Release Notes for Cisco Optical Network Controller, Release 3.1

First Published: 2023-09-30

Last Modified: 2024-04-02

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 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

NCS 1014 support	Cisco Optical Network Controller support NCS1010 and NCS1014 devices through Cisco Optical Site Manager, see Cisco Optical Site Manager Configuration Guide. It provides alarms information for the NCS 1014 platform. The information is live data from NCS 1014 platform, collected on demand from the platform when you open the alarms page in the UI. The cards manged by Cisco ONC through COSM are listed below for NCS 1014: • NCS1K14-CCMD-16-C • NCS1K4-QXP-K9 • NCS1K14-2.4T-K9 • NCS1K14-2.4T-X-K9
Multicarrier support	Cisco Optical Network Controller 3.1 only supports OCH-NC multi carrier.
Alien support	Cisco Optical Network Controller 3.1 topologies support non-Cisco optical products and Cisco non-optical platforms as alien devices. Cisco Optical Network Controller 3.1 supports alien wavelengths provisioning to include performance verification. You can add alien transceivers specs and the PCE calculates a circuit that meets the required alien transceiver specs. For NCS 1004 nodes, you can manage all possible NCS 1004 configuration modes.
Improved Integration	Cisco Optical Network Controller 3.1 supports improved integration and allows monitoring of all network elements and services in a managed network.

Note Cisco Optical Network Controller 3.1 adds an additional layer of security and works as a Single Authentication Agent, thus sharing local, LDAP and SAML users.

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

Application	Description
Topology	Cisco Optical Network Controller provides an interactive map view of each node in the Topology application screen representing each node and network. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Nodes	The Nodes application is used to view the details of each node that is part of a service at any given point in time. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Alien Import	Use this application to import new application codes as alien wavelengths. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Inventory	To view the various devices and circuits that are part of Cisco Optical Network Controller inventory you can use this application. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.

Application	Description
Service Manager	To create and manage circuits in Cisco Optical Network Controller, use this application. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Alarms	To view the alarm details for each node based on the severity level use this screen. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Workspaces	Workspaces option allows you to manage different workflows on a daily basis. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Service Assurance	The Service Assurance option helps in visualizing the circuits and the related nodes, links, and the circuit paths. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.
Monitoring	This application allows you to view the log messages and other related details. For details on how to view or use this application see *Cisco Optical Network Controller 3.1 Configuration Guide*.

Software and Hardware Requirements

Data Center Requirements

Cisco ONC 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 3.03.1 installation.

- Before installing Cisco Optical Network Controller 3.03.1, 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 3.03.1 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 3.03.1 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. However, in case of a High Availability (HA) cluster, this network is created between the servers where each node of the HA cluster is being created.

  - **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 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>12 vCPU</td><td>52 GB</td><td>200</td></tr>
<tr><td>S</td><td>30 vCPU</td><td>100 GB</td><td>300</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>
<tr><td>Highly Available (HA)</td><td>Control Plane: 3 IPs (this can be a private network) - IPs required for individual nodes.

VM Network: 4 IPs (this must be a public network) with 3 IPs for node management and 1 IP for Virtual IP, which is used for northbound communication and UI.</td></tr>
</table>
Note
For a High Availability (HA) deployment, nodes on different ESXi hosts should have a minimum link bandwidth of 10G between them. This is recommended to ensure efficient data communication and synchronization between the nodes.</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 3.1

Identifier	Headline
CSCwj17466	HA Service Critical: During Resync of COSM nodes, deployerstatus went to disconnected state
CSCwj23405	Deleted COSM Node details were present in OSA of CONC 3.1
CSCwi68546	CONC 3.1 may not support multiple restconf queries by multiple clients with "Basic Authentication"
CSCwj34266	HA Service Critical : Brownfield circuits were discovered with Greenfield Circuit Provision
CSCwj21673	ONC 3.1 memory increase detected at multiple pods
CSCwj34270	HA Service Critical : Circuits going to PENDING REMOVAL due to "Configuration Failure at NSO"
CSCwj17354	HA Node restart: Onboard and resync failed for one of devices after Powering down/up the Active VM
CSCwj21726	ONC does not support high rate of circuits creation/deletion
CSCwj34271	HA Service Critical : During Onboard of COSM nodes, Topology DM Service gets Timed out
CSCwi65273	CONC 3.1: inventory is not updated after HW replacement
CSCwj17451	Inventory data not update for plugable after plug-in/out of Line Card with plugable
CSCwj17730	CONC 3.1: RED CROSS on RED span shown when OLT is SW Reset, though traffic stays up

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 https://bst.cloudapps.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 3.1:

- Cisco Optical Network Controller 3.1 Installation Guide
- Cisco Optical Network Controller 3.1 Configuration Guide
- *Cisco Optical Network Controller API Documentation*

© 2024 Cisco Systems, Inc. All rights reserved.