Release Notes for Cisco Optical Network Controller, Release 2.0

First Published: 2022-11-02

Last Modified: 2023-03-16

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Cisco Optical Network Controller Overview

Cisco Optical Network Controller (ONC) is an SDN Domain Controller for Cisco Optical Networks. ONC 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 ONC are:

- Serves as a domain controller for optical products and provides data to Hierarchical Controllers. ONC 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 ONC services.

What's New in Cisco Optical Network Controller, Release 2.0

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements. It also includes links to detailed documentation, where available.

Feature	Description
NCS1010 support	Cisco ONC 2.0 onboarding of NCS 1010 devices and discovery of NCS 1010 inventory, links (OLT and ILA), and OCHNC services. Cisco ONC provides alarms information for the NCS1010 platform. The information is live data from NCS1010 platform, collected on demand from the platform when you open the alarms page in the UI. Cisco ONC supports a logical node model or site to aggregate multiple physical devices to create an aggregated optical domain node. This feature enables simpler management of NCS 1010 ROADM sites.
Multicarrier support	Cisco ONC 2.0 supports the following multicarrier configurations: • Multiple Trunk/Add-Drops (or combination) supporting the multicarrier assembly • Superchannel multicarrier configuration Cisco ONC 2.0 supports OCH-NC and OCH-Trail service types with multicarrier configurations.
Planning Data Import	Cisco ONC 2.0 can import planning data generated as a json file by Cisco ONP 5.0. You can push the imported configuration to the planned devices in the network.
Alien support	Cisco ONC 2.0 topologies support non-Cisco optical products and Cisco nonoptical platforms as alien devices. Cisco ONC 2.0 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. ONC 2.0 will manage following nonoptical platform trunks as alien interfaces: • QDD-400G-ZRP-S • QDD-400G-ZR-S • ONS-CFP2D-400G-C
Connection Verification	Cisco ONC 2.0 provides connection verification for NCS 1010 platform. Connection verification checks cable connections against the expected connections. During connection verification, Cisco ONC generates the tone from OLTs and detects the tone on passive modules to verify the connection against the expected connections. Connection Verification service generates the tone and measures the patch loss by reading the power values.
Improved Integration with Crosswork HCO	Cisco ONC 2.0 supports improved integration with Cisco Crosswork HCO. Cisco ONC allows monitoring of all network elements and services in a managed network.

Software and Hardware Requirements

Before installing Cisco ONC, you must install Cisco Crosswork Infrastructure 4.4.

The infrastucture requirements for installing Cisco Crosswork are listed below. For complete installation requirements, see the *Cisco Crosswork Infrastructure 4.4 and Applications Installation Guide*.

Data Center Requirements

Cisco Crosswork can be deployed in either a vCenter managed data center. To aid in the deployment, Cisco has developed a cluster installation tool. This tool works in both environments. However, there are limitations to the tool which are detailed later in this section.

Note

- The machine where you run the installer must have network connectivity to the data center (vCenter) where you plan to install the cluster. If this mandatory requirement cannot be met, you must manually install the cluster.
- Cisco Crosswork cluster VMs (Hybrid nodes and Worker nodes) must be hosted on hardware with Hyper Threading disabled.
- Ensure that the host resources are not oversubscribed (in terms of CPU or memory).
- Starting with the Cisco Crosswork 4.4 release, Crosswork deployment is no longer supported for the Cisco CSP platform. For more information, see End-of-Life Announcement for the Cisco Cloud Services Platform Operating System.

VMware Data Center Requirements

This section explains the data center requirements to install Cisco Crosswork on VMware vCenter.

Note The following requirements are mandatory if you are planning to install Cisco Crosswork using the cluster installer. If your vCenter data center does not meet these requirements, then the VMs have to be deployed individually, and connectivity has to be established manually between the VMs.

- Hypervisor and vCenter supported:
  - VMware vSphere 6.7 or above
  - VMware vCenter Server 7.0 and ESXi 7.0.
  - VMware vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 (Update 1)
- All the physical host machines must be organized within the same VMware Data Center, and while it is possible to deploy all the cluster nodes on a single physical host (provided it meets the requirements), it is recommended that the nodes be distributed across multiple physical hosts.
- The networks required for the Crosswork Management and Data networks need to be built and configured in the data centers, and must allow low latency L2 communication.
- To allow use of VRRP, DVS Port group needs to be set as follows:

Property	Value
Promiscuous mode	Reject

Property	Value
MAC address changes	Reject
Forged transmits	Accept

To edit the settings in vCenter, navigate to the Host > Configure > Networking > Virtual Switches, and select the virtual switch. In the virtual switch, select Edit > Security and confirm the settings as suggested. Repeat the process for each virtual switch used in the cluster.

- Ensure the user account you use for accessing vCenter has the following privileges:
  - VM (Provisioning): Clone VM on the VM you are cloning.
  - VM (Provisioning): Customize on the VM or VM folder if you are customizing the guest operating system.
  - VM (Inventory): Create from the existing VM on the data center or VM folder.
  - VM (Configuration): Add new disk on the data center or VM folder.
  - Resource: Assign VM to resource pool on the destination host, cluster, or resource pool.
  - Datastore: Allocate space on the destination datastore or datastore folder.
  - Network: Assign network to which the VM will be assigned.
  - Profile-driven storage (Query): This permission setting needs to be allowed at the root of the DC tree level.
- We also recommend you to enable vCenter storage control.

VM Host Requirements

This section explains the VM host requirements.

Table 1: VM Host Requirements

Requirement	Description
CPU/Memory/Storage Profiles (per VM)	The data center host platform has to accommodate three VMs of the following minimum configuration: **VMware vCenter:** • Large: 12 vCPUs | 96 GB RAM Memory | 1 TB disk space **Cisco CSP:** • Large: 12 CPU cores | 96 GB RAM Memory | 1 TB disk space **Note** For assistance in adjusting VM Memory and CPU sizes post installation, contact your Cisco Customer Experience team. Few things to note: • Storage requirements vary based on factors such as the number of devices being supported and the type of deployment selected. However, 1 TB disk space should work for most deployments. • Due to their performance, solid state drives (SSD) are preferred over traditional hard disk drives (HDD). • If you are using HDD, the minimum speed should be over 10,000 RPM. • The VM data store(s) need to have disk access latency of < 10 ms.
Additional Storage	10 GB (approximately) of storage is required for the Crosswork OVA (in **vCenter**), OR the Crosswork QCOW2 image on each CSP node (in **CSP**).
Network Connections	For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network. For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.
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 or IPv6). 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 Crosswork Data Gateway will be installed, or the installation will fail. • When deploying a IPv6 cluster, the installer needs to run on an IPv6 enabled container/VM. • At this time, your IP allocation is permanent and cannot be changed without re-deployment. For more information, contact your Cisco Customer Experience team.

Requirement	Description
NTP Servers	The IPv4 or IPv6 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 Crosswork 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 Crosswork application and Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 or IPv6 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 Crosswork 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.
- Dual stack configuration is not supported in Crosswork Platform Infrastructure. Therefore, **all** addresses for the environment must be either IPv4 or IPv6.

Caveats

Open Caveats

The following table lists the open caveats for Cisco ONC 2.0

Identifier	Headline
CSCwd32134	R2.0 - deleted connectivity-service is still present in TAPI and OSM response
CSCwd28290	Post reload or fiber cut: OMS fiber link is not present in TAPI model intermittently
CSCwd16765	after disabling a line port of an OLT, fiberspan and oms link disappeared
CSCwc95579	Chaos - Resync for 183 SVO + 10 NCS1010 devices taking more than 30 mins
CSCwc30621	Connection service and cross-connections inconsistency between OSA and NBI after repeat re-creation

Identifier	Headline
CSCwd27196	NCS1010 ILA device cannot be delete if added under the same site of another ILA device
CSCwb50077	NBI notification generated twice while adding ncs1010 devices via bulk import
CSCwd02377	after passive connect/disconnect many unexpected NEPs of OTS layer found in TAPI
CSCwd02950	a passive pre-provision request may be rejected bcs slot not empty but the slot was in fact empty
CSCwd17588	creating a brownfield circuit (BRK8), the circuit was not shown in the OSA model
CSCwd12211	Auto Resync fails in CONC after NCS1010 is reloaded using reload location all cli
CSCwd26835	Passive addition - Fixed - Validation in the MM response failed for addition for fixed passive
CSCwc96443	After a passive was connected in a pre-provisioned slot, resync failed
CSCwd07215	wrong data at TAPI and OSA (DBs misaligned) while performing card plug-in / plug-out
CSCwc48002	JT: NCS1010 inventory changes are not detected dynamically and requires resync
CSCwd23943	PCE channel failed for some application code as 00B08E#NCS1K4-1.2T-K9#3#1576#R200G

Exceptions

Connection Verification can be performed only when there is no service present on the patch-cord . Full management of OOB verification when services are present and patch loss measurement is planned in future releases.

CONP planning data input must be in lower case.

In case of fiber cuts, the link gets removed from TAPI topology and gets re-added with restore.

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

Scale Support

1. Device Onboarding
   a. Cisco ONC 2.0 supports up to 750 devices.
   b. You can onboard up to 200 devices at a time, for a bulk import. Wait for the previous batch to complete before importing the next batch.
   c. When the bulk import operation ends, Crosswork HCO shows all the relevant information.
   d. When onboarding devices that have configuration already present on them, onboarding can take longer depending on the number circuits present on the device.
2. Circuit Provisioning
   a. Cisco ONC 2.0 allows you to create 4 circuits in a minute. We recommend you wait for the previous provisioning operation to complete before initiating a new one.
   b. On SVO setup
      1. Time taken for OCHNC circuits to go to Installed state depends on the number of fiber spans involved.
      2. We recommend 75-seconds delay between each circuit provisioning.
   c. On an NCS 1010 5-node point-to-point setup
      1. OCHNC circuits typically go to Installed state in 20–60 seconds.
      2. We recommend 45-seconds delay between each circuit provisioning.

3. Device deletion
   a. We recommend you delete not more than 10 devices together and wait until the device deletion is complete. You can either monitor the NBI Notifications or wait for 5 minutes between each operation to ensure complete deletions.

Cisco Optical Network Controller Documentation

This section lists the guides that are provided with Cisco Optical Network Controller, Release 2.0.

Title	What is included
Cisco ONC 2.0 Configuration Guide	• Overview • Installation requirements • Installation instructions • Onboard and manage devices
CONC TAPI Northbound Interface API Guide	• APIs exposed by Transport API Northbound Interface supported by Cisco Optical Network Controller.
CONC TAPI Northbound Interface Description Document	• Interface descriptions of the Transport API Northbound Interface supported by Cisco Optical Network Controller.