Release Notes for Cisco Optical Network Controller, Release 24.3.1

First Published: 2024-10-01

Cisco Optical Network Controller Overview

Cisco Optical Network Controller is an SDN Domain Controller for Cisco Optical Networks. Optical Network Controller collects optical data which is used to provide network information in an abstracted format to higher layer controllers. This abstraction enables a centralized control of a Cisco Optical Network.

Some of the features of Cisco Optical Network Controller are:

- Serves as a domain controller for optical products and provides data to Hierarchical Controllers. Optical Network Controller supports a standardized TAPI model which enables it to abstract the device level details from hierarchical controller.
- As a Provisioning Network Controller (PNC), monitors the topology (physical or virtual) of the network, and collects information about the topology, and setup/teardown of optical circuits.
- PCE service provides optical path computation to other Cisco Optical Network Controller services.

Note For more details on how to model an alien wavelength or transceiver, etc through Cisco Optical Network Planner see Cisco Optical Network Planner Manage Alien.

What's New in Cisco Optical Network Controller, Release 24.3.1

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements.

Feature	Description
Single Sign On Authentication through SAMLv2	The Security Assertion Markup Language (SAML) SSO feature allows you to gain single sign-on access based on the SAMLv2 protocol. Also, SSO user credential authentication works only for local users.
Unmanaged Equipment Support	Cisco Optical Network Controller 24.3.1 supports unmanaged devices. Unmanaged devices are third party devices that can be included in the Cisco Optical Network Controller 24.3.1 circuit trails connected to transponders. The MXD65-ADVA-FSP-3000-METRO-DCI-OLS appearing as 3LS in the circuit link.

Sites Audit Log Support	Cisco Optical Network Controller 24.3.1 supports two set of logs: • **Audit logs**: Help in auditing all the Cisco Optical Network Controller operation. This includes both the user and traffic related operations done on COSM or node. . • **Debug logs**: Refer to developer logs. • **Archive logs**: Help in scheduling and archiving the logs.
PSM Fiber Protection Support	Protected Segment Monitoring (PSM) is a Cisco Optical Network Controller feature that protects the Optical Multiplex Section (OMS) segment in the optical network. It ensures the continuity of signal transmission by automatically switching circuit paths in case of any fiber cut. PSM card is supported by Cisco Optical Network Controller only on the NCS 1001 chassis.
Service Assurance and Topology Acknowledged Alarm Mute Support	Cisco Optical Network Controller 24.3.1 helps in muting low priority alarms and disable them from appearing in the **Topology**, **Service Assurance**, **Network Monitoring**, and **Circuit Monitoring** screens. As it helps in having only the selected alarms to appear on the screen, instead of the entire set of all the acknowledged alarms, there by avoiding unwanted clutter on the screen.
Service Assurance Live PM Support	From Cisco Optical Network Controller 24.3.1 release onwards, fiber information and span loss details are added newly to the **Topology** live PM tool tip. There are new details added for: **Fiber Type**, **Length**, **Source Min Expected Spanloss**, **Source Max Expected Spanloss**, **Destination Min Expected Spanloss**, **Destination Min Expected Spanloss**, **Destination Max Expected Spanloss**, **Destination Max Expected Spanloss**, **Span Loss**.
NCS1K4-OTN-XP and NCS1K4-2-QDD-C-K9 Line Cards Support	From CONC 24.3.1 onwards, the following line cards are enabled on the NCS 1004 chassis: • NCS1K4-OTN-XP • NCS1K4-2-QDD-C-K9
PM History Support	The Cisco Optical Network Controller 24.3.1 release includes a new application called PM History. The PM History application is made available in **Network Monitoring** workspace and it interacts with **Topology** for links. It is also available in the **Service Monitoring** workspace interacting with the **Detailed Service Path** if circuit is available.
Software Image Management and Upgrade Support	Software Image Management and Upgrade (SWIMU) application manages the software image backups, restores, and upgrades in Cisco Optical Network Controller.

Network Level Alarm Correlation Support	The Cisco Optical Network Controller 24.3.1 release includes Network Level Alarm Correlation (NLAC) which identifies and correlates the root cause alarm with other alarms in a network circuit during a loss of network connection.

In addition to these features the new Cisco Optical Network Controller 24.3.1 UI includes the following applications.

Application	Description
Software Image Management and Upgrade (SWIMU)	Cisco Optical Network Controller 24.3.1 provides an interactive map view for the software image backups, restores, and upgrades. **Software Image Management and Upgrade** application screen has the **Node Backup and Restore** screen which can be used for **Nodes and Groups**, **Topology** and the **Backup Jobs**. SWIMU helps in configuring SFTP servers using **Configure SFTP Server**. For details on how to view or use this application see *Cisco Optical Network Controller 24.3.1 Configuration Guide*.
PM History	Cisco Optical Network Controller 24.3.1 provides an interactive map view for **PM History** application. PM history allows you to view and generate PM data history reports for nodes or interfaces. For the sequential selection of each parameters in the order of nodes, interval, selected date time range, interface types, port name and locations. For details on how to view or use this application see *Cisco Optical Network Controller 24.3.1 Configuration Guide*.
Logs	Cisco Optical Network Controller 24.3.1 provides an interactive map view for **Logs** viewer application. The log viewer application supports two set of logs called **Audit** and **Debug** logs. Along with providing support **Archives** of logs. For details on how to view or use this application see *Cisco Optical Network Controller 24.3.1 Configuration Guide*.

Software and Hardware Requirements

Data Center Requirements

Cisco ONC 24.3.1 can be deployed using VMware vCenter server version 7.0, as well as vSphere server and client with version 7.0. It is deployed on rack or blade servers within vSphere. To aid in the deployment, Cisco has developed a cluster installation tool. This tool works in both environments.

The following list contains the pre-requisites of Cisco Optical Network Controller 24.3.1 installation.

- Before installing Cisco Optical Network Controller 24.3.1, you must first login in to the VMware customer center and download VMware vCenter server version 7.0, as well as vSphere server and client with version 7.0. Cisco Optical Network Controller 24.3.1 is deployed on rack or blade servers within vSphere.
- ESXi host must be installed on servers with vSphere version of 6.7.0 or 7.0 to support creating Virtual Machines (VM).
- Before the Cisco Optical Network Controller 24.3.1 installation, two networks are required to be created.

- **Control Plane Network**:

  The control plane network helps in the internal communication between the deployed VMs within a cluster. If you are setting up a standalone system, this can refer to any private network.

- **VM Network or Northbound Network**:

  The VM network is used for communication between the user and the cluster. It handles all the traffic to and from the VMs running on your ESXi hosts and this is your Public network through which the UI is hosted.

VM Host Requirements

This section explains the VM host requirements.

Table 1: VM Host Requirements

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td>CPU/Memory/Storage Profiles (per VM)</td><td>The minimum requirement for Cisco Optical Network Controller 24.3.1 installation is given in the table below.
Table 2: Minimum Requirement
<table>
<tr><th>Sizing</th><th>CPU</th><th>Memory</th><th>Disk</th></tr>
<tr><td>XS</td><td>16 vCPU</td><td>64 GB</td><td>800 GB</td></tr>
<tr><td>S</td><td>32 vCPU</td><td>128 GB</td><td>1.5 TB</td></tr>
</table>
The requirements based on type of deployment are given in the table below.
Table 3: Deployment Requirements
<table>
<tr><th>Deployment Type</th><th>Requirements</th></tr>
<tr><td>Standalone (SA)</td><td>Control Plane: 1 IP (this can be a private network).
Northbound Network/VM Network: 1 IP (this must be a public network)</td></tr>
</table></td></tr>
<tr><td>Additional Storage</td><td>10 GB (approximately) of storage is required for OVA installation.</td></tr>
<tr><td>Network Connections</td><td>For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Control Plane network.
For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.</td></tr>
</table>

Requirement	Description
IP Addresses	Two IP subnets, one for the Management network and one for Data network, with each allowing a minimum of four assignable IP addresses (IPv4). A Virtual IP (VIP) address is used to access the cluster, and then three IP addresses for each VM in the cluster. If your deployment requires worker nodes, you will need a Management and Data IP address for each worker node. • The IP addresses must be able to reach the gateway address for the network where Cisco ONC Data Gateway will be installed, or the installation will fail. • At this time, your IP allocation is permanent and cannot be changed without re-deployment. For more information, contact your Cisco Customer Experience team.
NTP Servers	The IPv4 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize the Cisco ONC application VM clock, devices, clients, and servers across your network. • Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached. • The ESXi hosts that will run the Cisco ONC application and Cisco ONC Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. • Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.

Important Notes

- Cisco ONC Infrastructure and applications are built to run as a distributed collection of containers managed by Kubernetes. The number of containers varies as applications are added or deleted.

Caveats

Open Caveats

The following table lists the open caveats for Cisco ONC 24.3.1

Identifier	Headline
CSCwm37061	CONC 3.2:PM -> Intermitently PM History values are not coming at CONC for all interfaces /ports
CSCwk44010	EDFA card of NCS1001 has a logicalPort with a reference to a not existing physical port
CSCwm64059	in ONC service assurance page, "composite power" values of transponder ports are reversed (TX/RX)
CSCwm65026	Frequency selection from chart allows frequencies out of range
CSCwk85765	ONC_REMOVE_ALL_DEVICES : COSM node deboard stuck due to NBIService: INIT
CSCwm47733	Issue in retrieving PM history
CSCwm60870	Device creation entries are not tracked randomly in audit logs
CSCwk80077	Inventory not update after adding 1004 device in already onboarded COSM
CSCwm65619	estimated power values are not correct for MD32 passive on NCS1001 setup
CSCwm66599	in ONC circuit monitoring page, "composite power" values of one PSM ports are reversed (TX/RX)
CSCwm39982	Circuit creation Failed with PCE Find Channel Failed[PCE-PR00001] - No routes available Error
CSCwi68546	CONC 3.1 may not support multiple restconf queries by multiple clients with "Basic Authentication"
CSCwm45410	Re-creating the Degree on the ADVA devices does not show the degree on the COSM UI
CSCwm27954	ONC_17842_ONC_17843: 4 OMS links in OSA but 3 OMS links in tapi(Due to inventory out-of-order notif)
CSCwm67803	Only on clicking the ack mute toggle config icon ack mute changes are reflected on workspace app
CSCwm47352	after cards swap on NCS1001, an unexpected PPM was present under PSM card
CSCwk79273	Abstract strands are not in line with expectation:
CSCwm49150	CONC 3.2: Service Assurance ->Wrong Alignment of Degree No. in Detailed service path
CSCwm10610	NCS1001 circuit operationalState on ILA path is not correct
CSCwm55487	Mismatch in Port Operational State: Expected 'ENABLED', Found 'DISABLED
CSCwh41027	cannot delete device immediately after onboard complete.
CSCwm65602	after NCS1001 EDFA card plugin/plugout, inventory data was not properly updated

Identifier	Headline
CSCwm56267	SSO users not supported in APIs
CSCwm34355	CONC 3.2:PM -> Repeated power value in CONC for different prev interval , in COSM its correct
CSCwm68474	after fiber restore, the fiberspan was still DISABLED in ONC
CSCwm14668	service path for NCS1001 ILA scenario is wrongly reported

Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Using the Cisco Bug Search Tool

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

Step 1 Go to the http://tools.cisco.com/bugsearch.

Step 2 Log in using your registered Cisco.com username and password.

The Bug Search page opens.

Step 3 Use any of these options to search for bugs, and then press Enter (Return) to initiate the search:

- To search for a specific bug, enter the bug ID in the Search For field.
- To search for bugs based on specific criteria, enter search criteria, such as a problem description, a feature, or a product name, in the Search For field.
- To search for bugs based on products, enter or select a product from the Product list. For example, if you enter “WAE,” you get several options from which to choose.
- To search for bugs based on releases, in the Releases list select whether to search for bugs affecting a specific release, bugs that were fixed in a specific release, or both. Then enter one or more release numbers in the Releases field.

Step 4 When the search results are displayed, use the filter tools to narrow the results. You can filter the bugs by status, severity, and so on.

To export the results to a spreadsheet, click **Export Results to Excel**.

Other Important Information and References

Cisco Optical Network Controller Documentation

This section lists the guides that are provided with Cisco Optical Network Controller, Release 24.3.1:

- Cisco Optical Network Controller 24.3.1 Installation Guide
- Cisco Optical Network Controller 24.3.1 Configuration Guide
- *Cisco Optical Network Controller API Documentation*