Release Notes for Cisco Optical Network Controller, Release 1.0

First Published: 2021-04-26

Last Modified: 2023-03-17

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.

Software and Hardware Requirements

Before installing Cisco ONC, you must install Cisco Crosswork Infrastructure 4.0.

The infrastucture requirements for installing Cisco Crosswork are listed below. For complete installation requirements, see the *Cisco Crosswork Infrastructure 4.0 and Applications Installation Guide*.

Data Center Requirements

Cisco Crosswork can be deployed in either a vCenter managed data center or onto Cisco CSP. 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 Cisco Crosswork cluster in order to complete the installation. If this mandatory requirement cannot be met, you must manually install the cluster.

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.

- VMware vSphere 6.5 or above
- vCenter Server 6.5 Update 2d or later (ESXi 6.5 Update 2 installed on hosts), OR vCenter Server 6.7 Update 3g or later (ESXi 6.7 Update 1 installed on hosts)
- 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 within the data center, and must allow L2 communication. A single pair of network names is required for these networks to be used across all the physical host machines hosting the Crosswork VMs.
- To allow use of VRRP, DVS Port group needs to be set to allow Forged Transmits setting as follows:

Property	Value
Promiscuous mode	Reject
MAC address changes	Reject
Forged transmits	Accept

- Ensure the user account you use for accessing vCenter have 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 (Provisioning): Read customization specifications on the root vCenter server 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.

CSP Data Center Requirements

This section explains the data center requirements to install Cisco Crosswork on Cisco Cloud Services Platform (CSP).

- Cisco CSP, Release 2.8.0.276
- Compatible Hardware:

UCSC-C220-M4S, UCSC-C240-M4SX
N1K-1110-X, N1K-1110-S
CSP-2100, CSP-2100-UCSD, CSP-2100-X1, CSP-2100-X2
CSP-5200, CSP-5216, CSP-5228
CSP-5400, CSP-5436, CSP-5444, CSP-5456

- CSP host or cluster is setup and installed with a minimum of 2 physical ethernet interfaces - one ethernet connected to the Management network, and the other to the Data network.

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 (applicable to VMware vCenter and Cisco CSP): **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, one 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

- Kubernetes runs within the Crosswork application VM and uses Docker for containerization. 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

There are some open caveats in Cisco ONC 1.0. Some of them can be resolved using simple workarounds. See the following table for more details:

Open Caveats	Workaround
Circuit deletion not possible when the device is not reachable.	The device that is not reachable cannot be replaced with a new device. If the user does not want to use the device because of some issue on the device, then: • Make the device reachable using config • Delete the associated circuits • Delete the device from CONC

Open Caveats	Workaround
Equipment Failure Alarm for circuits not managed by ONC.	Set the card right or replace it with a good card.
Partial Brownfield circuit discovery behaviour in ONC.	None
Circuit Provisioning failures.	HCO must retry the circuit creation with valid inputs.
Failures during Circuit Name Edit Request.	HCO must retry the circuit name edit request.
When two circuits starting from the same SVO have the same frequency and go in different directions, one of the two circuits (not related necessarily to OLA) is not discovered.	None
New circuit creation after brownfield circuit discovery (1 circuit remained stuck in planned state in TAPI (OSM is correctly in INSTALLED state)	Restart NBI Service
Deletion of the last circuit passing through MC NEP does not send the owned-node-edge-point → media-channel-node-edge-point-spec → mc-pool deletion notification to HCO.	HCO needs to fetch the owned-node-edge-point → media-channel-node-edge-point-spec → mc-pool information by making the RESTCONF call to the ONC as part of the circuit delete notification.
Circuit deletion failure	Retry the deletion again after sometime.
Device onboarding connectivity and collection failures.	Manually resync the device.
Consecutive device xls import within few seconds into the ONC is failing	Trigger the second import once the first import has been completed.
No soft reset support in ONC.	None
Resync for link discovery.	Manually resync from the GUI to recollect the topology link info for the devices on which the link was added.
No regen support for circuits in ONC.	None
Manual reconnect necessary when there is an error during connectivity check in the deployer.	Execute reconnect operation for the device on GUI.
Logical Port Add Notification, OTN Info (coming from interfaces/Otu_Otn) not updated.	Resync devices on Cisco ONC GUI.
Port rate not coming in inventory for one ethernet logical port created.	Resync devices on Cisco ONC GUI.
Unidirectional IPC not supported in ONC 1.0.	Use SVO GUI to check the IPC.
PPM delete not handled as part of card delete.	Resync devices on Cisco ONC GUI.

Open Caveats	Workaround
When the TNC/TSC card with ppms is added, ppms are not discovered.	Resync devices on Cisco ONC GUI.
SVO not sending notifications for physical ports when TNCS-20 card is added.	Resync devices on Cisco ONC GUI.
No notification after any card deletion which is without default ports (example 400G-XP) with all the ppms and ppm ports deleted.	Resync devices on Cisco ONC GUI.
No notifications for card plug-out and then delete of the access port.	Resync devices on Cisco ONC GUI.
ONC Notification handling failures in ONC.	Device Manager resyncAll REST API can be used and triggered periodically on all the devices as part of the script by the Admin.
Passive units place holders and improper removal alarm behavior.	None
IP address change not supported in ONC.	Delete and add the device again with the new IP.
Duplicate IP handling for some devices.	Delete and add the device again with the new IP.
Life cycle state of a circuit does not move into INSTALLED state.	Wait for 5 minutes, then delete the circuit and recreate the circuit again.
Chassis equipment (both active and passive) creation and contained-holder (slots) creation (in the TAPI equipment model) behavior not consistent.	Resync devices on Cisco ONC GUI.
Accessports not created in TAPI for some passive devices and old legacy modules.	None
Access Port not seen for unidirectional physical ports on legacy units as part of the notifications flow for ROADM cards	Execute resync on the device
Access Port on TXP is shown to have attached to card equipment (instead of Pluggable equipment) as part of the notifications flow. Resync points to the PPM equipment correctly, but old card equipment reference still exists as duplicate entry.	None
Access port notifications not coming after first plugin without provisioning for SMR card.	Resync devices on Cisco ONC GUI.
Logical port oper-state mismatch between Inventory and ModelMapper.	Resync devices on Cisco ONC GUI.
Alarms and PM (tx power, counters) information cannot be seen in ONC 1.0.	This information can be seen on the SVO Web UI by launching it.

Open Caveats	Workaround
With graceful shutdown of the VM some devices may be disconnected.	Use the reconnect option on GUI to connect the disconnected devices.
ONC does not support abrupt shutdown of the VM	Reinstall the cluster and the ONC application.
When Connectivity Service deletion is failed during the deployment phase (after validation by CircuitService/PCE), it is not possible to inform client about the failure (including the reason for failure).	The deleted service will get recreated in ONC as part of the deletion flow and user gets a create notification.
When SIP operational-state and lifecycle-state changes, the same states of CSEPs attached to the SIP (via connectivity-services) do not change. NEPs and CEPs are updated. CSEPs info can be seen in NEPs and CEPS	None
Transmit power configured as part of the circuit creation on the router generated by the PCE is not present in TAPI for discovered services.	HCO has actual value that is obtained from the ONC as part of the circuit response from the ONC.
Stale entries remaining in NBI service during pluggable deletion.	None
NBI Service has SIPs when OSM is empty after the devices have been deleted	Restart NBI Service
TAPI reference actual equipment and actual holders deletion for card plug-out does not send notifications to the HCO.	HCO has to pull the TAPI equipment context information using RESTCONF API and update itself at regular intervals.
Backup and Restore of ONC data	Contact your Cisco support representative or system administrator.

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

The number of nodes supported by Cisco ONC 1.0 is 100.

Cisco Optical Network Controller Documentation

This section lists the guides that are provided with Cisco Optical Network Controller, Release 1.0.

Title	What is included
Cisco ONC 1.0 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.