Release Notes for Cisco Optical Network Controller, Release 1.1

First Published: 2021-11-24

Last Modified: 2023-03-30

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.

Whats New in Cisco Optical Network Controller, Release 1.1

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
Configuration	

Feature	Description
Network Periodic Full Sync Configuration	You can now configure a periodic full sync for all the devices onboarded to Cisco ONC.
CONC TAPI Northbound Interface Description	
Transponder Domain Support	Cisco ONC and TAPI NBI support transponder domain in addition to the OLS domain. The TXP and OLS (disaggregated) network topology can contain TXP or MXP and regen nodes in addition to the ROADM and ILA nodes. The DSR (Digital Signal Rate) and OTN transport layers are also supported in addition to photonic media layers.
DSR/OTU Connectivity Service Support	Cisco ONC and TAPI NBI support provisioning of DSR or OTU connectivity services between TXP or MXPs. The service can include intermediate regeneration (3R) of the optical channel.
Optical Power Monitoring	Cisco ONC and TAPI NBI support optical power monitoring at service and link level. OTSiMC power monitoring at carrier level is available on ROADM add or drop and degree ports across the service path. OTS power monitoring is available on ROADM or ILA degree or line ports across OTS links.

Software and Hardware Requirements

Before installing Cisco ONC, you must install Cisco Crosswork Infrastructure 4.1.

The infrastucture requirements for installing Cisco Crosswork are listed below. For complete installation requirements, see the *Cisco Crosswork Infrastructure 4.1 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 data center (vCenter or CSP) 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).

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
MAC address changes	Reject
Forged transmits	Accept

- 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 (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 two 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: **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.

Requirement	Description
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.
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 1.1

Table 2: Open Caveats

Caveat ID Number	Description
CSCwa01468	Confd:Tailf query with limit value higher than 500 gives 500 Internal server Error for RESTCONF.
CSCwa24365	Additional physical span is obtained while deleting a single strand from bi-directional IPC on resync.
CSCwa24599	No notification for PPM plugin for the first time.
CSCwa24455	Access port notifications not displayed after first plugin without provisioning for SMR card.
CSCwa24533	The deployer status is disconnected, while trying to import device.
CSCwa24531	SDH/SONET Payload support - OCHCC impact for inventory.
CSCwa24750	Circuit service - brownfield discovery re-design and disabling lock/unlock.
CSCwa24551	OTSI sips are not created (deleted) on IPC creation (deletion).
CSCwa24536	SDH/SONET Payload support - OCHCC impact on NBI.
CSCwa24411	Circuit (CS and XC) stuck in Planned state when created with deployer shut.
CSCwa24413	NEPs and SIPs are not deleted on nodetermPoint deletion.
CSCvz32127	ONC Pods keeps crashing on ipv6 setup.
CSCwa24399	connectedTermPoints displayed as null in 12.1 and 12.2.
CSCwa14718	onc-mongo-service in the degraded state post reboot.
CSCwa24543	Deployer service fails after node is shutdown.
CSCwa24602	TAPI notification source-host incorrectly show pod IP address.
CSCwa00701	TAPI SIP inventory ID uses a parameter that may be not unique.
CSCwa24587	No alarm is raised when the passive chassis USB association for the first time.
CSCwa24582	The frequency is not updated by inventory when it is changed in the device.

Caveat ID Number	Description
CSCwa24374	OCH-CC maxLength and maxOptNoise constraints work for lesser length than actual length.
CSCvz70913	OMS-Link and FiberSpan are not re-created after SVO-OSC provisioning.
CSCwa24370	Power values collection for 600 devices takes more than 15 mins.
CSCwa01897	OMS link is partial after re-adding the deleted degree.
CSCwa24445	Inventory service does not send all degree data of a device for some time.
CSCwa24444	No support for uni-directional NEP in TAPI.
CSCwa24564	SDH/SONET Payload support - OCHCC impact for Circuit Service.
CSCwa24449	Degree Delete Notifications fail on topology side.
CSCwa24528	Issue of transitioned-layer-protocol-name value in TAPI.
CSCwa24529	Error in deletion for TAPI client in case of diversity constraint.
CSCwa24540	Immediate circuit deletion after creation leaves connectivity-service in TAPI.
CSCwa24524	Physical port creation notification not displayed as part of card addition for TNCS-20.
CSCwa24420	Stale NEETCONF notification sessions.
CSCwa24526	Route name changed after CW all service restart.
CSCwa24520	Error Message needs to be more descriptive for REGEN PCE error.
CSCwa24427	Tx power configured as part of circuit creation on router generated by PCE is not present in TAPI for Discovery Service.
CSCwa24557	Circuit (CC/NC) accepts device UUID as include-node constraint.

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 1.1 is 100.

Cisco Optical Network Controller Documentation

This section lists the guides that are provided with Cisco Optical Network Controller, Release 1.1.

Title	What is included
Cisco ONC 1.1 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.