



# Cisco Crosswork Hierarchical Controller 8.0

## Installation Guide

March 2024

## Introduction

This document is an installation guide for Cisco Crosswork Hierarchical Controller with or without High Availability. Cisco Crosswork Hierarchical Controller implements intra-node resiliency and a three-node cluster (which includes a witness node).

The document explains:

- Cisco Crosswork Hierarchical Controller Prerequisites
- Install Cisco Crosswork Hierarchical Controller Platform
- Upgrade Cisco Crosswork Hierarchical Controller Platform
- Install Cisco Network Services Orchestrator Crosswork Hierarchical Controller Function Pack

## Cisco Crosswork Hierarchical Controller Prerequisites

All Crosswork Hierarchical Controller components and applications can be installed in the same instance and work seamlessly together.

Cisco Crosswork Hierarchical Controller is released with a single VMWare OVA file distribution. OVA is a disk image deployed using vCenter on any ESXi host. This OVA packages together several components including a file descriptor (OVF) and virtual disk files containing a basic operating system and the Cisco Crosswork Hierarchical Controller installation files.

OVA can be deployed using vCenter or ESXi web clients on ESXi hosts supporting both Standalone (SA) or High Availability (HA) deployment models.

The three VMs for HA can run on any single or multiple ESXi hosts. In case of multiple ESXi hosts, 10 Gbps is required for connecting each host. The control plane network is also associated with the same 10 Gbps interface and a 10 Gbps communication channel between the hosts is required.

## Requirements

- VMware vCenter Server 7.0 Update 3
- VMware ESXi 7.0 Update 3
- High Availability, version 8.0, requires a latency of up to P95 15ms (95% of the requests to the system must be served faster than this) between nodes.

**Note:** The system was tested with version 7.0 Update 3. The system is expected to function as expected with other 7.0 sub-versions as well. If you are using a sub-version other than 7.0 Update 3 and you encounter any issues, contact your Cisco support representative.

## Hardware

### All Nodes

This spec is for active, standby, and witness, or standalone instances of Crosswork Hierarchical Controller.

Hardware	Requirement
CPU	10 Cores
Memory	96 GB

Hardware	Requirement
Multiple ESXi hosts	10 Gbps between hosts
Storage	500 GB SSD to 2 TB (Scale requirement) <b>Note:</b> This is without considering RAID configurations
HW Reservation	80% for CPU and memory
NICs	2

## Client

The client machine requirements are:

- PC or MAC
- GPU
- Web browser with GPU hardware acceleration support
- Recommended
  - Screen resolution 1920x1080
  - Google Chrome web browser

**Note:** GPU is mandatory to properly get all the benefits of the network 3D map.

## Communications Matrix

The following are the default port requirements if the items listed in the Description column are used. You can configure these ports differently.

User	Role	Description
Inbound	TCP 22	SSH remote management
	TCP 8443	HTTPS for UI access
Outbound	TCP 22	NETCONF to routers
	TCP 389	LDAP if using Active Directory
	TCP 636	LDAPS if using Active Directory
	Customer Specific	HTTP for access to an SDN controller
	Customer Specific	HTTPS for access to an SDN controller
	TCP 3082, 3083, 2361, 6251	TL1 to optical devices
Control Plane Ports (Internal network between cluster nodes, not exposed)	Kubernetes	TCP 443
	Kubernetes	TCP 6443
	Kubernetes	TCP 10250
	etcd	TCP 2379
	etcd	TCP 2380

User	Role	Description
	VXLAN	UDP 8472
	Ping between nodes (optional)	ICMP

## Storage

The storage volume required for Crosswork Hierarchical Controller production depends on the amount of storage needed for performance counters and for daily DB backups.

The performance monitoring storage is calculated based on the number of client ports and the amount of time the counters are stored. The ballpark figure is 700 MB for 1000 ports.

The detailed formula to calculate the storage is:

**<uncompressed data>=<number of ports>\*<samples per day>\*<number of days>\*60**

**Storage = (<uncompressed data>\*0.1)+<daily backup size>\*<number of days>\*<number of months>**

Taking the following assumptions into account:

- Samples – samples per day
- Sample size per port – 60 bytes
- Days – number of days the PM data is stored
- Compression ratio – data is compressed in DB, at a ratio of ~10%
- Daily backup – ~60 MB per day
- Number of backup days – 14 days
- Number of backup months – default is 12 months

## Control Plane and Northbound Networks Installation Requirements

The following list contains the pre-requisites of Cisco Crosswork Hierarchical Controller installation.

Before installing Cisco Crosswork Hierarchical Controller:

- Install the ESXi host on servers with vSphere to support creating VMs.
- Create two networks, one for the control plane and the other for the northbound network. The control plane network helps in the communication between the deployed VMs. The northbound network is used for communication between the client and the cluster.
- Ensure there is no firewall preventing Crosswork Hierarchical Controller adapters properly communicating southbound with the managed devices or domain controllers.
- Ensure that no firewalls prevent access between the Crosswork Hierarchical Controller platform and the remote hosts.

**To create the control plane and northbound networks:**

1. From the vSphere client, select the Datacenter where you want to add the ESXi host.
2. After adding the ESXi host, create the control plane and northbound network before deploying the SA or HA:
  - HA has four IPs, where one is the primary and the others can join as secondary and tertiary IP addresses. The VIP is the IP that exposes the active node to the user.

- 
- SA has two IPs.

---

## Install Crosswork Hierarchical Controller Platform

### Install Crosswork Hierarchical Controller

When you deploy the OVA template it installs the Crosswork Hierarchical Controller platform, 3D Explorer and the various Crosswork Hierarchical Controller applications.

Create three VMs for HA or one VM for SA. Repeat steps 1 to 10 for each of the VMs.

For HA, it is recommended that you create all three VMs before they are turned ON.

#### To install Crosswork Hierarchical Controller:

1. Right-click on the ESXi host in the vSphere client screen, and then click **Deploy OVF Template**.
2. On the **Select an OVF template** page, specify the location of the source OVA template:
  - **URL:** A URL to an OVA template located online.
  - **Local file:** A location with the OVA template.
3. Click **Next**.
4. On the **Select a name and folder** page, specify a unique name for the VM Instance (the virtual machine's name must be all lowercase). From the list of options select the location of the VM to be used as SA or HA (primary, secondary, or tertiary).
5. Click **Next**.
6. On the **Select a compute resource** page, select the destination compute resource on which you want to deploy the VM and click **Next**.  
**Note:** While selecting the compute resource the compatibility check proceeds until it completes successfully.
7. On the **Review details** page, verify the template details and click **Next**.
8. On the **Select storage** page, select the virtual disk format based on SSD. Set the **VM Storage Policy** to **Datastore Default** and click **Next**.
9. In the **Select networks** page, set the control and management network to **Control Plane and VM Network** and click **Next**.

In the **Customize template** page, set the values as follows:

Key	Value
Instance Hostname	<Instance hostname>
SSH Public Key	<ssh-public-key> This must be generated by the customer's admin. For example: <code>ssh-keygen -t ed25519 -f ~/.ssh/...</code>
Data Volume Size (GB)	The data storage limit set for the host. See <a href="#">Requirements</a> .
Cluster Join Token	<token-value> This is already filled in.
Control Plane Node Count	<CP-node-count> <ul style="list-style-type: none"> <li>• HA: 3</li> <li>• SA: 1</li> </ul>
Control Plane IP	<Private IP for the Instance> Control Plane Network. For standalone, this must be a local valid IP in the customer's hypervisor.
Initiator IP	The IP of the initiator node of the Control Plane. The initiator installs the cluster, or in the case of standalone, the single node. For standalone, use the same IP set as the Control Plane IP.
Protocol	Select Static IP or DHCP from the menu.
IP(ip[/subnet]) - if not using DHCP	<Public IP for the Instance> Northbound Network.
Gateway - if not using DHCP	<Gateway IP for the Instance> Northbound Network.
DNS	DNS Server IP.
Initiator Node	For HA, set to <b>True</b> for the primary node.
Northbound Virtual IP	The Northbound Network: <ul style="list-style-type: none"> <li>• <b>HA:</b> The external virtual IP of the cluster.</li> <li>• <b>SA:</b> The external public IP of the standalone instance.</li> </ul>

10. In the **Review the details** page, review the selections and click **Finish**.

11. Power on the VM.

12. Verify that the VM details are set to 96GB RAM and 10 vCPUs.

13. Try connecting to the VM. For this, use the private key associated with the public key used earlier during customizing public key options. Login to the VM:

```
# ssh -i <private-key_file> nxf@<hco_management_ip>
```

14. The nxf-boot process monitors the cluster (for standalone and HA):

```
journalctl -fu nxf-boot
```

---

15. The default user id or password can be retrieved from the nxf-boot process log on the primary node (this is randomly generated when the cluster boots). (You can use this password or log in via SSH and use sedo to change the password.)

16. Update the NTP configuration as shown in the example given below.

Example:

```
vi /etc/chrony/chrony.conf
NTP server IP/DNS iburst
# Apply the new ntp setting
systemctl enable chronyd
systemctl restart chronyd
## To Check the Server
chronyc sources
```

17. Change the default password:

```
sedo security user set --access role/admin admin
sedo security user set --password
```

18. Browse to the Crosswork Hierarchical Controller application using the following SA IP address or the HA VIP address, using the admin user account with the password just set.

## **View Installed Crosswork Hierarchical Controller Applications**

**To view the installed Crosswork Hierarchical Controller applications:**



1. After the installation is complete, **ssh** to the server.
2. Run the following command to see which applications are installed:

```
sedo hco apps list
```

NAME	VERSION	ENABLED
dashboard-app	v8.0.0-242-rc1	Yes
device-manager-srv	v8.0.0-328-rc1	Yes
explorer-app	v8.0.0-109-rc1	Yes
failure-impact-app	v8.0.0-172-rc1	Yes
fibers-srlg-app	v8.0.0-186-rc1	Yes
layer-relations-app	v8.0.0-125-rc1	Yes
link-assurance-app	v8.0.0-235-rc1	Yes
link-manager-app	v8.0.0-320-rc1	Yes
model-settings-srv	v8.0.0-129-rc1	Yes
network-history-app	v8.0.0-162-rc1	Yes
network-inventory-app	v8.0.0-313-rc1	Yes
notification-manager-app	v8.0.0-76-rc1	Yes
nso	v8.0.0-280-rc1	Yes
path-analysis-app	v8.0.0-190-rc1	Yes
performance-app	v8.0.0-495-rc1	Yes
rca-app	v8.0.0-217-rc1	Yes
service-assurance-app	v8.0.0-368-rc1	Yes
service-manager-app	v8.0.0-578-rc1	Yes
shql-query-app	v8.0.0-180-rc1	Yes
srlg-app	v8.0.0-177-rc1	Yes
topology-utils-app	TOD0-246.23-feature-dev	Yes

The output displays the installed applications with their name and version.

## Add Network Adapters and Discover Network Devices

For instructions on how to add network adapters and discover network devices, refer to the *Cisco Crosswork Hierarchical Controller Administration Guide*.

---

## Upgrade Cisco Crosswork Hierarchical Controller

Upgrading Crosswork Hierarchical Controller version 7.1 to version 8.0, requires you to install a new “upgrader” instance of Crosswork Hierarchical Controller version 7.1 (together with the hco-upgrader tool).

You then make a backup of your version 7.1 working environment and copy it to this upgrader instance.

Using the hco-upgrader, you create a version 8.0 backup file which can be copied on the Crosswork Hierarchical Controller version 8.0 environment.

The backup is then restored on the Crosswork Hierarchical Controller version 8.0 environment.

You also must install the adapters on Crosswork Hierarchical Controller version 8.0 with specific names, to match the adapters' name on version 7.1.

### To upgrade Crosswork Hierarchical Controller:

1. Install another Crosswork Hierarchical Controller version 7.1 instance and install the hco-upgrader tool:

```
docker pull registry.sedona.ciscolabs.com/nxf/hco-upgrader:2.0
```

2. Create a backup on the Crosswork Hierarchical Controller version 7.1 system you want to migrate to version 8.0.
3. Copy the backup file to the Crosswork Hierarchical Controller version 7.1 upgrader instance you created in step #1.
4. Restore the backup file on the upgrader instance.
5. Run the upgrader to create a version 8.0 backup file.

```
docker run -it --rm -v $PWD:/pgdatanew -v sedona_data:/pgdataold registry.sedona.ciscolabs.com/nxf/hco-upgrader:2.0 --password PW -v
```

**Note:** All users must have read permissions in the folder where upgrader is executed.

6. Copy the version 8.0 backup file to the Crosswork Hierarchical Controller version 8.0 environment.
7. Upload the version 8.0 backup file to NxF:

```
sedo backup upload [file] --password PW
```

8. List all available backups on NxF:

```
sedo backup list
```

9. Use the backup to restore the Crosswork Hierarchical Controller version 8.0 system:

```
sedo backup restore [backup name]
```

### To install adapters on Crosswork Hierarchical Controller version 8.0:

- 
1. Download the adapter Service Pack.
  2. Install it with the DYNAMIC\_APP\_GUID param:

```
sedo service install HCO-cisco-ios-xr-adpt-v8.0.0-rc1.tar.gz --param  
DYNAMIC_APP_GUID=[adapter name as it is displayed in Device Manager on v7.1]
```

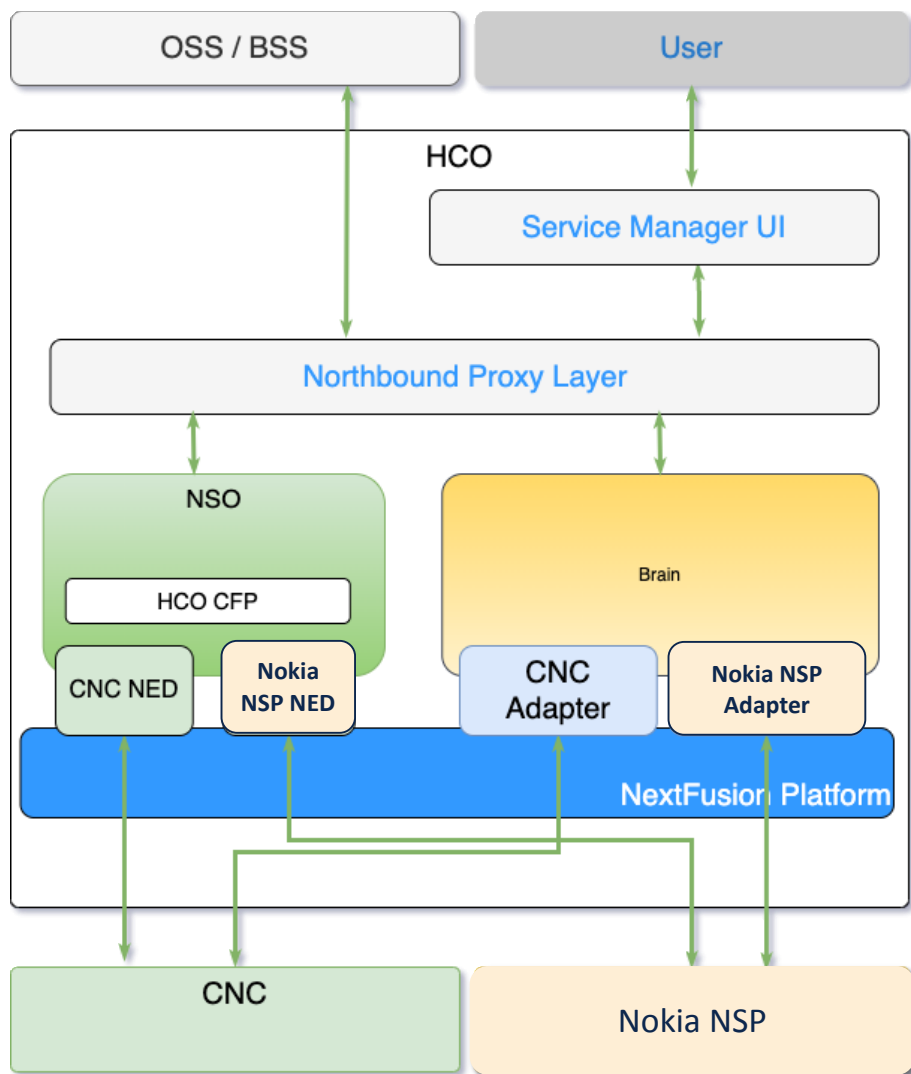
## Install a Cisco Network Services Orchestrator Crosswork Hierarchical Controller Function Pack

### NSO Engine Embedded Inside Crosswork Hierarchical Controller

NSO runs as an Crosswork Hierarchical Controller micro-service, alongside the Crosswork Hierarchical Controller applications and adapters.

This exposes the NSO NBI from Crosswork Hierarchical Controller and the NSO UI as an Crosswork Hierarchical Controller application (which will mostly be used for configuration of Function Packs/NEDs).

**Note:** Crosswork Hierarchical Controller HA and embedded NSO integrate seamlessly. The NSO database exists on both the Crosswork Hierarchical Controller Active and Standby nodes, and the database is synchronized continuously. If the Crosswork Hierarchical Controller Active node fails, and the Standby node takes over and becomes the Active node, NSO is updated automatically and switches nodes too.



**Figure 1.**  
Network Services Orchestrator (NSO)

The Crosswork Hierarchical Controller Function Pack integrates Cisco NSO with a controller to deploy services on the controller. This integration is with either a Nokia Service Provider (NSP) controller or a Cisco Crosswork Network Controller (CNC). The NEDs are installed as part of the Function Pack installation.

For full details on installing and using the **Network Services Orchestrator (NSO) Crosswork Hierarchical Controller Function Pack**, see the:

- *Cisco NSO Crosswork Hierarchical Controller - Function Pack Installation Guide*
- *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide.*

For full details on installing and using the **Cisco NSO Routed Optical Networking Core Function Pack**, see the:

- *Cisco NSO Routed Optical Networking Core Function Pack Installation Guide*
- *Cisco NSO Routed Optical Networking Core Function Pack User Guide*
- *Cisco RON Solution Guide*

## Install NSO Function Pack in Crosswork Hierarchical Controller Embedded Instance

The embedded NSO instance is a fully functional standalone container installation of NSO. The installation procedure is the same as the standard installation with one difference: the file system of NSO is not readily available on the host server.

To load the new function pack, the administrator must copy the function pack files onto the NSO pod, and then log into the pod shell and place the files in the correct directories. Once the files are on the NSO pod, follow the instructions in the *Function Pack Installation Guide*.

### To install NSO Function Pack in Crosswork Hierarchical Controller Embedded Instance:

1. Connect to the Crosswork Hierarchical Controller host server via SSH.
2. Download the NSO function pack.
3. Copy the NSO function pack into the NSO pod:

```
kubectl cp [function-pack-file] <zone-a/zone-b>/nso-manager-srv-0:/usr/app
```

4. Log into the pod shell:

```
sedo shell <zone-a/zone-b>/nso-manager-srv  
cd /usr/app/nso-temp
```

5. Continue with function pack extraction and installation as specified in the *Function Pack Installation Guide*.

## Considerations for a High Availability (HA) Deployment

HA in NSO needs to be disabled for installing and updating function packs.

1. On both the active and standby nodes, in the NSO CLI execute:

```
admin@ncs> request high-availability disable
```

2. On both the active and standby nodes, install the function pack.

3. Restart the NSO pods to reactive HA protection:

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n zone-a scale statefulset  
nso-manager-srv --replicas=0
```

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n zone-b scale statefulset  
nso-manager-srv --replicas=0
```

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n zone-a scale statefulset  
nso-manager-srv --replicas=1
```

```
sudo kubectl --kubeconfig /etc/kubernetes/admin.conf -n zone-b scale statefulset  
nso-manager-srv --replicas=1
```

## Example of How to Install the RON Function Pack

This describes an example of how to install a RON function pack on the NSO pod.

For the complete and most updated procedures, you must refer to the related *Function Pack Installation Guide*.

1. Copy the function pack file into the pod:

```
kubectl cp nso-6.1-ron-2.1.1.tar.gz zone-a/nso-manager-srv-0:/usr/app
```

2. Move into the NSO pod:

```
sedo shell zone-a/nso-manager-srv  
cd /usr/app/nso-temp
```

3. Untar the function pack tar.gz file:

```
tar xvzf nso-6.1-ron-2.1.1.tar.gz  
cd nso-6.1-ron-2.1.1/
```

4. Copy the function pack packages to the rundir:

```
cp ron/core-fp-packages/*.tar.gz $NCS_RUN_DIR/packages/
```

5. Initiate NSO CLI command from the specified path for loading packages:

```
cd $NCS_RUN_DIR/packages/  
ncs_cli -u admin
```

6. Load the packages:

```
request packages reload
```

7. Verify that the function pack has successfully loaded:

```
show packages package package-version | select build-info ncs version | select  
build-info file | select build-info package sha1 | select oper-status error-info  
| select oper-status up | tab
```

8. Set SSH algorithms public-key:

```
configure  
  
set devices global-settings ssh-algorithms public-key [ ssh-ed25519 ecdsa-sha2-  
nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 rsa-sha2-512 rsa-sha2-256 ssh-  
rsa ]  
  
commit
```

9. Initiate NSO CLI command from the specified path to load merge XMLs:

```
cd /nso/run/packages/nso-6.1-ron-2.1.1/ron/bootstrap-data  
ncs_cli -u admin
```

10. Load bootstrap data according to the function pack installation guide:

```
configure
```

```
unhide debug
unhide ron

load merge commit-queue-settings.xml

commit

...

<repeat for all files in installation guide>

...

load merge RON-status-codes.xml

commit
```

## Add Devices

The **device-type** and **ned-id** depend on the actual device you want to connect, as well as the NED version installed on NSO. Update the commands below accordingly.

### To add a device:

#### 1. Add credentials:

```
set devices authgroups group <credential_name> default-map remote-name <username>
remote-password <password>

commit
```

#### 2. Add device:

```
set devices device <device_name> address <IP> authgroup <device_authgroup_name>
device-type cli ned-id <cisco-iosxr-cli-7.49>

set devices device <device_name> state admin-state unlocked

commit

request devices device <device_name> ssh fetch-host-key

request devices device <device_name> connect

request devices device <device_name> sync-from

request devices device <device_name> check-sync
```

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)