NX-OS

Software/Hardware	Release
Minimum Cisco NX-OS version required for Software Telemetry	7.0(3)I7(6), 8.4(2)
Minimum Cisco NX-OS version required for Software and Hardware Telemetry	9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7), 9.3(8), 9.3(9), 9.3(10), 9.3(11), 9.3(12), 10.1(1), 10.2(1), 10.2(2), 10.2(3), 10.2(4), 10.2(5), 10.2(6), 10.3(1), 10.3(2), 10.3(3), 10.3(4), 10.4(1), 10.4(2), 10.4(3), 10.4(4)
Minimum Cisco NX-OS version required for Host Flow Overlay	9.3(4), 10.2(1)
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 Cisco NX-OS version required for Connectivity Analysis	9.3(7a)
Minimum Cisco NX-OS version required for Flow Telemetry Event (FTE)	9.3(5)
Minimum Intersight Device Connector version on Cisco Nexus Dashboard	1.0.9-828
Cisco Devices supported for Flow Telemetry Events	Cisco Nexus 9000 -FX, -FX2, -FX3, and -GX platform switches and 9700 -FX line cards
Cisco Device supported for Flow Telemetry	• Cisco Nexus 9000 -FX3, Cisco Nexus 9300-EX, -FX, -FX2, -FX3, and -GX platform switches and 9500-EX and FX • N9K-X9716D-GX line card • Cisco Nexus 9300-GX2 Platform Switches • Cisco Nexus 9408 switch • Cisco N9K-C9332D-H2R with NX-OS release 10.4(1) and later • Cisco N9K-C93400LD-H1 with NX-OS release 10.4(2) and later • Cisco N9K-C9364C-H1 with NX-OS release 10.4(3) and later **Note:** Cisco Nexus 9300-GX2 platform switches support Flow Telemetry for NX-OS release 10.4(2) and later.
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

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

Software/Hardware	Release
	• Cisco Nexus 9000 -FX3, Cisco Nexus 9300-GX, 9300-FX3 and platform switches • N9K-X9716D-GX line card • Cisco Nexus 9300-GX2 platform switches • Cisco Nexus 9808 and Cisco Nexus 9804 switches • Cisco Nexus 9800 Line Cards: N9K-X9836DM-A, N9K-X98900CD-A • Cisco N9K-C9332D-H2R with NX-OS release 10.4(1) and later • Cisco N9K-C93400LD-H1 with NX-OS release 10.4(2) and later • Cisco N9K-C9364C-H1 with NX-OS release 10.4(3) and later
Cisco Device not supported for Software Telemetry	• 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
Micro-Burst support	See Supported Platforms for details.

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

Verified scalability limits for Nexus Dashboard

The following table lists the maximum verified scalability limits for the Nexus Dashboard platform.

Table 22 Verified scalability limits for Nexus Dashboard

Category	Scale
Number of primary and worker nodes in a cluster	Depends on cluster form factor and the specific services enabled in the cluster. See the Nexus Dashboard Capacity Planning tool for detailed information.
Number of standby nodes in a cluster	For physical cluster, up to 2 standby nodes For virtual and cloud clusters, standby nodes are not supported
Fabrics per cluster	Depends on the specific services deployed in the cluster: • For Nexus Dashboard Orchestrator, see the Nexus Dashboard Orchestrator Verified Scalability Guide for a specific release. • For Nexus Dashboard Fabric Controller, see the Verified Scalability Guide for Cisco Nexus Dashboard Fabric Controller for a specific release. • For Nexus Dashboard Insights, see the Nexus Dashboard Capacity Planning for a specific release.
Admin users	50
Operator users	1000

Category	Scale
API sessions	2000 for Nexus Dashboard and Nexus Dashboard Orchestrator 100 for Nexus Dashboard Insights
Login domains	8
Clusters connected via multi-cluster connectivity	12
Fabrics across all clusters connected via multi-cluster connectivity	40
Switches across all clusters connected via multi-cluster connectivity	3000
Maximum latency between any two clusters connected via multi-cluster connectivity	500ms

Verified scalability limits for Orchestrator

For Nexus Dashboard Orchestrator verified scalability limits, see Cisco Nexus Dashboard Orchestrator Verified Scalability Guide.

For Cisco ACI fabrics verified scalability limits, see Cisco ACI Verified Scalability Guides.

For Cisco Cloud ACI fabrics releases 25.0(1) and later verified scalability limits, see Cisco Cloud Network Controller Verified Scalability Guides.

Verified scalability limits for Fabric Controller

For Cisco NDFC fabrics verified scalability limits, see the Cisco Verified Scalability Guide for Cisco Nexus Dashboard Fabric Controller.

Verified scalability limits for Insights

For Nexus Dashboard Insights verified scalability limits see Nexus Dashboard Capacity Planning.

Rollup and retention numbers for Nexus Dashboard Insights telemetry

Nexus Dashboard Insights implements a multi-level roll-up strategy for the telemetry streamed that enables better management of the data. The following table provides information about roll-up and retention policy in Nexus Dashboard Insights.

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

Table 23 Rollup and retention numbers for Nexus Dashboard Insights telemetry

Statistics Name	Granularity (Time difference between sample points)	Retention proposed for Nexus Dashboard Insights
Interfaces and Protocols Statistics and Error Counters	1 minute	3 days
	5 minutes	7 days
	3 hours	30 days
Resources and Environmental Statistics	5 minutes	7 days
	3 hours	30 days
Integrations Statistics (AppDynamics)	5 minutes	7 days
	3 hours	30 days
Anomalies and Advisories	On-event*	30 days
Microburst	On-event*	7 days
Endpoints History**	On-event*	7 days
Events	On-event*	15 days
Flows and Flow Telemetry Events	-	7 days
Delta Analysis	-	30 days

*On-event: The data is sent from the switch or stored in the database only if the state of the object has changed.

** Endpoint History tracks the moves and modifications of an endpoint for last 7 days.

Related content

Additional documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, and release notes, as well as other information, which you can access at the following links:

- Cisco Nexus Dashboard
- Cisco Nexus Dashboard Orchestrator
- Cisco Nexus Dashboard Insights
- Cisco Nexus Dashboard Fabric Controller

In addition to the documentation, see the following content:

Table 24 Additional content

Document	Description
Nexus Dashboard Capacity	Provides cluster sizing guidelines based on the type and number of services you plan to run in

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

Document	Description
Planning	your Nexus Dashboard as well as the target fabrics' sizes.
Nexus Dashboard and Services Compatibility Matrix	Provides Cisco Nexus Dashboard and Services compatibility information for specific Cisco Nexus Dashboard, services, and fabric versions.
Cisco ACI YouTube channel	Contains videos that demonstrate how to perform specific tasks in the Cisco Nexus Dashboard Orchestrator.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

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 in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative context is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.

Printed in USA Cxx-xxxxxx-xx 01/20