



Cisco Nexus Dashboard Insights  
Integrations, Release 6.3.1 - For Cisco  
ACI

# Table of Contents

New and Changed Information .....	2
Integrations .....	3
About Integrations .....	3
AppDynamics Integration .....	5
About AppDynamics Integration .....	5
Guidelines and Limitations .....	6
Installing AppDynamics .....	7
Onboard AppDynamics Controller .....	7
Nexus Dashboard Insights and AppDynamics Integration Dashboard .....	8
Topology View .....	9
vCenter Integration .....	11
About VMware vCenter Server Integration .....	11
Prerequisites .....	11
Guidelines and Limitations .....	11
Add vCenter Server Integration .....	12
vCenter Virtual Machine Dashboard .....	12
vCenter Hosts Dashboard .....	16
DNS Integration .....	25
About DNS Integration .....	25
Guidelines and Limitations .....	26
Configure DNS .....	26
Nexus Dashboard Orchestrator Integration .....	29
About Nexus Dashboard Orchestrator Integration .....	29
Guidelines and Limitations .....	29
Add a Nexus Dashboard Orchestrator Live Setup .....	30
Add a Nexus Dashboard Orchestrator Using Uploaded File Method .....	31
Copyright .....	32

First Published: 2023-09-08

Last Modified: 2024-01-09

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

# New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or the new features up to this release.

*Table 1. New Features and Changed Behavior in the Cisco Nexus Dashboard Insights*

<b>Feature</b>	<b>Description</b>	<b>Release</b>	<b>Where Documented</b>
Reorganized Content	Content within this document was originally provided in the Cisco Nexus Dashboard Insights User Guide. Starting with release 6.3.1, this content is now provided solely in this document and is no longer provided in the Cisco Nexus Dashboard Insights User Guide.	6.3.1	Entire document

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at [www.cisco.com](http://www.cisco.com). For the latest version of this document, visit [Cisco Nexus Dashboard Insights Documentation](#).

# Integrations

## About Integrations

Navigate to **Admin > Integrations**.

Name	Connectivity Status	Type	IP	Last Active	Associations
dns_mapping_file	Active	DNS (Mapping File)	-	Aug 23 2023 10:42:09 AM	carid-scak2
ind-net-eag1-intel	Connected	Nexus Dashboard Orchestrator	-	-	carid07@nexus1.office.aug17, carid08@nexus1.office.aug17, carid09@nexus1.office.aug17, carid10@nexus1.office.aug17, carid11@nexus1.office.aug17, carid12@nexus1.office.aug17, carid13@nexus1.office.aug17, carid14@nexus1.office.aug17, carid15@nexus1.office.aug17, carid16@nexus1.office.aug17, carid17@nexus1.office.aug17, carid18@nexus1.office.aug17, carid19@nexus1.office.aug17, carid20@nexus1.office.aug17, carid21@nexus1.office.aug17, carid22@nexus1.office.aug17, carid23@nexus1.office.aug17, carid24@nexus1.office.aug17, carid25@nexus1.office.aug17, carid26@nexus1.office.aug17, carid27@nexus1.office.aug17, carid28@nexus1.office.aug17, carid29@nexus1.office.aug17, carid30@nexus1.office.aug17, carid31@nexus1.office.aug17, carid32@nexus1.office.aug17, carid33@nexus1.office.aug17, carid34@nexus1.office.aug17, carid35@nexus1.office.aug17, carid36@nexus1.office.aug17, carid37@nexus1.office.aug17, carid38@nexus1.office.aug17, carid39@nexus1.office.aug17, carid40@nexus1.office.aug17, carid41@nexus1.office.aug17, carid42@nexus1.office.aug17, carid43@nexus1.office.aug17, carid44@nexus1.office.aug17, carid45@nexus1.office.aug17, carid46@nexus1.office.aug17, carid47@nexus1.office.aug17, carid48@nexus1.office.aug17, carid49@nexus1.office.aug17, carid50@nexus1.office.aug17, carid51@nexus1.office.aug17, carid52@nexus1.office.aug17, carid53@nexus1.office.aug17, carid54@nexus1.office.aug17, carid55@nexus1.office.aug17, carid56@nexus1.office.aug17, carid57@nexus1.office.aug17, carid58@nexus1.office.aug17, carid59@nexus1.office.aug17, carid60@nexus1.office.aug17, carid61@nexus1.office.aug17, carid62@nexus1.office.aug17, carid63@nexus1.office.aug17, carid64@nexus1.office.aug17, carid65@nexus1.office.aug17, carid66@nexus1.office.aug17, carid67@nexus1.office.aug17, carid68@nexus1.office.aug17, carid69@nexus1.office.aug17, carid70@nexus1.office.aug17, carid71@nexus1.office.aug17, carid72@nexus1.office.aug17, carid73@nexus1.office.aug17, carid74@nexus1.office.aug17, carid75@nexus1.office.aug17, carid76@nexus1.office.aug17, carid77@nexus1.office.aug17, carid78@nexus1.office.aug17, carid79@nexus1.office.aug17, carid80@nexus1.office.aug17, carid81@nexus1.office.aug17, carid82@nexus1.office.aug17, carid83@nexus1.office.aug17, carid84@nexus1.office.aug17, carid85@nexus1.office.aug17, carid86@nexus1.office.aug17, carid87@nexus1.office.aug17, carid88@nexus1.office.aug17, carid89@nexus1.office.aug17, carid90@nexus1.office.aug17, carid91@nexus1.office.aug17, carid92@nexus1.office.aug17, carid93@nexus1.office.aug17, carid94@nexus1.office.aug17, carid95@nexus1.office.aug17, carid96@nexus1.office.aug17, carid97@nexus1.office.aug17, carid98@nexus1.office.aug17, carid99@nexus1.office.aug17, carid100@nexus1.office.aug17
nt	Down	DNS (Zone Transfer)	12.3.4.11	-	carid08
id	Inactive	DNS (Query Server)	12.3.4.12	-	ntesid-nd-a-1
NDD211	Active	Nexus Dashboard Orchestrator	172.31.161.211	Aug 23 2023 10:42:09 AM	-
AppD	Active	AppDynamics	nexusdashboardinsights-norprod-kasa.appdynamics.com:443	Aug 23 2023 10:42:09 AM	carid0-scak2, carid08, carid07

All the integrations are listed in a tabular form with the following fields:

- Name
- Connectivity Status
- Type
- IP
- Last Active
- Associations

The connected status indicates that the controller is active to fetch data. The down status indicates that the Nexus Dashboard Insights will not fetch data from the controller. Use the filter bar to search for a specific integration. You can filter based on the name and type of integration.

Click  to perform any of the following actions:

- Edit
- Delete
- Run Analysis

**Add Integration** allows you to create a new integration.

Click the integration names to view further details about the integration.



DNS Integrations are not clickable and do not have any further information to display apart from the data available in the table.

## Guidelines and Limitations

- In Nexus Dashboard Insights, Integrations are supported on both Management and Data networks.
- By default, Nexus Dashboard Insights will use Data network to connect to the Integrations such as vCenter server, DNS, AppDynamics, Nexus Dashboard Orchestrator. If you want to use Management network, you can add a specific route in Nexus Dashboard from **Admin > System Settings > General > Routes**. The route can be a /32 pointing to Integrations or a larger subnet that includes it.

# AppDynamics Integration

## About AppDynamics Integration

Cisco Nexus Dashboard Insights provides the ability to monitor the most common and complex challenges in the maintenance of infrastructure operations, which involves monitoring, troubleshooting, identification and resolving the network issues.

AppDynamics provides application performance management (APM) and IT operations analytics that helps manage the performance and availability of applications in the data center. It also provides the required metrics for monitoring, identifying, and analyzing the applications that are instrumented with AppDynamics agents.

AppDynamics is associated only at the Site level. Onboarding of the AppDynamics controller is only at the Site level.

AppDynamics hierarchy consists of the following components:

- Network Link—Provides the functional means to transfer data between network entities.
- Node—A working entity of an application and is a process running on a virtual machine.
- Tier—Grouping of nodes into a logical entity. Each tier can have one or more nodes.
- Application—A set of tiers make up an application.
- Controller—A controller consists of a set of accounts with each account comprising a list of applications. Each account in the controller is an instance.

Integrating AppDynamics allows Nexus Dashboard Insights to collect operational data and metrics of the applications monitored by AppDynamics, and then correlate the collected information with the data collected from the Cisco ACI site.

In a scenario where an application communicates through the Cisco ACI site, AppDynamics provides various metrics about the application and the network, which can be used to isolate the cause of the anomaly. The anomaly can be in the application or the underlying network. This in turn allows network operators to monitor the network activity and detect anomalies.

The AppDynamics agents are plug-ins or extensions, hosted on the application. They monitor the health, and performance of the network nodes and tiers with minimal overhead, which in turn report to the AppDynamics controller. The controller receives real-time metrics from thousands of agents and helps troubleshoot and analyze the flows.

Nexus Dashboard Insights connects to the AppDynamics controller and pulls the data periodically. This data from AppDynamics controller, rich in application specific information is fed to Nexus Dashboard Insights, thereby providing Cisco Nexus Dashboard Insights for the traffic flowing through the Cisco ACI site.

From AppDynamics, you can create your own health rule on the available metrics, which contributes to the overall anomaly score of the entity.

The integration of Nexus Dashboard Insights with AppDynamics enables the following:

- Monitoring and presenting AppDynamics hierarchy in Nexus Dashboard Insights.
- Gathering and importing network related metrics into the Nexus Dashboard Insights.
- Presenting statistics analytics, flow analytics, and topology view on the data collected from AppDynamics controller.
- Detecting anomaly trends on metrics collected from AppDynamics controller and raising anomalies on detection of such events.
- The AppDynamics integration uses API server and multiple instances of Telegraph data collecting container to support load balancing of the onboarded controllers.
- Fabric flow impact calculation for AppDynamics anomalies.

## Onboarding for SaaS or Cloud Deployments

Starting from Nexus Dashboard Insights release 6.0.2, you can connect to AppDynamics controller using a proxy for SaaS or cloud deployments. For onboarding an AppDynamics Controller running on cloud, Nexus Dashboard Insights uses proxy configured on Cisco Nexus Dashboard to connect to AppDynamics Controller.

## Guidelines and Limitations

- After Nexus Dashboard Insights upgrade, AppDynamics takes about 5 minutes to report the information in AppDynamics GUI.
- The health and count of AppDynamics business transactions displayed in the application details do not match the flow count in Nexus Dashboard Insights.
- Nexus Dashboard Insights does not support fabric topologies as transit-leaf does not have the VRF deployed and flow table in transit-leaf will not export the flow record to Nexus Dashboard Insights. Hence Nexus Dashboard Insights will not stitch the path fully and will not display complete path summary with all the information.
- To connect an HTTPS AppDynamics controller using an HTTP proxy you must configure HTTPS proxy in Nexus Dashboard with the HTTP proxy server URL address.
- To connect an HTTP AppDynamics controller using an HTTP proxy you must configure HTTP proxy in Nexus Dashboard with the HTTP proxy server URL address.
- Configuration import and export are not supported for AppDynamics integrations.
- Scale limits for AppDynamics integration:
  - Number of apps: 5
  - Number of tiers: 50
  - Number of nodes: 250
  - Number of net links: 300
  - Number of flow group: 1000



# Installing AppDynamics

Before you begin using Nexus Dashboard Insights **Integrations**, you must install AppDynamics Application Performance Management and Controller. See [Getting Started](#) for details.


## Onboard AppDynamics Controller

Use this procedure to onboard a AppDynamics Controller on to Nexus Dashboard Insights using GUI. For Cisco Nexus Dashboard Insights and AppDynamics integration, the Cisco Nexus Dashboard's data network must provide IP reachability to the AppDynamics controller. See the [Cisco Nexus Dashboard Deployment Guide](#).

### Before you begin

- You must have installed AppDynamics application and controller.
- You must have administrator credentials for Nexus Dashboard Insights.
- You must have user credentials for AppDynamics controller.
- You must have configured proxy on Nexus Dashboard to connect to AppDynamics controller using a proxy. See section **Cluster Configuration** in the [Cisco Nexus Dashboard User Guide](#)

### Procedure

1. Click **Admin > Integrations > Add Integration**.
  2. Select **App Dynamics** for **Integration Type**.
  3. AUTHENTICATION
    - Enter Controller Name, Controller IP or Hostname, Controller Protocol and Controller Port. Controller Name can be alphanumeric and spaces are not allowed.
- 
- AppDynamics Controller Name cannot be the same name as Nexus Dashboard site name.
- Check the **Enable** checkbox to connect to AppDynamics controller using a proxy. The proxy must be configured on Nexus Dashboard.
    - Enter AppDynamics Account Name, User Name, and Password.
  4. ASSOCIATIONS
    - Select a site or multiple sites. You can view the number of anomalies for each severity level, SW Analytics, Flow Collection, and the Anomaly Trend for each site before selecting it.
    - Click **Select**
  5. The Summary displays an overview of the Integration created.
  6. Click Submit to add the integration. The post completion success screen allows you to **Add Another Integration** or **View Integrations**. When the **Status** is Connected, the onboarding for the controller is complete.

Each controller supports multiple account names for the same host name. Each account name supports multiple applications monitored by the controller. Therefore, a controller can support multiple applications monitored by AppDynamics.

## Nexus Dashboard Insights and AppDynamics Integration Dashboard

The AppDynamics Dashboard allows you to onboard controllers and presents a view of the **Top 5 Applications by Anomaly Score** along with various metrics. Once a controller is onboarded, data related to applications monitored by that controller is pulled by Nexus Dashboard Insights. It can take up to 5 minutes for the first set of data to appear on the GUI. The AppDynamics health state information provided for each entity is aggregated and reported by Nexus Dashboard Insights on the dashboard.


The AppDynamics dashboard displays the overview of the applications monitored by the AppDynamics controller.

- **Controller Connectivity** - represents the number of integrations that are **Up** or **Down**.
- **Anomalies by Severity** — The Nexus Dashboard Insights runs statistical analytics on the metrics received from the AppDynamics controller.
- **Top 5 Applications by Anomaly Score** - displays top five out of all the applications based on the anomaly score.
- **Anomalies by Severity** - to see the Anomalies page.
- **Application Widget** - displays the top application by anomaly score. This includes the anomaly score of the application as computed in Nexus Dashboard Insights, health state of tiers and nodes as reported by AppDynamics. Click the widget for additional details about the monitored application.

### AppDynamics Integration Application

Detailed information including operational, statistics, and metrics, for each tier or application is also presented.

- **Summary** lists the anomaly score, controller name, account, application name, number of tiers, number of nodes, throughput, TCP loss, and errors.
- **Analyze Anomaly** details displays estimated impact application, recommendations, mutual occurrences, and other details affected by the anomaly. Click an anomaly in the summary to display additional details.
- **View Report** displays the flow groups affected where each flow group can correspond to multiple fabric flows. View reports also display the proxy/entity IP address, node source, and node destination IP address.
- **Number of Tiers** to list the available tiers. Click each tier from the list to display health score, number of nodes, and usage statistics.

- **Number of Nodes** to list the available nodes. Click each node from the list to display statistics about the node.
- **Application Name** to display additional details such as general information of the application, controller name, controller IP, account name, health of the tier, health of the node, business transaction health, and usage analytics.
-  icon to open **AppDynamics Application** details. This displays application statistics details such as anomaly score, application tiers summary, application nodes summary, network charts for the node communication, and summary table of anomalies.
- **Application Network Links** table shows how the different components of AppDynamics application network flow map are communicating among each other. Detailed information about a network link, including flow counts and anomalies are used for further analysis.
- **AppDynamics Application View** shows the summary for the particular AppDynamics monitored application to display page.

## AppDynamics Application View

The AppDynamics Application View presents an overview of the application health state including tier health, node health, and business transaction health.

- **Application Statistics** displays the graphical representation of the flow properties and a timeline graph representing the properties.
- **Tiers** displays the health state of the tiers in the application. Click each row in the tier section for the side panel to display additional tier usage details.
- **Nodes** displays the health state of the nodes in the application. Click each row in the node section for the side panel to display additional node usage details.
- **Application Network Links** displays the link summary for the nodes.
- **Network Connection** displays additional flow connection details.
- **Browse Network Flows** to navigate to **Browse Flows Records** with the flow properties set in the filter.
- **Anomalies** summarizes the anomalies with severity and other essential details of the anomaly. Click each row in the **Anomalies** section to see additional details of the anomaly.
- **Analyze** for in-depth analysis, mutual occurrences, estimated impact, lifespan, and recommendations on the anomaly.

## Topology View

The topology view represents the stitching between nodes where these nodes are connected to the Cisco ACI site.

The topology view includes application nodes and leaf nodes. Toggle between show or not show to view/hide the nodes with anomaly score. The anomaly score is represented by the dot in the topology.

The topology view represents a hierarchical view of **Application > Node > Cisco ACI Leaf** and the

links between them with a logical or network view of how various objects are related.

## **AppDynamics Anomalies**

From AppDynamics application, you can create your own health rule on the available metrics, which contributes to the overall anomaly score of the entity. If the health rules are violated and a violation is generated by the AppDynamics controller, then Nexus Dashboard Insights pulls these health violations and generates anomalies on these violations.

The anomalies in the summary table include the following:

- Anomalies raised on the metrics from the AppDynamics controller.
- Health violation on the network metrics that the AppDynamics controller raised.
- Anomalies at the application level and node level.

If there is an anomaly on the interface of application(s) impacted by the interface, then an anomaly is identified and shown.

Depending on the anomaly score and the level at which the anomaly occurs, the corresponding flows impacted are identified. Information related to the flow metrics with the Cisco ACI leaf information enable statistics analytics, pin point the source of the anomaly, whether it is the application or network, and the impacted entities.

The fabric flow impact calculation for AppDynamics anomalies calls flow APIs to fetch the fabric flows corresponding to the AppDynamics flow groups that were affected by the anomaly. Nexus Dashboard Insights app displays the top 100 fabric flows ordered by the anomaly score for AppDynamics anomalies.

# vCenter Integration

## About VMware vCenter Server Integration

Integrating VMware vCenter server allows Nexus Dashboard Insights to collect data and metrics of the virtual machines and hosts monitored by VMware vCenter, and then correlate the collected information with the data collected from the Cisco ACI or Cisco NDFC fabric.

Data collected from vCenter includes

- Virtual machine data
- Network data
- Virtual machine NIC data
- Host data
- Datastore data
- Standard switch information
- DVS information
- vCenter Alarms

Nexus Dashboard Insights collects data from vCenter every 15 minutes. A system anomaly is raised if Nexus Dashboard Insights is unable to reach vCenter.

### vCenter Anomalies

In Nexus Dashboard Insights, the alarms from vCenter are displayed as anomalies. The following types for anomalies are generated for vCenter Integration in the category **vCenter**.

- Host, VM, and Datastore alarms from vCenter
- Baseline anomalies for checks such as CPU, memory, storage
- Threshold anomalies

### Prerequisites

- You have installed VMware vCenter 6.5 and later.
- You have read-only privileges for VMware vCenter.

### Guidelines and Limitations

- Number of VMs supported for VMware vCenter integration is 1000.
- Number of vNIC hosts supported for VMware vCenter integration is 10,000.
- In Nexus Dashboard Insights release 6.3.1.15 and 6.3.1.40 only a single vCenter per site is supported.

- In Nexus Dashboard Insights release 6.3.1.44 and later multiple vCenters per site are supported.

## Add vCenter Server Integration

1. Click **Admin > Integrations > Add Integration**.
2. Select **vCenter Server** for the **Integration Type**.
3. Complete the following fields for **AUTHENTICATION**.
  - a. Enter Controller Name, Controller IP or Hostname, and Controller Port. Controller Name can be alphanumeric and spaces are not allowed.
  - b. Enter vCenter Username and Password.
4. Complete the following fields for **ASSOCIATIONS**.
  - a. Select a site. You can view the number of anomalies for each severity level, SW Analytics, Flow Collection, and the Anomaly Trend for each site before selecting it.
  - b. Click **Select**.
5. The Summary displays an overview of the Integration created.
6. Click **Submit** to add the integration. The post completion success screen allows you to **Add Another Integration** or **View**.

## vCenter Virtual Machine Dashboard

Select **Virtual Machines**. Select the timeline.

The dashboard presents the **Top Virtual Machines** by CPU plotted on a timeline. From the drop-down list, select CPU, memory, storage, or network usage to view the graphical representation of the top virtual machines based on drop-down list selection.

Use the filter bar to filter by vCenter IP, vCenter Controller, VM, Host, State, Status, Guest OS, DNS Name, Datacenter, Network Adapters, Network Usage, CPU, Memory, and Storage.

Use the following operators for the filter refinement:

Operator	Description
==	With the initial filter type, this operator, and a subsequent value, returns an exact match.
!=	With the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
contains	With the initial filter type, this operator, and a subsequent value, returns all that contain the value.

Virtual Machines also displays the virtual machines in a tabular format.

The **Virtual Machines** table displays the following information:

- Anomaly Score
- vCenter IP address
- Virtual machine IP address
- State
- Network Adapters
- IP address
- Network Usage
- CPU
- Memory
- Storage

The **Gear** icon to customize the columns to be displayed in the table.

Select any entry in the table to display the additional details:

- **Anomaly score** categorized by Critical, Major, Minor and Warning.
- **General Information** like State, Status, Guest OS, DNS Name, Host, IP Addresses, VCenter, Datacenter, and Network Adapters.
- **Usage graphs** for CPU, Memory, Storage and Network.
- **Storage** which displays the number of Datastores.

## Virtual Machine Details

Virtual machine details can be navigated to in two ways:

Click any VM name in the table to view details

OR

Click the  icon (Expand Icon) after clicking any row in the table to view details.



The details mentioned below consist of all the data available in both the views of Virtual Machine Details.

### Overview

The overview section displays the following information:

- Host IP address to view details for the selected host.

See [vCenter Hosts Dashboard](#) for more information.

- The "+" under IP addresses to view all the addresses for the virtual machine.

- The usage graph can be viewed as separate graphs for each type of virtual machine or as a cumulative graph of all virtual machines.

### ***Datstore***

Click the datastore name to view the Status, Type, Cluster, Hosts, Virtual Machines and the Usage graph for the datastore selected.

### ***Adapter State***

The adapter state shows details for network adapters.

### ***Port Group***

Click the number for port groups to view the entire list of port groups available. Select any of the port groups to view details.



The information available for the port group listed is the same as the information available from Overview.

### **Alerts**

Alerts displays the alarms from vCenter. In Nexus Dashboard Insights, the alarms from vCenter are displayed as anomalies. From the **Actions** drop-down menu, select an action to configure properties on an anomaly. The alerts can be filtered based on the following:

- Acknowledgement
- Anomaly ID
- Assignee
- Category
- Check Code
- Comment
- Description
- Detection Time
- Entity Name
- Last Seen Time
- Nodes
- Severity
- Status
- Sub-category
- Tags
- Title
- Verification Status



- IP Address
- MAC Address
- Interface
- VPC
- EPG
- VRF
- BG

## Topology

Topology represents a hierarchical view of **virtual machine > host > leaf switch** in the fabric and the links between them with a logical or network view of how various objects are related.

When there is an intermediate switch between the host and the leaf switch, the leaf switch in the host topology view is displayed as detached. Nexus Dashboard Insights is unable to determine the attached leaf switch port in such topologies. This will affect Cisco UCS B Series Blade Servers that have fabric switches between host blades and leaf switches, and it will also affect any other topologies with intermediate switches.

Topology can be filtered for the following different objects:

- Host
- Datastore
- DVS
- Network
- VM Network
- VSS
- Leaf
- Application

Click any of the nodes to view more information about it.

## Trends and Statistics

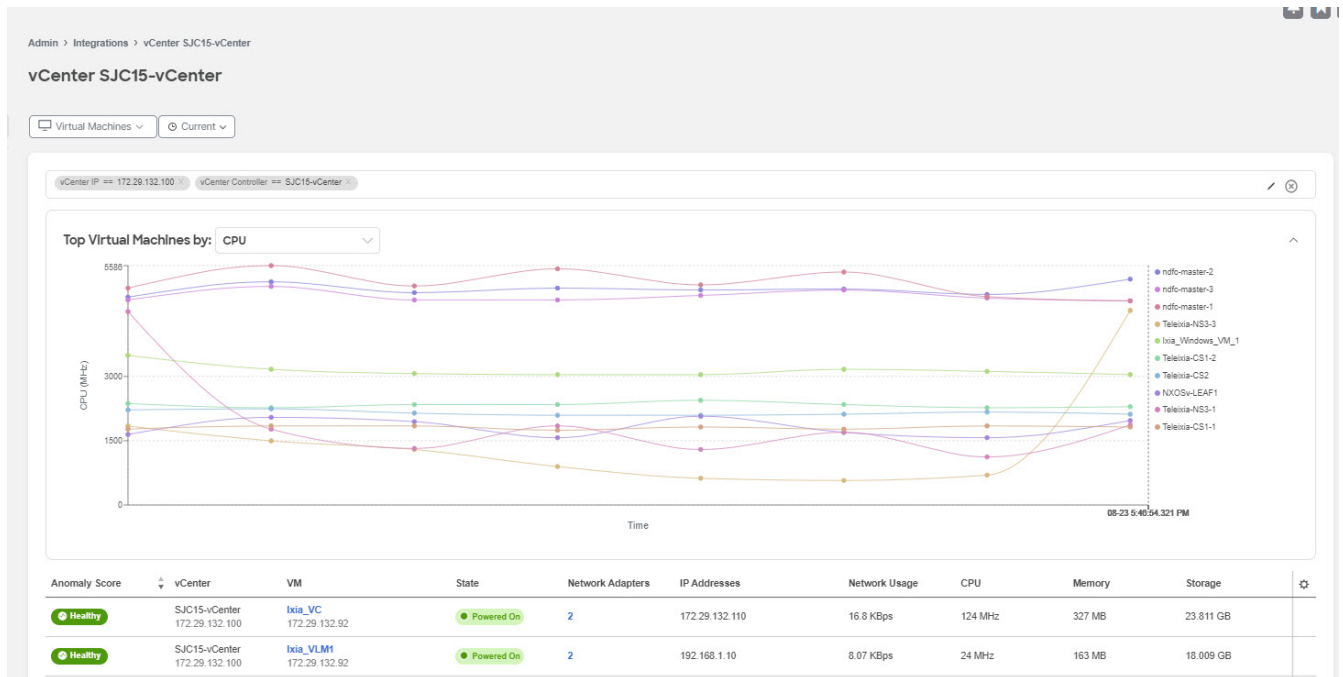
Trends and Statistics displays the usage graphs for CPU, Memory, Storage and Network. It can be viewed as separate graphs for each type of virtual machine or as a cumulative graph for all.

## Anomalies

See [Anomalies and Advisories](#) for more information.

# vCenter Hosts Dashboard

Select **Hosts**. Select the timeline.



The dashboard presents the **Top Hosts** by CPU plotted on a timeline. From the drop-down list, select CPU, memory, storage, or network usage to view the graphical representation of the top virtual machines based on drop-down list selection.

Use the filter bar to filter by vCenter IP, vCenter Controller, VM, Host, State, Status, Guest OS, DNS Name, Datacenter, Network Adapters, Network Usage, CPU, Memory, and Storage.

Use the following operators for the filter refinement:

Operator	Description
==	With the initial filter type, this operator, and a subsequent value, returns an exact match.
!=	With the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
contains	With the initial filter type, this operator, and a subsequent value, returns all that contain the value.

Hosts also displays the hosts in a tabular format.

The **Hosts** table displays the following information:

- Anomaly Score
- vCenter IP address

- Host IP address
- State
- NVirtual Machines
- Cluster
- Network Usage
- CPU
- Memory
- Storage

The **Gear** icon can be used to customize the columns to be displayed in the table.

Select any entry in the table to display the additional details:

- **Anomaly score** categorized by Critical, Major, Minor and Warning.
- **General Information** like State, Status, Guest OS, DNS Name, Host, IP Addresses, VCenter, Datacenter, and Network Adapters.
- **Usage graphs** for CPU, Memory, Storage and Network.
- **Storage** which displays the number of Datastores.

## Hosts Details

Host details can be navigated to in two ways:

Click any host name in the table to view details

OR

Click the  icon (Expand Icon) after clicking any row in the table to view details



The details mentioned below consist of all the data available in both the views of Host Details.

### Overview

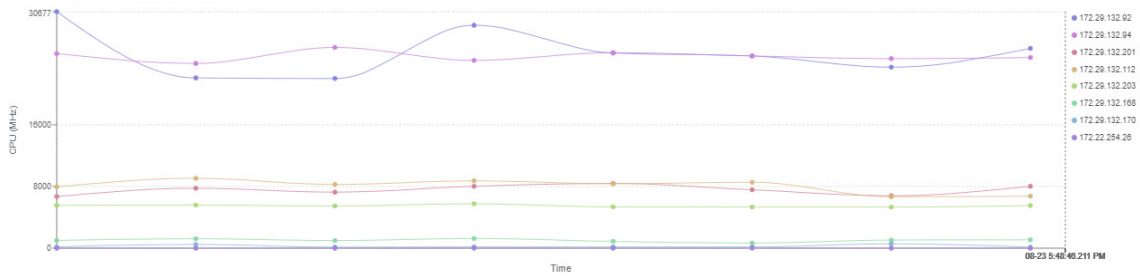
Overview displays the general information for the host along with the Anomaly Score, and tables listing the Virtual Machines, Datastores, Standard Switches, and Distributed Switches.

## vCenter SJC15-vCenter

Host ▾ Current ▾

vCenter IP == 172.29.132.100 vCenter Controller == SJC15-vCenter

Top Hosts by: CPU ▾



Anomaly Score	vCenter	Host	State	Virtual Machines	Cluster	Network Usage	CPU	Memory	Storage
Healthy	SJC15-vCenter 172.29.132.100	172.29.132.92 NXOS_NAE_SYSTEST	Connected	11	-	1.73 MBps	25.91 of 139.66 GHz	490.22 of 523.63 GB	2.95 of 3.12 TB
Healthy	SJC15-vCenter 172.29.132.100	172.29.132.203 NDFC	Connected	1	-	3.92 MBps			

### Host 172.29.132.92

Overview Anomalies Topology Trends and Statistics

#### Anomaly Score

**No anomalies found**

No anomalies found

#### General Information

Name	State	Status	Cluster	Up Time	Physical Adapters	Datacenter	Hypervisor	Model	Processor Type
172.29.132.92	Connected	Warning	-	134 Days	10	NXOS_NAE_SYSTEST	VMware ESXi 6.7.0 build-20497097	UCSC-C240-M5SX	Intel(R) Xeon(R) Platinum 8180M CPU @ 2.50GHz
Logical Processors	112								

#### VMs

Anomaly Score	vCenter	VM	State	Status	Network Adapters	IP Addresses	Network Usage	CPU	Memory	Storage
Healthy	SJC15-vCenter 172.29.132.100	Ixia_VC	Powered On	Normal	2	172.29.132.110	16.8 KBps	124 MHz	327 MB	23.811 GB
Healthy	SJC15-vCenter 172.29.132.100	Ixia_VLM1	Powered On	Normal	2	192.168.1.10	8.07 KBps	24 MHz	163 MB	18.009 GB
Healthy	SJC15-vCenter 172.29.132.100	Teleixia-NS3-1	Powered On	Normal	1	172.29.132.212	149.8 KBps	1.87 GHz	6.39 GB	248.086 GB
Healthy	SJC15-vCenter 172.29.132.100	Teleixia-NS3	Powered On	Normal	1	172.29.132.211	149.8 KBps	897 MHz	4.92 GB	248.086 GB
Healthy	SJC15-vCenter 172.29.132.100	Teleixia-NS3-2	Powered On	Normal	1	172.29.132.213	105.13 KBps	1.47 GHz	6.39 GB	248.085 GB

### Datstores


Filter

Name	Status	Type	VMs	Hosts
datstore1 (1)	Critical	VMFS	11	1

10 Rows Page 1 of 1 << 1-1 of 1 >>

### Distributed Switch

Filter

  
No data

### Standard Switch

Filter

## ***Physical Adapters***

Click the number for Physical Adapters to view the entire list of adapters available. Select any of the adapters to view details like:

- Link Status
- Protocol
- Interface
- Node
- Chassis ID
- Management Address
- Usage graphs for Network, Network Broadcast and Network Multicast

**Physical Adapters - 172.29.132.92**

Search

- vmnic3
- vmnic0
- vmnic1
- vmnic2
- vmnic4
- vmnic5
- vmnic6
- vmnic7
- vmnic8
- vmnic9

Status	Network
● Normal	2
● Normal	2
● Normal	1
● Normal	1
● Normal	1

Physical Adapter  
**vmnic3**

**General Information**

Link Status  
● 10 Gbps, Full

**Neighbor**

Protocol  
**cdp**

Interface  
[eth1/10](#)

Node  
[CANDID-SYS-S3-L1](#)

Chassis ID  
-

Management Address  
**172.29.132.175**

**Usage**

Network Usage  
0 KBps →

### Network Adapters

Click the number for Network Adapters to view the entire list of adapters available. Select any of the adapters to view details like Endpoint address, Port Group, Type, Virtual Switch, VLAN, Adapter State, Physical Adapters, IP Addresses. Click on the Expand icon to view more details.

### VMs

Click the number for VMs to view the entire list of virtual machines available. Select any of the virtual machines to view details.

## Virtual Machines - datastore1 (1)



<b>DCNM_11.5</b> NXOS_NAE_SYSTEST
<b>DCNM_11.5_Compute_Standby</b> NXOS_NAE_SYSTEST
<b>lxia_VC</b> NXOS_NAE_SYSTEST
<b>lxia_VLM1</b> NXOS_NAE_SYSTEST
<b>lxia_Windows_VM_1</b> NXOS_NAE_SYSTEST
<b>lxia_Windows_VM_3</b> NXOS_NAE_SYSTEST
<b>NXOS-ISE</b> NXOS_NAE_SYSTEST
<b>Telelxia-NS3</b> NXOS_NAE_SYSTEST
<b>Telelxia-NS3-1</b> NXOS_NAE_SYSTEST
<b>Telelxia-NS3-2</b> NXOS_NAE_SYSTEST
<b>Telelxia-NS3-3</b> NXOS_NAE_SYSTEST

Virtual Machine  
**DCNM\_11.5**

0 Critical

0 Major

0 Minor

0 Warning

### General Information

State  
**Powered On**

Status  
**Normal**

Guest OS  
**CentOS 4/5/6/7 (64-bit)**

DNS Name  
**candid-sys-nxos-dcnm-11-5.cisco.com**

Host  
**172.29.132.92**

IP Addresses  
**6**

VCenter  
**172.29.132.100**

Datacenter  
**NXOS\_NAE\_SYSTEST**

Network Adapters  
**3**

### Hosts

Click the number for hosts to view the entire list of hosts available. Select any of the hosts to view details.

The screenshot shows a web interface for monitoring hosts. On the left, a search bar contains the text '172.29.132.92' and 'NXOS\_NAE\_SYSTEST'. On the right, the host details for 'Host 172.29.132.92' are displayed. At the top right of the details panel, there are four status indicators: '0 Critical' (red), '0 Major' (orange), '0 Minor' (yellow), and '0 Warning' (green). Below these, the 'General Information' section includes: State (Connected), Up Time (134 Days), Status (Warning), Cluster (-), Hypervisor (VMware ESXi 6.7.0 build-20497097), Model (UCSC-C240-M5SX), Processor Type (Intel(R) Xeon(R) Platinum 8180M CPU @ 2.50GHz), and Logical Processors (112). The 'Usage' section is partially visible at the bottom.



The information available for the host listed is the same as the information available from the Host Details screen.

## Anomalies

Anomalies displays the list of anomalies. The anomalies can be viewed as grouped or ungrouped and can be viewed for a selected timeline.

See [Anomalies and Advisories](#) for more information.

## Topology

Topology represents a hierarchical view of **virtual machine** > **host** and the links between them with a logical or network view of how various objects are related.



OPTIONS

Show Lines

Show Names

OBJECTS

D Datastore 1

DVS 0

H Network 0

VM Virtual Machines 11

VSS 0

Leaf 1

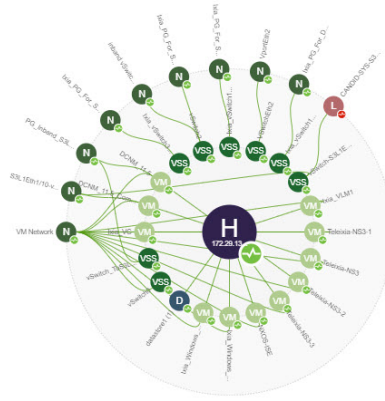
ANOMALY SCORE

Healthy 20

Warning 0

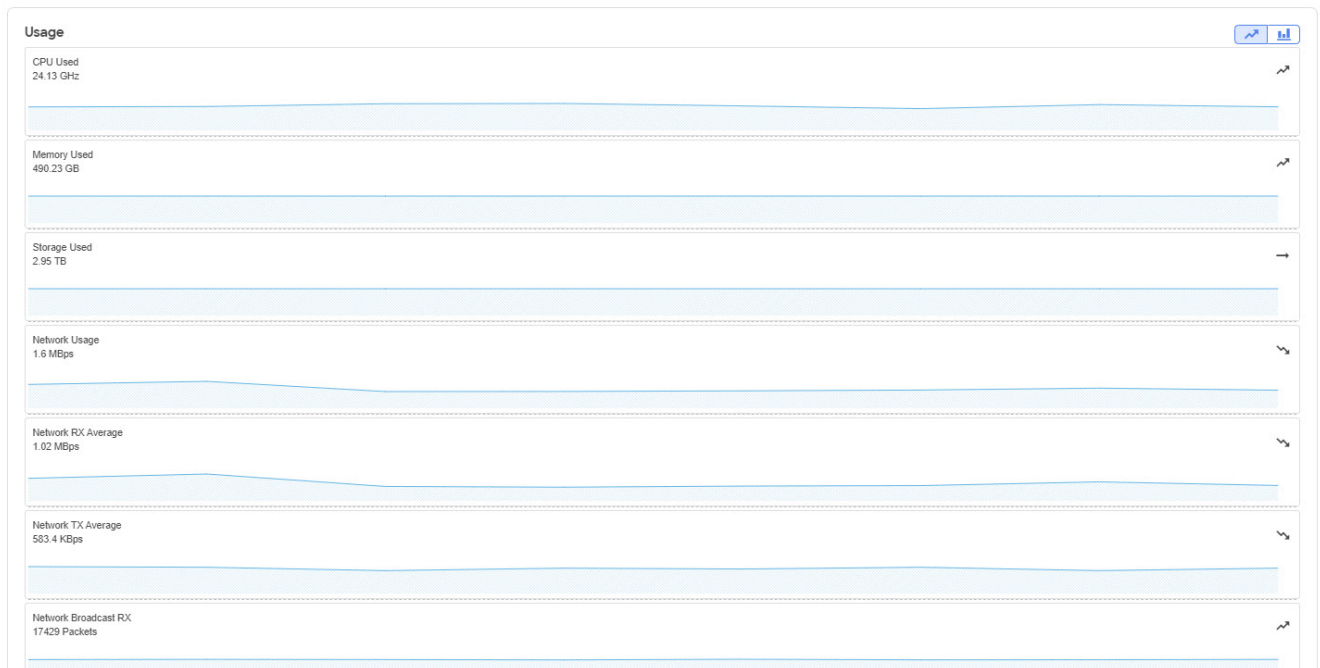
Major 0

Critical 1



## Trends and Statistics

Trends and Statistics displays the usage graphs for Network, Network Broadcast and Network Multicast and can be viewed as separate graphs for each type of network or as a cumulative graph of all networks.



## Alerts

Alerts displays the alarms from vCenter. In Nexus Dashboard Insights, the alarms from vCenter are displayed as anomalies. From the **Actions** drop-down menu, select an action to configure properties on an anomaly. The alerts can be filtered based on the following:

- Acknowledgement
- Anomaly ID

- Assignee
- Category
- Check Code
- Comment
- Description
- Detection Time
- Entity Name
- Last Seen Time
- Nodes
- Severity
- Status
- Sub-category
- Tags
- Title
- Verification Status
- IP Address
- MAC Address
- Interface
- VPC
- EPG
- VRF
- BG

# DNS Integration

## About DNS Integration

The Cisco Nexus Dashboard Insights Domain Name System (DNS) integration feature enables the name resolution feature to telemetry data. DNS integration can be associated at the Site level.

For DNS integration you can use any of the following 3 data source methods:

### DNS File Upload

This method is simple because mappings do not change often. In the GUI, you can upload a file containing mappings. Use one of the supported formats (.csv and .json). Cisco Nexus Dashboard Insights verifies the integrity of the file.

If no VRF, or Site name, or Tenant information is specified, DNS will be applied to the sites for which the DNS server is configured based on the selections in **Add Integrations** and **Associations** section. If the DNS server is configured for a site, then DNS will be applied to all the sites in the group.

The DNS file upload size is limited to 1.8 MB.

### DNS Query

Use this method one query at a time to retrieve data from the DNS server using reverse lookup. Reverse lookup zone(s) must be configured on the DNS server.

Cisco Nexus Dashboard Insights queries the DNS server at regular intervals and resolves IP addresses that are learned using endpoints.

Cisco Nexus Dashboard Insights allows one primary and multiple secondary DNS servers, the primary DNS server will be polled first. If the resolution does not succeed, the secondary servers will be polled thereafter.

### DNS Zone Transfer

DNS Zone Transfer is also known as AXFR downloads. Nexus Dashboard Insights can retrieve zone data in bulk from the DNS server using AXFR downloads. This method is convenient for large quantities of data as you no longer have to work on one query at a time.

A zone transfer requires at least one DNS zone. If you configure a forward mapping zone, then all the A and AAAA records will be fetched from a DNS server if you configure a reverse mapping zone, then PTR records will be fetched. When onboarding the DNS server, you must provide a list of zones from which to fetch the data. Cisco Nexus Dashboard Insights will fetch the data from each zone configured from the DNS server.

TSIG (transaction signature) is a computer-networking protocol defined in RFC 2845. Primarily it enables the DNS to authenticate updates to a DNS database. For a secure transfer, Cisco Nexus Dashboard Insights allows you to configure the TSIG key for a zone to initiate the transaction.

Configure the zone with the TSIG key, and an associated algorithm. In the Cisco Nexus Dashboard Insights GUI, the supported algorithms are displayed in a drop-down list.

When you delete an onboarded DNS server, all the zones will be un-configured automatically. A zone can be a forward mapping or a reverse mapping zone.

When information is changed on the DNS server it may take up to 3 hours to update corresponding name mappings on Cisco Nexus Dashboard Insights. During that interval, the old name will be displayed for endpoints until the sync is completed.

## Guidelines and Limitations

- DNS onboarding can be done at a site level.
- Only one type of DNS integration method is supported in one site. For example, in a site, you cannot configure using DNS file uploads as well as DNS Zone Transfer methods.
- Multiple DNS integration onboarding of the same type is allowed in a site. For example, multiple files can be onboarded, to a site using the DNS file uploads method.
- If you perform DNS integration onboarding for multiple sites, you cannot also onboard a site in that group.
- When a corrupted or malformed .CSV or .JSON file is uploaded to the DNS server, Cisco Nexus Dashboard Insights raises system anomalies. However, the connectivity status of the third-party onboarding server, remains in the initialized state and does not change to display a failed state. If the third-party onboarding server remains in the initialized state, check the system anomalies for any anomalies related to the specific integration.
- The supported scale for DNS integration is 40,000 DNS entries. For vND application profiles, the supported scale for DNS integration is 10,000 DNS entries.
- Data from DNS servers will be polled or refreshed every 3 hours. So, any changes in the mapping on the DNS server will reflect after the next polling cycle.

## Configure DNS



The .json or .csv file used in this task must be uploaded in a specific schema. See the following section for the formats to use.

1. Click **Admin** > **Integrations** > **Add Integration**.
2. Select **DNS** for the **Integration Type**.
3. In the **Authentication** section, select one of the following DNS types to view the corresponding fields:
  - a. Zone Transfer - Enter the **Name**, **DNS Server IP**, **DNS Server Port**, and **Zones**. In the **Zones** area, enter the value for Zone Name. Optional values that can be entered are TSIG Key Name, TSIG Key Value, TSIG Algorithm. The **TSIG Algorithm** dropdown menu selections are hmac-sha1, hmac-sha256, hmac-sha512, hmac-md5.

- b. Query Server - Enter the **Name**, **DNS Server IP**, **DNS Server Port**, and **Secondary Servers**.
  - c. Mapping File - Enter the **Name**, **Description**, and **Upload a JSON or CSV file**.
4. In the **Associations** area, click **Add Associations** to associate a site or multiple sites. The Summary displays an overview of the Integration created.
  5. Click Save to add the integration. The post completion success screen allows you to **Add Another Integration** or **View Integrations**.

## Edit or Delete DNS Configuration

To edit your DNS configuration, click the Actions icon and click **Edit**. When you have completed editing, click **Add**.

To delete your DNS configuration, click the Actions icon and click **Delete**.

## Formats for Files Used in DNS File Uploads

When configuring the DNS file uploads, .json and .csv formats are supported. Use the formats provided below for the files that you upload.

The fields in a DNS file upload can have optional VRF, or Site name, or Tenant information. If you specify details for one of these options you must specify all of them. If you have a file that contains the site name, you must specify the VRF and Tenant also.

### Format .json

```
[
  {
    "recordType": "dnsEntry",
    "fqdn": "host1.cisco.com",
    "ips": ["1.1.0.0"],
    "vrf": "vrf-1",
    "siteName": "swmp3",
    "tenant": "tenant-1"
  },
  {
    "recordType": "dnsEntry",
    "fqdn": "host2.cisco.com",
    "ips": ["1.1.0.1"],
    "vrf": "vrf-1",
    "siteName": "swmp3",
    "tenant": "tenant-1"
  }
],
  {
    "recordType": "dnsEntry",
    "fqdn": "host3.cisco.com",
    "ips": ["1.1.0.2"],
  },
]
```

## Format .csv

```
recordType,fqdn,ips,siteName,tenant,vrf  
dnsEntry,swmp3-leaf1.cisco.com,"101.22.33.44",swmp3,tenant-1,vrf-1  
dnsEntry,swmp5-leaf1.cisco.com,"10.2.3.4,10.4.5.6,1.2.3.4",fabric2,tenant-2,vrf-2  
dnsEntry,swmp4-leaf1.cisco.com, "1.1.1.1",,,
```

# Nexus Dashboard Orchestrator Integration

## About Nexus Dashboard Orchestrator Integration

Click the NDO integration type to view a slide in with the following information:

- Name
- Connectivity status
- Type
- IP
- Last Update
- Associations
- Managed Sites

With Nexus Dashboard Orchestrator assurance, you have the following features available:

- Explore site-to-site connectivity
- See anomalies specific to Nexus Dashboard Orchestrator
- Raise anomalies for inconsistencies across sites
- See the aggregated anomalies for single or multiple sites
- See anomalies for individual sites

For details about Nexus Dashboard Orchestrator Assurance for Explore Workflows, see [Explore for Nexus Dashboard Orchestrator Assurance](#).

## Guidelines and Limitations

- You must have at least one site added in Nexus Dashboard Insights before you integrate Nexus Dashboard Orchestrator with Nexus Dashboard Insights.
- If, at a later time, you add additional sites that are managed by Nexus Dashboard Orchestrator, Nexus Dashboard Insights will automatically incorporate assuring the added sites.
- If a site is Nexus Dashboard Orchestrator assured, then for each site you must associate a unique Nexus Dashboard Orchestrator instance. You cannot add multiple Nexus Dashboard Orchestrators to one site. Neither can you add multiple sites to one Nexus Dashboard Orchestrator.
- A Site must contain at least one of the sites that will be assured by Nexus Dashboard Orchestrator before you associate the Nexus Dashboard Orchestrator.
- After you create an Nexus Dashboard Orchestrator integration with a live setup, you cannot edit the integration.
- After you upload a file with an Nexus Dashboard Orchestrator integration and run assurance on it, you can swap the already uploaded file for a new file if desired. However, when you run

Nexus Dashboard Orchestrator assurance analysis on an uploaded file, it looks for the latest snapshots of the uploaded file/s in the site.

- For uploaded files, to run snapshot analysis for Inter-Site Assurance after you have run the analysis once, you must first **Run Snapshot Analysis** on the individual sites, and then you will be able to click **Run Snapshot Analysis** for Inter-Site Assurance.

## Add a Nexus Dashboard Orchestrator Live Setup

### Before you begin

You must have at least one site added in Nexus Dashboard Insights before you integrate Nexus Dashboard Orchestrator with Nexus Dashboard Insights. This is required because when you integrate Nexus Dashboard Orchestrator, you must associate a site.

### Procedure

1. Click **Admin > Integrations > Add Integration**.
2. Select **Nexus Dashboard Orchestrator** for the **Integration Type**.
3. In the **Authentication** area, perform the following actions:
  - a. In the **Orchestrator Data Collection Type** field, choose **Live Setup**.
  - b. In the **Orchestrator Name** field, enter the name.
  - c. In the **Orchestrator IP or Hostname** field, enter the Orchestrator IP address or the hostname.
  - d. In the **User** and **Password** fields, enter the Orchestrator username and password credentials.
4. Click Save to add the integration. The post completion success screen allows you to **Add Another Integration** or **View Integrations**.



The admin account must be used to perform these actions. Enter your Nexus Dashboard Orchestrator username and password values.

5. In the **Associations** area, click **Add Associations** to associate the appropriate Site.



The sites may be a subset of all the sites that are managed by Nexus Dashboard Orchestrator. It is not necessary that all the sites that belong to a group are managed by Nexus Dashboard Orchestrator. There may be sites in this list that are part of the group but are not managed by Nexus Dashboard Orchestrator.

6. The Summary displays an overview of the Integration created.

To configure assurance analysis for a Nexus Dashboard Orchestrator, navigate to **Sites > Integrations > Analyze Now > Assurance**.



# Add a Nexus Dashboard Orchestrator Using Uploaded File Method

You upload the file in the **Add New Site** step.

## Before you begin

For Orchestrator Data Collection Type, you must have at least one site with an uploaded file added in Nexus Dashboard Insights before you integrate Nexus Dashboard Orchestrator with Nexus Dashboard Insights. This is required because when you integrate Nexus Dashboard Orchestrator, you must associate a site.

## Procedure

1. Navigate to **Admin > Integrations > Add Integration**.
2. Select **Nexus Dashboard Orchestrator** for the **Integration Type**.
3. AUTHENTICATION
  - In the **Orchestrator Data Collection Type** field, choose **Upload file**.



Make sure to upload only those files that are part of your sites and that are managed by Nexus Dashboard Orchestrator.

- In the **Integration Name** field, enter the name of the orchestrator.
  - Upload the required JSON or CSV file.
4. In the **Associations** area, click **Add Associations** to associate the appropriate Site.



There may be sites in this list that are part of the group but are not managed by Nexus Dashboard Orchestrator.

5. The Summary displays an overview of the Integration created. Click **Save** to add the integration. The post completion success screen allows you to **Add Another Integration** or **View Integrations**.

# Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

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.

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: <http://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)

© 2017-2024 Cisco Systems, Inc. All rights reserved.